GEUTEBRÜCK

G-SIM
User Manual

Version: 11

15.04.2024

Table Of Contents

About This Documentation

Current software version: G-SIM 11.

The latest features and changes of the current software version are listed in the Release Notes.

ℹ **Note that the illustrations in this documentation may not match those of your software version.**

Legal Notice

This documentation may not be copied, translated or converted to a machine-readable form, whether in whole or in part, without prior permission.

GEUTEBRÜCK GmbH cannot guarantee the correctness of any information provided in this documentation, nor for the software or the information it contains. Any suggested guarantee, assurance of marketable quality or suitability for a specific purpose of the documentation, the software or other information is hereby explicitly rejected.

Under no circumstances is GEUTEBRÜCK GmbH liable for direct or indirect subsequent damage or for special subsequent damage resulting from or in association with this documentation, regardless of whether this arises as a result of illegitimate action, of a contract, or for other reasons in association with this documentation, the software or of the information contained or used within it.

GEUTEBRÜCK GmbH retains the right to change this documentation or the information contained within it at any time without warning. The software described in it is subject to the conditions of a special license contract.

Getting Started

G-SIM is the Security Information Management Software of Geutebrück. It is based on G-Core by using data from its video and audio database, but adds some features to it.

These functions are primarily aimed at making the operation of the system as intuitive as possible.

For use and configuration of the G-SIM software, use the Management Console and the Operator Console:

Management Console

Operator Console

Planning Overview

G-SIM

Plan your G-SIM configuration carefully, as so many things impact each other. How you group your sites and what your camera naming and labeling conventions are can have a huge impact on maintenance.

Sites

Choose a site naming convention that makes sense. Remember: sites are physical or logical groupings. If in your installation it makes sense to have a site per building, then do that. Another installation may group all the buildings in one site, the perimeter in another, and entrances/ exits to the facility in yet another. Or it could be low, medium, and high security areas.

Camera Grouping

Again, think carefully about how you will group the cameras, and remember that cameras get their display attributes from the camera group they belong to. Usual methods of grouping the cameras are via camera type (fixed, PTZ, movement sensing, ...) or camera function (stairwell, exit, ...).

Camera Names and Labels

This is an extremely important decision. Most people would want a simple increasing number sequence for cameras, perhaps with a type or location prefix. The only time this works is if nothing changes — ever. Of course, this is hardly ever the case.

IMPORTANT: Cameras IDs must be uniquely assigned and cannot have duplicates.

The above means that in conjunction with your customer, you need to come up with a camera naming and labeling convention that is flexible enough to allow for additions or removals (or reassigning) of cameras. Every suggested convention should be tested against at least the following criteria:

- Does it make sense to the customer?
- Can it cope with camera additions or deletions?
- If strict adherence to the convention is required, could it ever be necessary to change existing camera mappings? This could become a lot of work - think of all the alarm and map linking that has been done. Also think about alarm and event history in the data base.

You also need to think of how things are defined at the GeViSoft, GeViScope, G-Core and Health Agent levels.

Alarms

It is important not only to decide on which event should create an alarm, but to decide on other factors as well:

- Should the alarm be generated by GeViSoft or by the NVR itself?
- Is it a derived alarm, where two or more events are taken to create a new one? E.g. an activity detection alarm from a camera is within 2 seconds of a

microwave barrier being breached. Together they constitute a major alarm, whereas each by itself may only indicate a spurious trigger.

- Are the alarms designated as auto pop-up really that important? If they happen too often, then they cannot be that critical (and these are only to be used for the most absolutely critical alarms). Should auto pop-up alarms use separate window (tab view mode), or use viewers on the screen layout (viewer group mode)?
- Which alarms are more events than alarms? In other words, they need to be recorded for auditing purposes only — "live" investigation by an operator would be a waste of time. Make sure that these are then never displayed.
- Some alarms are hybrid in the sense that though they may not require action by operators, it is nevertheless good for the operators to know about them. In such a case, mark them as auto-expiry after a pre-defined period.

These are just a few of the things to think about. As you gain experience with G-SIM, you will develop your own list to use at installations and during maintenance.

Rights and Restrictions

In a role-based security model as G-SIM has, it is vital to define and configure rights and restrictions correctly. Be careful to have the correct definitions for privileges, permission, and restrictions. Getting them wrong is a sure way of having complete chaos at go-live.

Pay special attention to the differences between restricting and allowing access, particularly the implications on what happens when new kit is added.

Maps

Maps are absolutely core to the functioning of G-SIM, showing operators where something is taking place. Here we look at maps in broad brush strokes only.

A good approach is a combination of geo-accurate (GIS), fixed and variable scale maps.

A good example is the railways. The distance between stations is simply too great to use fixed scale maps, nor is it useful to indicate the route that the railway takes. What is important when looking at an overview of a rail network is to know that station A and B are connected, and that if something is wrong at either end or in between, you will be able to represent it. Once you are at station level, though, it may be important to use a fixed scale map. In other words, use the correct map for the correct purpose.

Once you have this understanding, you need to decide on at least the following:

- How large the maps should be in the display (impacting your templates).
- What is the color scheme? We once encountered a graphic designer who saw no problem with orange grass and green water!
- Will they be based on CAD drawings, on aerial photos, or a combination?
- Who will supply the maps?
- Who will pay for the extra work to prepare the maps?
- Which graphics formats will be used?
- Investigate the map sizes, looking particularly at the difference between a compressed map image (e.g. a PNG file) and its uncompressed size in RAM, as the difference can be vast. As an example, a random photograph in my collection is 1.25 MB on disc, but has a memory size of 22.9 MB. All map images would need to be investigated, and edited (color and resolution reduction, for example) before they are used.
- Which information needs to be shown, and which not?
- If your maps should cover city or even country level and cameras have geo-coordinates, then GIS maps are good choice. Think carefully about choosing of map provider, it's tariff plans and map using mode.

Lastly, time the whole process of going from nothing to a completed map for a few of them. There is always more work to this than anticipated.

Remote Consoles

Make sure that your customer understands the power of Remote Consoles (ReCons). Show them different use cases and work through these with them until they themselves come up with how they will be using Remote Consoles in their particular installation. Once you are at this point, the following can be addressed:

- Use the output from your work on rights to decide who will have access to which Remote Consoles.
- Where will the Remote Consoles be placed, and what will be displayed on them?

Video Walls

It is important that your customer understands that though Remote Consoles and video walls are related, their purposes and their use are often very different. A Remote Consoles can have, say, four screens, while with a video wall you also need to consider layout of the screens relative to each other; how many Remote Consoles you are going to need to make up a video wall; which graphics cards to use, etc.

Remember that you need not only display security related information. You can use video capture from a machine running a software-only NVR to capture a news or stock feed to display in a foyer, for example (or some sporting event). Just factor in all the costs!

Firewall Settings

G-SIM uses TCP and UDP ports for its connections. These ports must be enabled in the firewall settings (firewall rule). The table shows the ports used for TCP and UDP:

Port	Description
TCP 8090	G-SIM Server <-> Operator Console/ ManCon/ ReCon
TCP 8090	G-SIM Control Server <-> G-SIM Controlled Client Servers
TCP 8090	G-SIM Server <-> Agent and Health Agent
TCP 8091	G-SIM Cluster Servers Sync (G-SIM Server <-> G-SIM Server)
TCP 8098	G-SIM Server SAM Proxy
TCP 8099	Agent and Health Agent <-> G-SIM Server
UDP 8099	Agent and Health Agent Cluster
TCP 8092	Data Access Server

Port	Description
TCP 13180	Export Service
TCP 13181	Map Tiles Service
TCP 13210	App Instance Manager Service

Comments:

- Operator Console, Management Console and Agent use ICMP for “pinging”.
- GeViSoft Proxy connections run only locally via NamedPipes (URL `net.pipe://localhost/GSIM`), so that no firewall rules need to be created.
- G-Core, GeViScope, Pelco and GeViSoft use standard ports for outgoing connections to the servers. The same ports are also used for connections via SDK.
- G-Core SAM connections from third-party systems are handled via SDK.
- If an SQL server runs on a remote machine, then the SQL TCP ports also need to be enabled.

Other Factors

Network Infrastructure

Computer networks are now so pervasive that they often receive very little thought. Their installation has also been commoditized to the point where someone with no training at all is able to install a small network.

In our experience, even qualified network engineers do not appreciate the important differences between a network designed for general business use, and one required for a video security system. Do your preparation well and meet way in advance with the network designers, otherwise you will experience similar (if not longer) delays.

The following points should help:

- Most often, TCP is used in Geutebrück installations.
- Cameras send their images to specific NVRs, which both record the images and pass the live data to connected viewers.
- Video between any given NVR-viewer pair happens via one TCP connection only. Thus even if, say, video from four cameras connected to one NVR is

being viewed at one Operator Console, that NVR would send all the video data from those four cameras to the Operator Console via one TCP connection (i.e., over one socket).

- Two specifications of a computer monitor are important here: refresh rate and refresh time. The rate refers to how many times a second the screen gets updated, and the time to how long each update takes to complete.
- LCD monitors are typically set to a 60Hz refresh rate (once every 16.7ms).
- Above about 25fps (or less than 40ms), the human eye cannot discern the differences between frames, instead seeing a single, smooth video. Conversely, below about 25fps (or more than 40ms), single-frame differences can be seen. These values are not cast in stone, as different people are more or less sensitive. The amount of ambient light also plays a role, as does the refresh rate of fluorescent lighting used.
- To display video smoothly, the inter-frame gap needs to stay constant. For 15fps (a common rate for live video), this means that from the start of one frame to the next, the time should be in the order of 66.7ms.
- If multiple frames are sent to the graphics card, their inter-frame gap must be no greater than the screen's refresh rate, otherwise not all frames will be displayed. For a screen with a 60Hz refresh rate, this means that if more than one frame is sent in 16.7ms, only the last frame will be displayed, because before the screen has been able to start displaying one frame, another frame has arrived. Thus it throws away one of them.

All of the above shows how important it is to look at all the factors. One particularly troublesome point is that in business networks it does not matter if data delivery is bursty — if a lot arrives at once, then nothing for a while, then a lot again. In video networks, this is a disaster (think of freezing in YouTube), as you need to stay current, so you won't have time to view all the frames which you've been waiting for. Thus you will have to throw some away in order to ensure that you are always viewing the most recent frames.

When struggling with a misbehaving network, it is most useful first to do an analysis of the inter-packet delay. The "ImageTimeStamp" value is what you need. Look at the deltas between them, and run basic statistical analyses on them. Plotting a frequency distribution graph of the inter-packet delay will be very instructive.

Time

Even more invisible than the network infrastructure, is time. To convince your customer of the importance of having a dedicated time server for this installation.

Extremely good time server software is available for free, or if the customer wants commercially supported software, then for not very much. We have found Tardis2000 to be quite acceptable.

Installation Process

Software Installation

Prerequisites

Dependencies list:

- G-Core_SQLServerInstaller.exe (can be placed into "Dependencies" folder)
- Microsoft .NET Framework 4.7.2 (should be installed separately)

If you do not have the prerequisites installed, you can create a folder called "Dependencies" in the folder where the installer is. The installer will first try in that folder before it downloads the dependencies from Microsoft.

Limitations G-SIM 10

i **With version G-SIM 10, the use of the security-related functions Enhanced Security Mode (FIPS), Change Communication Protocol and Encryption Settings is introduced. These installation modes are automatically installed with the upgrade to G-SIM 10.**

- Clients are no longer able to connect to OLDER servers.
- There is no longer the possibility to use a hybrid / mixed environment with different versions.
- Every system component must have the same version.

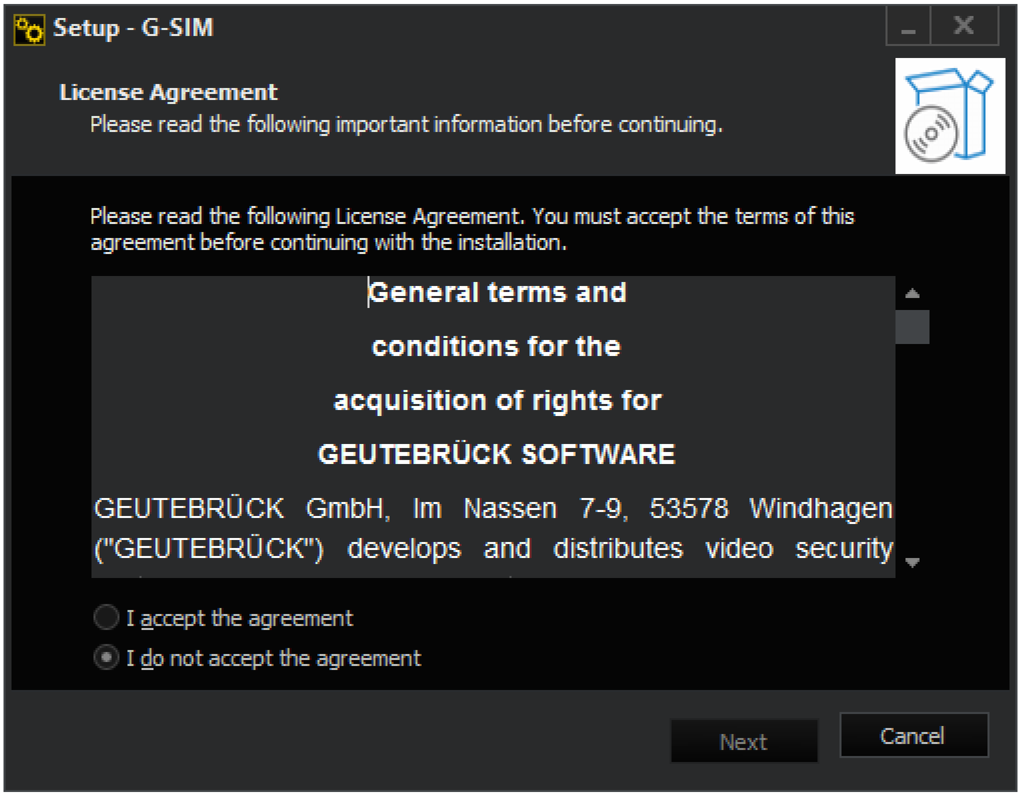
- Upgrade to the major version 10 is only possible from 9.4 and 9.4.1.

  See the Upgrade 9.4 to 10 guide.

How to Install G-SIM

To install G-SIM, do the following:

1. Double click on the installation file. The installation dialog opens.
2. Accept the agreement and click **Next**.



Setup - G-SIM

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

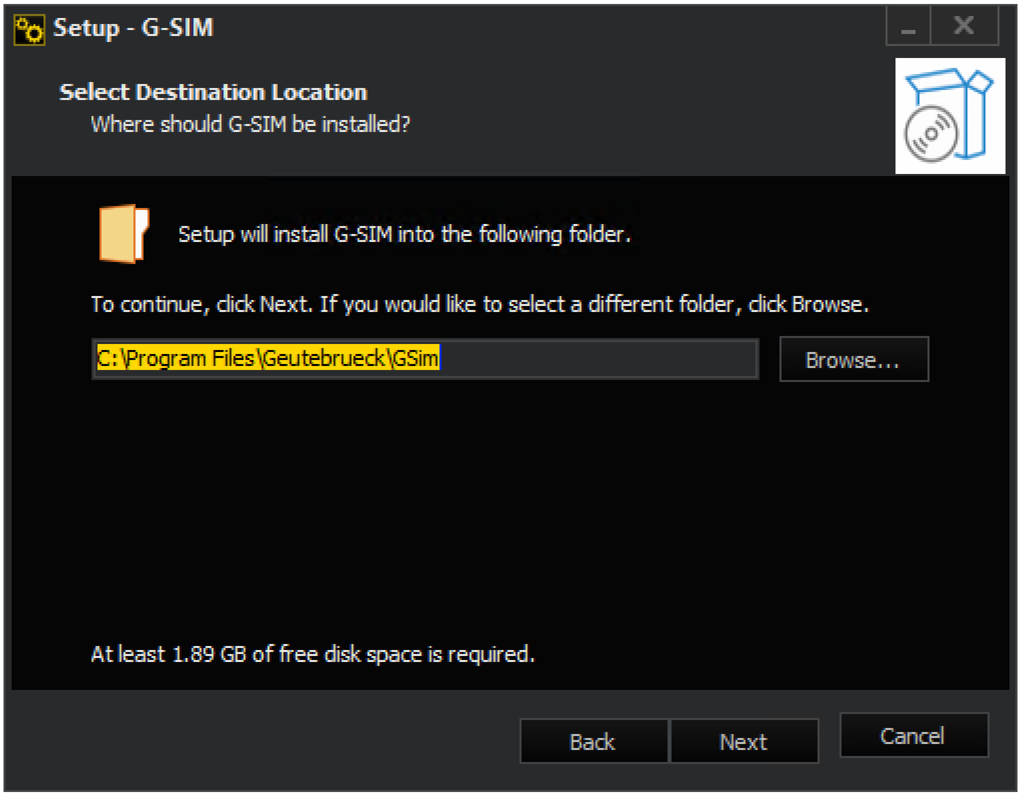
General terms and conditions for the acquisition of rights for GEUTEBRÜCK SOFTWARE

GEUTEBRÜCK GmbH, Im Nassen 7-9, 53578 Windhagen ("GEUTEBRÜCK") develops and distributes video security

○ I accept the agreement

● I do not accept the agreement

3. Select a folder for the installation (or use the default one) and click **Next**.



Select Destination Location

Where should G-SIM be installed?

Setup will install G-SIM into the following folder.

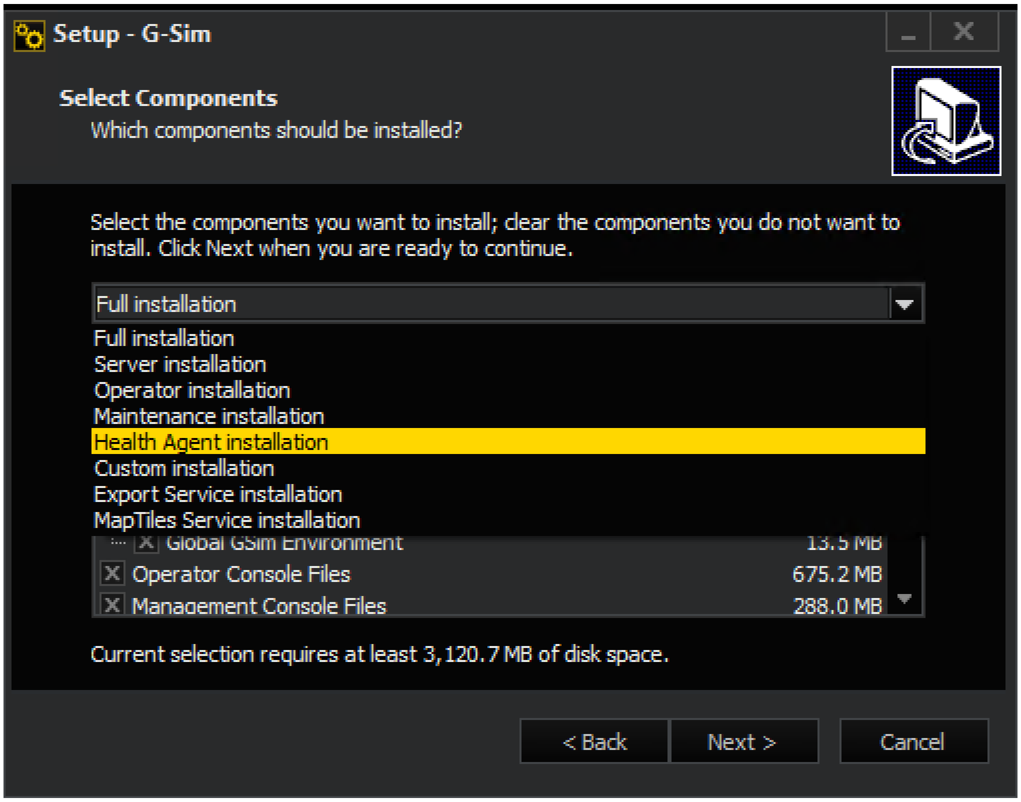
To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Geutebrueck\GSim

At least 1.89 GB of free disk space is required.

4. Select the type of installation you want to install. You can choose between different installations:

    - Full installation
    - Server installation
    - Operator installation
    - Maintenance installation
    - Health Agent installation
    - Custom installation
    - Export Service installation
    - Map Tiles Service installation



Setup - G-Sim

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

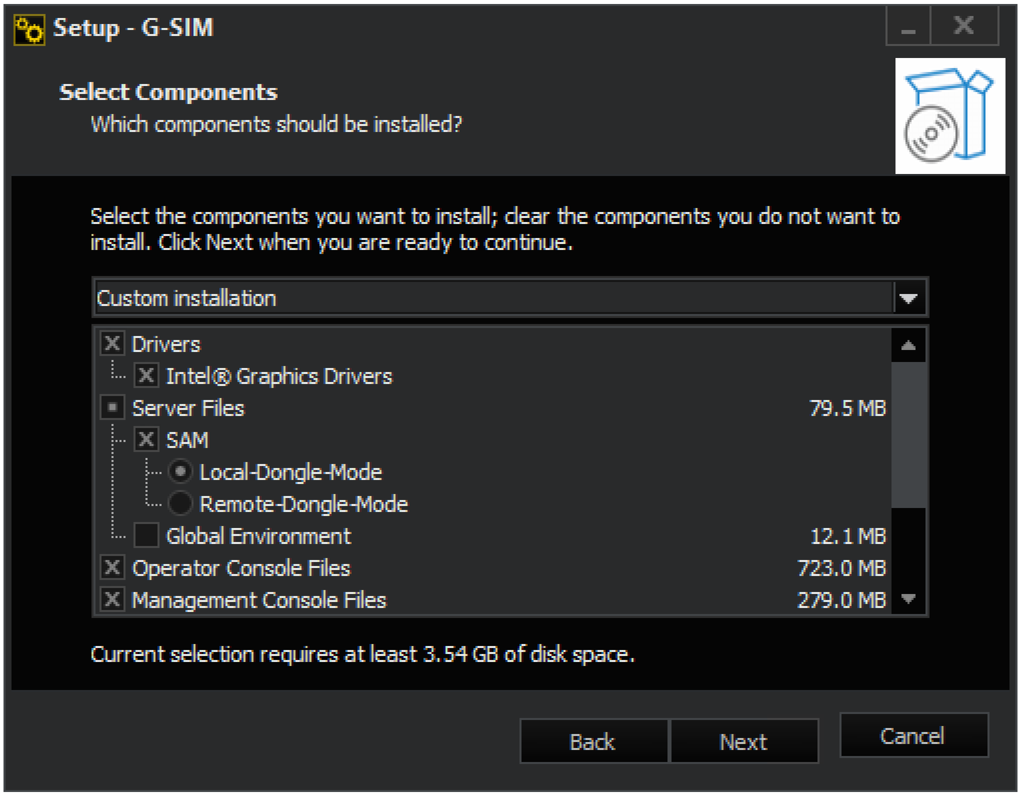
Full installation

- Full installation
- Server installation
- Operator installation
- Maintenance installation
- Health Agent installation
- Custom installation
- Export Service installation
- MapTiles Service installation

☒ Global GSim Environment	13.5 MB
☒ Operator Console Files	675.2 MB
☒ Management Console Files	288.0 MB

Current selection requires at least 3,120.7 MB of disk space.

5. Select the components you want to install or deselect the components you do not want to install.



Setup - G-SIM

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom installation

☒ Drivers
- ☒ Intel® Graphics Drivers

■ Server Files 79.5 MB
- ☒ SAM
  - ● Local-Dongle-Mode
  - ○ Remote-Dongle-Mode
- □ Global Environment 12.1 MB

☒ Operator Console Files 723.0 MB

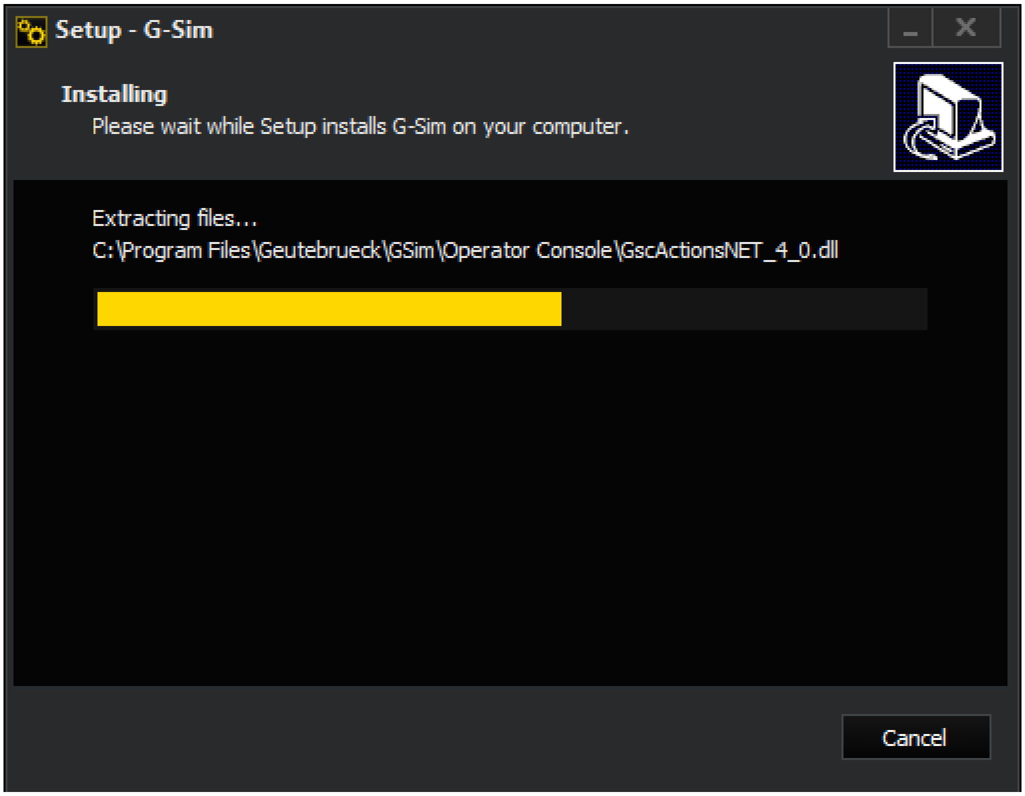
☒ Management Console Files 279.0 MB

Current selection requires at least 3.54 GB of disk space.

During installation you must decide whether to use a physical USB dongle for licensing (Physical SAM) or a central, remote SAM service (Virtual SAM) on a virtual machine.
More on G-Core SAM can be found in the G-Core documentation.

6. Then click **Next**.

7. If all conditions are met, G-SIM Setup will start installation process.



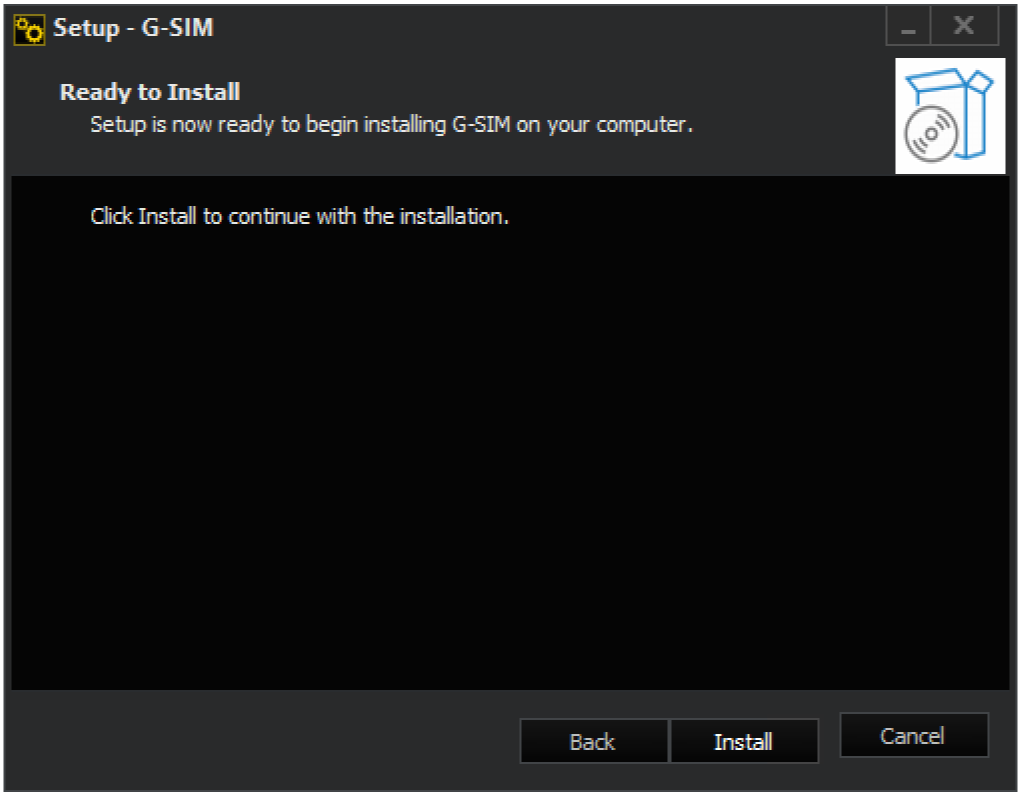
Installing

Please wait while Setup installs G-Sim on your computer.

Extracting files...

C:\Program Files\Geutebrueck\GSim\Operator Console\GscActionsNET_4_0.dll

8. Wait until the G-SIM installation is complete.



Setup - G-SIM

Ready to Install

Setup is now ready to begin installing G-SIM on your computer.

Click Install to continue with the installation.

9. To complete the installation, click **Finish**.

→ Installation is now completed. You see two icons on the desktop: one for the Management Console, one for the Operator Console.

Change Default Username and Password

G-SIM and G-Core use a default username and password. It is strongly recommended to change your username and password during the setup. In addition, it is recommended to save your login data in a suitable system (e.g. a password manager).

Strategies to create a difficult to decrypt password:

- For admin accounts use at least 16 characters.
- For user/viewer accounts use at least 12 characters.
- Remember a sentence and only use the first letter (or only the second or last letter) of each word. Subsequently, you can convert certain letters into numbers or special characters.

- Use a whole sentence as a password or string different words together using special characters.
- Randomly select five to six words from the dictionary and separate them with spaces.

Setup G-SIM in a VM

Physical (Local-Dongle-Mode) Installation

On the network there must be a Windows machine where the G-SIM Dongle can be plugged in. This machine will act as a proxy to the G-SIM virtual machine.
The G-Core_SAM Installer must be run on this machine to perform the "physical" installation of the SAM.

Configure SAM

After installation, the SAM must be configured. This happens through a Web Interface by the
address `http://localhost:13080/config`.

ⓘ **This page can only be accessed from the local machine, it is not possible to reach this page remotely.**
The browser must be run with admin privileges!

On the upcoming page there is a input field where the computer name (not IP-Address!) must be entered and added. After that, the machine appears in the list of allowed machines and with a click on G-SIM, this machine is enabled to gather G-SIM Licenses.

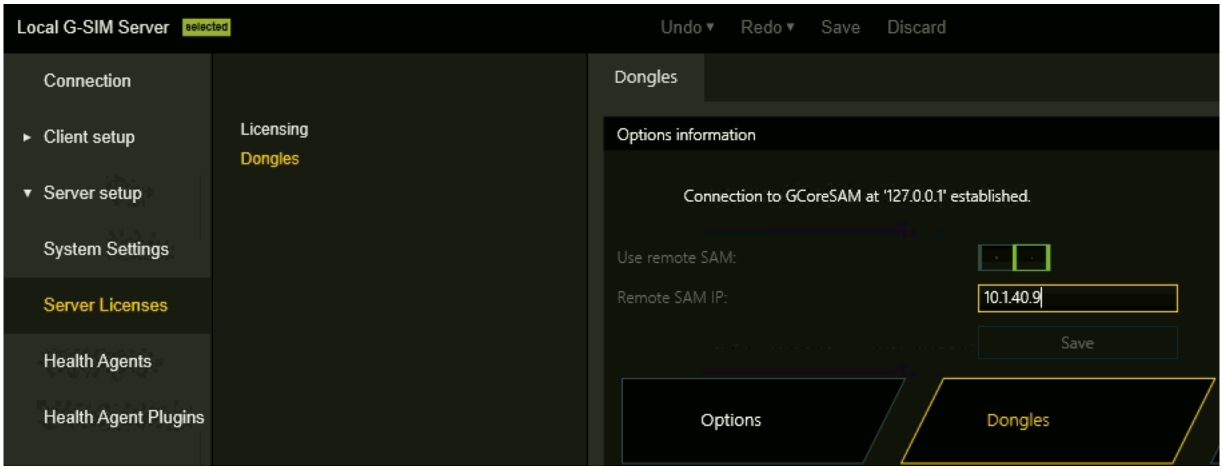
Virtual (Remote-Dongle-Mode) Installation

On the virtual machine, run G-SIM Setup and choose Remote Dongle Mode within the SAM Installer.

⚠ **IMPORTANT:** You can only use one G-SIM instance in Remote-Dongle-mode and only connect this instance to the central option server (Remote SAM).

Configure G-SIM

Run Management Console and go to Server Setup > Server Licenses > Dongles. At Remote SAM IP, the IP address of the physical machine must be entered:



Connection to GCoreSAM at '127.0.0.1' established.

Use remote SAM:

Remote SAM IP: 10.1.40.9

After you have changed this, G-SIM will require the licenses from the physical SAM.

Management of Certificates

The certificate is used for the TLS client server connections of the following G-SIM components:

- G-SIM Server (including DAS)
- Management Console / Operator Console / Remote Console
- Agent / Health Agent
- Export Service
- App Instance Manager Service
- Map Tiles Service

Default Certificate Mode

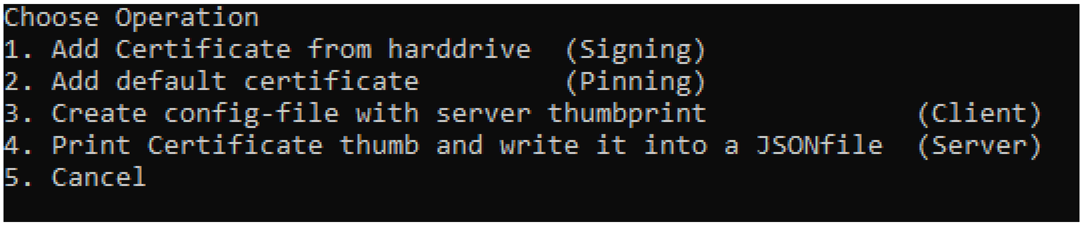
During installation G-SIM adds a default certificate for the TLS client server connections. No additional configuration is required.

Custom Certificate Mode

G-SIM enables you to configure a custom certificate for the TLS client server connections.

Use the `CertManager.exe` command line tool to configure the used certificate. You can find the tool in the folder `C:\Programme\Geutebrueck\GSim\Common`.

You can perform the following configuration steps:



```
Choose Operation
1. Add Certificate from harddrive  (Signing)
2. Add default certificate         (Pinning)
3. Create config-file with server thumbprint             (Client)
4. Print Certificate thumb and write it into a JSONfile  (Server)
5. Cancel
```

To set up the custom certificate mode, you have three options:

- Perform step 1 or step 2 on the server.
- Perform step 4 on the server.
- Perform step 3 on the client, using the thumbprint you created in step 4.

1. Add Certificate from hard drive (Signing)

In this step you add a certificate from the hard drive by specifying the path of the certificate. The certificate is uploaded and stored in the Windows certificate store. Also, the certificate is bound to the ports used by G-SIM.

This step needs to be performed only on the G-SIM server host.

2. Add default certificate (Pinning)

In this step you add a default certificate by creating a self-signed certificate. The certificate is stored in the Windows certificate store. Also, the certificate is bound to the ports used by G-SIM.

This step needs to be performed only on the G-SIM server host.

3. Create config-file with server thumbprint (Client)

In this step, you create a configuration file using the thumbprint you created on the server in step 4. The file is applied to the local configuration.

This step must be performed on the client so that the client knows which server certificate to accept.

4. Print Certificate thumb and write it into a JSON file (Server)

In this step, you create a thumbprint for the certificate and write it into a JSON file. The certificate is identified by the certificate name and applied to the local configuration.

The thumbprint can be used to create a configuration file on the client (see step 3).

This step must be performed on the server so that the server knows which certificate to use.

SQL Server and User Role

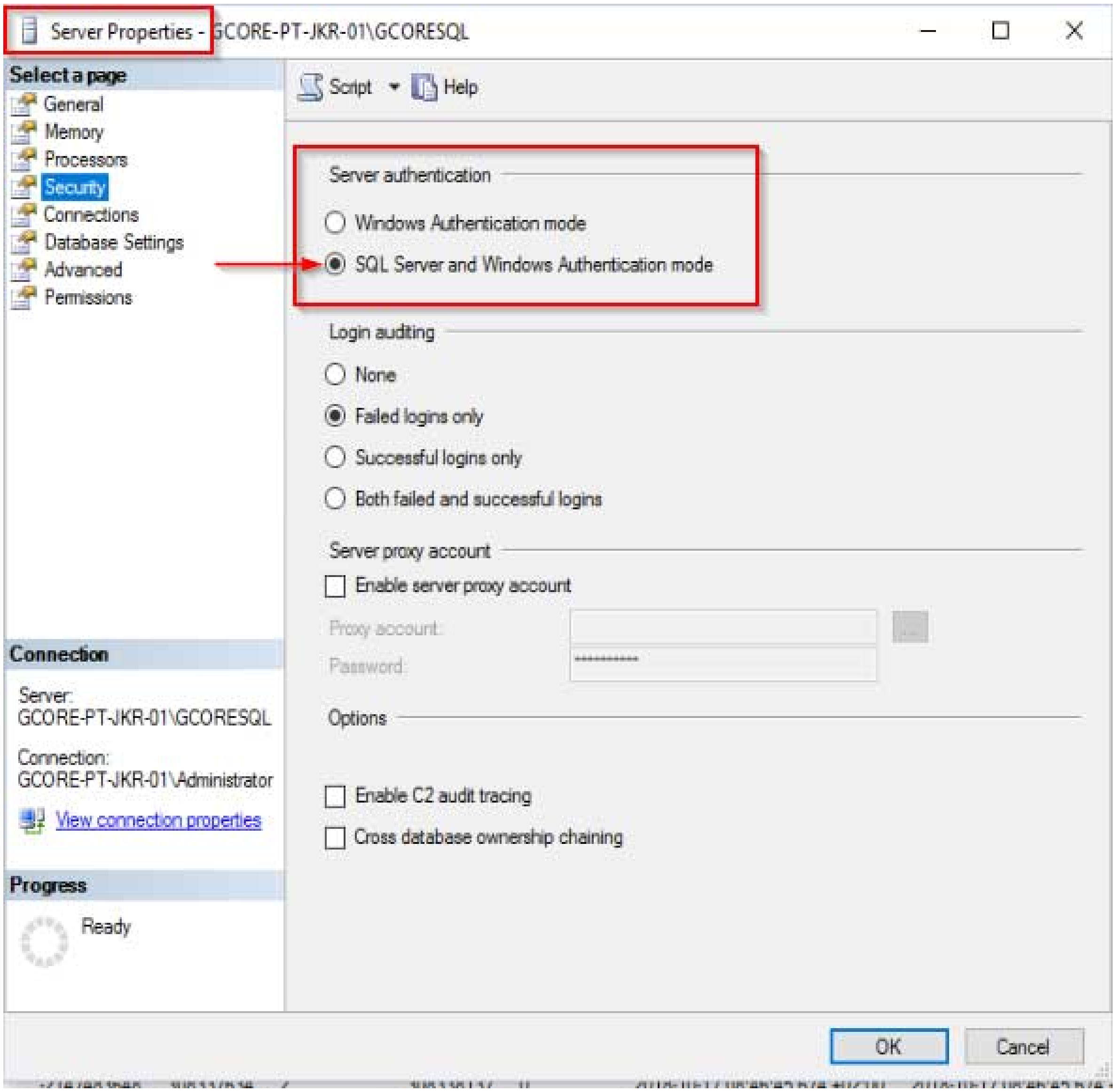
Configuration of the SQL Server

In connection with the configuration of the SQL Server, the question arises again and again whether a role as sysadmin is required for SQL Server authentication. A distinction must be made between an initial installation and later work with the SQL Server.

⚠ **IMPORTANT:** The first start of G-SIM immediately after installing SQL Server and G-SIM must be performed by a user with the server role **Sysadmin**, because G-SIM creates databases.
After initializing G-SIM and creating all databases, it is not necessary to have a user with the server role **Sysadmin**. We show this with an example of a fictitious user **GSIM_6566**. Please note that the database file size settings in the G-SIM server config file will be inactive for this case.

First, the SQL Server must be configured to run in Mixed mode.

For SQL Server, open Server Properties. Under Security > Server authentication, select SQL Server and Windows Authentication mode.



Server: GCORE-PT-JKR-01\GCORESQL

Connection: GCORE-PT-JKR-01\Administrator

Progress: Ready

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

● Failed logins only

○ Successful logins only

○ Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

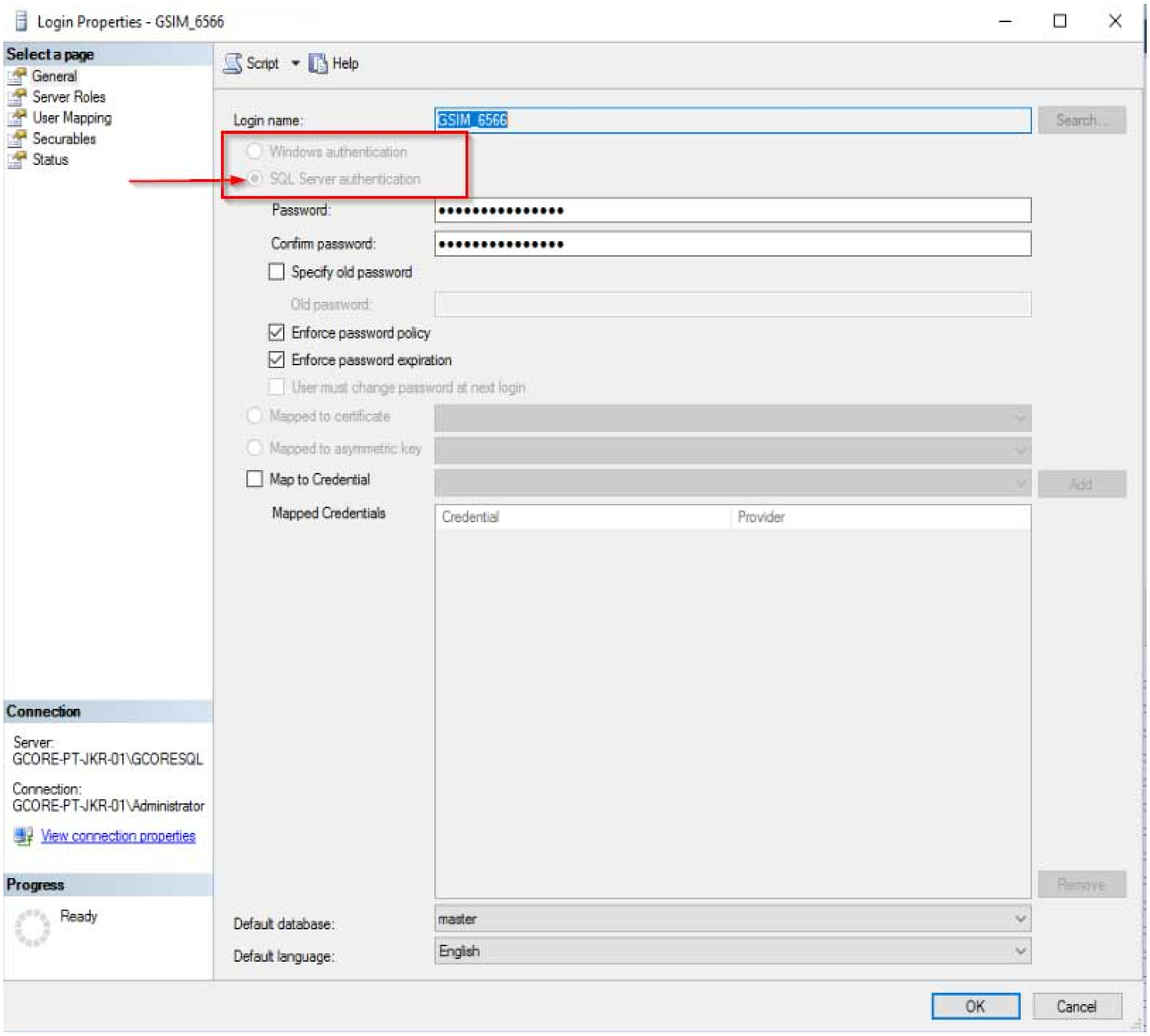
Password: ***********

Options

□ Enable C2 audit tracing

□ Cross database ownership chaining

Now the user **GSIM_6566** is created with **SQL Server authentication**.



Login Properties - GSIM_6566

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server:
GCORE-PT-JKR-01\GCORESQL

Connection:
GCORE-PT-JKR-01\Administrator

View connection properties

Progress

Ready

Login name: GSIM_6566

○ Windows authentication

● SQL Server authentication

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

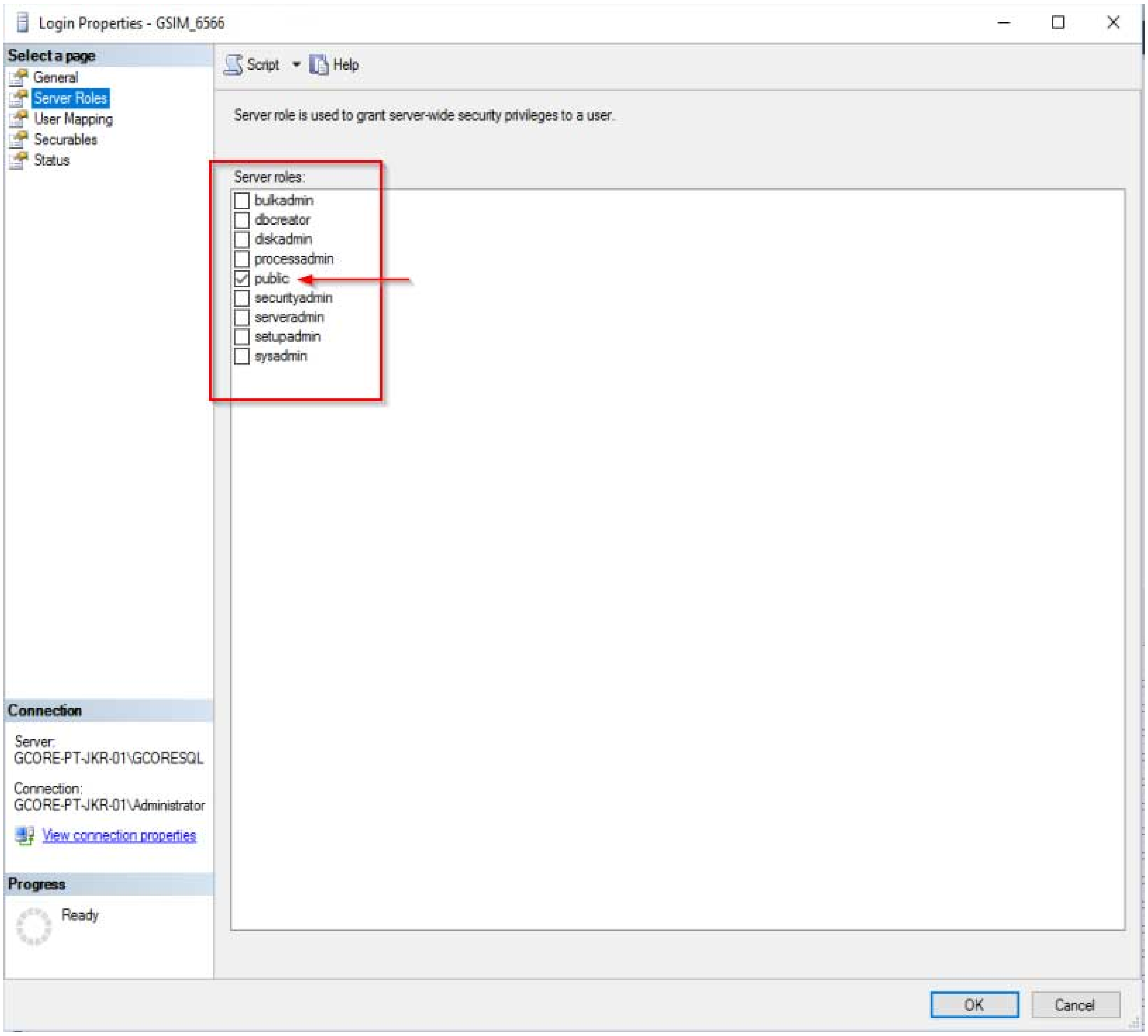
Mapped Credentials

Credential	Provider

Default database: master

Default language: English

The user is then assigned the server role **public**.



Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- □ sysadmin

Connection

Server:
GCORE-PT-JKR-01\GCORESQL

Connection:
GCORE-PT-JKR-01\Administrator

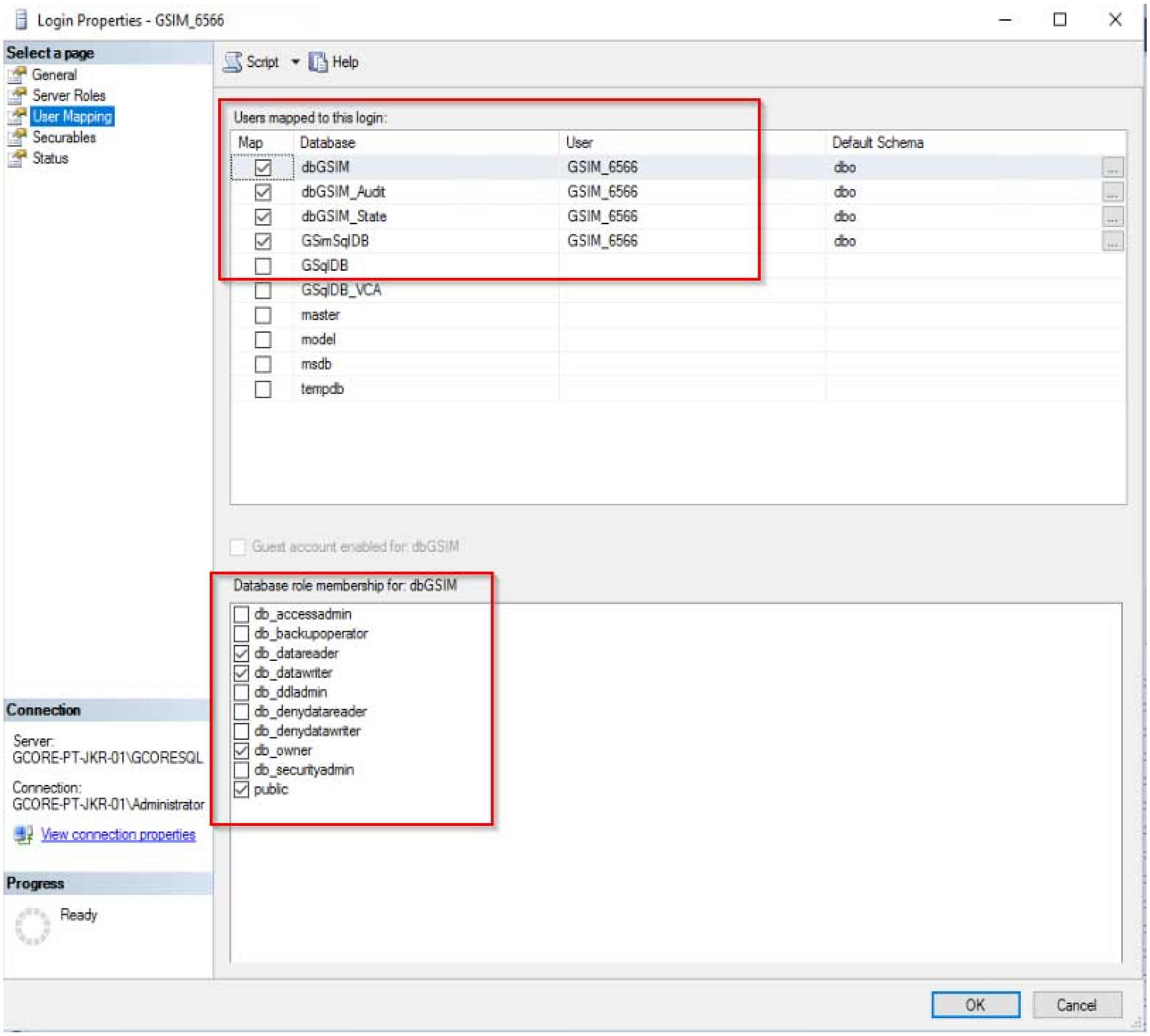
View connection properties

Progress

Ready

All G-SIM databases must now be adapted to the login of this user. For each database, in addition to the **public** role and the [dbo] as default schema, the following role assignments must also be defined:

- db_datareader
- db_datawriter
- db_dbowner.



Login Properties - GSIM_6566

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Users mapped to this login:

Map	Database	User	Default Schema
☑	dbGSIM	GSIM_6566	dbo
☑	dbGSIM_Audit	GSIM_6566	dbo
☑	dbGSIM_State	GSIM_6566	dbo
☑	GSimSqlDB	GSIM_6566	dbo
□	GSqlDB		
□	GSqlDB_VCA		
□	master		
□	model		
□	msdb		
□	tempdb		

□ Guest account enabled for: dbGSIM

Database role membership for: dbGSIM

□ db_accessadmin
□ db_backupoperator
☑ db_datareader
☑ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin
☑ public

Connection

Server:
GCORE-PT-JKR-01\GCORESQL

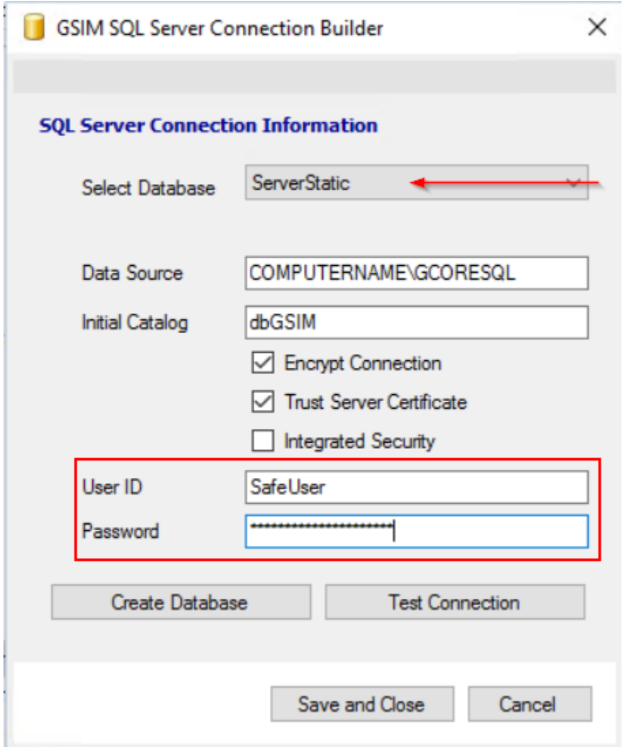
Connection:
GCORE-PT-JKR-01\Administrator

View connection properties

Progress

Ready

Then the **GSIM SQL Server Connection Builder** must be used to change the user used and his credentials. This must also be done for each database:


GSIM SQL Server Connection Builder

SQL Server Connection Information

Select Database: ServerStatic

Data Source: COMPUTERNAME\GCORESQL

Initial Catalog: dbGSIM

☑ Encrypt Connection

☑ Trust Server Certificate

☐ Integrated Security

User ID: SafeUser

Password: ********************

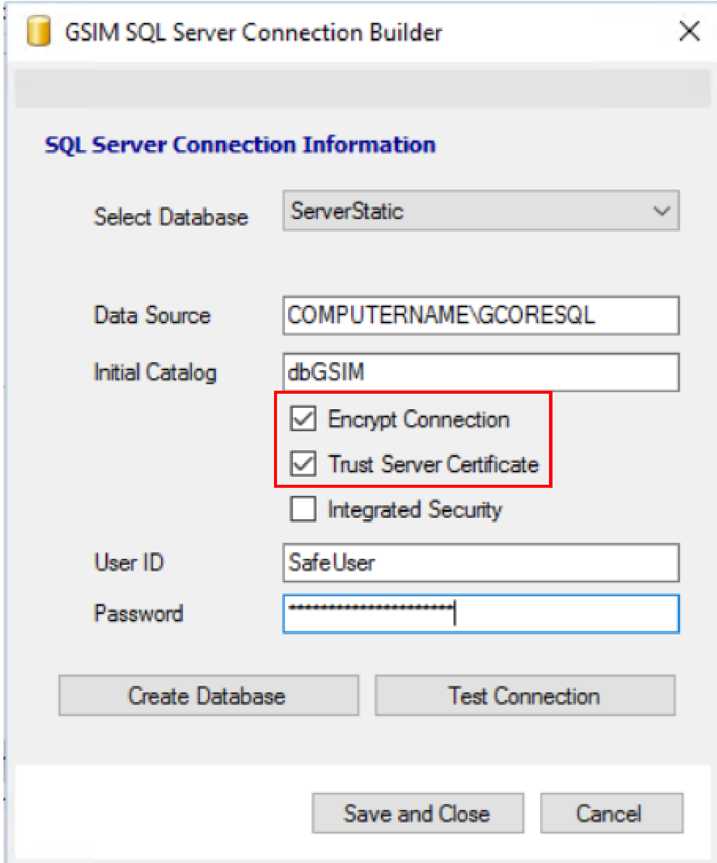
After restarting the services, the user **GSIM_6566** has the required SQL Server authentication.

SQL Server Encryption

To establish an encrypted connection to an SQL Server, you must first configure it. You can use the following instructions to do this:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15

Afterwards you have to configure the client with the help of the G-SIM SQL Server Connection Builder. For each database, you need to check the **Encrypt Connection** checkbox. If you are using a self-signed certificate or the certificate cannot be verified for other reasons, you must also check the **Trust Server Certificate** checkbox.



SQL Server Connection Information

Select Database: ServerStatic

Data Source: COMPUTERNAME\GCORESQL

Initial Catalog: dbGSIM

☑ Encrypt Connection

☑ Trust Server Certificate

□ Integrated Security

User ID: SafeUser

Password: **********************

SAML Authentication

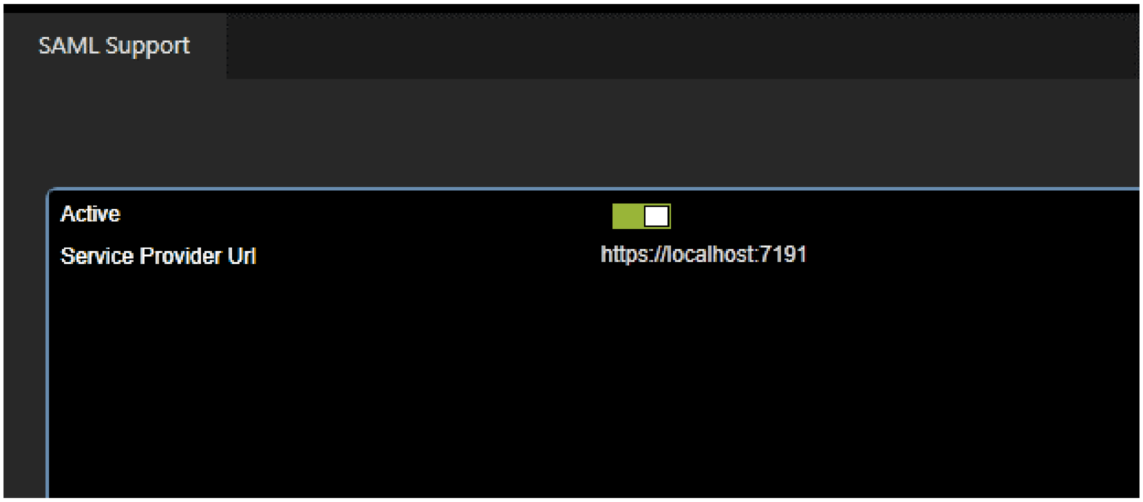
Installing the ASP.Net Application

1. Run the G-SIM installation program.
2. In the **Select Components** dialog window, select the **SAML APP** component.
3. Follow the further installation steps and complete the installation.

→ The ASP.Net application is installed.

Activate SAML in ManCon

1. In the ManCon, navigate to **Server Setup** > **System Settings** > **SAML Support**.



Active

Service Provider Url https://localhost:7191

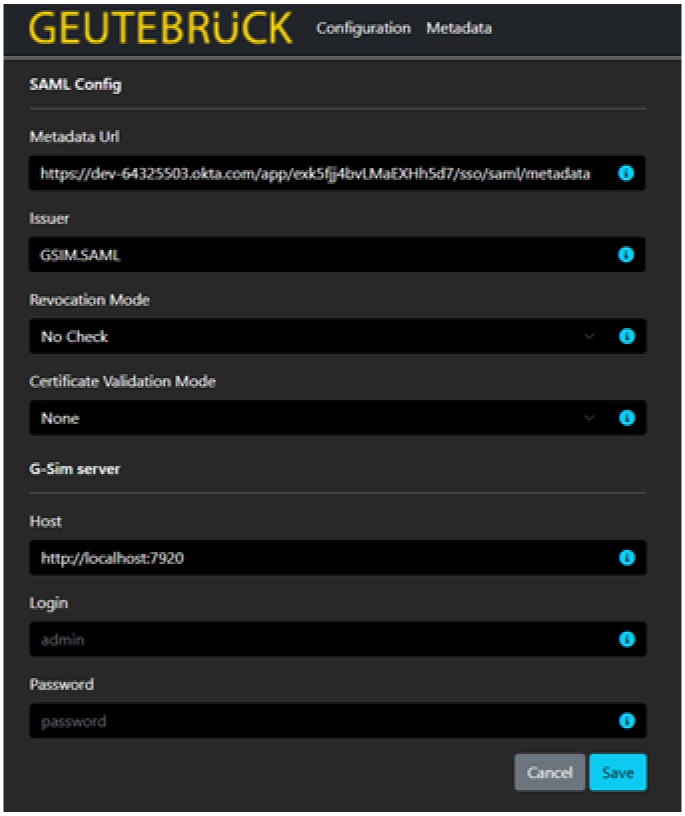
2. Activate the **Active** slider.

3. In the **Service Provider URL** setting, specify the URL of the ASP.Net application. This setting is mandatory.

Configure the SAML Service Provider

1. Open the address of the ASP.Net application in a browser (example: `https://localhost:7191/`).

2. The dialog window for configuring the SAML service provider opens.



SAML Config

Metadata Url: https://dev-64325503.okta.com/app/exk5fjj4bvLMaEXHh5d7/sso/saml/metadata

Issuer: GSIM.SAML

Revocation Mode: No Check

Certificate Validation Mode: None

G-Sim server

Host: http://localhost:7920

Login: admin

Password: password

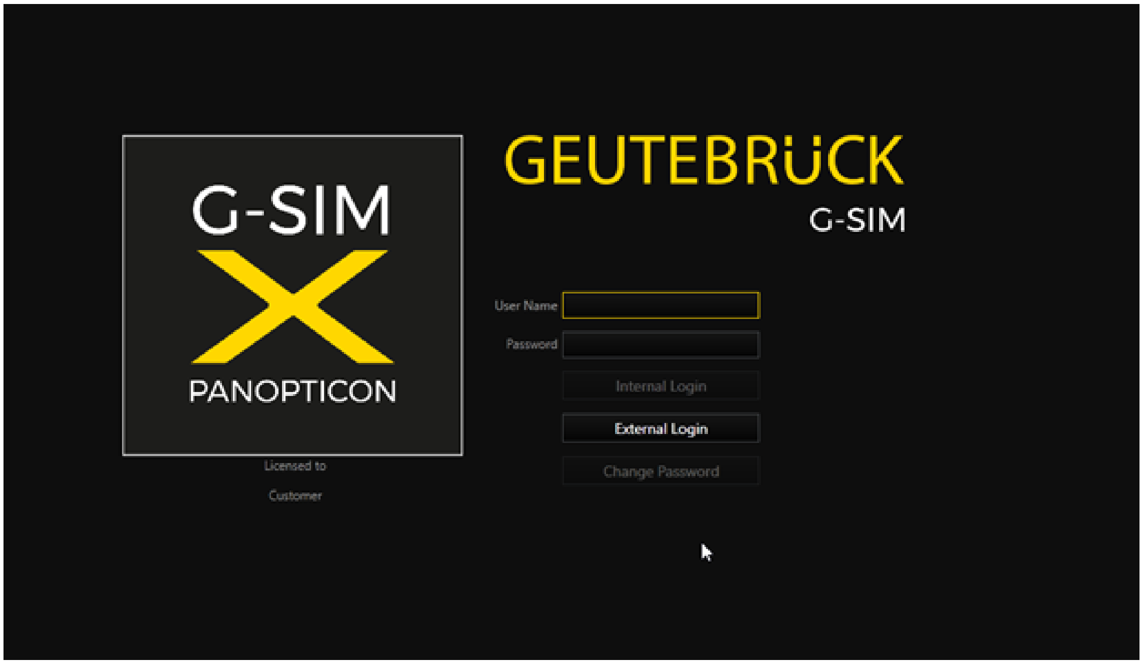
3. Enter the following information:

Name	Description
SAML Config	
Metadata URL	URL of the metadata from the IDP (mandatory). Example: `https://localhost/saml2/metadata`
Issuer	The application-defined unique identifier that is the intended audience of the SAML assertion. In most cases, this is the SP entity ID of your application.
Revocation Mode	Specifies the mode used to check for X509 certificate revocation.
Certificate Validation Mode	Specifies the mode used to validate a certificate.

Name	Description
G-SIM Server	
Host	URL for API (ASP.Net application) on the G-SIM server (mandatory).
Login	Username for the G-SIM server (mandatory).
Password	Password for the G-SIM server (mandatory).

Login to OpCon with SAML User

1. Open the OpCon. The login window opens.



You have two login options:

- **Internal Login** - Login to the G-SIM server with regular G-SIM user credentials.
- **External Login** - Login to the G-SIM server with SAML user credentials.

2. Click on the **External Login** button.

→ You are logged in as SAML user in the OpCon.

Local Server Identity

Configure G-SIM Server IP/ Hostname/ FQDN as a Local Server Identity

The local server identity is an IPv4 address, a host name, or a fully qualified domain name of the G-SIM server computer. By default, the hostname of the computer is used as the local server identity.

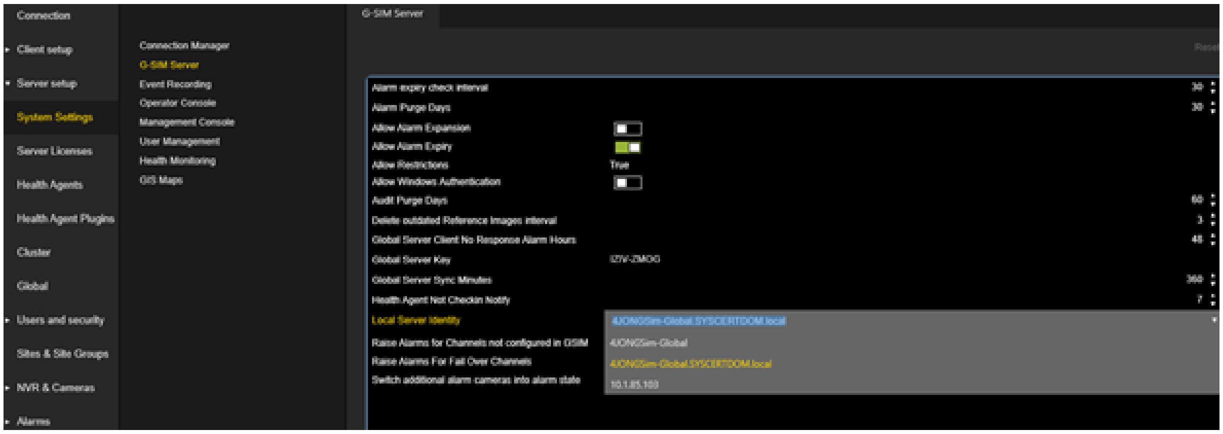
The local server identity is used by:

- **Operator Console**: Used to connect to the local G-SIM server in the cluster or global environment.
- **Operator Console**: Used as the address of the data access server (part of the G-SIM server) to perform process data, alarm, audit, and OSD requests.
- **G-SIM Server**: Used to redirect process data, alarm, audit, and OSD requests to the other global or cluster G-SIM servers.

For these reasons, the local server identity must be resolvable for the G-SIM server clients (operator consoles or other G-SIM servers in the global or cluster environment).

Management Console

The administrator can configure the local server identity in the system settings category **G-SIM Server**.



Alarm expiry check interval	30
Alarm Purge Days	30
Allow Alarm Expansion	□
Allow Alarm Expiry	☑
Allow Restrictions	True
Allow Windows Authentication	□
Audit Purge Days	60
Delete outdated Reference Images interval	3
Global Server Client No Response Alarm Hours	48
Global Server Key	IZIV-ZMOG
Global Server Sync Minutes	360
Health Agent Not Checkin Notify	7
Local Server Identity	4JONGSim-Global.SYSCERTDOM.local 4JONGSim-Global 4JONGSim-Global.SYSCERTDOM.local 10.1.85.103
Raise Alarms for Channels not configured in GSIM	
Raise Alarms For Fail Over Channels	
Switch additional alarm cameras into alarm state	

The **Local Server Identity** combo box contains the list of network identities determined by the G-SIM server:

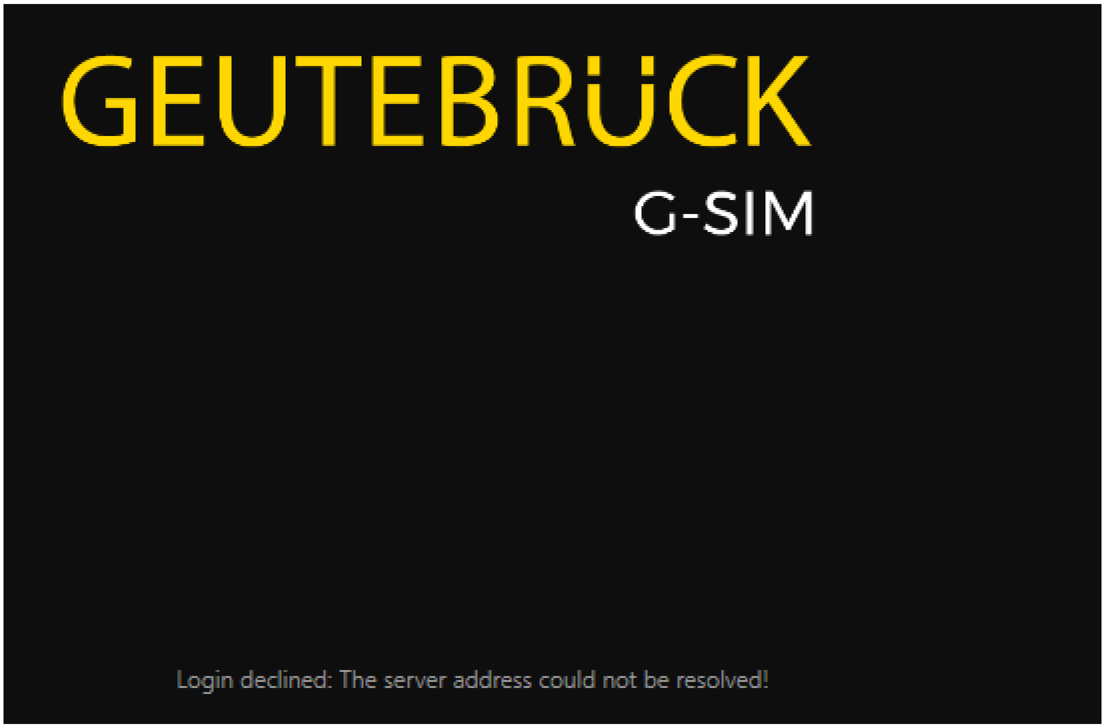
- IPv4 addresses of the active network interfaces
- Hostname
- FQDN (only if the computer is included in the domain or the primary DNS suffix is set)

The administrator can select one of the items in the combo box or make an individual entry.

⚠ **IMPORTANT:** Make sure that the entry is resolved by each computer that wants to access G-SIM.

Operator Console

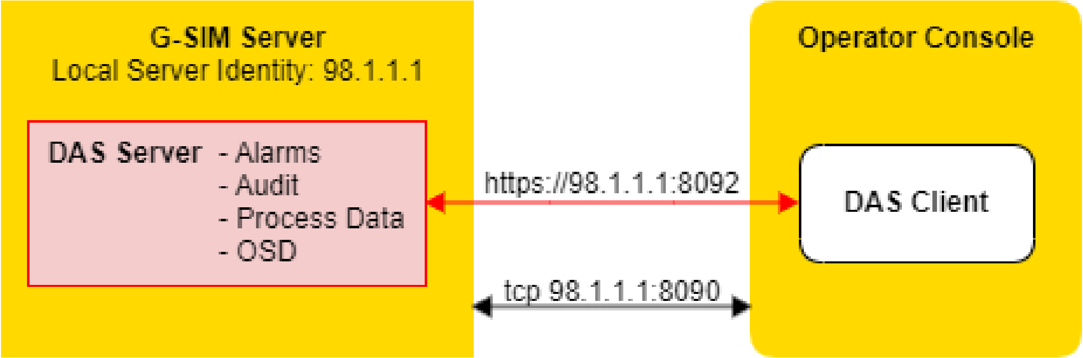
The operator console terminates the connection to the G-SIM server if the local server identity cannot be resolved. The error message **Login declined: The server address could not be resolved!** appears.



Login declined: The server address could not be resolved!

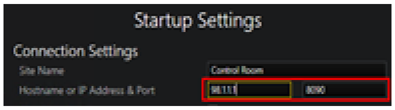
Use of the Local Server Identity in G-SIM

Standalone Environment



The entered address is used to establish the connection to the G-SIM server. This address is stored in the file `%ProgramFiles%\ Geutebrueck\GSim\Operator Console\ GSIM.OperatorUI.exe.Config`.

The local server identity is used to establish the connection to the DAS Server.



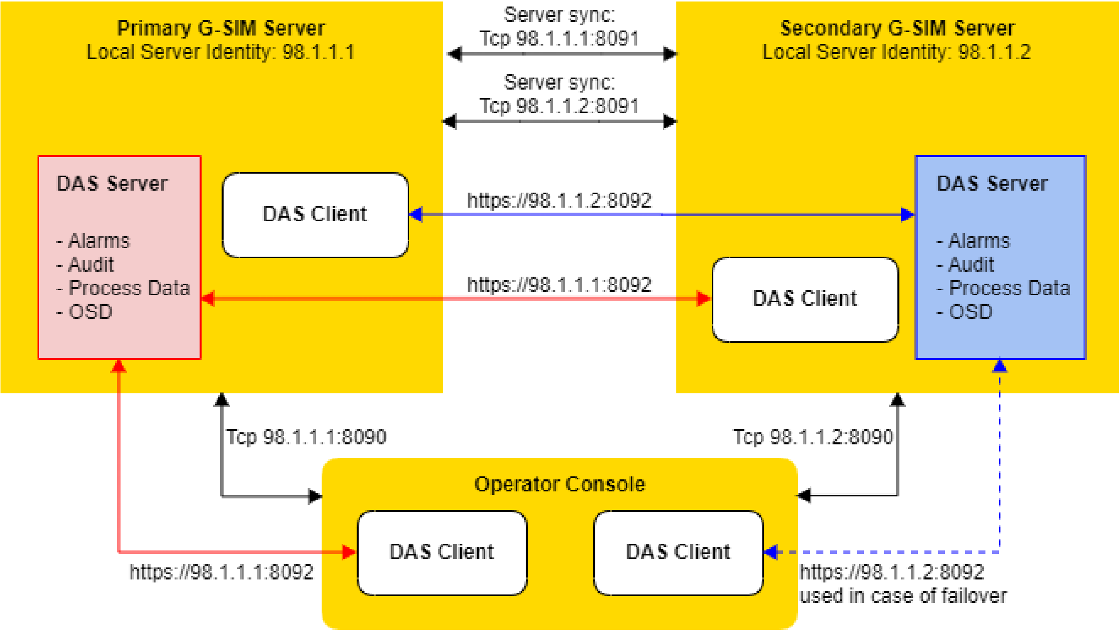
Startup Settings

Connection Settings

Site Name: Control Room

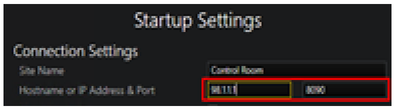
Hostname or IP Address & Port: 98.1.1.1 8090

Cluster Environment



The entered address is used only the first time to obtain a list of local server identities of the servers. This list is stored in the file `%ProgramData%\G-SIM\OpCon\Cluster\SiteServer.backup`.

The local server identity is used to establish the connections to the G-SIM server and to the DAS server.



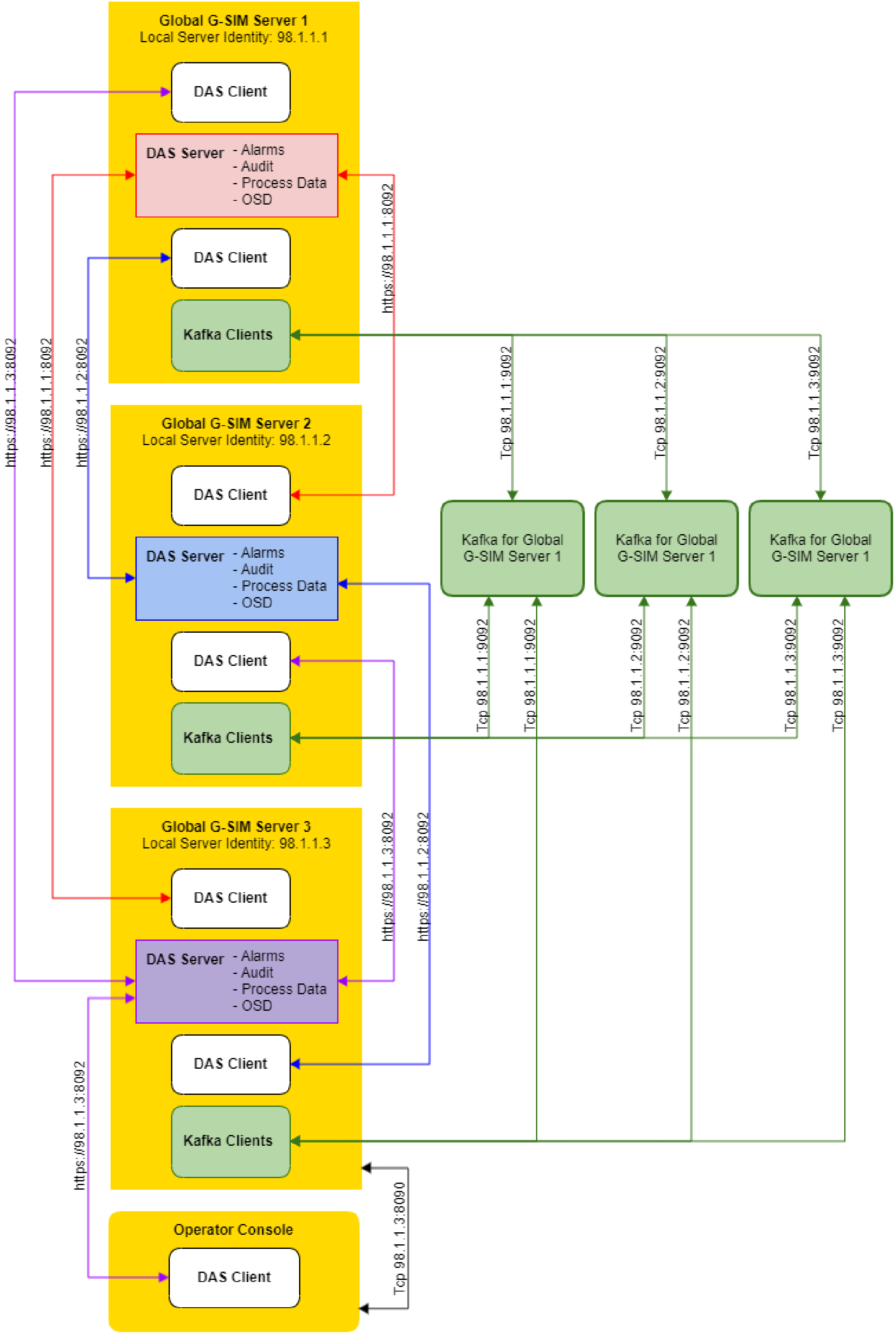
Startup Settings

Connection Settings

Site Name: Control Room

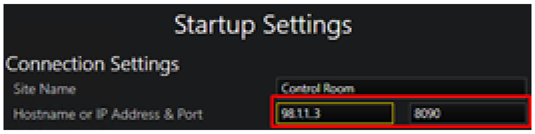
Hostname or IP Address & Port: 98.1.1.1 8090

Global Environment


Global G-SIM Server 1
Local Server Identity: 98.1.1.1
DAS Client
DAS Server - Alarms - Audit - Process Data - OSD
DAS Client
Kafka Clients
Global G-SIM Server 2
Local Server Identity: 98.1.1.2
DAS Client
DAS Server - Alarms - Audit - Process Data - OSD
DAS Client
Kafka Clients
Global G-SIM Server 3
Local Server Identity: 98.1.1.3
DAS Client
DAS Server - Alarms - Audit - Process Data - OSD
DAS Client
Kafka Clients
Operator Console
DAS Client
Kafka for Global G-SIM Server 1
Kafka for Global G-SIM Server 1
Kafka for Global G-SIM Server 1
https://98.1.1.3:8092
https://98.1.1.1:8092
https://98.1.1.2:8092
https://98.1.1.1:8092
https://98.1.1.3:8092
https://98.1.1.2:8092
https://98.1.1.3:8092
Tcp 98.1.1.1:9092
Tcp 98.1.1.2:9092
Tcp 98.1.1.3:9092
Tcp 98.1.1.1:9092
Tcp 98.1.1.1:9092
Tcp 98.1.1.2:9092
Tcp 98.1.1.2:9092
Tcp 98.1.1.3:9092
Tcp 98.1.1.3:9092
Tcp 98.1.1.3:8090

The entered address is used only the first time to obtain a list of local server identities of the servers. This list is stored in the file `%ProgramData%\G-SIM\OpCon\Cluster\ GlobalServer.backup`.

The local server identity is used to establish the connections to the G-SIM server and to the DAS server.



Startup Settings

Connection Settings

Site Name: Control Room

Hostname or IP Address & Port: 98.1.1.3 8090

G-SIM Password Requirements

Create a New User in ManCon

When you create a new user in the ManCon (see **Users**), the password is validated.

The default validation parameters are:

- The default password length is a minimum of 12 characters.
- Passwords are not valid if the characters match the user ID or the user's first and last name.

Changing an Existing User in ManCon

When you change an existing user in the ManCon (see **Users**), the password is validated.

The default validation parameters are:

- The default password length is a minimum of 12 characters.
- Passwords are not valid if the characters match the user ID or the user's first and last name.

Changing an Existing User in OpCon

When you change an existing user in the OpCon, the password is validated.

The default validation parameters are:

- The default password length is a minimum of 12 characters.
- Passwords are not valid if the characters match the user ID or the user's first and last name.

Additional Validation Parameters

Additional validation parameters can be configured in the ManCon System Settings in the User Management category.

- If the Enforce Password History option is enabled, the users cannot repeat any of the previous 24 passwords. Independent of the change path (OpCon, ManCon).
- The setting Minimum Password Length can be changed.

Software Licensing

Geutebrück software is subject to licensing and can only be used after installing a license.

License Overview

There are different types of licensing. Depending on the software, there are different license models and license types. Refer to the respective documentation of your products.

Traditional Licensing

With Traditional Licensing, the licenses and options are always bound to a dongle ID (hard or soft dongle).

ℹ **G-SIM version up to 10.x uses Traditional Licensing.**

Smart Licensing

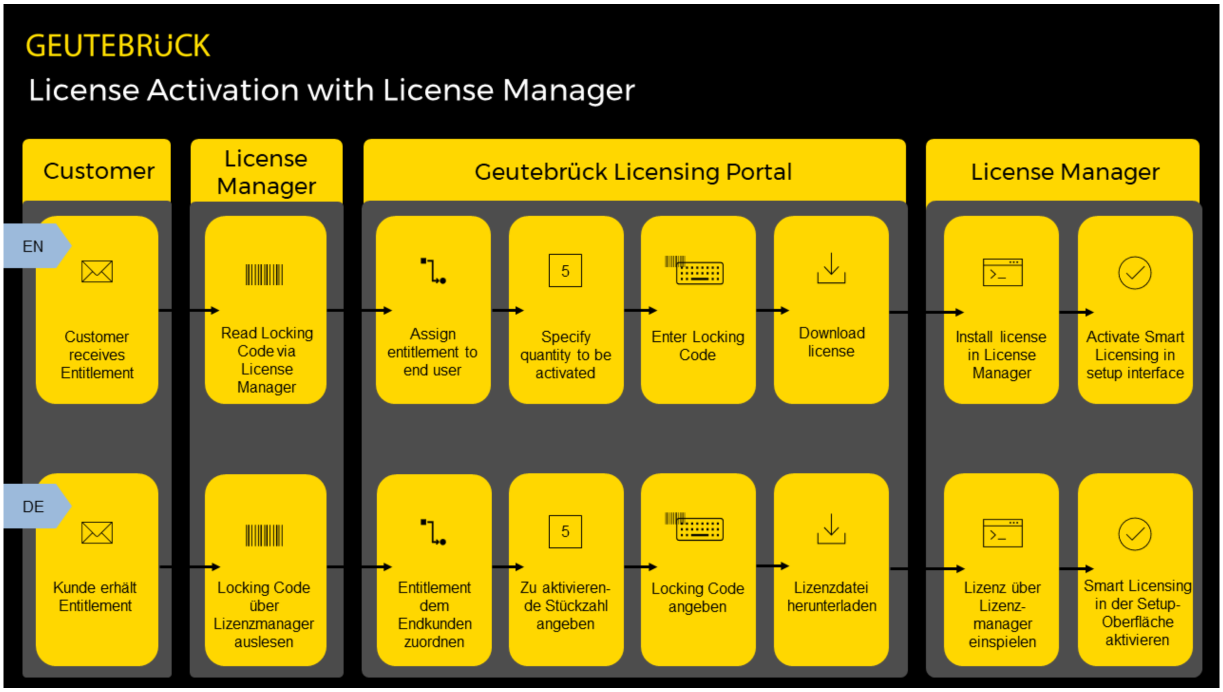
Smart Licensing allows you to purchase software packages and options without knowing where and when they need to be activated. There is no need to assign them to a device before purchase. In addition, Smart Licensing also allows you to independently deactivate software options on a device and activate them on a new device.

ℹ **Smart Licensing is available from G-SIM version 11.0. No new hardware dongles or software dongles are issued with the switch to Smart Licensing.**

License Activation

With Smart Licensing, the purchased entitlements are not directly activated, i.e. they are not assigned to a system. You or your Geutebrück partner activate them yourself in the Geutebrück license portal.

ℹ **If you do not yet have access to the license portal, contact our sales department.**



GEUTEBRÜCK

License Activation with License Manager

Customer

License Manager

Geutebrück Licensing Portal

License Manager

EN

Customer receives Entitlement

Read Locking Code via License Manager

Assign entitlement to end user

Specify quantity to be activated

Enter Locking Code

Download license

Install license in License Manager

Activate Smart Licensing in setup interface

DE

Kunde erhält Entitlement

Locking Code über Lizenzmanager auslesen

Entitlement dem Endkunden zuordnen

Zu aktivieren-de Stückzahl angeben

Locking Code angeben

Lizenzdatei herunterladen

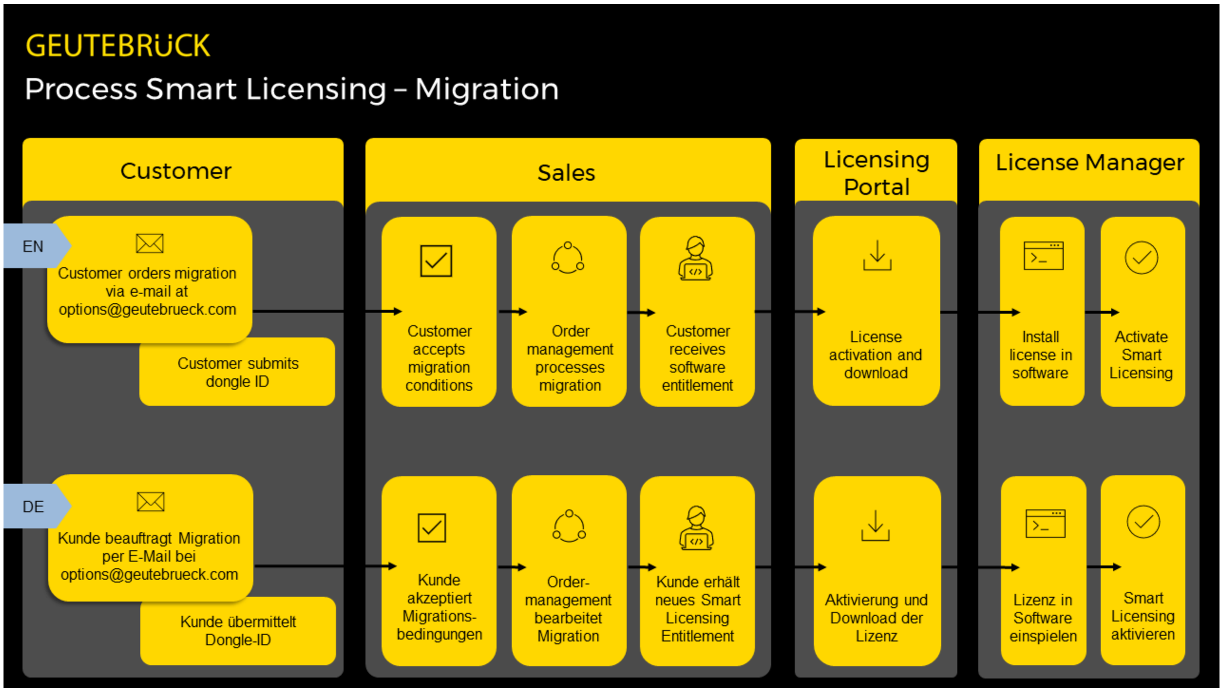
Lizenz über Lizenz-manager einspielen

Smart Licensing in der Setup-Oberfläche aktivieren

License Migration

You can migrate your existing licenses to Smart Licensing and enjoy all the new benefits.

i **To migrate existing dongles to Smart Licensing, contact our sales department.**



GEUTEBRÜCK

Process Smart Licensing – Migration

Customer

Sales

Licensing Portal

License Manager

EN

Customer orders migration via e-mail at options@geutebrueck.com

Customer submits dongle ID

Customer accepts migration conditions

Order management processes migration

Customer receives software entitlement

License activation and download

Install license in software

Activate Smart Licensing

DE

Kunde beauftragt Migration per E-Mail bei options@geutebrueck.com

Kunde übermittelt Dongle-ID

Kunde akzeptiert Migrations-bedingungen

Order-management bearbeitet Migration

Kunde erhält neues Smart Licensing Entitlement

Aktivierung und Download der Lizenz

Lizenz in Software einspielen

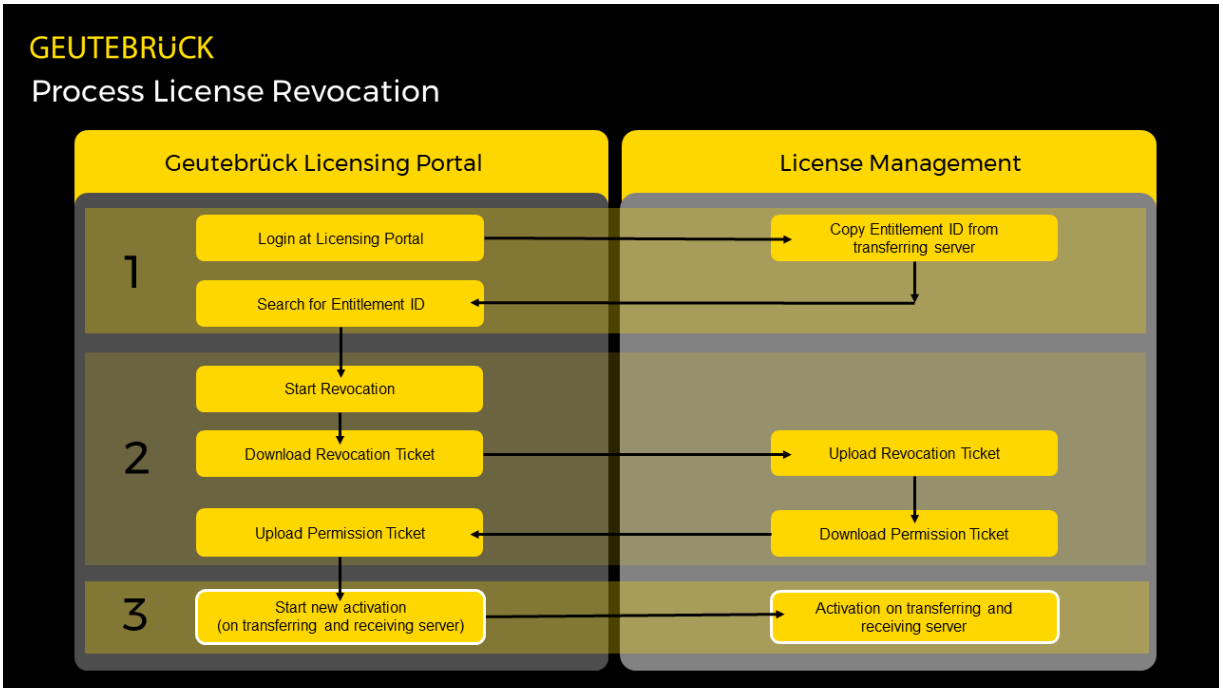
Smart Licensing aktivieren

License Revocation

With Smart Licensing, you can independently deactivate software options on a device and activate them on a new device.

To start the revocation process, go to the Geutebrück license portal. There you can select the activation you want to revoke and download the permission ticket. You must then upload this ticket in the License Manager (see **Revoke License**).

⚠ **IMPORTANT:** Only the full amount of license can be deactivated. Deactivated licenses will be removed immediately. Reactivate the necessary licenses on your source and target system.



GEUTEBRÜCK

Process License Revocation

Geutebrück Licensing Portal

License Management

1

Login at Licensing Portal

Copy Entitlement ID from transferring server

Search for Entitlement ID

2

Start Revocation

Download Revocation Ticket

Upload Revocation Ticket

Download Permission Ticket

Upload Permission Ticket

3

Start new activation (on transferring and receiving server)

Activation on transferring and receiving server

Upgrade Expiration Date

Each software product has an individual upgrade expiration date. When you purchase the software, you automatically receive one year of upgrade entitlement from the date of activation. With the appropriate upgrade packages you can extend the upgrade entitlement for one year. This is possible at the earliest 60 days before the current upgrade entitlement expires.

Note that prematurely activated upgrade packages cannot be installed. This is only possible 60 days before the upgrade expiration date.

Upgrade licenses cannot be migrated.

Installation

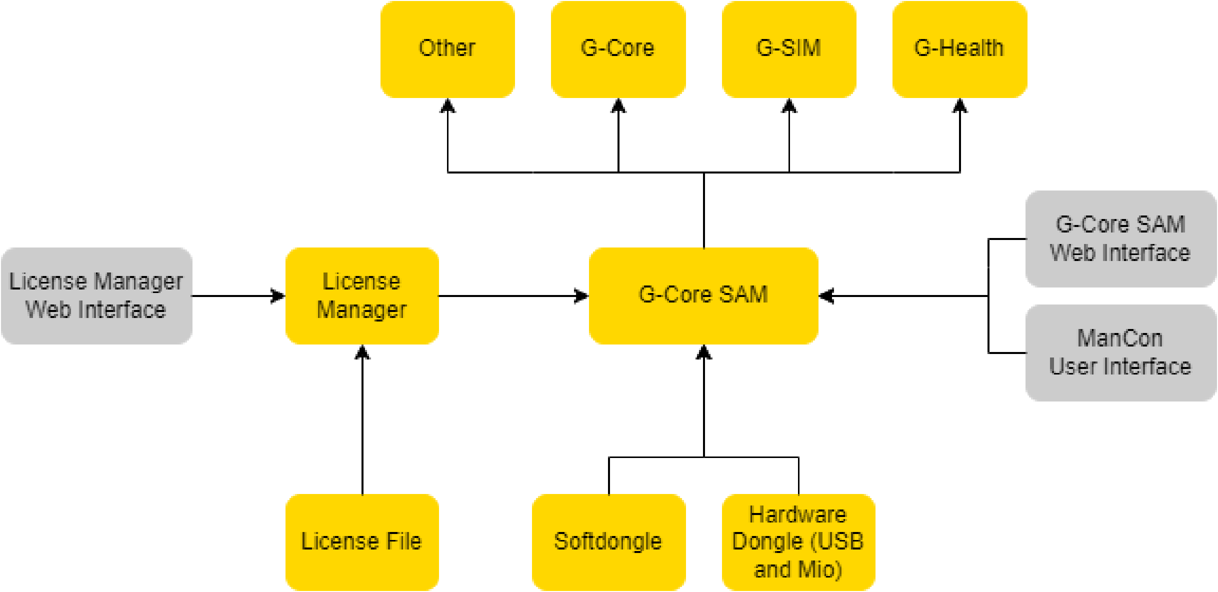
To use Smart Licensing, the License Manager is required. You can install this with the G-SIM Installer. For information on installing and using the License Manager, see **License Manager**.

Legacy

For older software there are legacy license models. These are not described here, if you have questions about them, contact the sales department.

Architecture and Configuration Interfaces

The following overview shows the architecture and configuration interfaces:

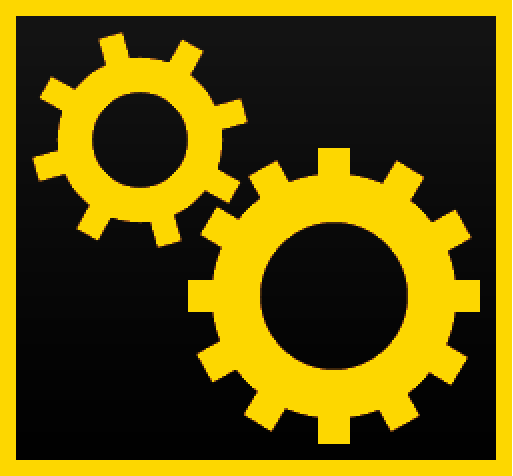


G-Core SAM manages licenses internally and provides them to the software products.

It is possible to operate with the Smart Licensing or Traditional Licensing license model (see **License Overview**).

- With Smart Licensing, G-Core SAM receives the license files via the License Manager. You manage the licenses via the web interface of the License Manager (see **License Manager**).
- With Traditional Licensing, G-Core SAM receives the license files via a software or hardware dongle. You manage the licenses via the G-Core SAM web interface (see **G-Core SAM**) or the Management Console user interface (see **Server Licenses**).

License Manager



The License Manager is a server system that provides its available options or licenses for remote systems.

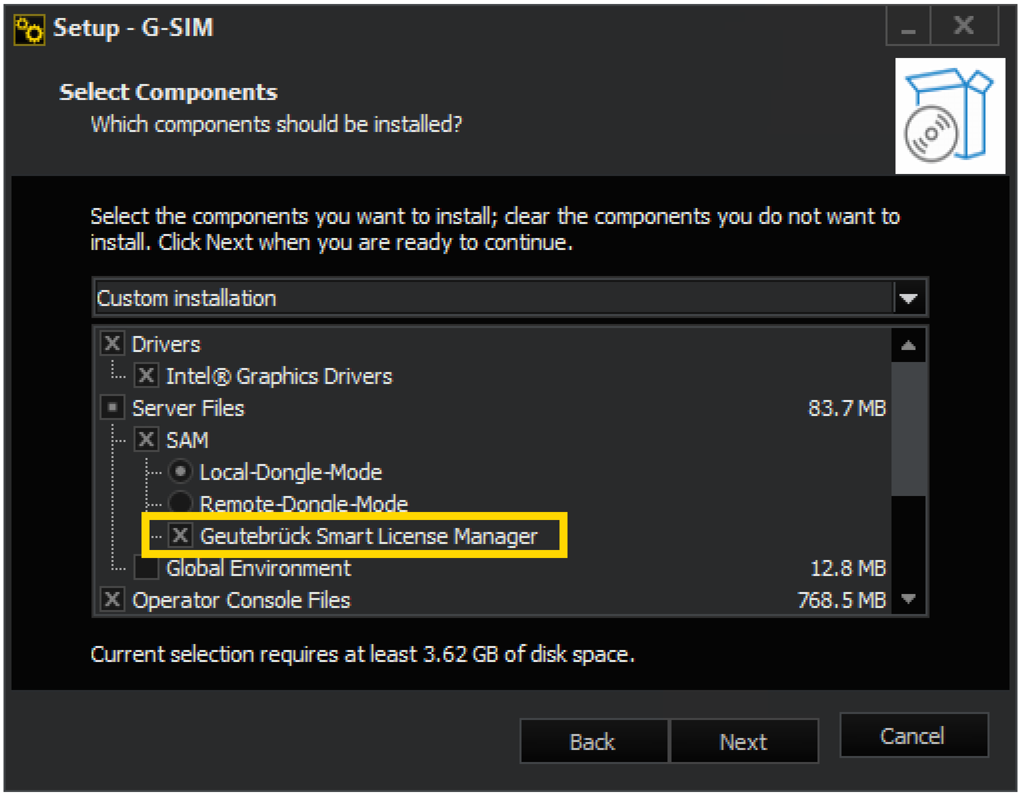
This license management is accessible via a web interface.

Installation

Server Installation

Install the License Manager on the G-SIM server using the G-SIM installer.

1. Run the `G-SIM_Installer.exe` file.
2. Accept the **License Agreement** and click **Next**.
3. In the **Select Components** dialog window, select **Geutebrück Smart License Manager**.



Setup - G-SIM

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom installation

☒ Drivers
☒ Intel® Graphics Drivers
■ Server Files 83.7 MB
☒ SAM
● Local-Dongle-Mode
○ Remote-Dongle-Mode
☒ Geutebrück Smart License Manager
□ Global Environment 12.8 MB
☒ Operator Console Files 768.5 MB

Current selection requires at least 3.62 GB of disk space.

4. Click **Next** and follow the further installation steps (see **Software Installation**).
5. In the **Ready to Install** dialog window, click **Install**.
6. G-SIM and the License Manager are installed.
7. To complete the installation, the computer must be restarted.

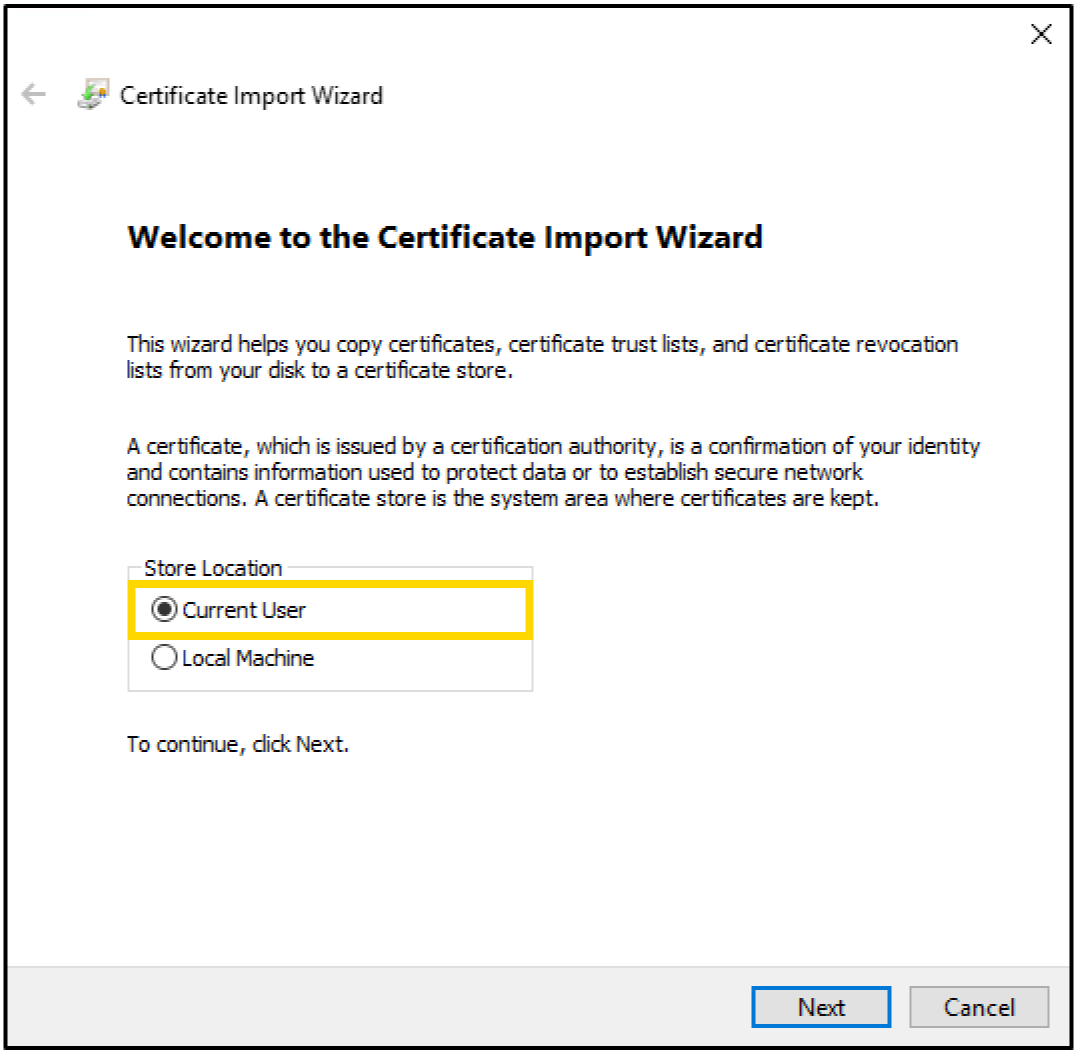
i **Make sure that both the installation of the License Manager and the G-SIM installation are completed before performing the restart.**

Client Installation

The authentication certificate for the License Manager web interface is automatically installed for the server and stored for the Microsoft Edge and Google Chrome browsers. To access the License Manager web interface via remote access from another client, install the authentication certificate on the respective client.

How to install the authentication certificate:

1. After installing the License Manager on the G-SIM server, you will find the certificate files in the folder `C:\Program Files\Geutebrueck-\Licensing\child-root`. Copy these folder to the respective client.
2. Run the certificate file `child-GeutebrueckLicenseManager.Auth-xxx.pfx`.
3. In the **Certificate Import Wizard**dialog window, select **Current User** as **Store Location** and click **Next**.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

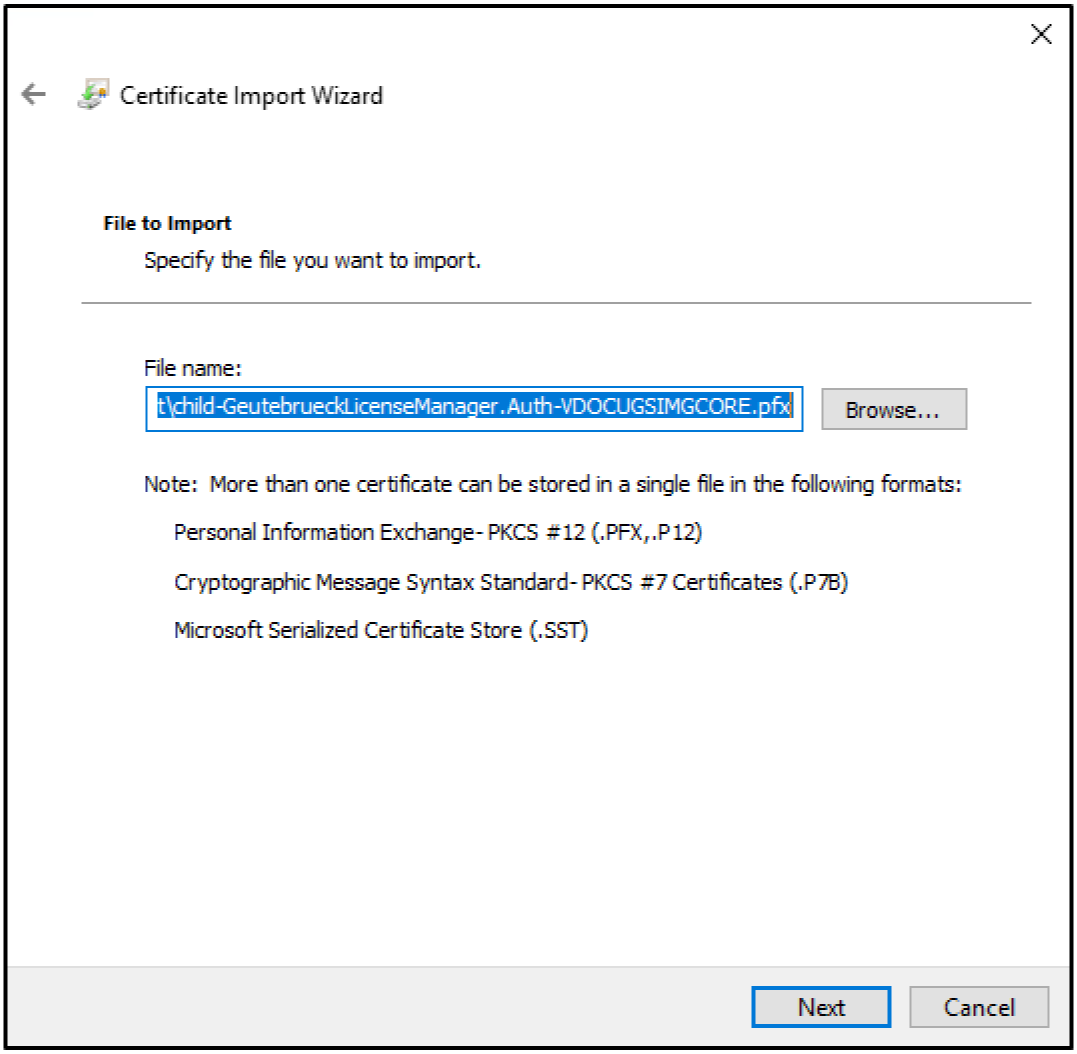
Store Location

● Current User

○ Local Machine

To continue, click Next.

4. In the **File to Import** dialog window, the certificate file is already selected by default. Click **Next**.



File to Import

Specify the file you want to import.

File name:

t\child-GeutebrueckLicenseManager.Auth-VDOCUGSIMGCORE.pfx

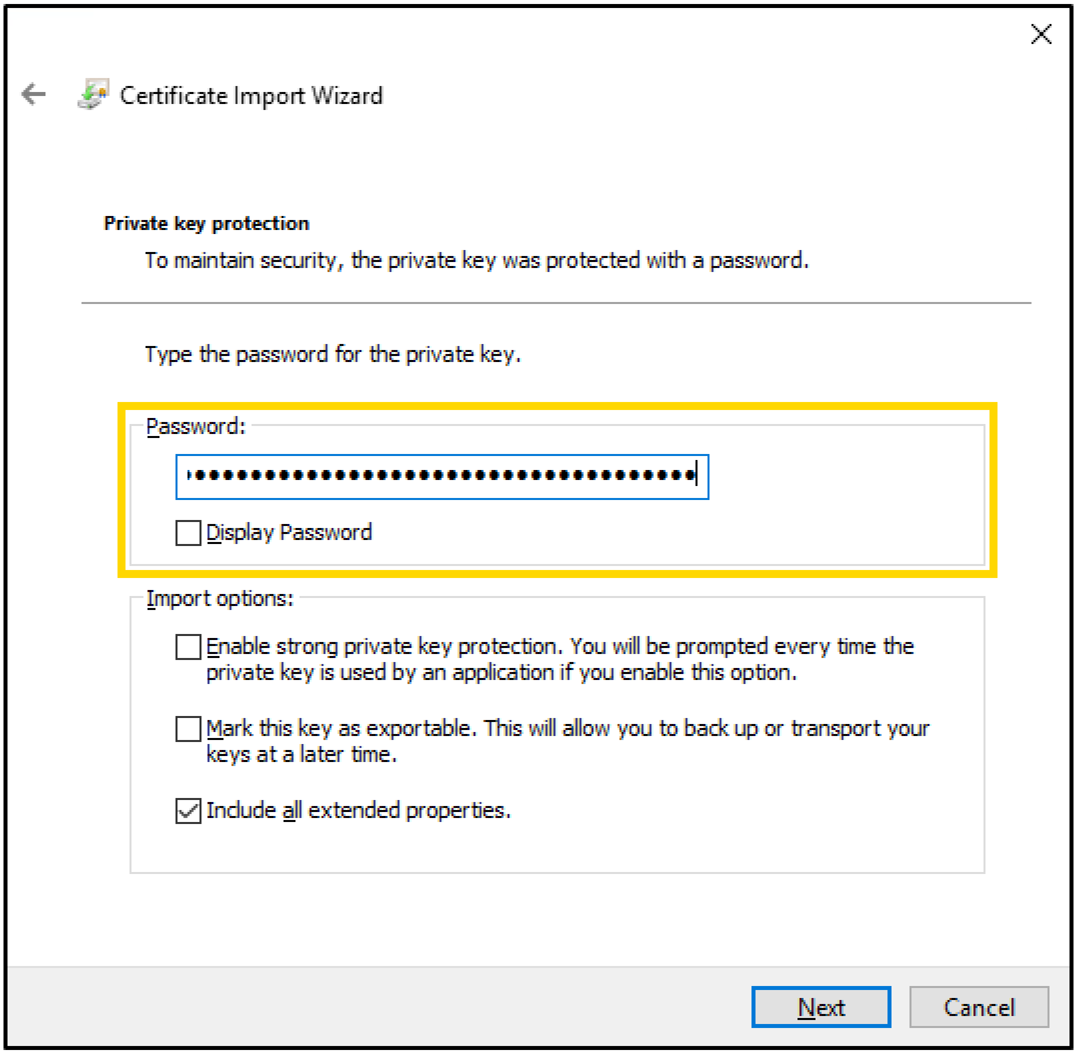
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

5. In the **Private key protection** dialog window, type the password for the private key. This password is noted in the file `child-Geutebrueck-LicenseManager.Auth-xxx.pfx.$password.txt`. Click **Next**.



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••••••••••••••••••••••••••••••••

□ Display Password

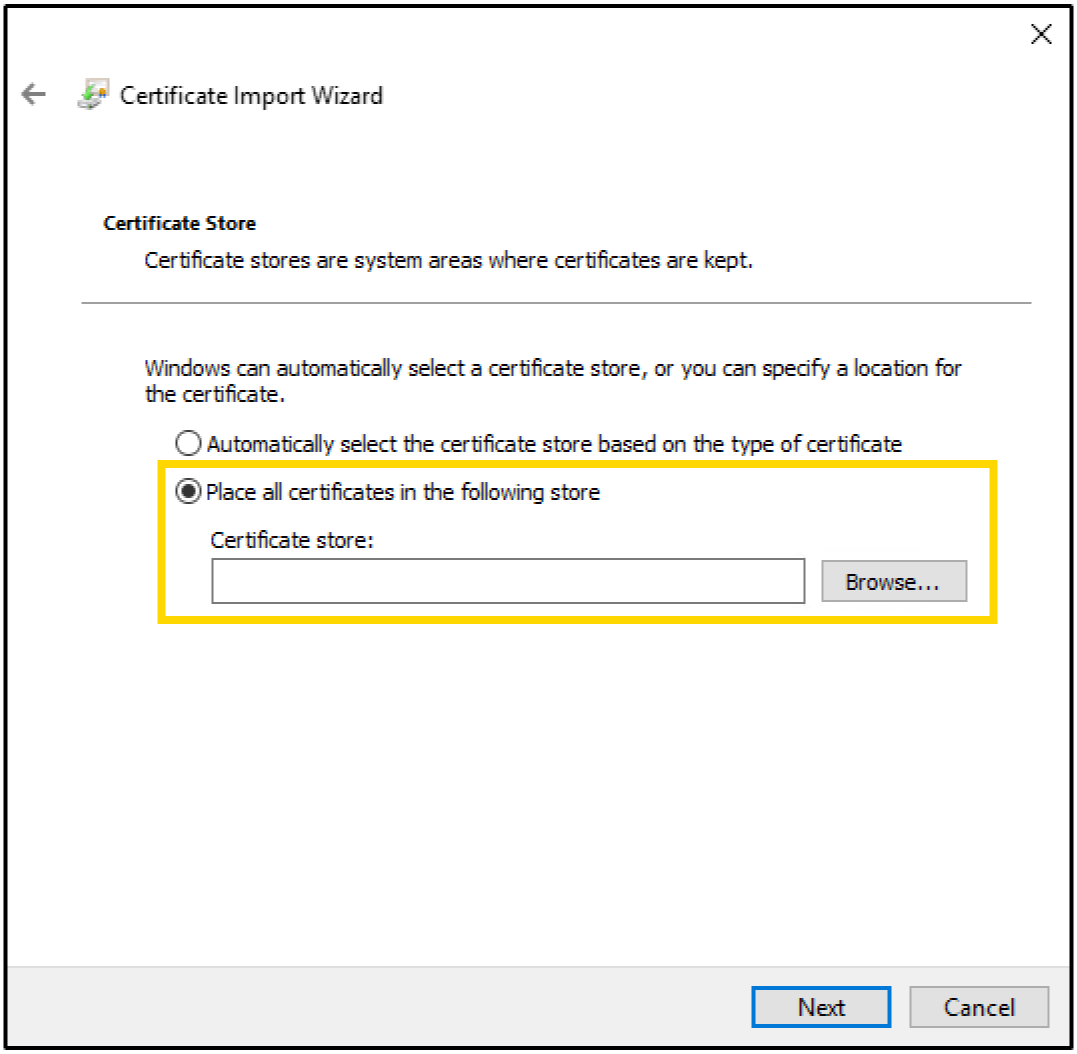
Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

6. In the **Certificate Store** dialog window, select the option **Place all certificates in the following store** and click **Browse...**.



Certificate Store

Certificate stores are system areas where certificates are kept.

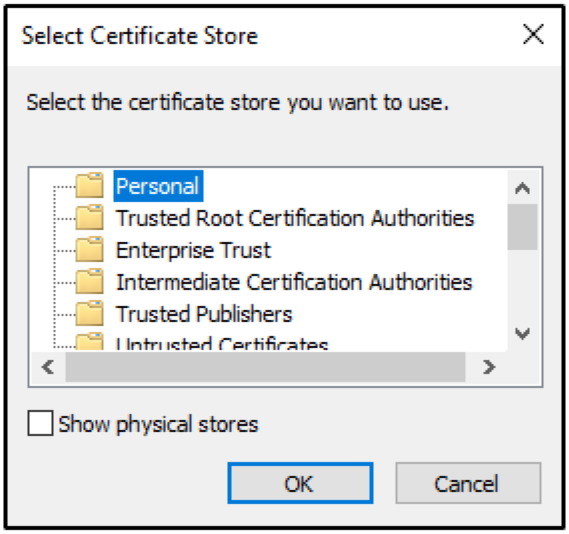
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

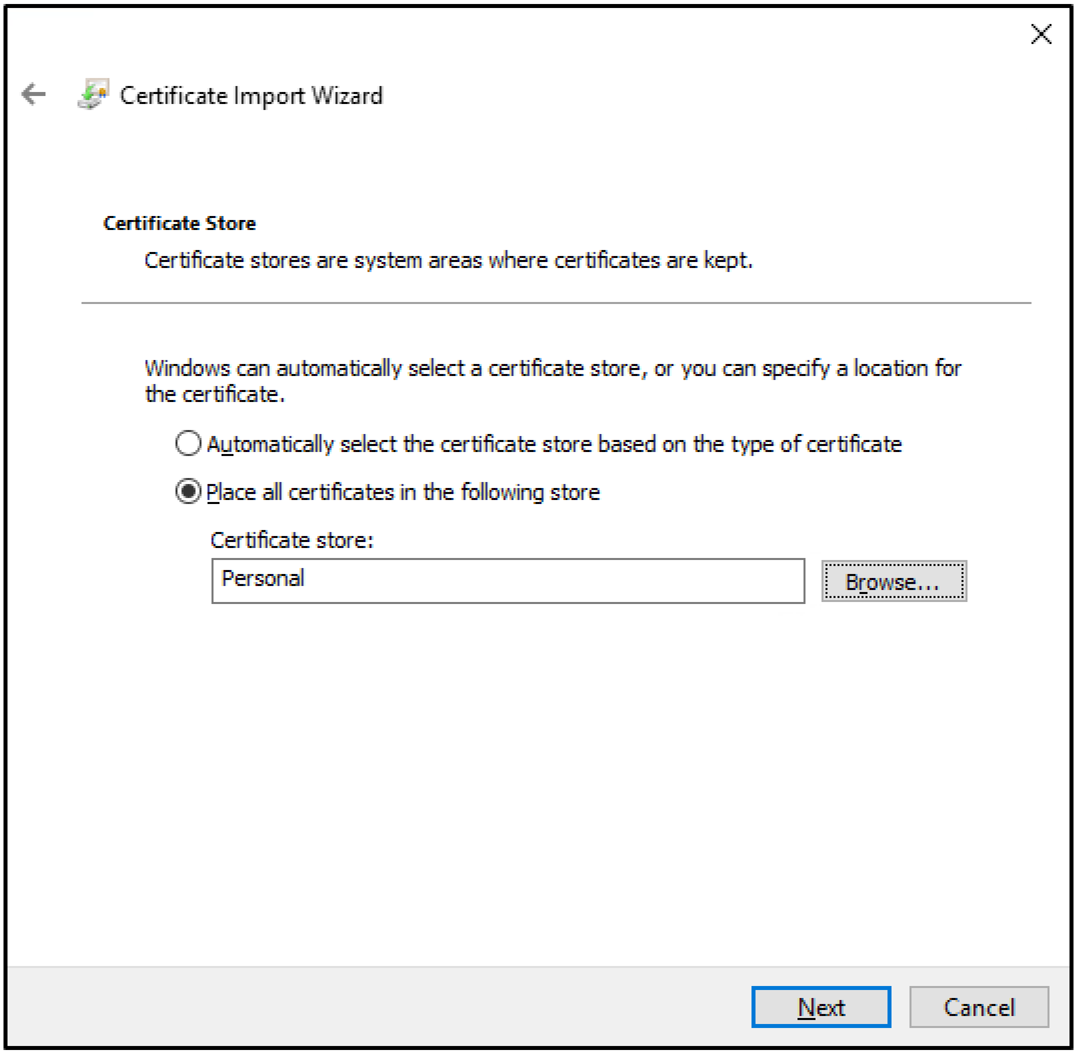
7. In the **Select Certificate Store** dialog window, select the **Personal** folder. Click **OK**.



Select Certificate Store

Select the certificate store you want to use.

8. In the **Certificate Store** dialog window, click **Next**.



Certificate Store

Certificate stores are system areas where certificates are kept.

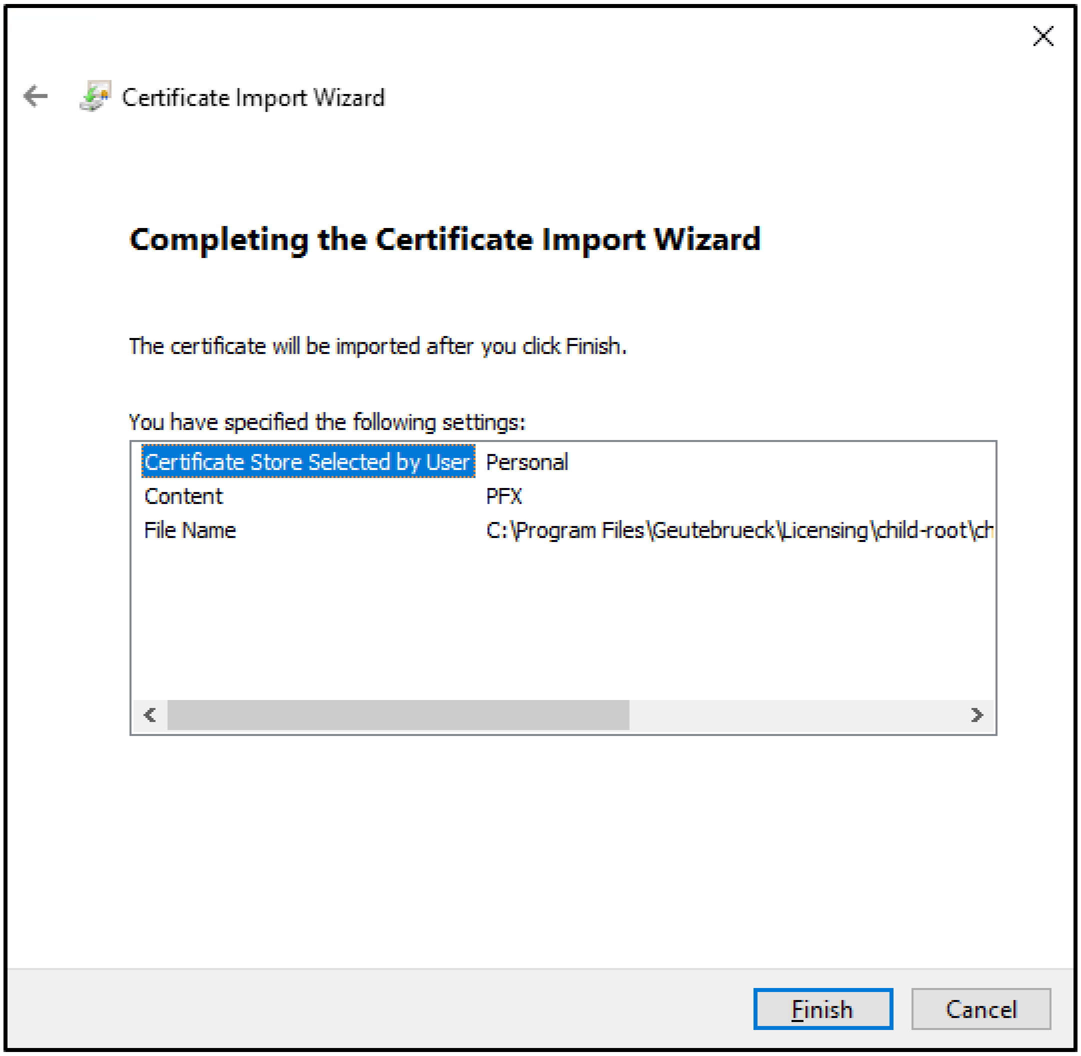
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Personal

9. In the **Completing the Certificate Import Wizard** dialog window, click **Finish**.



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Program Files\Geutebrueck\Licensing\child-root\ch

Open the License Manager web interface from the server on which the License Manager is installed or via remote access from a client (see **Open the Web Interface**).

Open the Web Interface

You can open the web interface of the License Manager from the server on which the License Manager is installed or via remote access from a client.

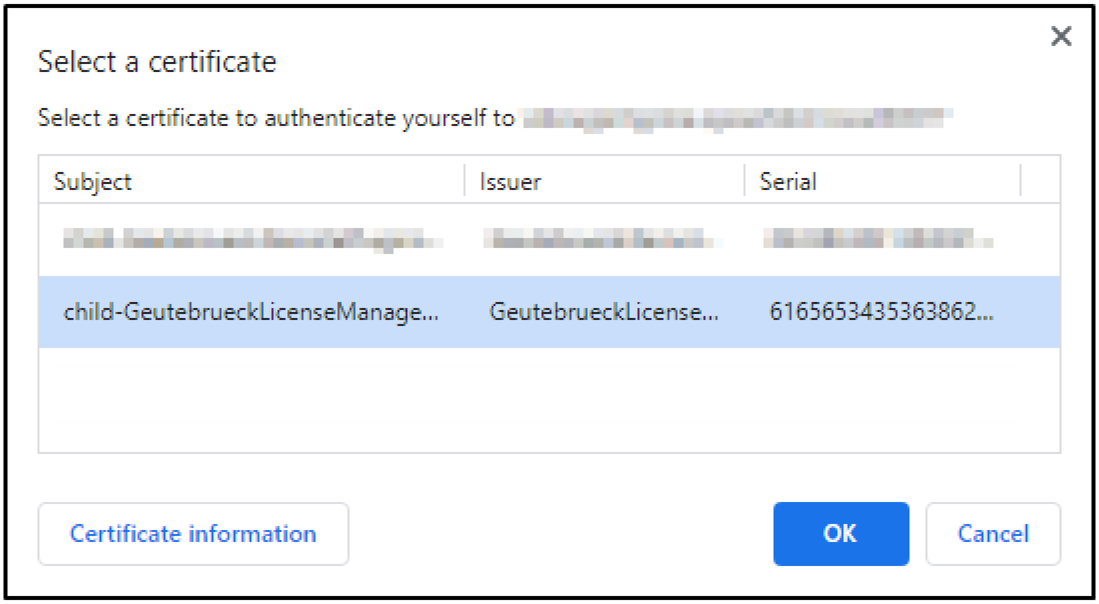
How to open the web interface:

- On the server: Open the web interface with the URL `https://localhost:30317/administration/features` or the desktop icon.

- **On the client:** Open the web interface with the URL `https://`**`<hostname or host-ip>`**`:30317/administration/feature`.

Open the web interface in the browser for the first time:

- The error message **Your connection isn't private** appears. Click the **Advanced** button and then **Continue to localhost (unsafe)**.
- The pop-up window **Select a certificate** appears, asking you to select a certificate for authentication. Select the `child-Geutebrueck-LicenseManagerAuth` certificate and confirm with **OK**.



Select a certificate

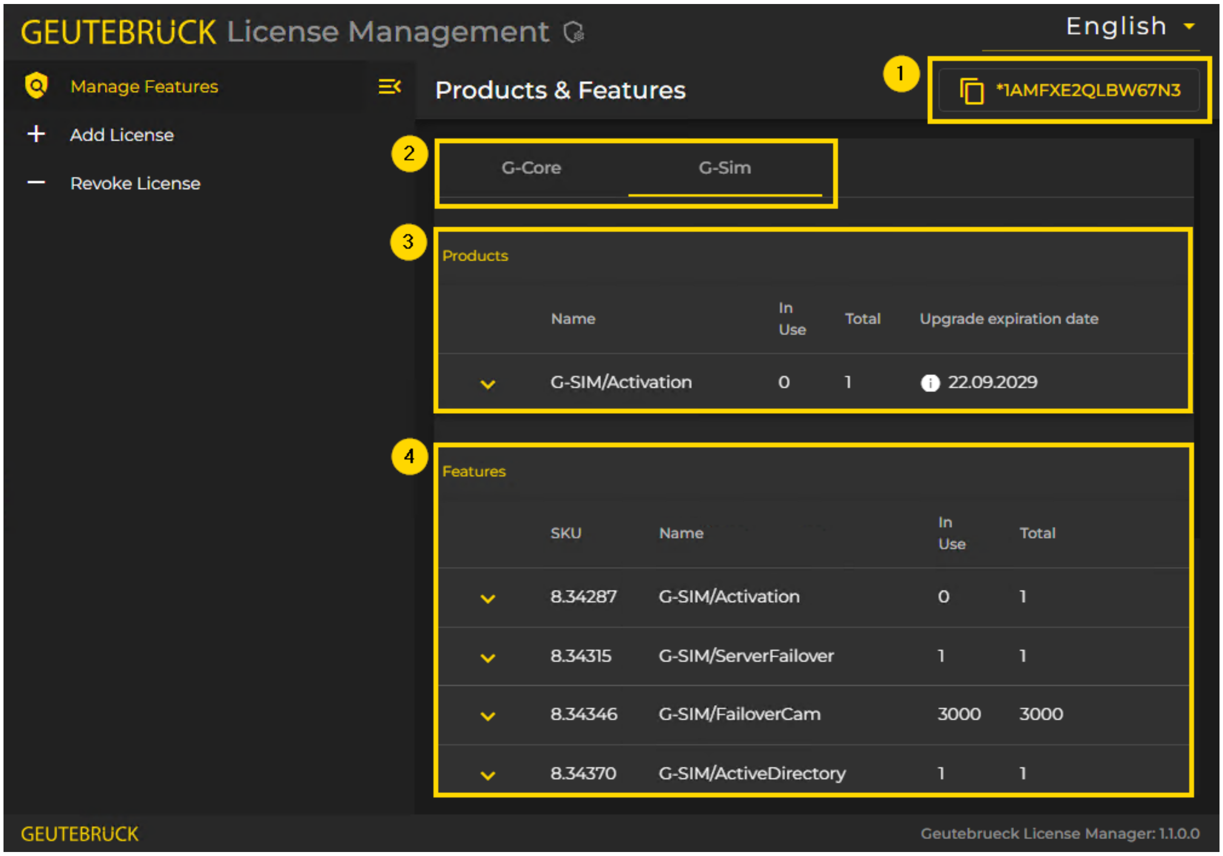
Select a certificate to authenticate yourself to [redacted]

Subject	Issuer	Serial
[redacted]	[redacted]	[redacted]
child-GeutebrueckLicenseManage...	GeutebrueckLicense...	6165653435363862...

- The default page of the License Manager web interface is empty and does not show any licenses.

Manage Features

In the **Products & Features** view, you can manage the licenses. The view provides an overview of the available licenses and options.



*1AMFXE2QLBW67N3

Products

	Name	In Use	Total	Upgrade expiration date
⌄	G-SIM/Activation	0	1	ⓘ 22.09.2029

Features

	SKU	Name	In Use	Total
⌄	8.34287	G-SIM/Activation	0	1
⌄	8.34315	G-SIM/ServerFailover	1	1
⌄	8.34346	G-SIM/FailoverCam	3000	3000
⌄	8.34370	G-SIM/ActiveDirectory	1	1

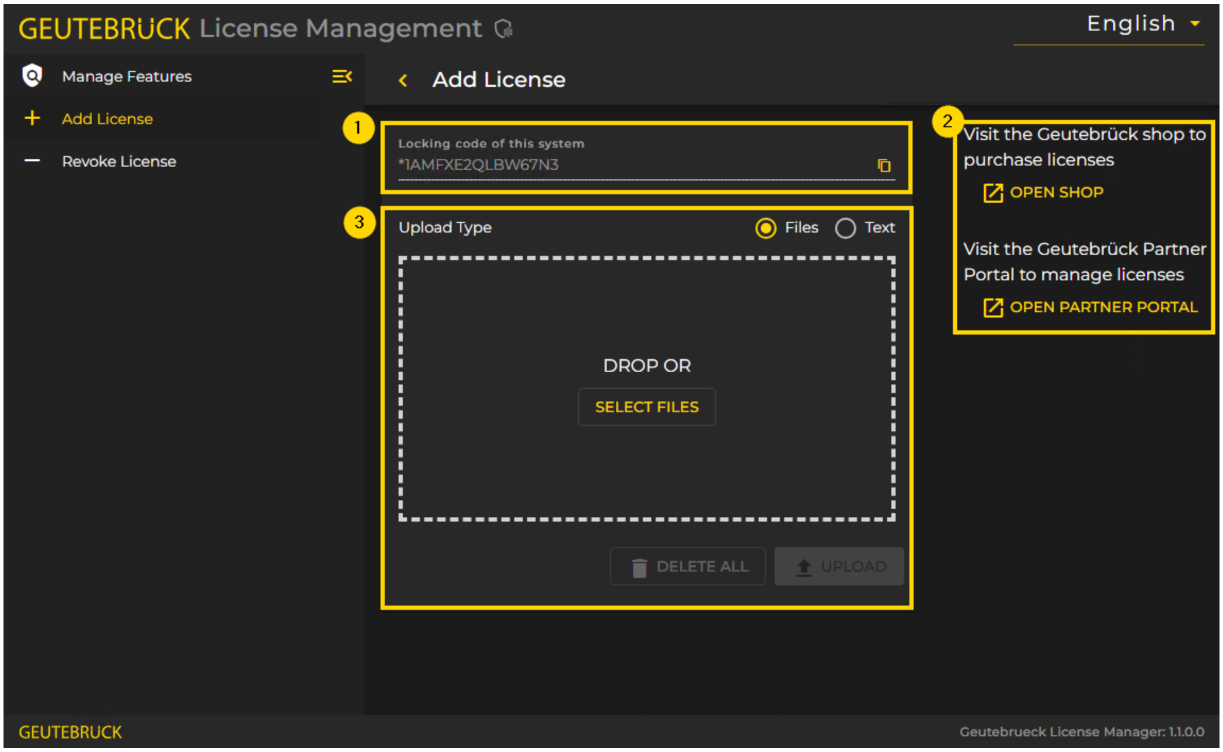
The user interface consists of the following elements:

	Element	Description
1	Locking Code	The locking code is required to activate licenses for this system (see **License Activation**). Click the ⧉ icon to copy it to the clipboard.
2	Category	The product category.
3	Products List	In the product list all ordered products are listed. Each entry consists of the following information: • **Name:** Name of the product. • **In Use:** Number of licenses in use. • **Total:** Total number of available licenses.

	Element	Description
		• **Upgrade expiration date:** Expiration date of the upgrade. Only activation options (e.g. G-SIM Activation) have an upgrade expiration date. If you click on an entry, a detailed view opens, which contains more information about the product: • **Quantity:** Quantity of available licenses. • **Entitlement ID:** Entitlement ID of the license. Click on the entitlement ID to copy it to the clipboard. • **Activation Date:** Activation date of the license. • **Customer Name:** Customer of the license. • **Upgrade permission:** Time until and expiration date of the upgrade.
4	Features List	In the features list all related features are listed. Each entry consists of the following information: • **SKU:** SKU (Stock Keeping Unit) of the feature. • **Name:** Name of the feature. • **In Use:** Number of licenses in use. • **Total:** Total number of available licenses. If you click on an entry, a detailed view opens, which contains more information about the product: • **Quantity:** Quantity of available licenses. • **Entitlement ID:** Entitlement ID of the license. Click on the entitlement ID to copy it to the clipboard. • **Activation Date:** Activation date of the license. • **Customer Name:** Customer of the license.

Add License

In the **Add License** view, you can upload your licenses to the system.



Locking code of this system
*1AMFXE2QLBW67N3

Upload Type ● Files ○ Text

Visit the Geutebrück shop to purchase licenses

Visit the Geutebrück Partner Portal to manage licenses

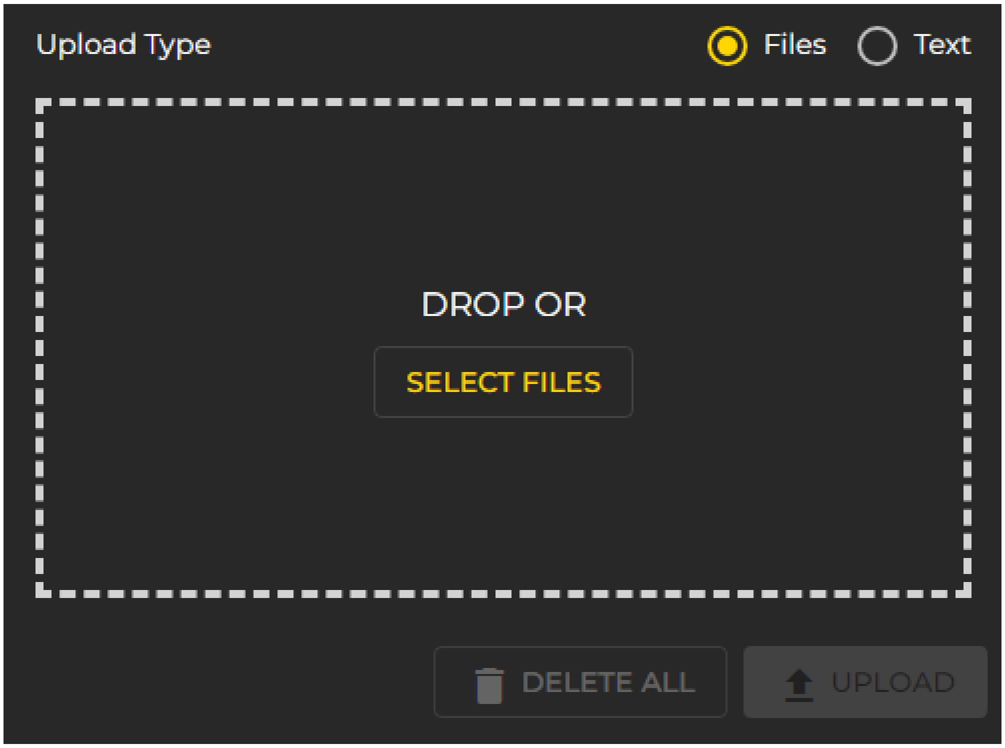
Geutebrueck License Manager: 1.1.0.0

The **Add License** view consists of the following elements:

	Element	Description
1	Locking Code	The locking code is required to activate the license for this system (see **License Activation**). Click the ⧉ icon to copy it to the clipboard.
2	Links to Geutebrück Pages	Click **Open Shop** to open the Geutebrück shop and purchase licenses. Click **Open Partner Portal** to open the Geutebrück Partner Portal and manage licenses.
3	License Upload	In this field you can upload the retrieved license to the system as a file or as text.

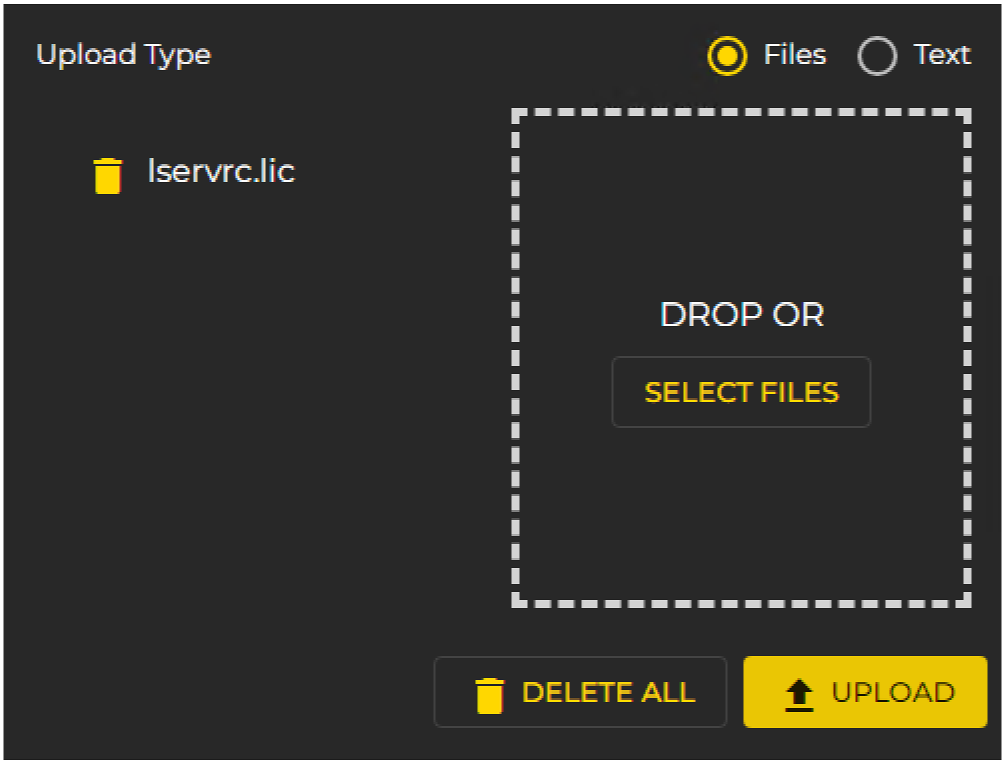
How to add a license as a file:

1. Select the **Files** option as **Upload Type**.



Upload Type ● Files ○ Text

2. Drag and drop the license file (.lic) into the upload field or click the **Select Files** button.
3. The file is displayed in the upload field and the **Upload** button is enabled. You can select further files.

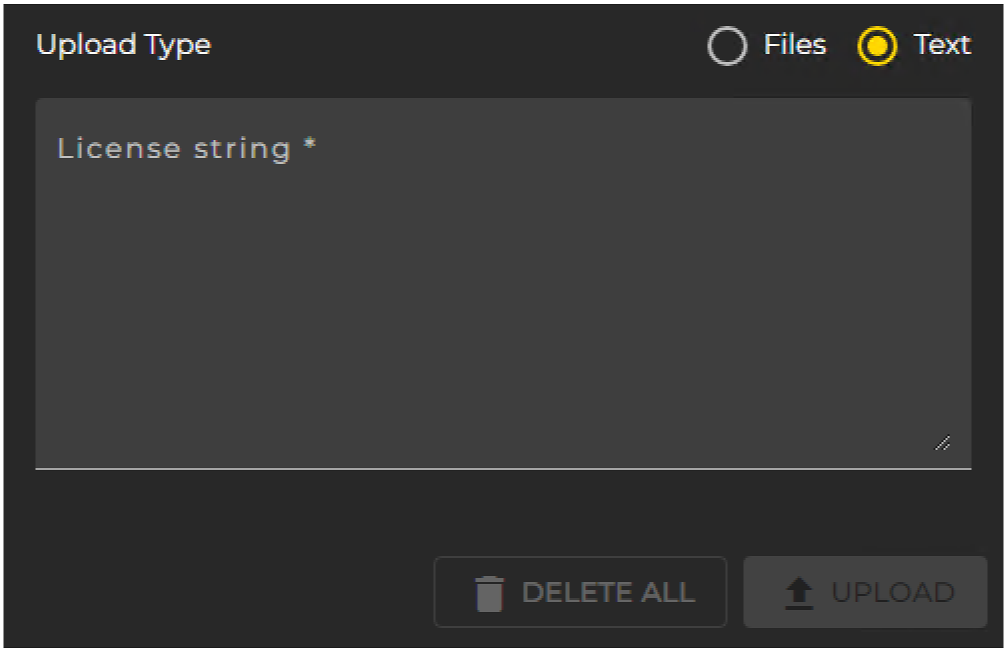


4. Click the **Upload** button to add the license.

5. After uploading a valid license, you will be automatically redirected to the feature list (see **Manage Features**).

How to add a license as text:

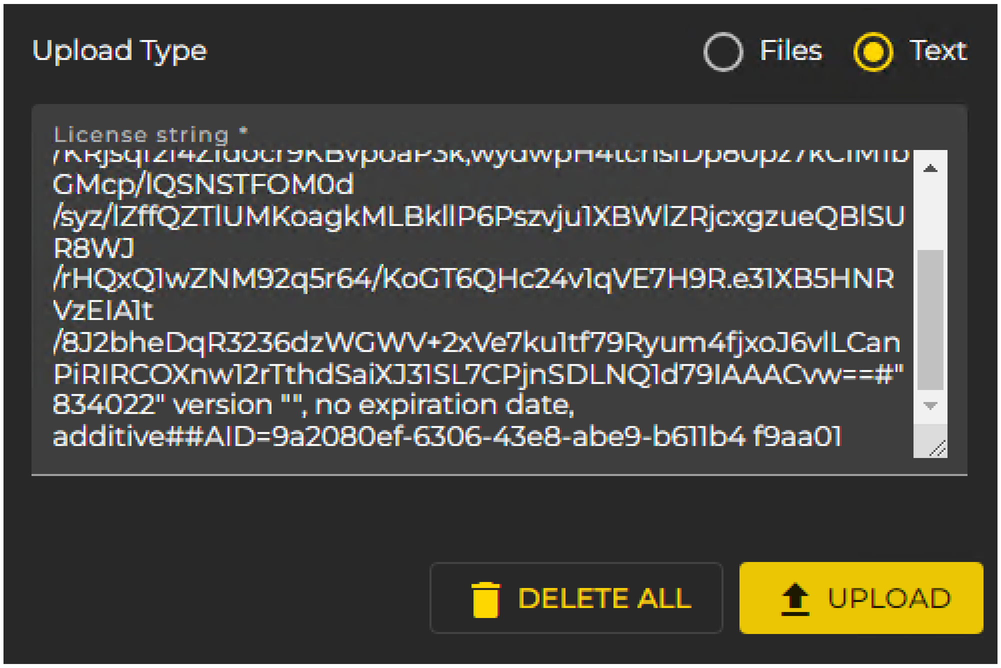
1. Select the **Text** option as **Upload Type**.



Upload Type ○ Files ● Text

License string *

2. Paste the license text into the text field. The **Upload** button is enabled.



Upload Type ○ Files ● Text

License string *

```
/KRjsqI2I4ZIdocr9KBvpdaP3k,wydwpH4tcrIsIDp8op27kCIMIb
GMcp/lQSNSTFOM0d
/syz/lZffQZTlUMKoagkMLBkllP6Pszvju1XBWlZRjcxgzueQBlSU
R8WJ
/rHQxQ1wZNM92q5r64/KoGT6QHc24v1qVE7H9R.e31XB5HNR
VzEIA1t
/8J2bheDqR3236dzWGWV+2xVe7ku1tf79Ryum4fjxoJ6vlLCan
PiRIRCOXnw12rTthdSaiXJ31SL7CPjnSDLNQ1d79IAAACvw==#"
834022" version "", no expiration date,
additive##AID=9a2080ef-6306-43e8-abe9-b611b4 f9aa01
```

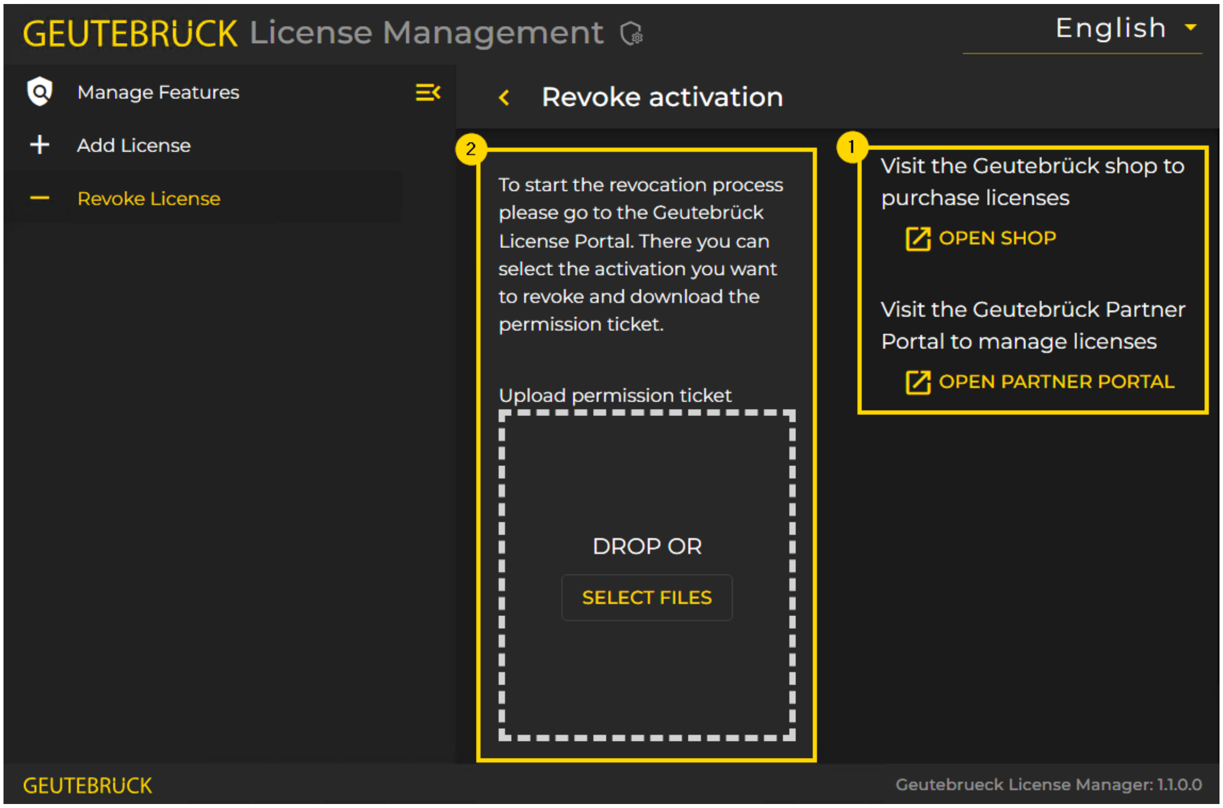
3. Click the **Upload** button to add the license.

4. After uploading a valid license, you will be automatically redirected to the feature list (see **Manage Features**).

Revoke License

In the **Revoke activation** view, you can revoke your licenses.

> **IMPORTANT:** Only the full amount of license can be deactivated. Deactivated licenses will be removed immediately. Reactivate the necessary licenses on your source and target system accordingly.



To start the revocation process please go to the Geutebrück License Portal. There you can select the activation you want to revoke and download the permission ticket.

Visit the Geutebrück shop to purchase licenses

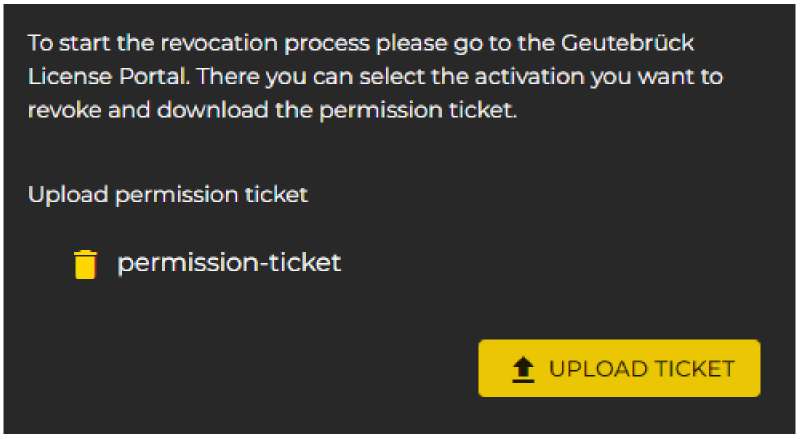
Visit the Geutebrück Partner Portal to manage licenses

The **Revoke activation** view consists of the following elements:

	Element	Description
1	Links to Geutebrück Pages	Click **Open Shop** to open the Geutebrück shop and purchase licenses. Click **Open Partner Portal** to open the Geutebrück Partner Portal and manage licenses.
2	Upload Permission Ticket	In this field you can upload the retrieved permission ticket to the system.

How to revoke a license:

1. In the Geutebrück License Portal, select the activation you want to revoke and download the permission ticket (see **License Revocation**).
2. Drag and drop the permission ticket file into the upload field or click the Select Files button.
3. The file is displayed in the upload field and the Upload button is enabled.



To start the revocation process please go to the Geutebrück License Portal. There you can select the activation you want to revoke and download the permission ticket.

Upload permission ticket

4. Click the Upload Ticket button to upload the permission ticket.
5. After uploading a valid permission ticket, you will be automatically redirected to the feature list (see **Manage Features**).

Management Console

In the Server Licenses menu of the Management Console you have an overview of your available licenses.

You can choose between operating with the Traditional or Smart Licensing license model. For Traditional Licensing, you can also request and import a softdongle.

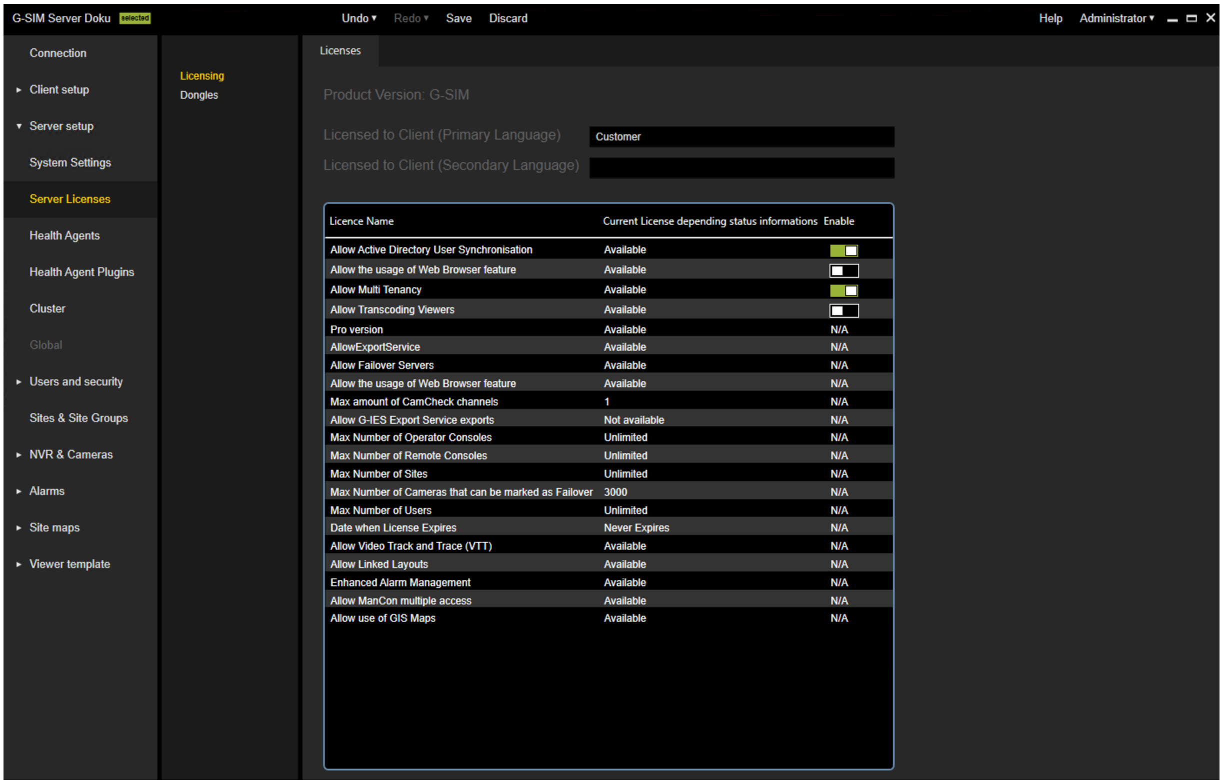
Server Licenses

The Server Licenses menu contains dialog windows: **Licensing** and **Dongles**.

Licensing

The Licensing dialog window provides a list of the dongle-related licenses and their status. You can activate or deactivate some of the available licenses. Move the mouse cursor over an entry to display a description of the license.

You can configure the Licensed to Client setting for both primary and secondary languages. This setting is displayed in the login screen of the Operator Console.



Product Version: G-SIM

Licensed to Client (Primary Language): Customer

Licensed to Client (Secondary Language):

Licence Name	Current License depending status informations	Enable
Allow Active Directory User Synchronisation	Available	☑
Allow the usage of Web Browser feature	Available	☐
Allow Multi Tenancy	Available	☑
Allow Transcoding Viewers	Available	☐
Pro version	Available	N/A
AllowExportService	Available	N/A
Allow Failover Servers	Available	N/A
Allow the usage of Web Browser feature	Available	N/A
Max amount of CamCheck channels	1	N/A
Allow G-IES Export Service exports	Not available	N/A
Max Number of Operator Consoles	Unlimited	N/A
Max Number of Remote Consoles	Unlimited	N/A
Max Number of Sites	Unlimited	N/A
Max Number of Cameras that can be marked as Failover	3000	N/A
Max Number of Users	Unlimited	N/A
Date when License Expires	Never Expires	N/A
Allow Video Track and Trace (VTT)	Available	N/A
Allow Linked Layouts	Available	N/A
Enhanced Alarm Management	Available	N/A
Allow ManCon multiple access	Available	N/A
Allow use of GIS Maps	Available	N/A

Dongles

In the **Options** dialog window you can manage your licenses or options and import new licenses.

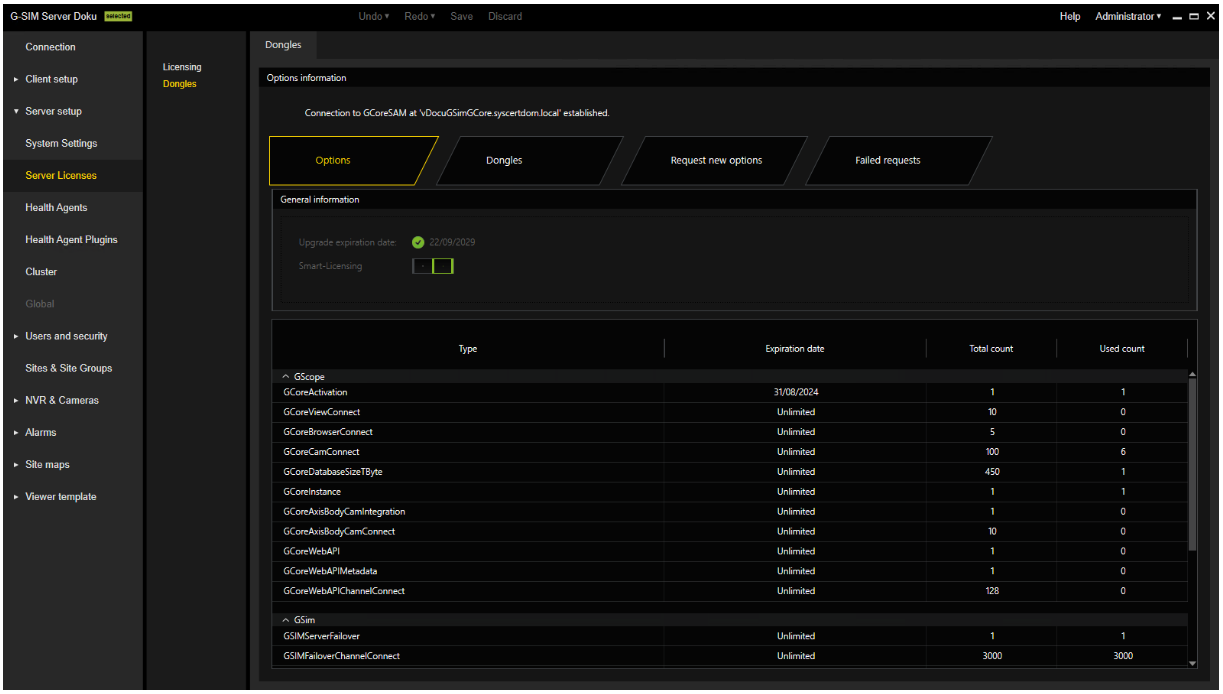
The dialog consists of the following tabs:

- **Options**
- **Dongles**
- **Request New Options**
- **Failed Requests**
- **SoftDongle**

Options

This tab provides an overview of the available licenses. It contains information about the options in the database and displays all available options. Right-click on an entry to expand the list with more information.

You can choose between operating with the Traditional or Smart Licensing license model by enabling or disabling the **Smart-Licensing** option. For more information see **Activate Smart Licensing**.



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

Upgrade expiration date: ✓ 22/09/2029

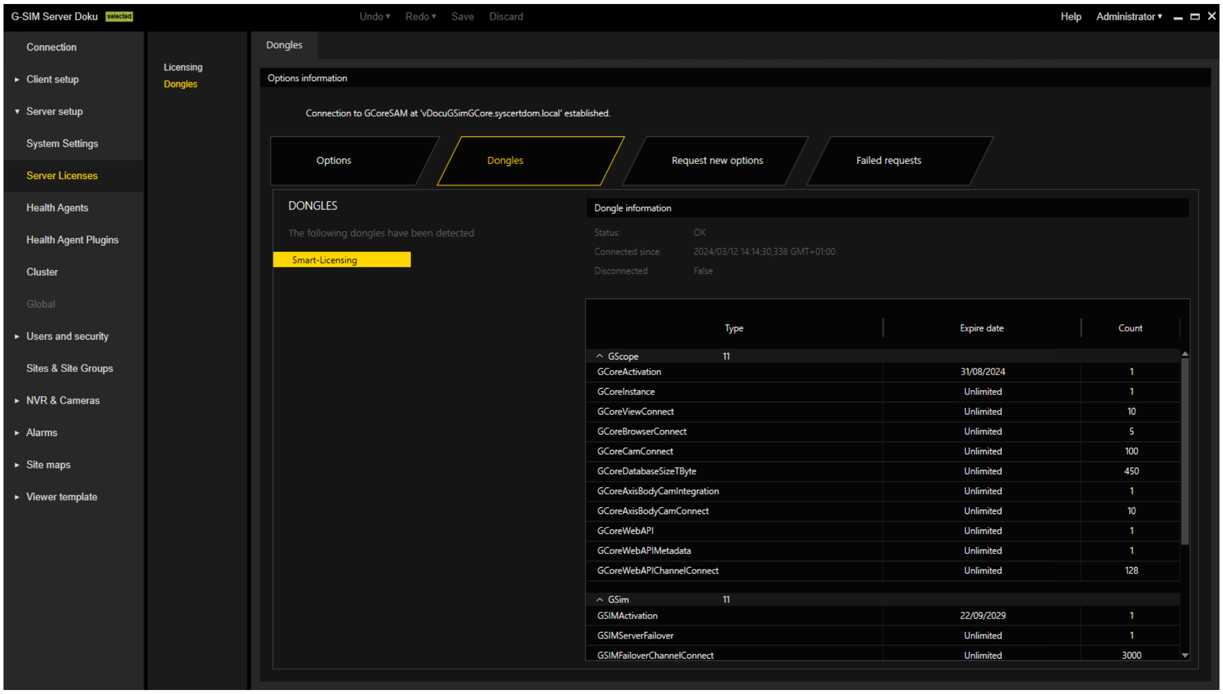
Smart-Licensing

Type	Expiration date	Total count	Used count
^ GScope			
GCoreActivation	31/08/2024	1	1
GCoreViewConnect	Unlimited	10	0
GCoreBrowserConnect	Unlimited	5	0
GCoreCamConnect	Unlimited	100	6
GCoreDatabaseSizeTByte	Unlimited	450	1
GCoreInstance	Unlimited	1	1
GCoreAxisBodyCamIntegration	Unlimited	1	0
GCoreAxisBodyCamConnect	Unlimited	10	0
GCoreWebAPI	Unlimited	1	0
GCoreWebAPIMetadata	Unlimited	1	0
GCoreWebAPIChannelConnect	Unlimited	128	0
^ GSim			
GSIMServerFailover	Unlimited	1	1
GSIMFailoverChannelConnect	Unlimited	3000	3000

Dongles

All identified dongles are displayed on this tab. In our case, a Smart Licensing dongle was found. If a dongle is clicked on, all information about this dongle is read out.

With Smart Licensing, one Smart Licensing dongle is available for all licenses and options. With Traditional Licensing, you can import multiple dongles.



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

The following dongles have been detected

Status: OK
Connected since: 2024/03/12 14:14:30,338 GMT+01:00
Disconnected False

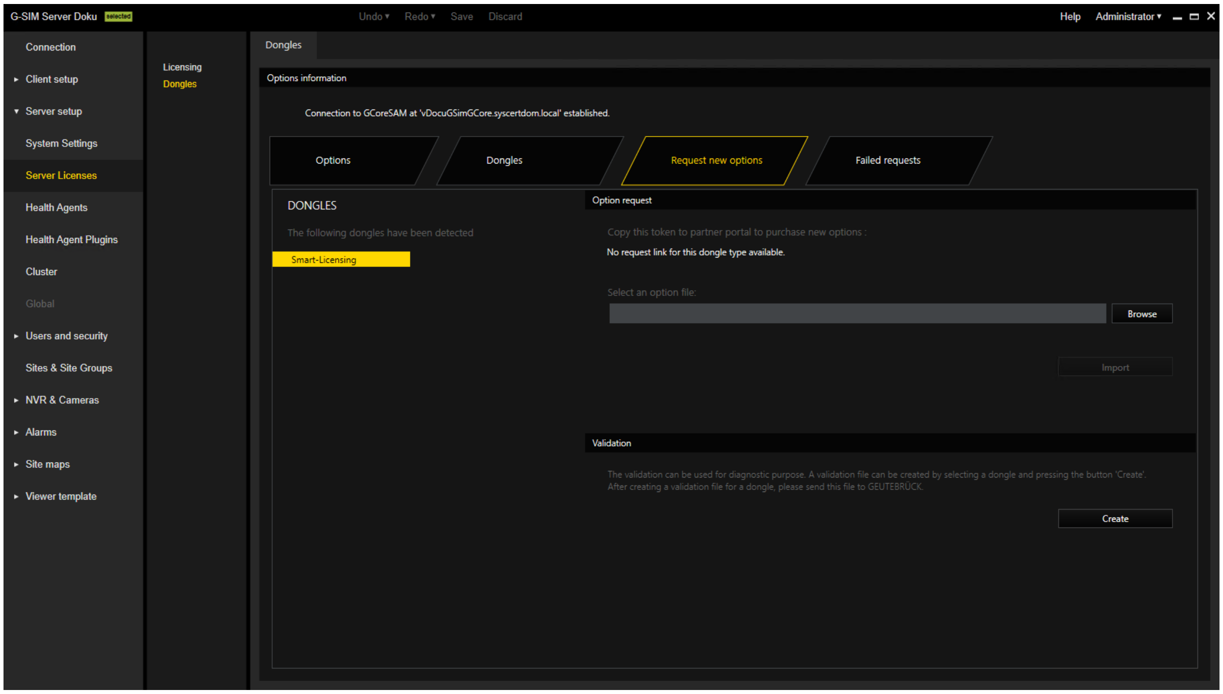
Type	Expire date	Count
^ GScope 11		
GCoreActivation	31/08/2024	1
GCoreInstance	Unlimited	1
GCoreViewConnect	Unlimited	10
GCoreBrowserConnect	Unlimited	5
GCoreCamConnect	Unlimited	100
GCoreDatabaseSizeTByte	Unlimited	450
GCoreAxisBodyCamIntegration	Unlimited	1
GCoreAxisBodyCamConnect	Unlimited	10
GCoreWebAPI	Unlimited	1
GCoreWebAPIMetadata	Unlimited	1
GCoreWebAPIChannelConnect	Unlimited	128
^ GSim 11		
GSIMActivation	22/09/2029	1
GSIMServerFailover	Unlimited	1
GSIMFailoverChannelConnect	Unlimited	3000

Request New Options

This tab is only for requesting Traditional Licensing options (see License Overview).

New options for Traditional Licensing can be requested via this dialog. When you click on the dongle to which the new options are to be assigned, a URL appears in the **Copy this token to partner portal to purchase new options** field. Right-clicking on this URL opens a menu where the URL can be copied, saved or opened in the default browser.

After you pass the URL to a browser, follow the instructions on the website.



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

The following dongles have been detected

Copy this token to partner portal to purchase new options :

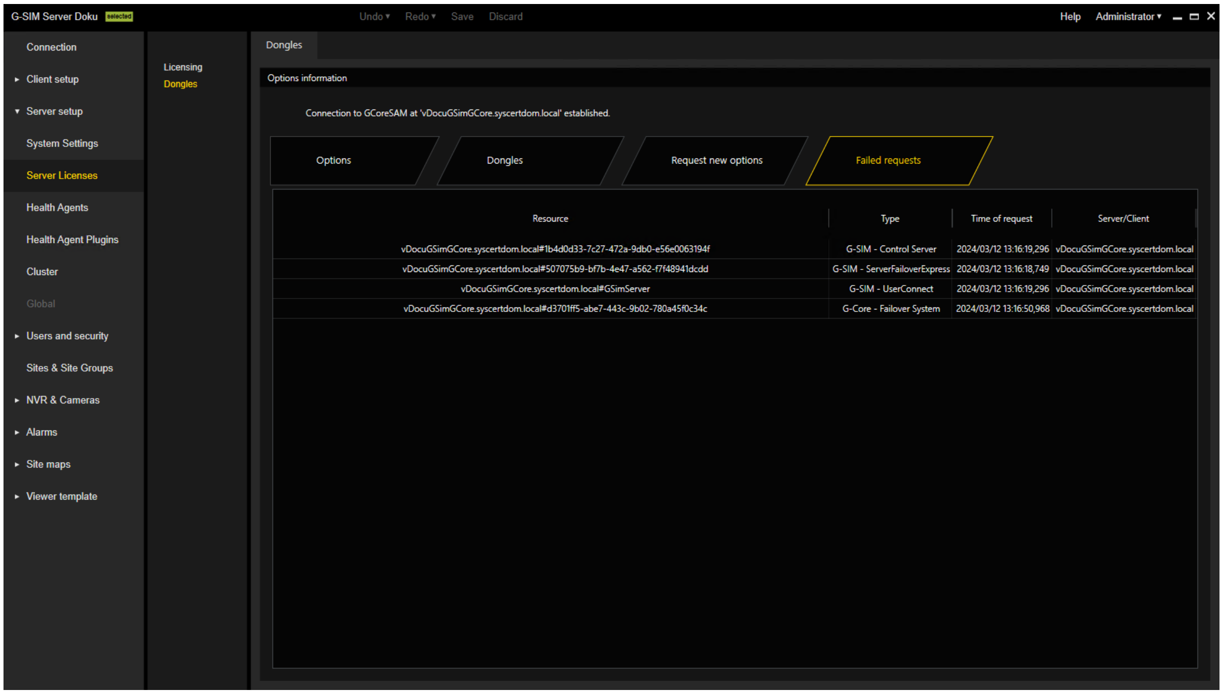
No request link for this dongle type available.

Select an option file:

The validation can be used for diagnostic purpose. A validation file can be created by selecting a dongle and pressing the button 'Create'. After creating a validation file for a dongle, please send this file to GEUTEBRÜCK.

Failed Requests

All failed requests of the software where no license is available are listed on this tab.



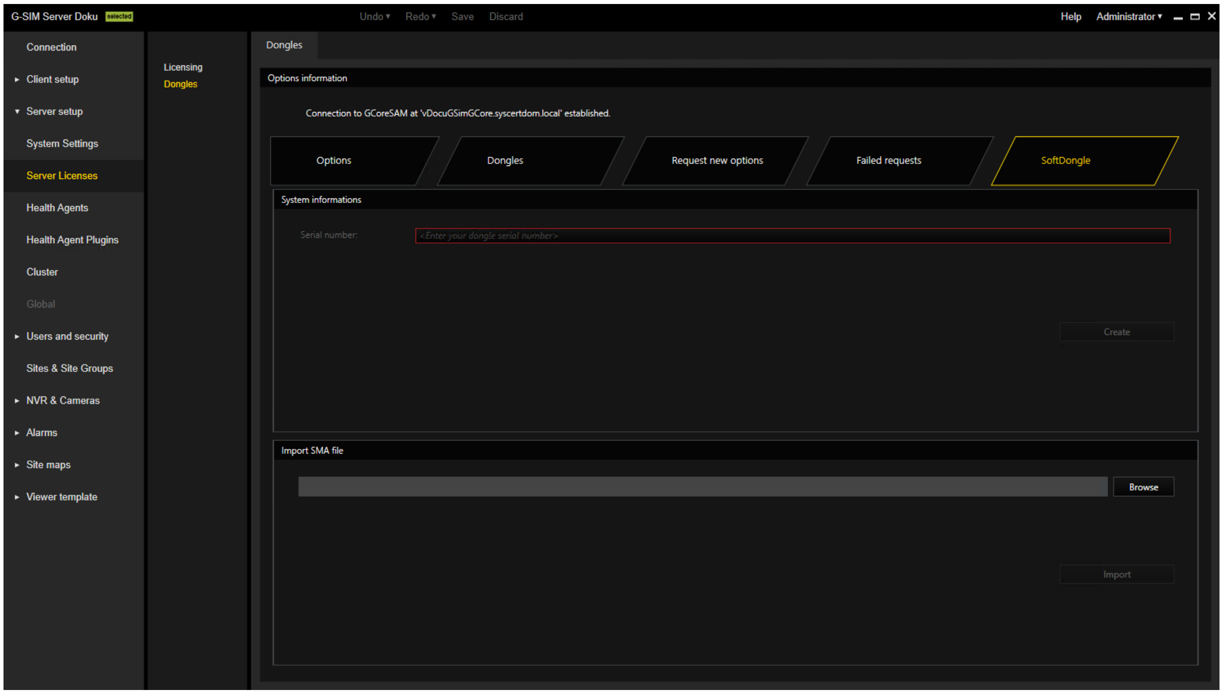
Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

Resource	Type	Time of request	Server/Client
vDocuGSimGCore.syscertdom.local#1b4d0d33-7c27-472a-9db0-e56e0063194f	G-SIM - Control Server	2024/03/12 13:16:19,296	vDocuGSimGCore.syscertdom.local
vDocuGSimGCore.syscertdom.local#507075b9-bf7b-4e47-a562-f7f48941dcdd	G-SIM - ServerFailoverExpress	2024/03/12 13:16:18,749	vDocuGSimGCore.syscertdom.local
vDocuGSimGCore.syscertdom.local#GSimServer	G-SIM - UserConnect	2024/03/12 13:16:19,296	vDocuGSimGCore.syscertdom.local
vDocuGSimGCore.syscertdom.local#d3701ff5-abe7-443c-9b02-780a45f0c34c	G-Core - Failover System	2024/03/12 13:16:50,968	vDocuGSimGCore.syscertdom.local

SoftDongle

In this tab you can request and import a softdongle. For information on how to activate a softdongle, see **Activate Softdongle**.

This tab is available only if you use the Traditional Licensing license model (see License Overview).



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

Activate Smart Licensing

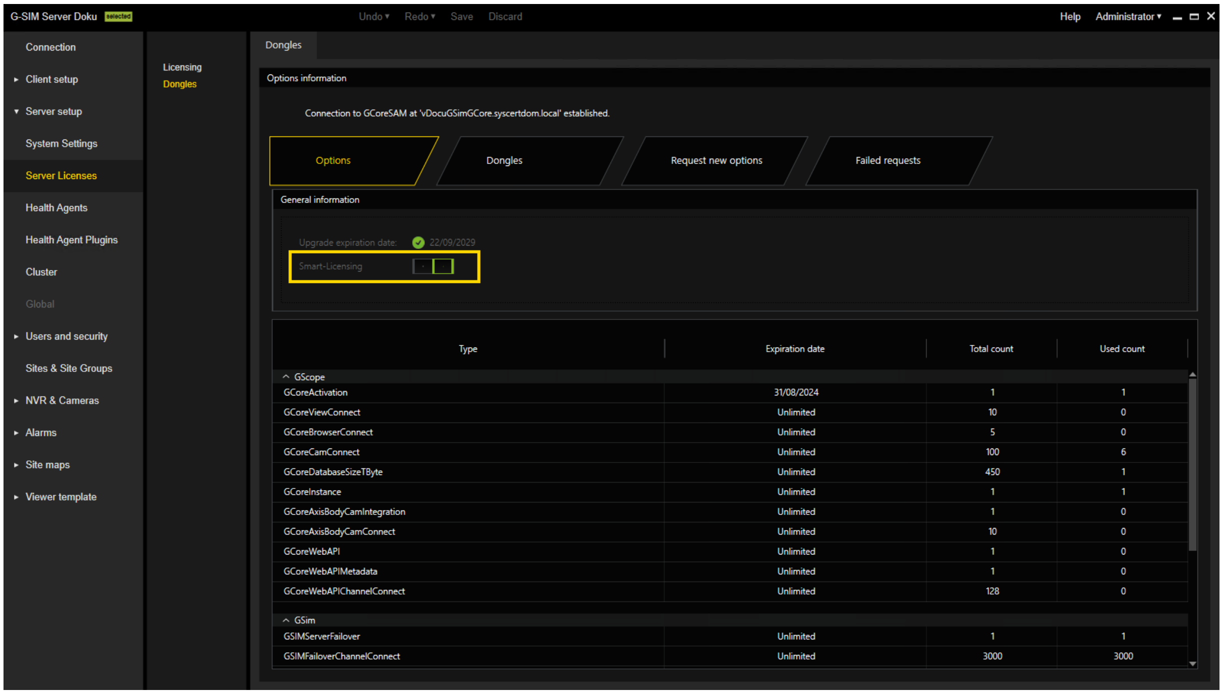
G-SIM 11 is required to use Smart Licensing. Make sure you have installed the appropriate Smart Licensing licenses in advance.

You can activate Smart Licensing in the Management Console by enabling the Smart-Licensing option in the Server Licenses menu. Confirm the dialog Are you sure you want to switch to Smart Licensing? with OK. The new licensing model is activated and the Smart Licensing licenses are used. The G-SIM server is restarted to complete the switch.

Deactivate the Smart-Licensing option to use the Traditional Licensing licenses.

It is possible to switch the licensing model at any time. Parallel operation of both licensing models on a single license server is not possible. G-SIM uses Smart Licensing as the default license model starting with version 11. For information on Geutebrück Software Licensing, see **here**.

For detailed information about the Server Licenses menu, see **Server Licenses**.



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

Upgrade expiration date: ✓ 22/09/2029

Smart-Licensing

Type	Expiration date	Total count	Used count
GScope			
GCoreActivation	31/08/2024	1	1
GCoreViewConnect	Unlimited	10	0
GCoreBrowserConnect	Unlimited	5	0
GCoreCamConnect	Unlimited	100	6
GCoreDatabaseSizeTByte	Unlimited	450	1
GCoreInstance	Unlimited	1	1
GCoreAxisBodyCamIntegration	Unlimited	1	0
GCoreAxisBodyCamConnect	Unlimited	10	0
GCoreWebAPI	Unlimited	1	0
GCoreWebAPIMetadata	Unlimited	1	0
GCoreWebAPIChannelConnect	Unlimited	128	0
GSim			
GSIMServerFailover	Unlimited	1	1
GSIMFailoverChannelConnect	Unlimited	3000	3000

Activate Softdongle

A softdongle is only required if you use the traditional licensing model (see License Overview**).**

Using a softdongle for your system environment requires a few steps. If it is a virtual machine, it must be in a domain. You also need a serial number. This serial number will be sent to you with the order confirmation if you have ordered a softdongle from your service partner.

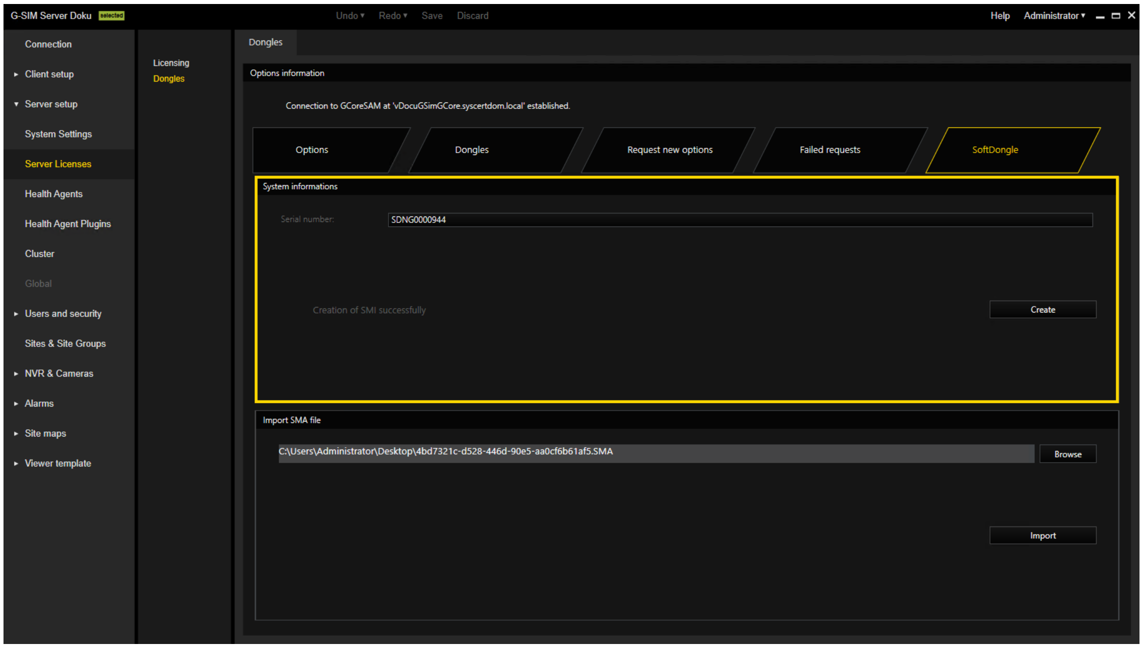
You can also activate your soft dongle in the G-Core SAM (see **Activate Softdongle**).

How to activate a softdongle in the Management Console:

On the Dongles page of the Server License menu, you can generate an SMI file containing all the necessary information about your system.

1. Click on the SoftDongle tab and enter the received serial number. Then click Create.

Enter the received serial number and make sure that it is correct, otherwise the request will be rejected and you will have to repeat the process.



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

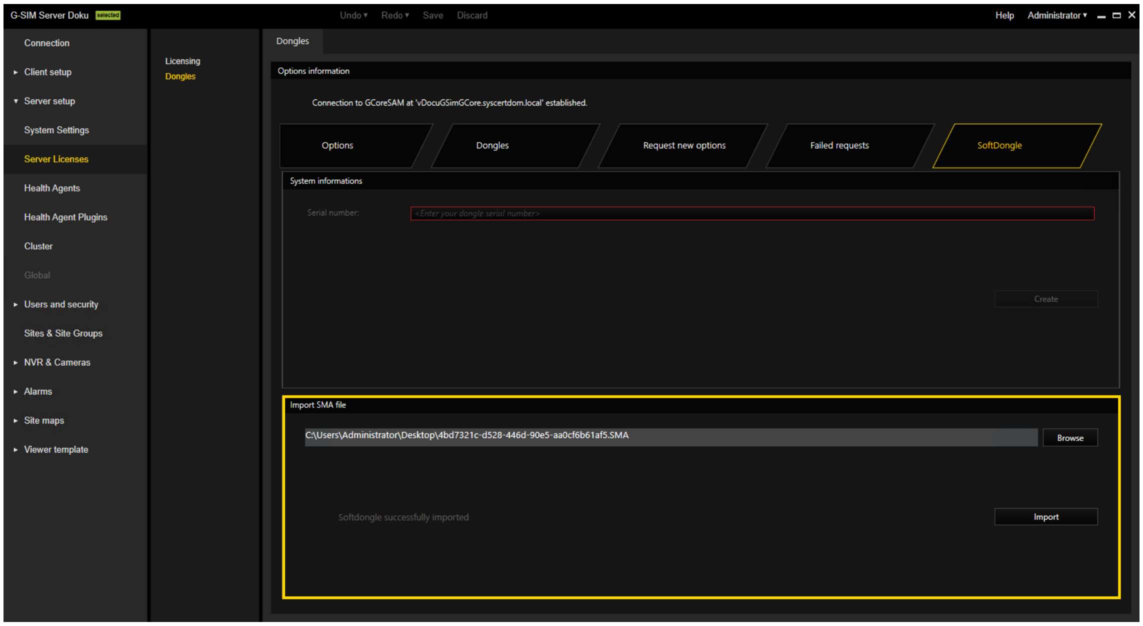
Serial number: SDNG0000944

Creation of SMI successfully

C:\Users\Administrator\Desktop\4bd7321c-d528-446d-90e5-aa0cf6b61af5.SMA

2. If the system requirements are met, you can download the dongle request file (.SMI) and send it to your service partner to create the softdongle file.

3. If you have received the dongle activation file (.SMA) from your service partner, you must import it. Click **Browse** to select the SMA file and then **Import** to import it.



Options information

Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

System informations

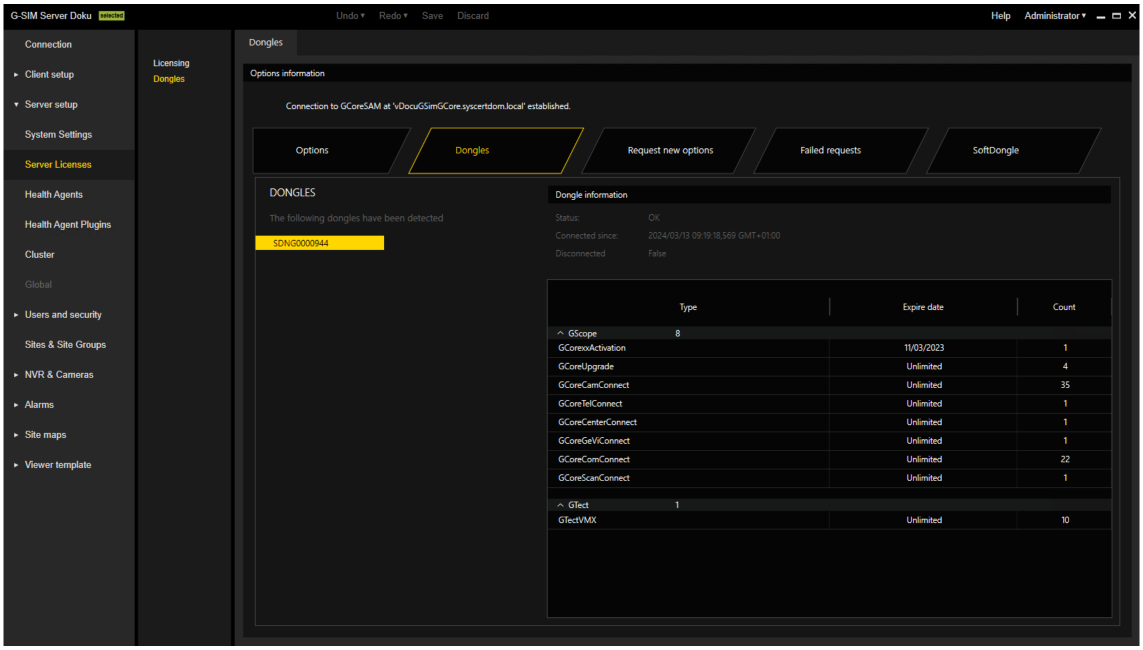
Serial number: <Enter your dongle serial number>

Import SMA file

C:\Users\Administrator\Desktop\4bd7321c-d528-446d-90e5-aa0cf6b61af5.SMA

Softdongle successfully imported

4. If the import and creation of the soft dongle was successful, the connection will be disconnected, and after reconnecting to the server, the new dongle with the license will be in the **Dongles** tab.



Options information

Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

DONGLES

The following dongles have been detected

SDNG0000944

Dongle information

Status: OK

Connected since: 2024/03/13 09:19:18,569 GMT+01:00

Disconnected False

Type		Expire date	Count
^ GScope	8		
GCorexxActivation		11/03/2023	1
GCoreUpgrade		Unlimited	4
GCoreCamConnect		Unlimited	35
GCoreTelConnect		Unlimited	1
GCoreCenterConnect		Unlimited	1
GCoreGeViConnect		Unlimited	1
GCoreComConnect		Unlimited	22
GCoreScanConnect		Unlimited	1
^ GTect	1		
GTectVMX		Unlimited	10

G-Core SAM

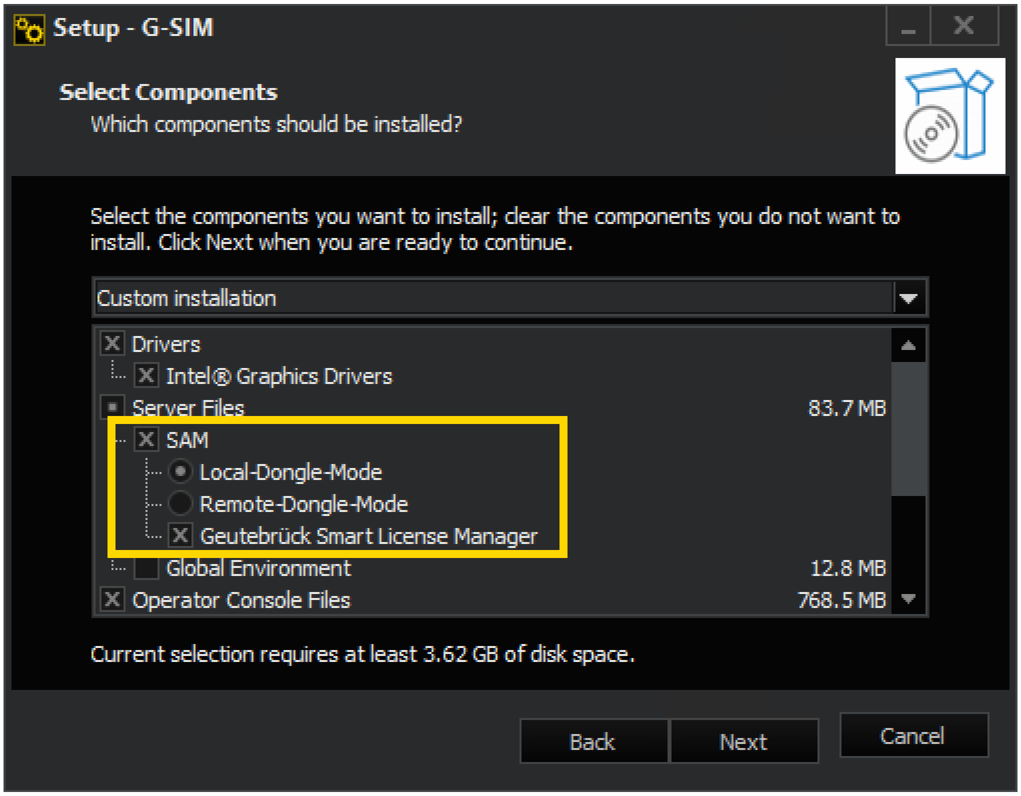
G-Core SAM is the central Software Asset Manager (SAM) that manages the licensing of all software packages of a distributed overall system with any number of VMS instances and software options. Depending on the operating mode, it manages all local dongles or remote connections to other G-Core SAM services.

Installation

Install G-Core SAM using the G-SIM installer.

1. Run the `G-SIM_Installer.exe` file.
2. Accept the **License Agreement** and click **Next**.
3. In the **Select Components** dialog window, select **SAM** and the required operation mode **Local-Dongle-Mode** or **Remote-Dongle-Mode** (see **Operation Modes**).

   ⚠ **IMPORTANT:** You can only use one G-SIM instance in Remote-Dongle-mode and only connect this instance to the central option server (Remote SAM).



Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom installation

☒ Drivers
☒ Intel® Graphics Drivers
■ Server Files 83.7 MB
☒ SAM
● Local-Dongle-Mode
○ Remote-Dongle-Mode
☒ Geutebrück Smart License Manager
□ Global Environment 12.8 MB
☒ Operator Console Files 768.5 MB

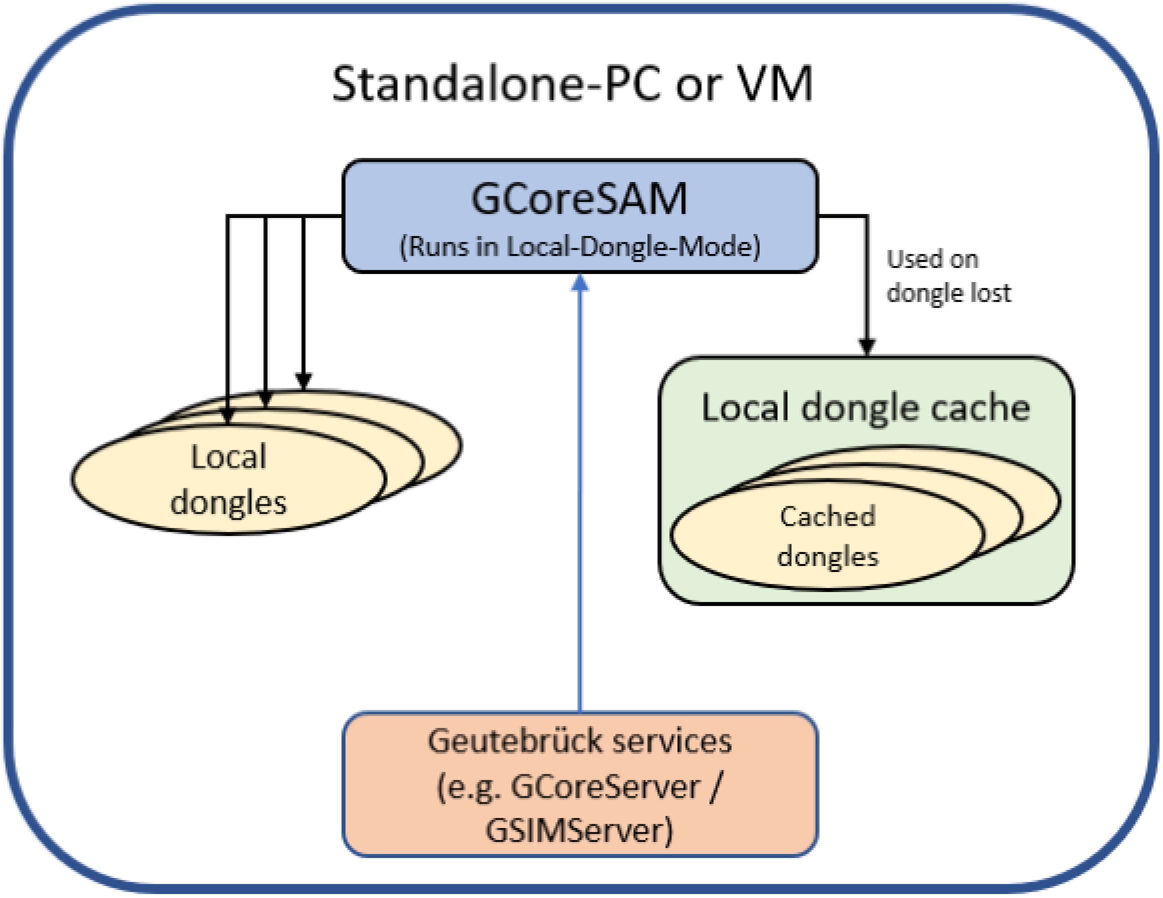
Current selection requires at least 3.62 GB of disk space.

4. Click **Next** and follow the further installation steps (see **Software Installation**).
5. In the **Ready to Install** dialog window click **Install**.
6. G-SIM and G-Core SAM are installed.
7. To complete the installation, the computer must be restarted.

Operation Modes

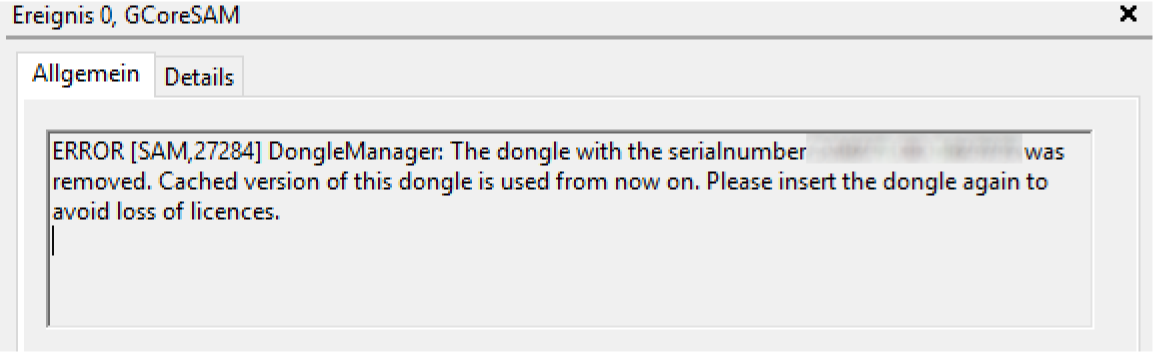
Local-Dongle-Mode

In the Local-Dongle-Mode, the G-Core SAM service connects to all local dongles, reads their information and processes all requests. Select this mode for a server installation with locally connected dongles or for a central options server installation.



Local Dongle Cache:

The local dongle cache is a backup mechanism that saves all local dongle information on the system and makes it available for up to 30 days in case a dongle fails. In case of an error, a windows event log entry is created.

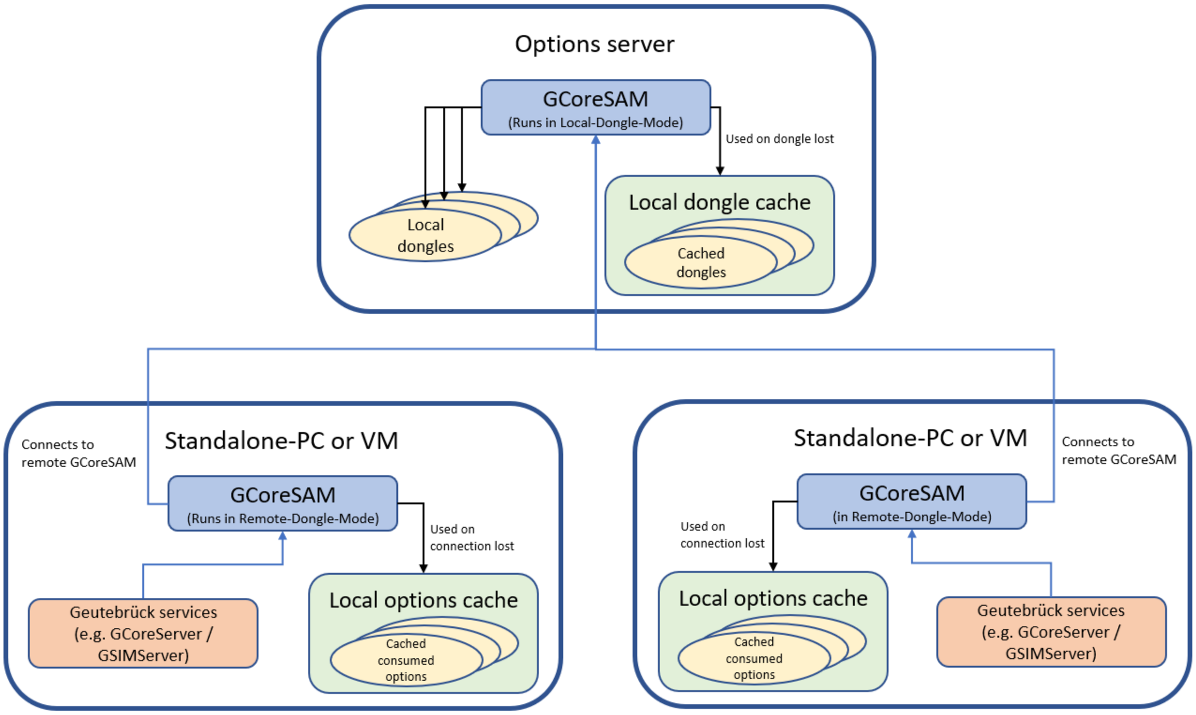


ERROR [SAM,27284] DongleManager: The dongle with the serialnumber [redacted] was removed. Cached version of this dongle is used from now on. Please insert the dongle again to avoid loss of licences.

Remote-Dongle-Mode

In the Remote-Dongle-Mode, the G-Core SAM service is connected to a remote SAM and forwards all requests and responses. Use this mode if you have a central option server. You must then select this mode for all remote systems connected to the central option server.

⚠ **IMPORTANT:** You can only use one G-SIM instance in Remote-Dongle-mode and only connect this instance to the central option server (Remote SAM).

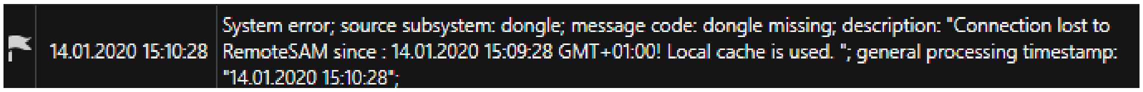


Local Options Cache:

The local options cache is a backup mechanism that saves all requested options of this system on the system and makes them available for up to 30 days if the connection to the remote SAM is lost.

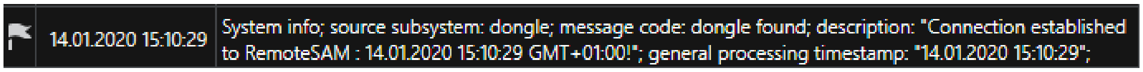
Two different actions are generated in the G-Core system depending on the current state of the system:

- SystemError: This action is triggered repeatedly when the connection to the remote SAM is lost and contains the last time the connection was established.



```
14.01.2020 15:10:28  System error; source subsystem: dongle; message code: dongle missing; description: "Connection lost to RemoteSAM since : 14.01.2020 15:09:28 GMT+01:00! Local cache is used. "; general processing timestamp: "14.01.2020 15:10:28";
```

- SystemInfo: This action is triggered when the connection to the remote SAM is established or reestablished.



```
14.01.2020 15:10:29  System info; source subsystem: dongle; message code: dongle found; description: "Connection established to RemoteSAM : 14.01.2020 15:10:29 GMT+01:00!"; general processing timestamp: "14.01.2020 15:10:29";
```

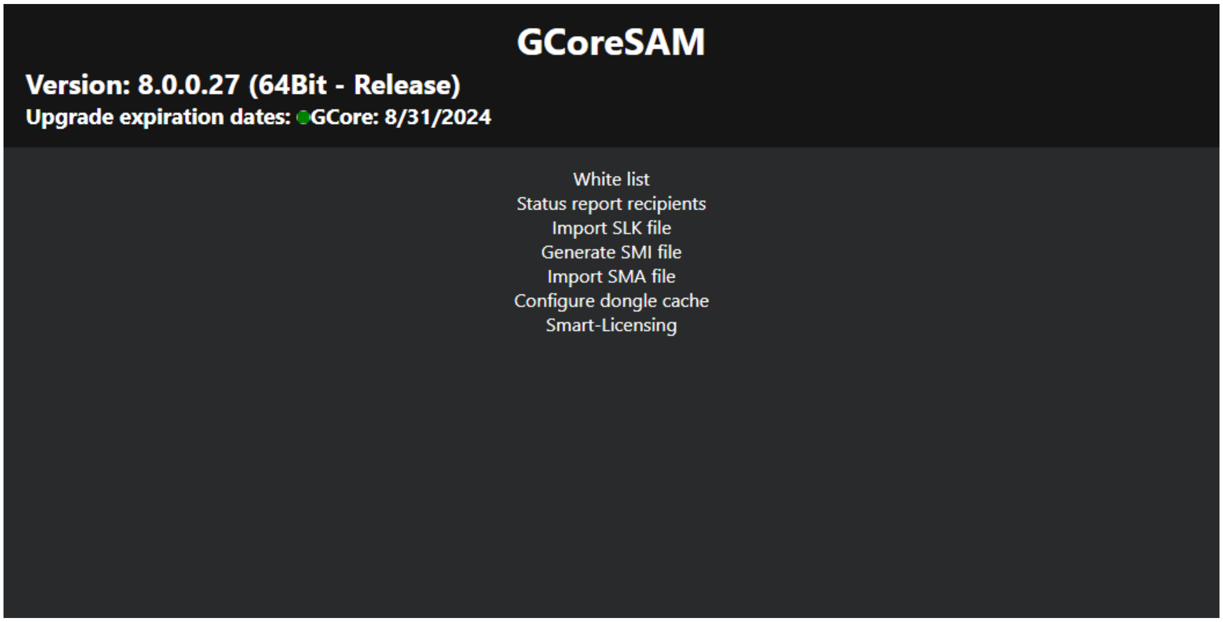
Configuration

Some configurations are made via the G-Core SAM web interface. All other configurations must be made in the configuration software of the installed software package. You can open the web interface via the URL: `http://localhost:13008/config`.

Access to this URL requires authentication via NTLM (NT LAN Manager), which is performed automatically in the background. The logged-in user must have administration rights, i.e. the user must be a member of the administration group of the server on which the central SAM service is running.

The web interface consists of the following menu items:

- **White List**
- **Status Report Recipients**
- **Import SLK File**
- **Generate SMI File**
- **Import SMA File**
- **Configure Dongle Cache**
- **Smart Licensing**



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: ●GCore: 8/31/2024

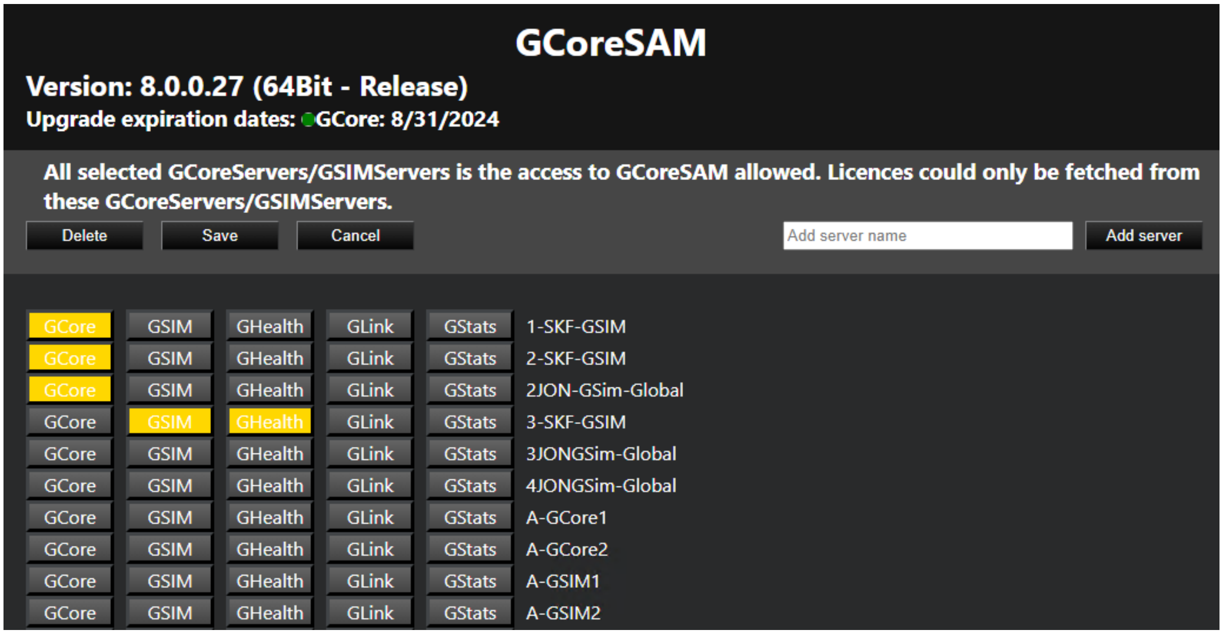
White List

The SAM service is equipped with a blocking filter that only allows localhost connections in its default configuration. Thus, it is not possible to connect to the SAM service from a remote computer without configuring the blocking filter.

If you use the Local-Dongle-Mode (see Operation Modes), i.e. a single system with a local dongle connected, you do not have to make any configurations.

In the White list menu, you can configure the blocking filters. The list contains all G-Core, G-SIM, G-Health, G-Stats and G-Link servers that are currently running on the network (and all that are included in the current blocking filter settings). The access to the individual SAM servers and software types (e.g. G-SIM or G-Core) can be disabled by clicking the corresponding buttons. The servers highlighted in orange are currently disabled.

If the desired server does not appear in the list, it you can add it by clicking the Add Server button. To do this, enter the network name of the associated computer in the text field.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: GCore: 8/31/2024

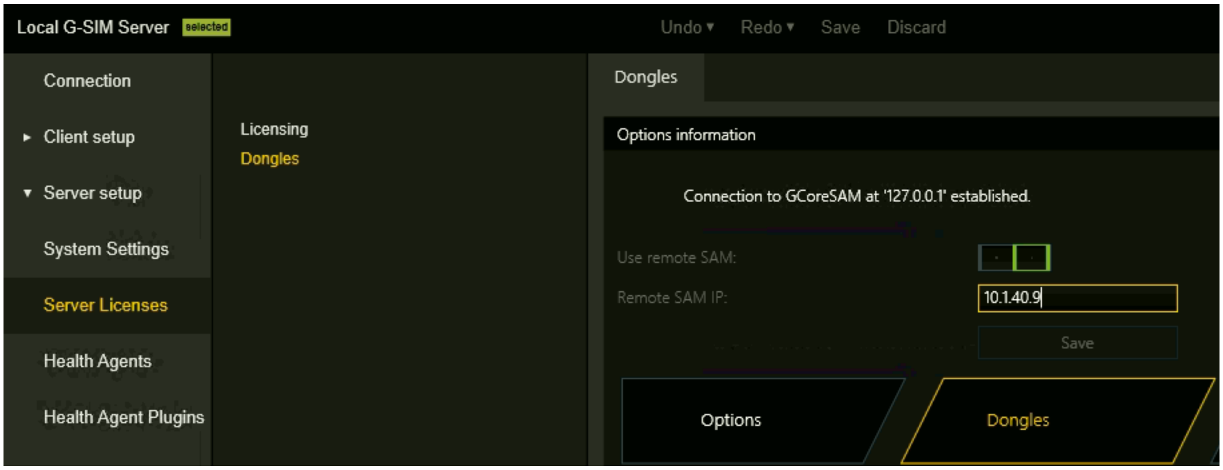
All selected GCoreServers/GSIMServers is the access to GCoreSAM allowed. Licences could only be fetched from these GCoreServers/GSIMServers.

GCore	GSIM	GHealth	GLink	GStats	1-SKF-GSIM
GCore	GSIM	GHealth	GLink	GStats	2-SKF-GSIM
GCore	GSIM	GHealth	GLink	GStats	2JON-GSim-Global
GCore	GSIM	GHealth	GLink	GStats	3-SKF-GSIM
GCore	GSIM	GHealth	GLink	GStats	3JONGSim-Global
GCore	GSIM	GHealth	GLink	GStats	4JONGSim-Global
GCore	GSIM	GHealth	GLink	GStats	A-GCore1
GCore	GSIM	GHealth	GLink	GStats	A-GCore2
GCore	GSIM	GHealth	GLink	GStats	A-GSIM1
GCore	GSIM	GHealth	GLink	GStats	A-GSIM2

If you use the Remote-Dongle-Mode (see **Operation Modes**), you have to configure the connection to the central SAM service in the Management Console in the **Server Licenses** menu after installing the software package.

Enable the **Use remote SAM** option to activate the use of the central SAM service and specify the IP address of the central SAM server in the **Remote SAM IP** text box. Then click the **Save** button.

> **IMPORTANT:** You can only use one G-SIM instance in Remote-Dongle-mode and only connect this instance to the central option server (Remote SAM).



Connection to GCoreSAM at '127.0.0.1' established.

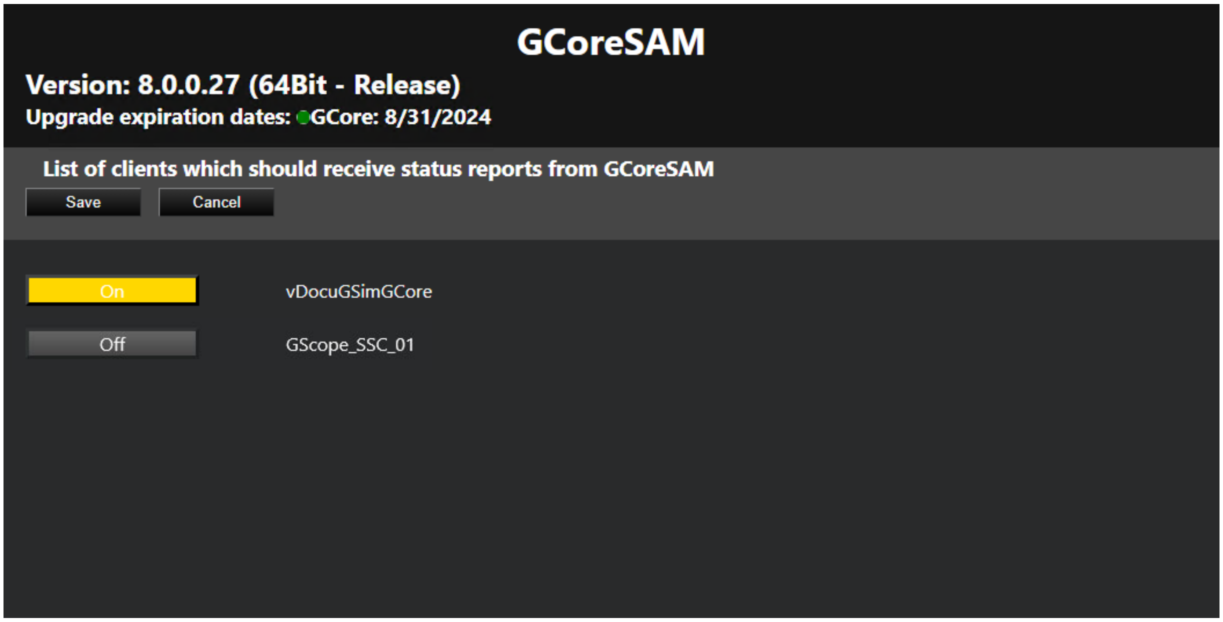
Use remote SAM: ☑

Remote SAM IP: 10.1.40.9

Status Report Recipients

The SAM service sends status messages to the connected G-Core client. These status reports provide notifications, for example, about newly detected or removed dongles, expired activation options, or other important events.

In the **Status report recipients** menu, you can select the computers to receive these reports. All clients on the selected computer will receive a status report.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: ● GCore: 8/31/2024

List of clients which should receive status reports from GCoreSAM

On	vDocuGSimGCore
Off	GScope_SSC_01

The connected G-Core server converts the status reports into actions. The following actions are sent:

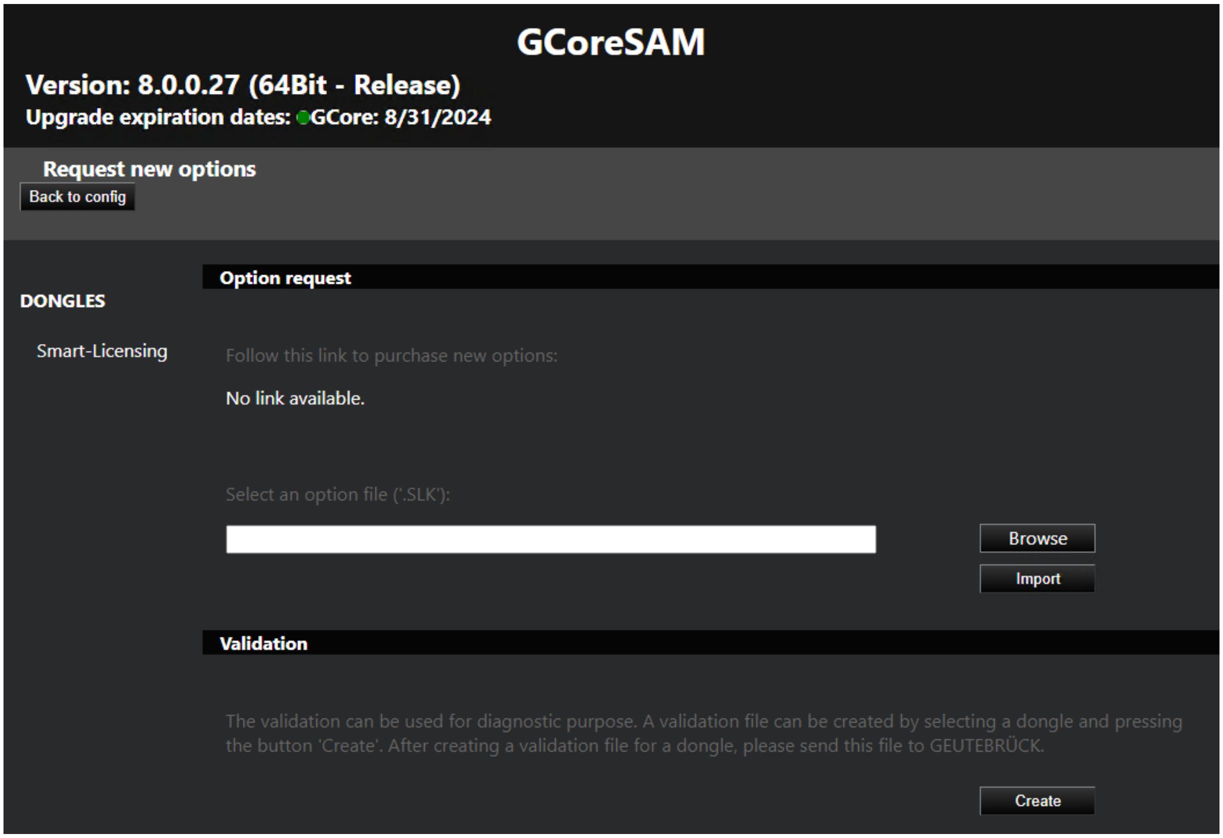
Event	Action	Parameter
Dongle removed	System Error	"source subsystem" = "dongle" "message code"= "Dongle missing"
Dongle added/recognized	SystemInfo	"source subsystem" = "dongle" "message code"="Dongle found"
Activation option lost	SystemError	"source subsystem"="dongle" "message code"="unlicensed" "description"="… activation has been expired."
New activation option	SystemInfo	"source subsystem"="dongle"

Event	Action	Parameter
recognized		"message code"="unlicensed" "description"="... activation expired at..."
Activation option expired	SystemInfo	"source subsytem"="dongle" "message code"="unlicensed"

Import SLK File

In the **Import SLK File** menu, you can import SLK files, export requested links and create GDV files.

This web interface for importing SLK files uses the same layout and functionality as the options dialog in the Management Console (see **Server Licenses**).



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: GCore: 8/31/2024

Request new options

Follow this link to purchase new options:

No link available.

Select an option file ('.SLK'):

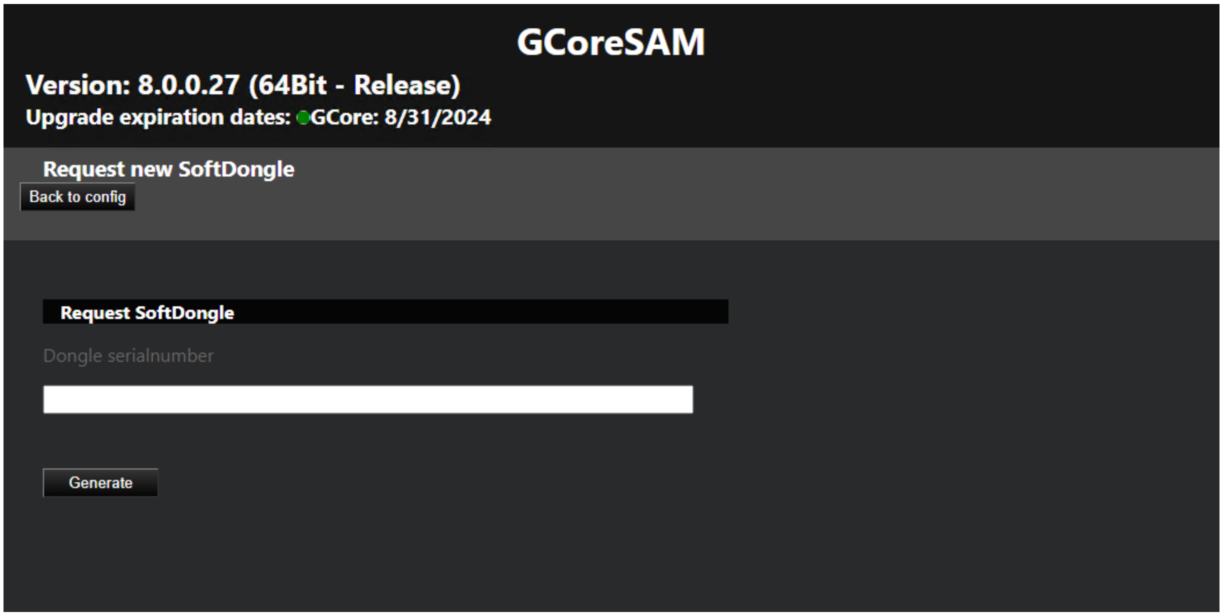
The validation can be used for diagnostic purpose. A validation file can be created by selecting a dongle and pressing the button 'Create'. After creating a validation file for a dongle, please send this file to GEUTEBRÜCK.

Generate SMI File

In the **Generate SMI file** menu, you can generate SMI files for soft dongle request files. The SMI file contains information about the system and is required when asking for a soft dongle for the system.

For virtual systems, it is required that the system is part of a domain to be able to generate an SMI file.

To generate an SMI file, enter the dongle serial number of the requested soft dongle and generate the file by clicking the **Generate** button. Download the generated SMI file to proceed with the soft dongle request.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: GCore: 8/31/2024

Request new SoftDongle

Request SoftDongle

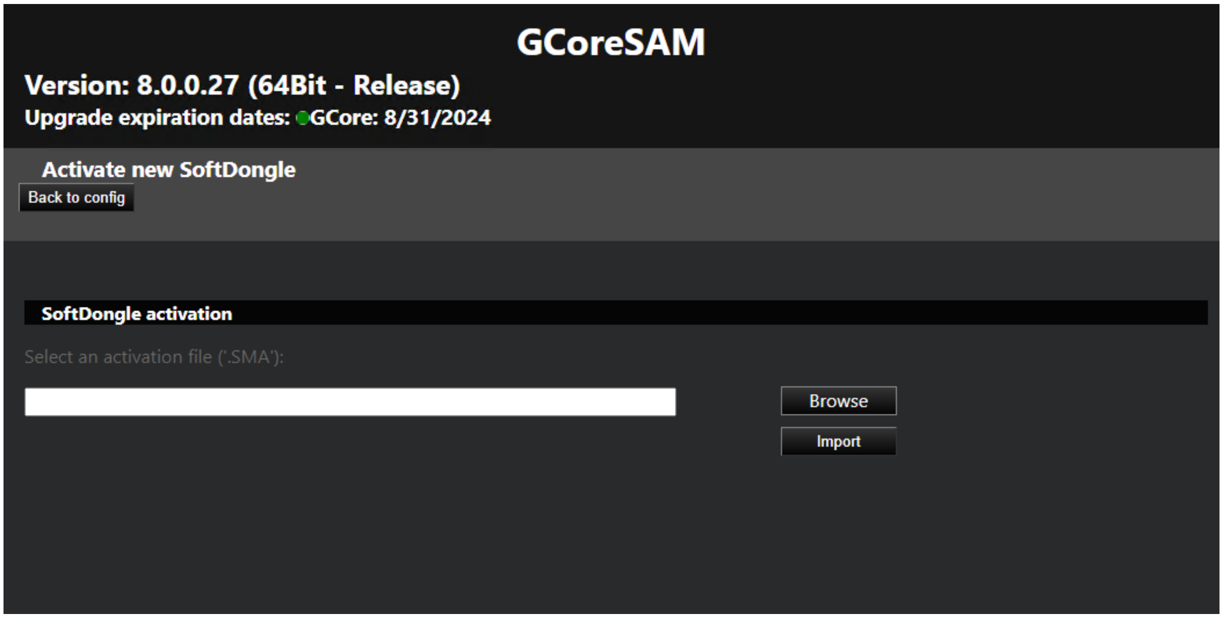
Dongle serialnumber

Import SMA File

In the **Import SMA file** menu, you can import the SMA soft dongle files and activate the received soft dongle in the system.

A soft dongle can only be activated on the system on which the request (SMI) was generated.

To activate a soft dongle, click **Browse** to select the SMA activation file and import the SMA activation file by clicking **Import**.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: ●GCore: 8/31/2024

Activate new SoftDongle

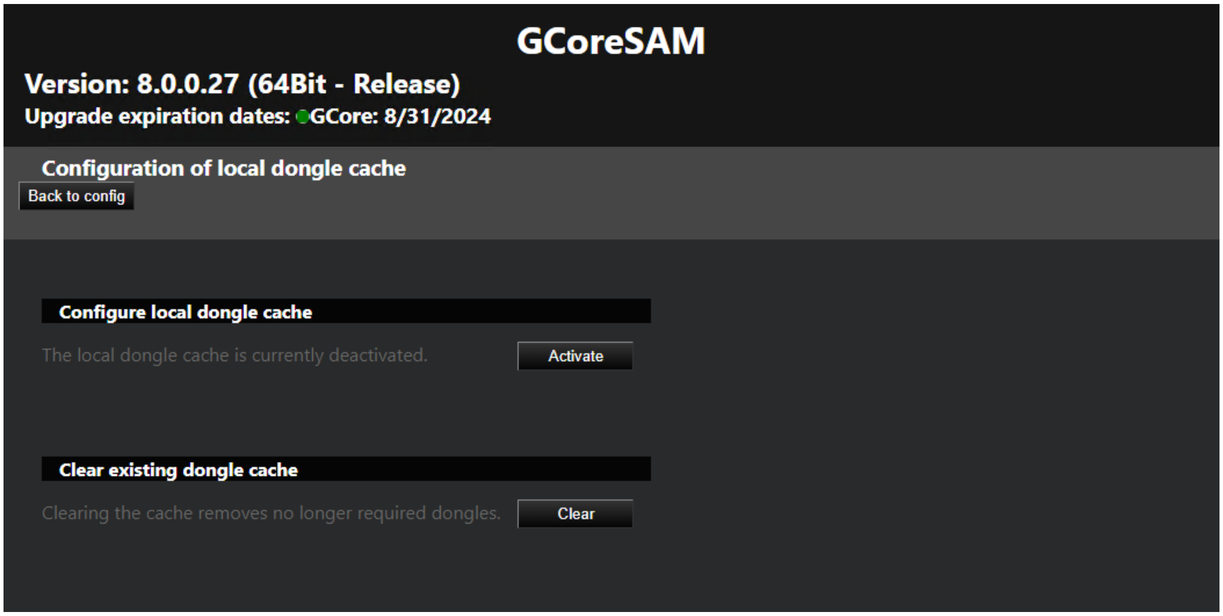
SoftDongle activation

Select an activation file ('.SMA'):

Configure Dongle Cache

In the **Configure local cache** menu, you can activate or deactivate the local dongle cache for your system. To do this, click **Activate** or **Deactivate** button.

The dongle cache is used for all currently connected dongles (physical and soft dongles). If one or more local dongles need to be changed and both the old dongle and its cache are obsolete, the dongle cache must be cleared. To do this, click the **Clear** button.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: ●GCore: 8/31/2024

Configuration of local dongle cache

Configure local dongle cache

The local dongle cache is currently deactivated.

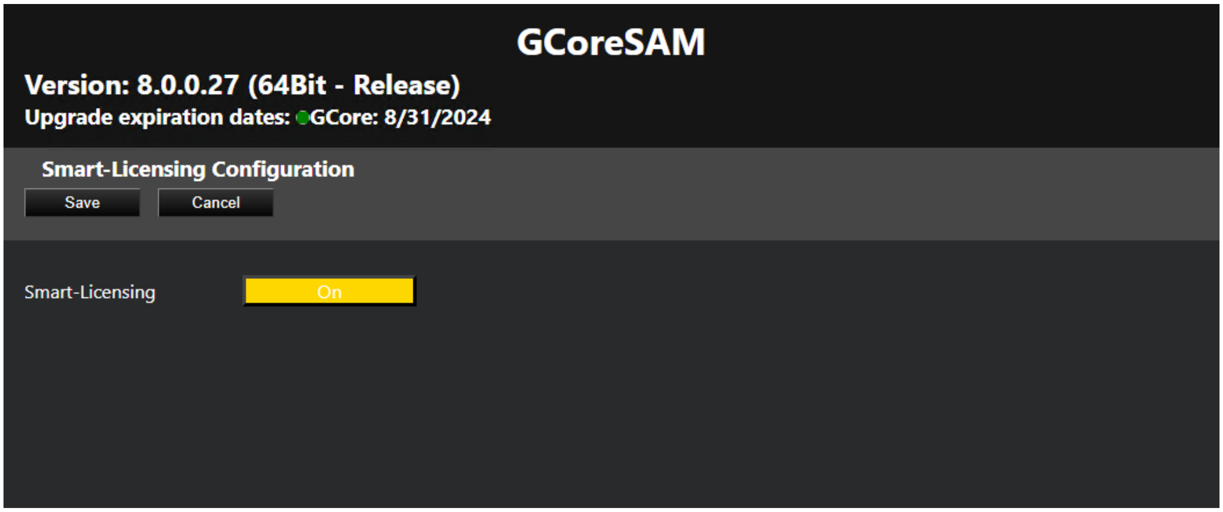
Clear existing dongle cache

Clearing the cache removes no longer required dongles.

Smart Licensing

In the **Smart Licensing** menu, you can activate Smart Licensing. To do this, set the Smart Licensing button to **On** and click **Save**. The new licensing model is activated and the Smart Licensing licenses are used. The G-Core SAM server is restarted to complete the switch.

Deactivate the **Smart-Licensing** option to use the Traditional Licensing licenses. It is possible to switch the licensing model at any time. Parallel operation of both licensing models on a single license server is not possible.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: ●GCore: 8/31/2024

Smart-Licensing Configuration

Smart-Licensing: On

Activate Softdongle

A soft dongle is only required if you use the traditional licensing model (see License Overview).

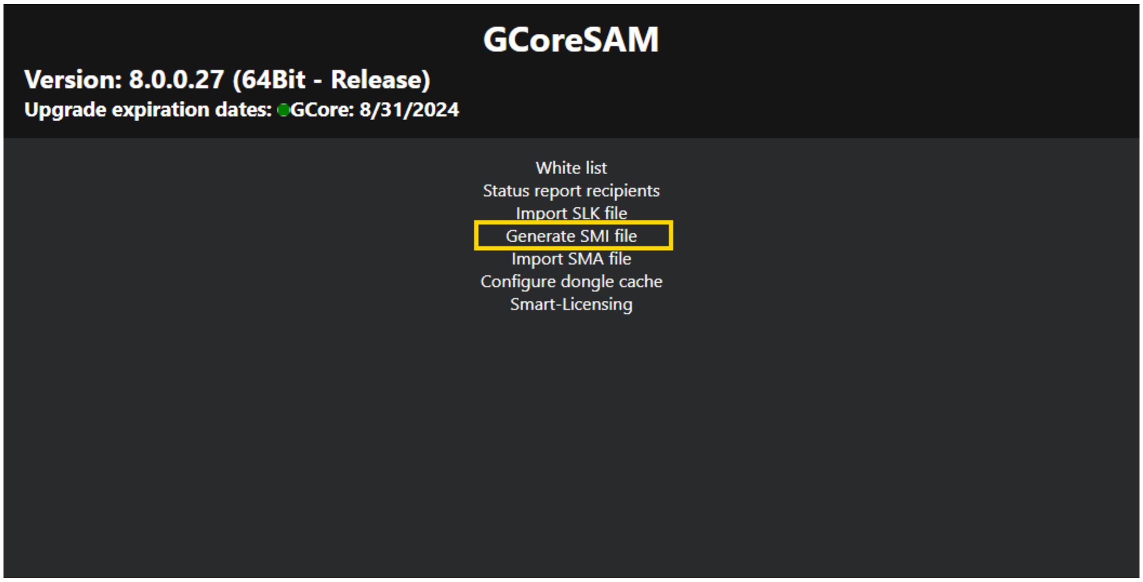
Using a softdongle for your system environment requires a few steps. If it is a virtual machine, it must be in a domain. You also need a serial number. This serial number will be sent to you with the order confirmation if you have ordered a softdongle from your service partner.

You can also activate your soft dongle in the Management Console (see **Activate Softdongle**).

How to activate a Softdongle in G-Core SAM:

In the G-Core SAM, you can generate an SMI file containing all the necessary information about your system.

1. Open the Generate SMI file menu.



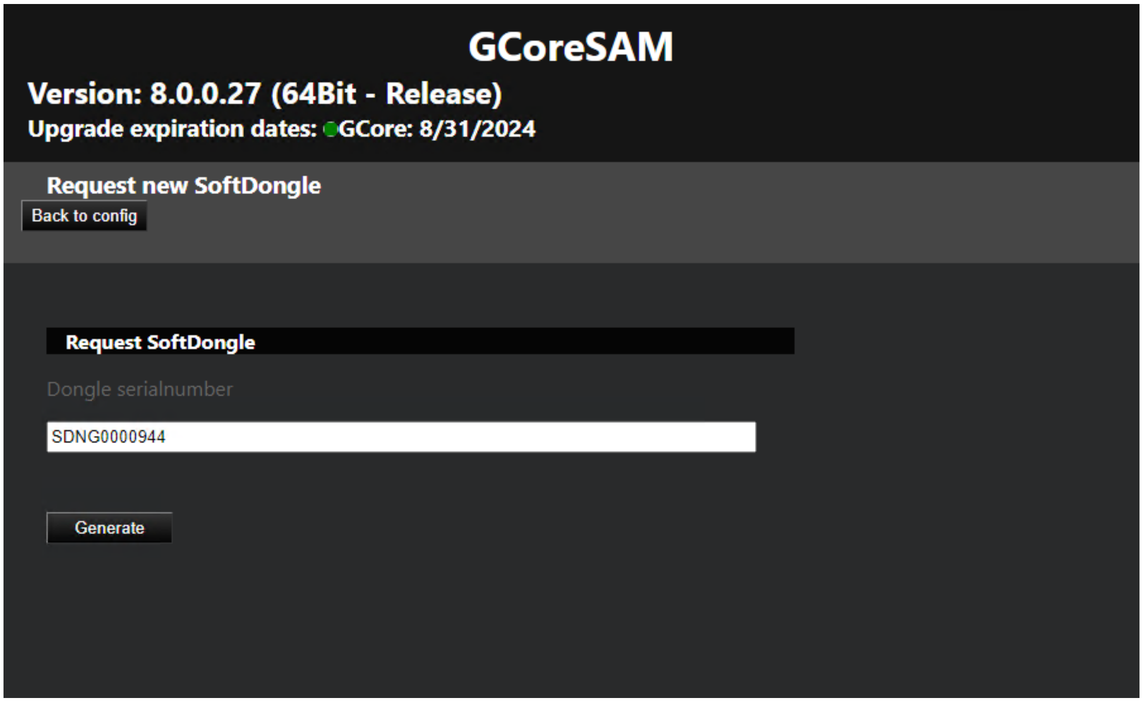
GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: GCore: 8/31/2024

2. Enter the received serial number. Then click Generate.

Enter the received serial number and make sure that it is correct, otherwise the request will be rejected and you will have to repeat the process.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: GCore: 8/31/2024

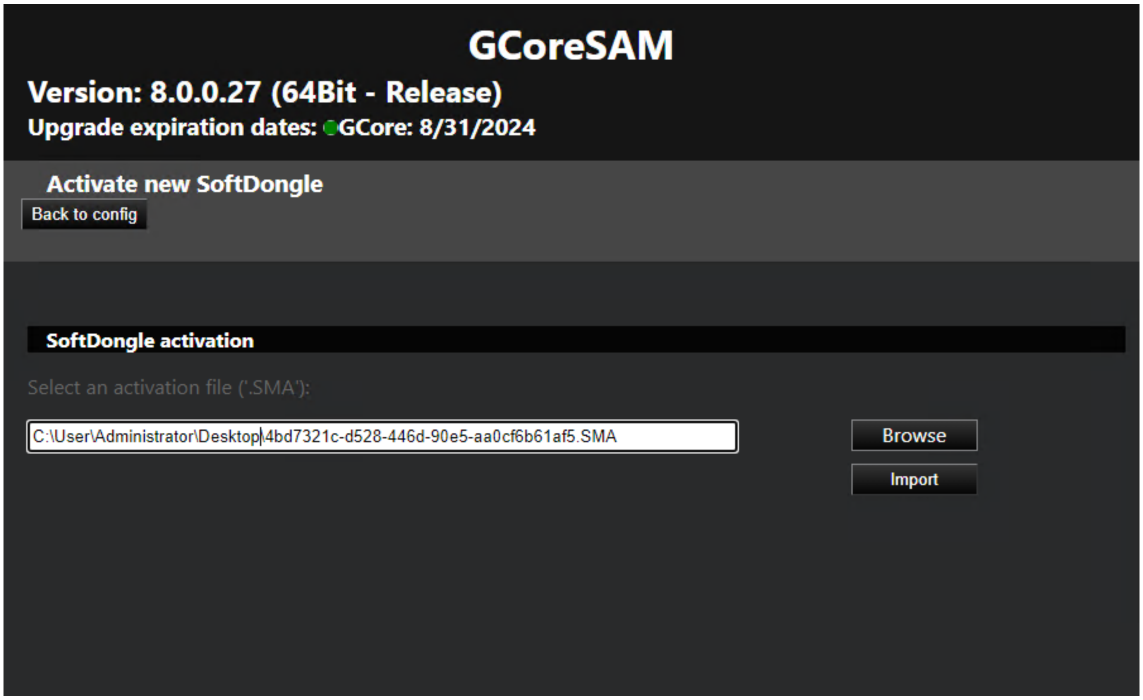
Request new SoftDongle

Request SoftDongle

Dongle serialnumber: SDNG0000944

3. If the system requirements are met, you can download the dongle request file (.SMI) and send it to your service partner to create the softdongle file.

4. If you have received the dongle activation file (.SMA) from your service partner, you must import it. Open the Import SMA file menu and click Browse to select the SMA file.



GCoreSAM

Version: 8.0.0.27 (64Bit - Release)

Upgrade expiration dates: ●GCore: 8/31/2024

Activate new SoftDongle

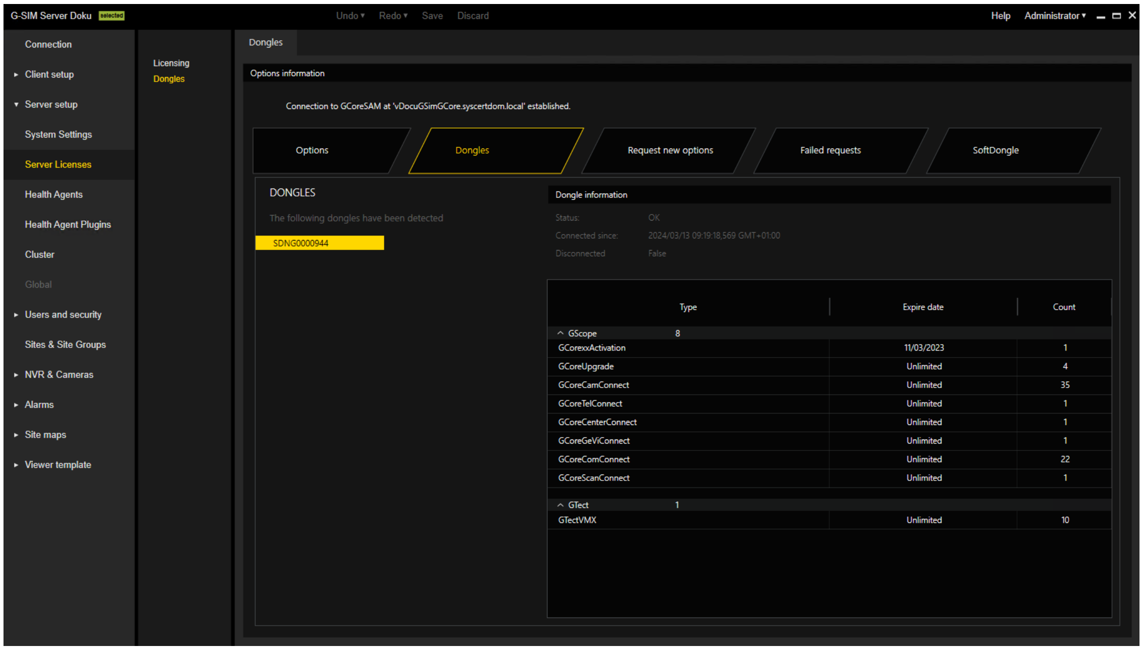
SoftDongle activation

Select an activation file ('.SMA'):

C:\User\Administrator\Desktop\4bd7321c-d528-446d-90e5-aa0cf6b61af5.SMA

5. Click Import to import it.

6. If the import and creation of the soft dongle was successful, the connection will be disconnected. After reconnecting to the server, the new dongle with the license will be in the Dongles tab in the Server Licenses menu of the Management Console (see **Server Licenses**).



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

The following dongles have been detected

SDNG0000944

Status: OK

Connected since: 2024/03/13 09:19:18,569 GMT+01:00

Disconnected False

Type	Expire date	Count
^ GScope 8		
GCorexxActivation	11/03/2023	1
GCoreUpgrade	Unlimited	4
GCoreCamConnect	Unlimited	35
GCoreTelConnect	Unlimited	1
GCoreCenterConnect	Unlimited	1
GCoreGeViConnect	Unlimited	1
GCoreComConnect	Unlimited	22
GCoreScanConnect	Unlimited	1
^ GTect 1		
GTectVMX	Unlimited	10

Glossary

Term	Description
Product Package	A product package contains basic functionalities plus a number of features.
Feature	A feature is a distinguishing feature within our software. A feature can activate one or more functionalities within the software. There are features which have a quantity specification (e.g. number of channels) and thus activate a certain number of functionalities.
Entitlement	With Smart Licensing, you receive an entitlement when you purchase your software. The Entitlement entitles you to use the software to the defined extent. The Entitlement ID is the identification number of the Entitlement.
License	Through the "Activation" process, you connect the Entitlement to a specific end device or server. During activation you will receive a license file that you can install in the software.
Activation Date	The date on which you activated the entitlement in the Geutebrück license portal. Your upgrade entitlement period

Term	Description
	starts with the activation date of a product package.
Option	Option or also license option (see Feature).
Locking Code	The locking code uniquely identifies your end device or server. The locking code links the entitlement to your server. Fingerprint is used synonymously here.
G-Core SAM	The central option service that manages all local dongles or remote connections to other G-Core SAM services, depending on the operating mode.
Physical Dongle	Either an internal MIO device or an externally connected USB G-Dongle.
Soft Dongle	A local file-based dongle container that is bound to the computer.
Local Dongle	A dongle (physical or soft) that is connected to the local computer.
Remote Dongle	A dongle (physical or soft) that is connected to a remote computer.
Smart Licensing Dongle	When Smart Licensing is activated, the G-Core SAM uses the Smart Licensing dongle internally.
Local Dongle Mode	The G-Core SAM service connects to all local dongles, reads their information and processes all requests.
Remote Dongle Mode	The G-Core SAM service connects to a remote SAM and forwards all requests and responses. This is used when you have a central option server.
Local Dongle Cache	A 30-day cache for all local dongles to prevent system failures if a local dongle is lost or defective.
Local Options Cache	A 30-day cache for all consumed options when a G-Core SAM is running in remote dongle mode to prevent system failure when the connection to the remote SAM is lost.
Central License Server	A server system that provides its available options or licenses to remote systems.

Term	Description
Geutebrück License Portal	Through the License Portal, your purchased software products and options are delivered in the form of "Entitlements". You can manage your purchased software products and options by activating them and assigning them to customers. In addition, the portal provides a complete overview and management capabilities during the life cycle of the software products and options.
File extensions	There are following file extensions: • ***.lic**: License file (Smart Licensing license) • ***slk**: License file (Traditional Licensing license) • ***.smi**: Softdongle request file • ***.sma**: Softdongle activation file

Upgrade

Before You Start

Requirements

- Before upgrading, create a backup of all SQL databases and G-SIM setup and verify that the backup restore works properly.
- Check the required system requirements.
- Check the validity of your upgrade license.

Upgrading the G-SIM Components

To upgrade the various G-SIM components, simply run the installer. You do not need to stop any services before starting the installer. Stopping and restarting services is done automatically.

If special steps are required for certain upgrades, corresponding instructions are published in the release notes as well as the upgrade guides.

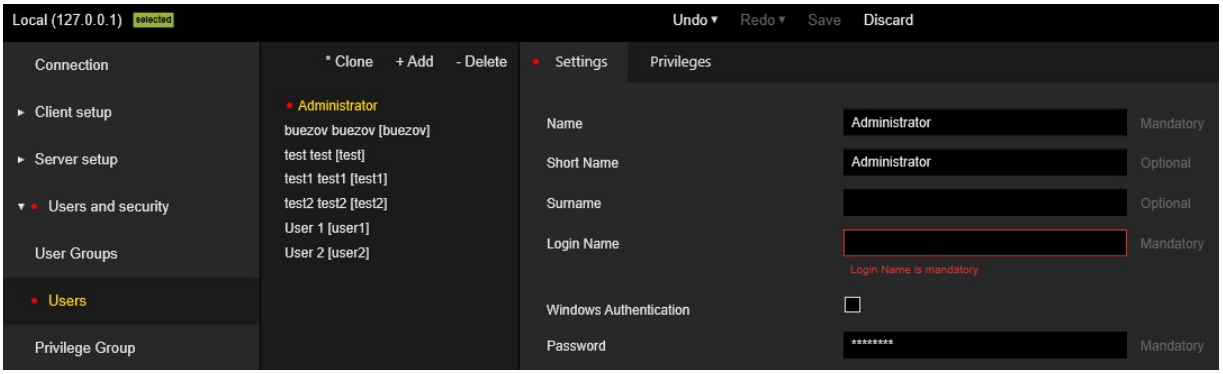
There is the Updater Service, which is available up to G-SIM version 8. If required, you can request the documentation for the Updater Service from Support.

Import of Existing Setups

Starting with version 9.2, G-SIM has a new management console with improved structuring and new features. When upgrading from an older version to version 9.2 or newer, the existing setups are transferred to the new system.

The management console performs the validation of the setup. Any validation errors that occur are highlighted in the ManCon and can be corrected manually.

- Settings with validation errors cannot be saved.
- Main menu items and their configurable elements that have validation errors are marked with red dots.
- Controls that contain invalid settings are marked with red frames and notes with error descriptions.
- Tabs that contain controls with invalid settings are marked with red dots.



• Administrator
buezov buezov [buezov]
test test [test]
test1 test1 [test1]
test2 test2 [test2]
User 1 [user1]
User 2 [user2]

Name	Administrator	Mandatory
Short Name	Administrator	Optional
Surname		Optional
Login Name	Login Name is mandatory	Mandatory
Windows Authentication	□	
Password	********	Mandatory

Restoring or Upgrading Maps

The G-SIM server stores maps in a cache local to each Operator Console. The Operator Console and Management Console program request each map in question the first time it is used. This is to conserve both bandwidth and to save on time, as the maps can be very large. Each time a map is accessed, the Operator Console (or Management Console) checks with server what the latest version is and updates it if required.

The maps are updated automatically. However, it may be necessary to fill the local cache for maps. This is especially important if you are performing an installation on a remote OpCon and you want to avoid transferring data over a slow or expensive network.

In your original server installation folder, there is a folder called Maps. Copy the Maps folder from the server to `C:\ProgramData\G-SIM\OpCon` on the computer where the Operator Console is installed to populate the local Maps cache.

Installation Modes

G-SIM has several installation modes that have security-related changes to help you upgrade your system:

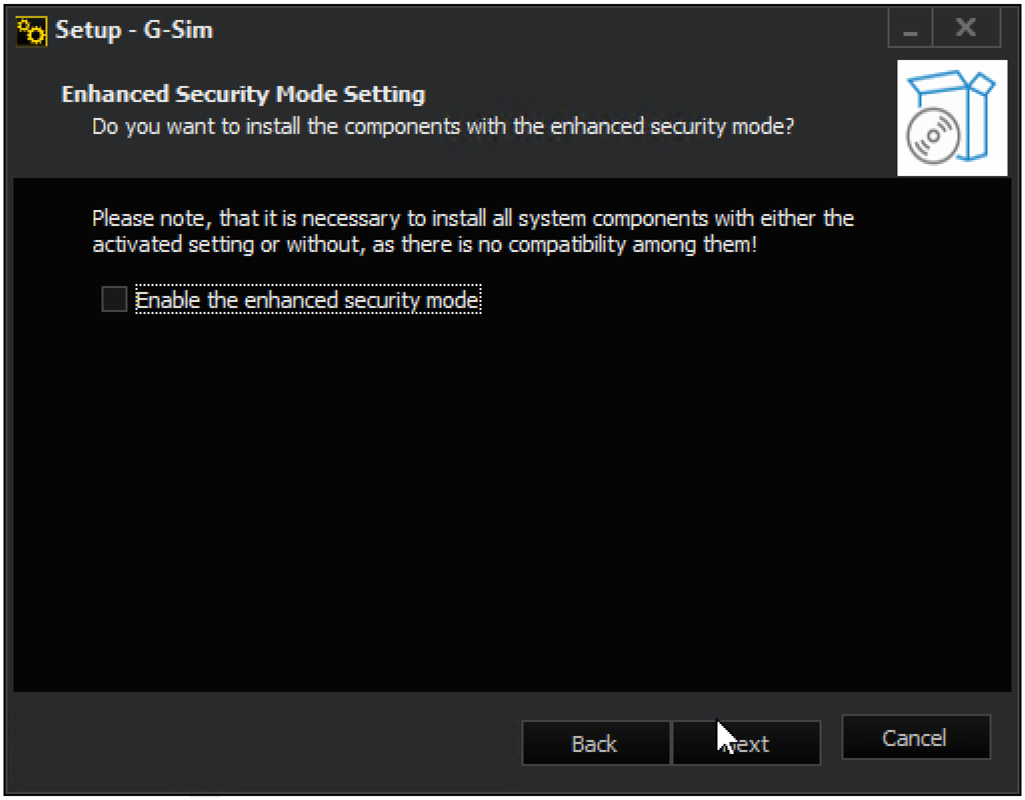
- **Enhanced Security Mode**
- **Compatibility Mode**
- **Encryption Settings**

This section provides explanations and important notes about each installation mode. For more detailed information on which mode is available and selectable for which upgrade, refer to the respective upgrade guide.

Enhanced Security Mode

The enhanced security mode is available from system version G-SIM 9.4.

This enhanced security mode has higher encryption and general security standards and enables support for systems running under FIPS (Federal Information Processing Standard).



Enhanced Security Mode Setting

Do you want to install the components with the enhanced security mode?

Please note, that it is necessary to install all system components with either the activated setting or without, as there is no compatibility among them!

□ Enable the enhanced security mode

Enable Enhanced Security Mode for G-SIM

The enhanced security mode is optional. You can enable the mode for G-SIM by selecting the **Enable the enhanced security mode** option.

Your G-SIM system will continue to run normally in enhanced security mode, and your settings in G-SIM will not be changed.

If the FIPS mode is already enabled in the Windows settings of your respective system, the mode is automatically enabled for G-SIM. The **Enable the enhanced security mode** option is then selected by default and grayed out.

Enable FIPS Mode in the Operating System

To enable the FIPS mode in the operating system, you can enable the Windows Group Policy setting.

To use the Group Policy setting, do the following:

1. Open the Group Policy Editor.
2. Navigate to `Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options`.
3. Enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting.

Compatibility Towards Older Versions

The compatibility towards older system versions is no longer possible in the FIPS mode. If you have enabled the enhanced security mode, you must upgrade all system components (server and clients) to version 9.4, with the enhanced security mode enabled.

> ⚠ **IMPORTANT:** All system components must be installed in the enhanced security mode, otherwise no connection between the server and the clients (Operator or Management Console, Health Agent) is possible.

ⓘ **If you enabled the enhanced security mode when installing the clients, no compatibility mode is available for this installation because it does not support the enhanced security mode.**

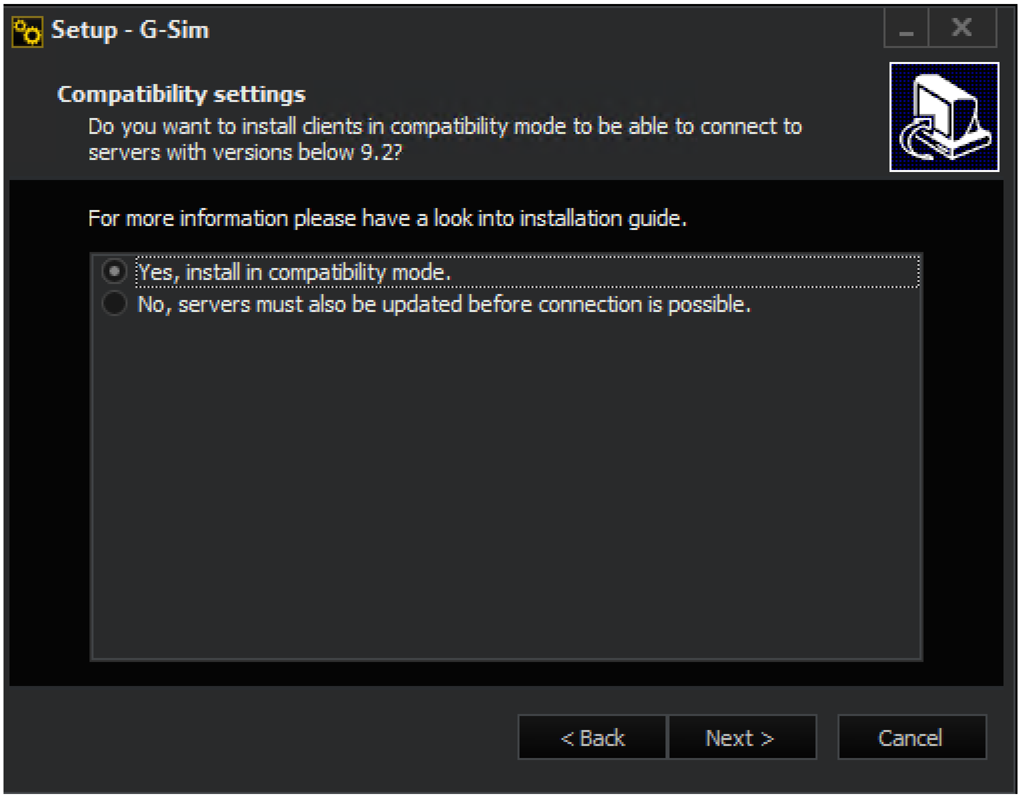
Compatibility Mode

The compatibility mode is available from system version 9.2.

G-SIM 9.2 and newer versions have security-related changes that result in incompatibility with older G-SIM versions (version below 9.2). Clients (Operator or Management Console, Health Agent) in version 9.2 or newer can no longer connect to older G-SIM servers.

The compatibility mode allows clients in version 9.x to connect to G-SIM servers in a version older than 9.2. Thus, the mode ensures that an upgrade of the system to version 9.2 or newer can be performed during operation without interruptions.

ⓘ **If you enabled the enhanced security mode during installation, no compatibility mode is available for this installation because it does not support the enhanced security mode.**



Setup - G-Sim

Compatibility settings

Do you want to install clients in compatibility mode to be able to connect to servers with versions below 9.2?

For more information please have a look into installation guide.

● Yes, install in compatibility mode.

○ No, servers must also be updated before connection is possible.

Upgrade in Compatibility Mode

If you are installing clients (Operator or Management Console, Health Agent) and are using an older server (version below 9.2), select the **Yes, install in compatibility mode** option.

To upgrade in compatibility mode, follow these steps:

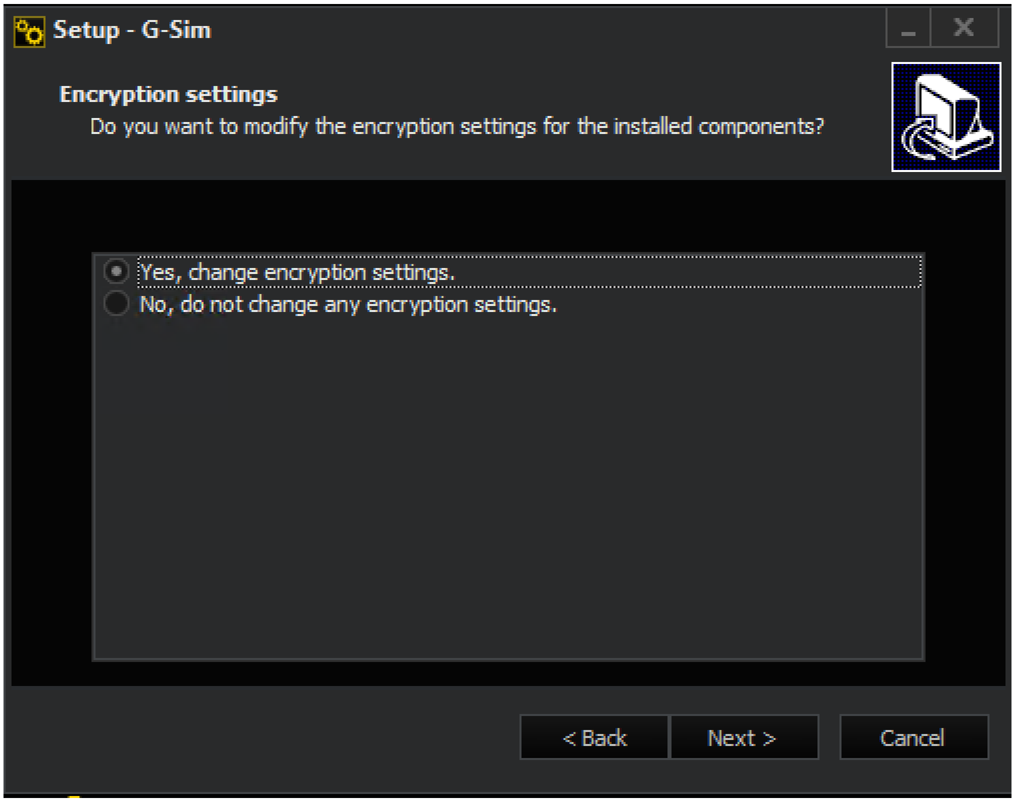
1. Install all clients that you want to work without interruption during the upgrade with compatibility mode enabled, selecting the **Yes, install in compatibility mode** option.
2. Upgrade all G-SIM servers.
3. After the server upgrade, upgrade all clients again without compatibility mode.

> **IMPORTANT:** The compatibility mode is intended only for transition during system upgrade to avoid interruption of service. The clients should not run in compatibility mode for an extended period of time or permanently. Therefore, upgrade all clients again without compatibility mode after the server upgrade.

Encryption Settings

G-SIM has security-related encryption settings.

When you upgrade an existing version of G-SIM, the installer can automatically change the encryption settings.



Encryption settings

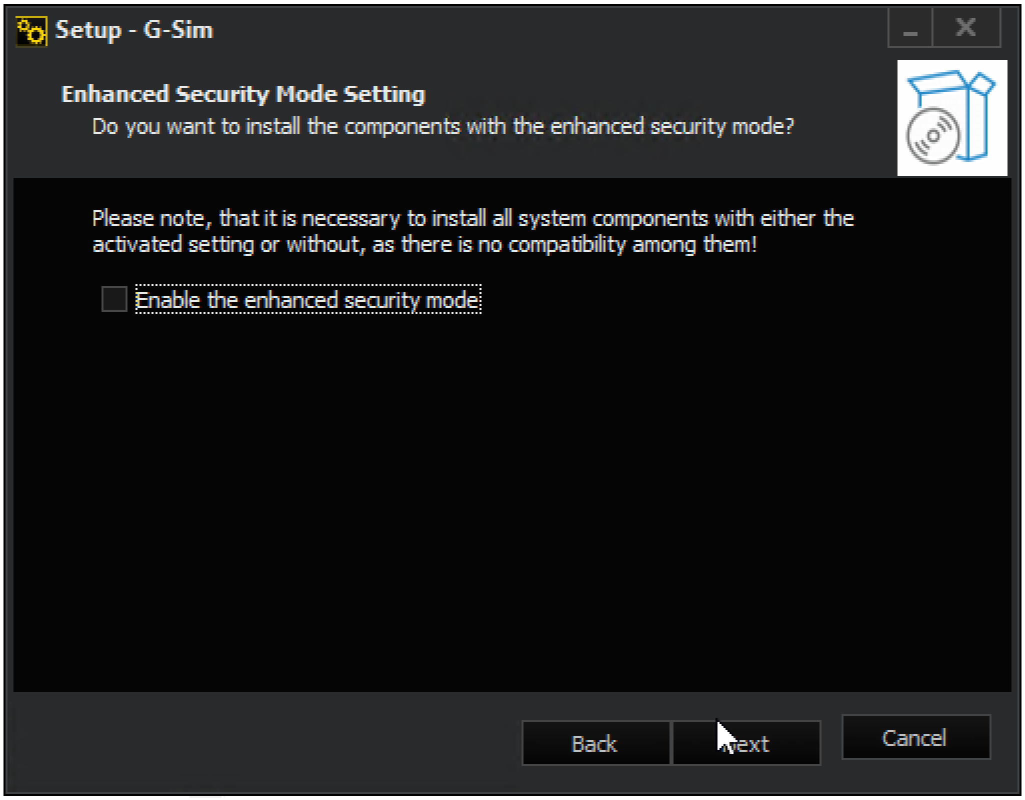
Do you want to modify the encryption settings for the installed components?

● Yes, change encryption settings.

○ No, do not change any encryption settings.

To change the encryption settings automatically, select the **Yes, change encryption settings** option.

If you selected this option, you can enable encryption for all system components of G-SIM (Server, Operator Console, Management Console and Health Agent) in the following step.



Setup - G-Sim

Enhanced Security Mode Setting

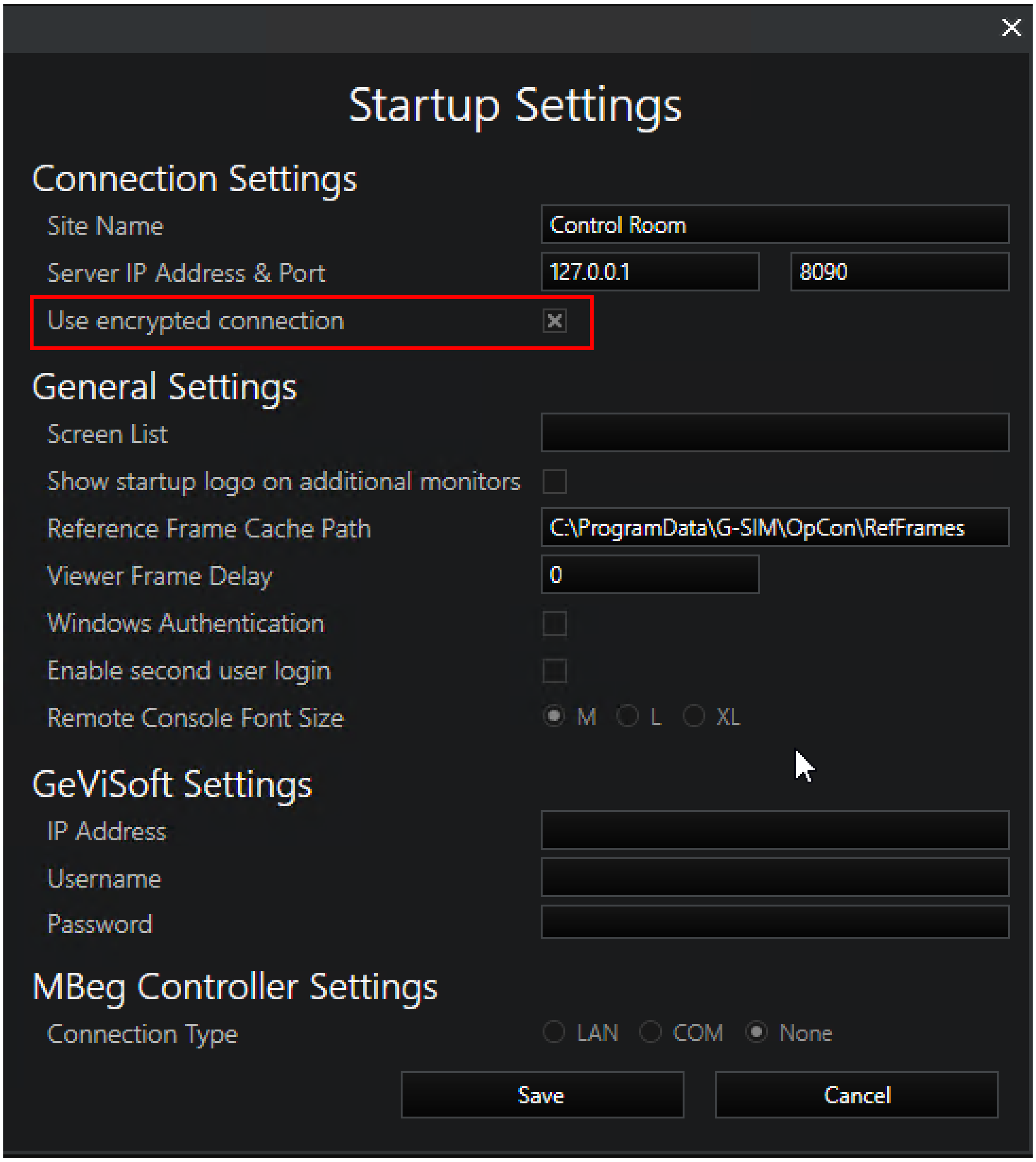
Do you want to install the components with the enhanced security mode?

Please note, that it is necessary to install all system components with either the activated setting or without, as there is no compatibility among them!

□ Enable the enhanced security mode

If you select the **Disable encryption for these components** option, the encryption of the G-SIM system components will be disabled, and the installation will be performed without encryption.

If the encryption of the system components is activated, the option **Use encrypted connection** must be activated in the startup settings of the OpCon for a connection of the G-SIM servers and the operator console.



Startup Settings

Connection Settings

Site Name: Control Room

Server IP Address & Port: 127.0.0.1 8090

Use encrypted connection ☒

General Settings

Screen List:

Show startup logo on additional monitors □

Reference Frame Cache Path: C:\ProgramData\G-SIM\OpCon\RefFrames

Viewer Frame Delay: 0

Windows Authentication □

Enable second user login □

Remote Console Font Size ● M ○ L ○ XL

GeViSoft Settings

IP Address:

Username:

Password:

MBeg Controller Settings

Connection Type ○ LAN ○ COM ● None

Upgrade 8.4 or older to 9.4

Before You Start

In system versions 8.4 or older, G-SIM uses MD5 hashing to encrypt user passwords. Due to improved technologies, with G-SIM version 8.5 the storage of passwords has been changed and a new hashing technology has been introduced.

⚠ **IMPORTANT:** This updated password encryption requires changing the user passwords in OpCon when upgrading the G-SIM version. A compatibility mode is available for the management console to log in and change the password.

To perform an error-free upgrade of a G-SIM version 8.4 or older to version 9.4, you must first upgrade to version 8.5, 8.7 or 8.8 and change the passwords of all users. In the next step, you can then upgrade to version 9.4.

ⓘ **It is recommended to upgrade to system version 8.8 first.**

How to Proceed

You can perform the upgrade in one step as a full installation or as a single OpCon and Server installation.

1. Start the installer for version G-SIM 8.5, 8.7 or 8.8.
2. In the **Select Components** dialog window, choose between the following installation:
   - **Full Installation** to upgrade the entire system, i.e. G-SIM Server and selected clients, in one step.
   - **Operator installation** and **Server installation** separately.
3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Start the installer.

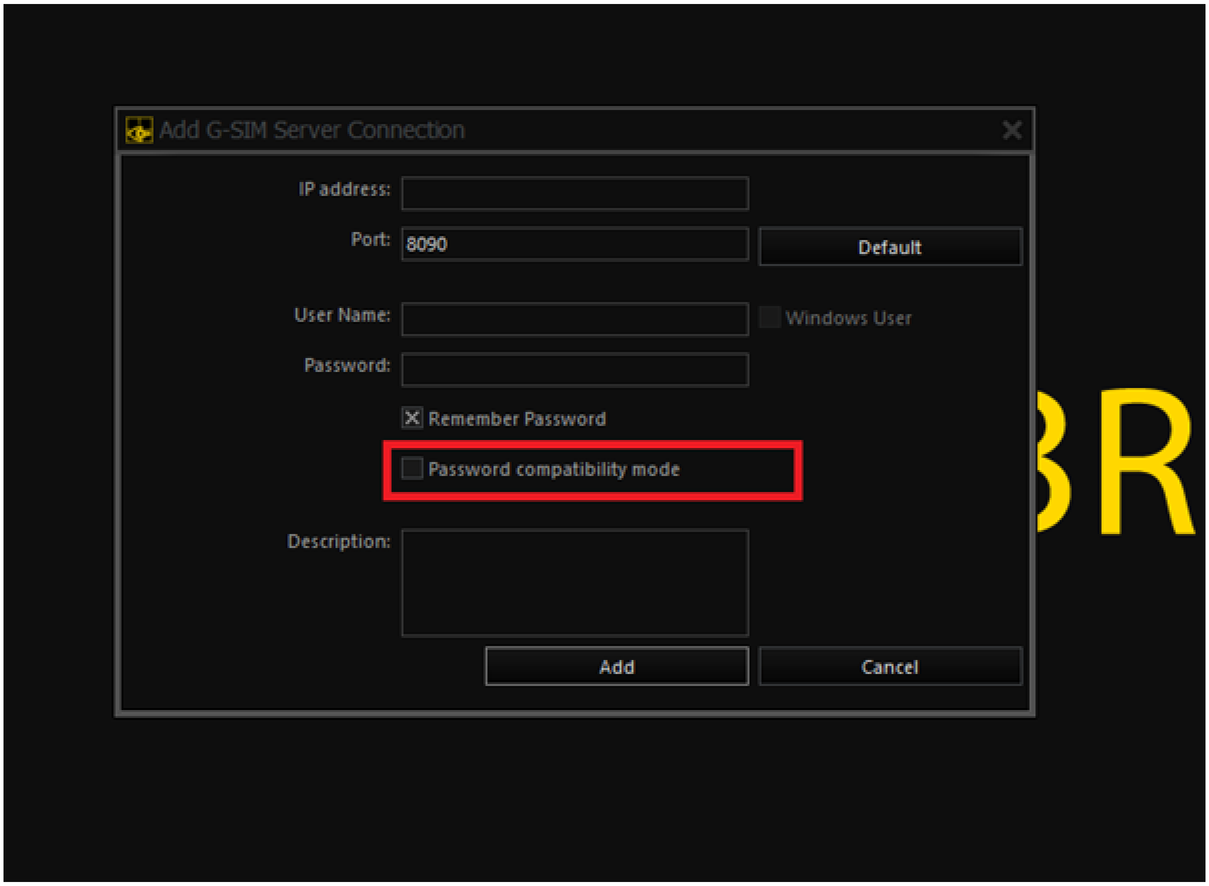
   → The G-SIM server and the selected clients are upgraded.
5. Activate the **Password compatibility mode** and change the passwords of all users in the OpCon. Refer to **Password Hashing**.
6. Perform the upgrade to version 9.4. See **Upgrade 8.8 or older to 9.4**.

Password Hashing

Management Console

The **Password compatibility mode** checkbox can be used for backward compatibility purposes.

In G-SIM version 8.x, you can enable this mode in the **Add G-SIM Server Connection** dialog window:



Add G-SIM Server Connection

IP address:

Port: 8090

User Name:

☐ Windows User

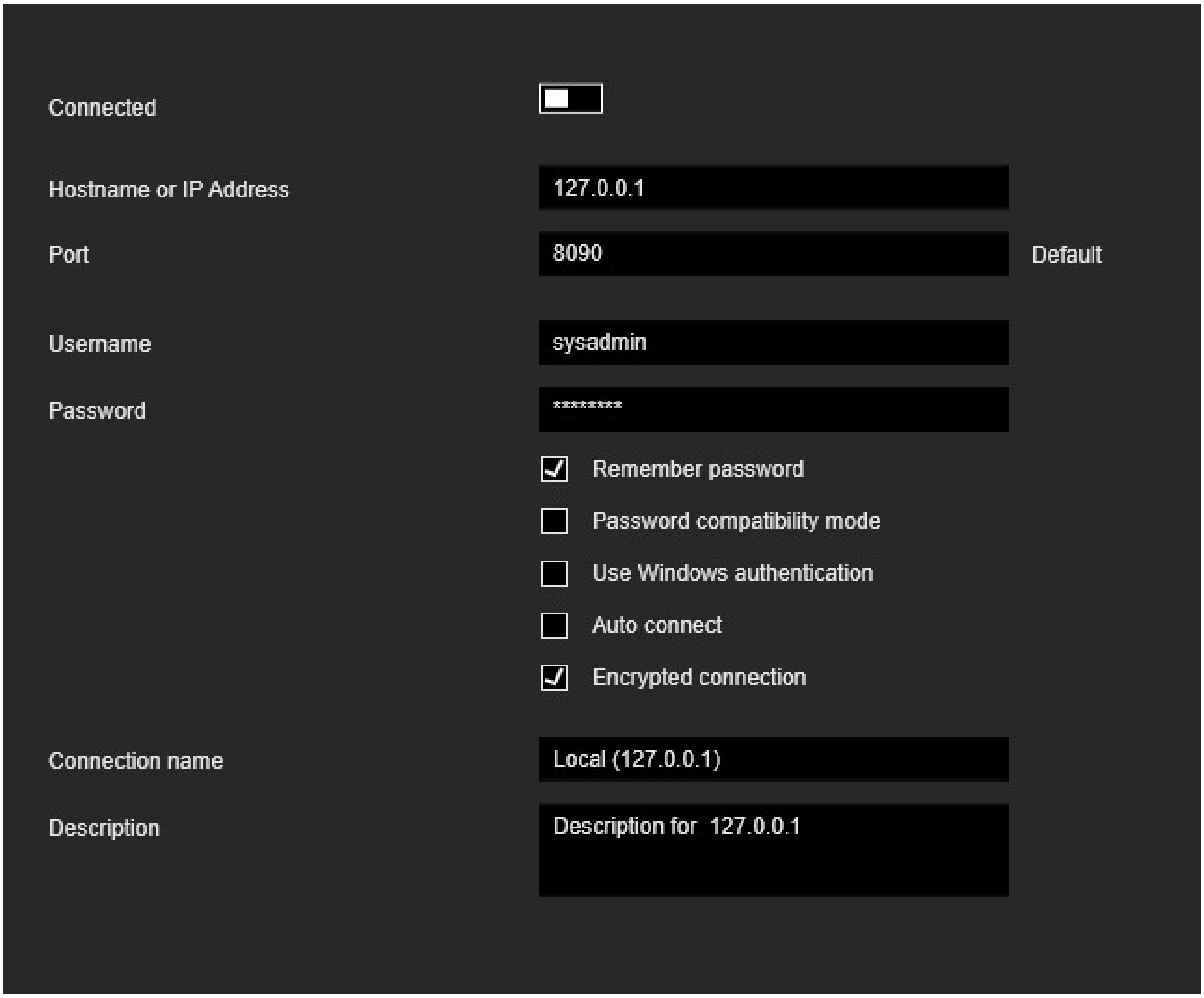
Password:

☒ Remember Password

☐ Password compatibility mode

Description:

As of G-SIM version 9.2, you can activate this mode in the **Connection** view:



Connected		
Hostname or IP Address	127.0.0.1	
Port	8090	Default
Username	sysadmin	
Password	********	

☑ Remember password

□ Password compatibility mode

□ Use Windows authentication

□ Auto connect

☑ Encrypted connection

Connection name	Local (127.0.0.1)
Description	Description for 127.0.0.1

Enable the **Password compatibility mode**:

- To connect to a server that does not support password hashing.
- To connect to a server that has been upgraded to a version that supports the new password hashing and for which no administrator password has been set yet.

Disable the **Password compatibility mode**:

- To connect to a server that has been upgraded to a version that supports the new password hashing and for which an administrator password has been set again.
- To connect to a server that supports the new password hashing and that has been installed on a cleaned environment.

ⓘ **Downgrade is not supported.**
Example: A ManCon version that does not support the new password hashing cannot connect to another server that supports the new password hashing. In addition, if a server that supports the new password hashing is downgraded to a version that does not support the new password hashing, all user accounts are invalidated.

Import/export settings

The settings can be imported successfully in the following two cases:

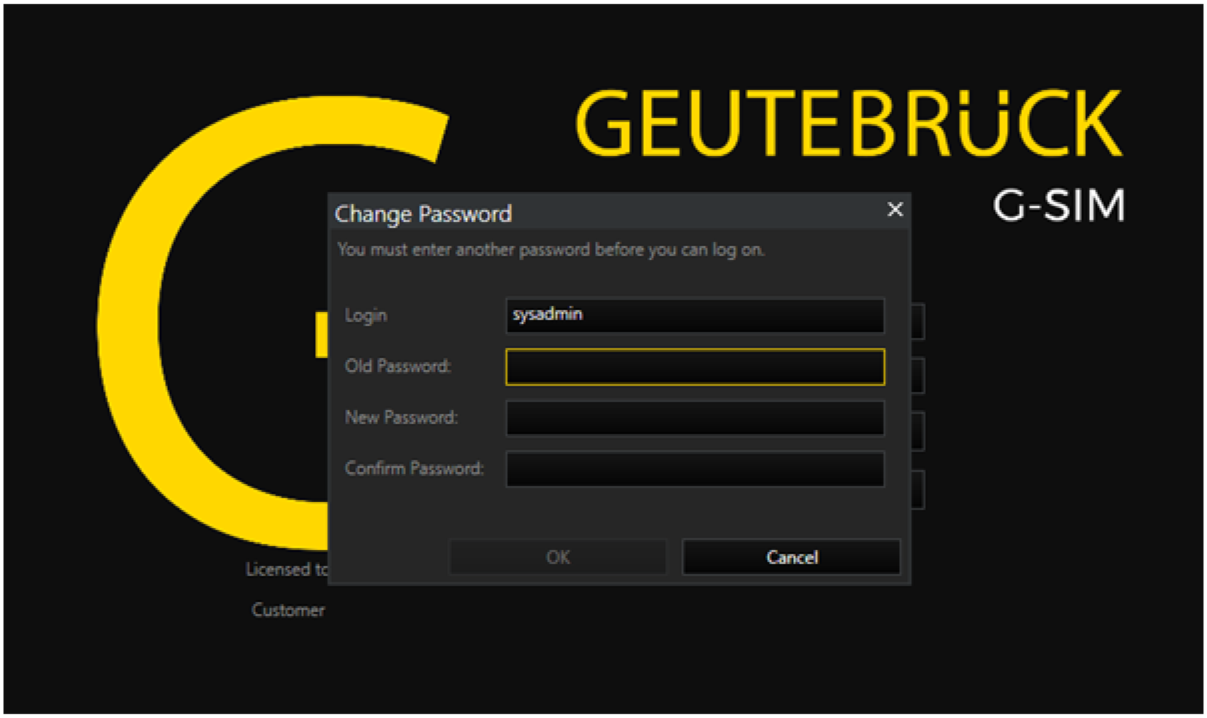
- If the setting was exported from a version that supports the new password hashing.
- If the setting was exported from a version that does not support the new password hashing.

ⓘ **A setting exported from a version that supports the new password hashing is not compatible with a version that does not support the new password hashing.**

Operator Console

In the case of an imported setting with old password hashes or an upgrade to a new version that does not support the new password hashing, the Change Password dialog window opens when the user first attempts to log in to OpCon. It prompts the user to change the password.

ⓘ **If the administrator changes the password in OpCon, a corresponding password must be set in the ManCon server connection settings.**



Change Password

You must enter another password before you can log on.

Login: sysadmin

Old Password:

New Password:

Confirm Password:

Upgrade 8.8 or older to 9.4

Requirements

- Before upgrading, create a backup of all SQL databases and G-SIM setup and verify that the backup restore works properly.
- Check the required system requirements.
- Check the validity of your upgrade license.

Note

A system with a control server is no longer supported as of G-SIM version 9.2. You can now use the global function that allows all servers to communicate directly with each other.

- The servers are equal and communicate directly with each other. There is no hierarchy with a "main server" (unlike the control server with sub-servers).
- All administrators can access all servers. The reason for this is that users and restrictions are mapped and synchronized throughout the system. For example, an administrator from site A can log on to site B and have the

same rights.

- For the operator, there are no changes compared to a system with one control server. You can still apply restrictions to individual sites. If required, you can also view the information of several sites here.

Full Installation

The full installation upgrades the entire system, i.e. the G-SIM server and the selected clients, in one step.

1. Start the Installer.
2. The note **Please note that Pelco is not longer supported by GSIM** appears. Click **OK**.

   ⓘ **As of G-SIM Version 9.2, the Pelco integration is no longer supported.**

3. In the **Select Components** dialog window, select **Full installation**.
4. Select the components you want to upgrade or install. By default, the existing components are selected.
5. Optionally, you can install G-SIM Global by selecting the **Global GSim Environment** component.
6. Click **Next**.
7. The **Enhanced Security Mode Setting** dialog window opens.
   - Select the **Enable the enhanced security mode** option to enable the enhanced security mode. Detailed information about this mode can be found **here**.

     ⓘ **If the FIPS mode is already enabled in the Window settings of your respective system, the mode is automatically enabled for G-SIM. The Enable the enhanced security mode option is then selected by default and grayed out.**

     ⚠ **IMPORTANT:** The compatibility towards older system versions is no longer possible in the enhanced security mode. All system components must be installed in FIPS mode, otherwise no connection between the server and the clients (operator or management console, health agent) is possible.

- Do not select the **Enable the enhanced security mode** option to install G-SIM without the enhanced security mode.

8. Click **Next**.

9. The **Compatibility settings** dialog window opens.

   ℹ **If you enabled the enhanced security mode during installation, no compatibility mode is available for this installation.**

   - Select the **Yes, install in compatibility mode** option to allow the clients (Operator or Management Console, Health Agent) to connect to an older server (version below 9.2) without interrupting operation. Detailed information about this mode can be found **here**.

     ⚠ **IMPORTANT:** The compatibility mode is intended only for transition during system upgrade to avoid interruption of service. The clients should not run in compatibility mode for an extended period of time or permanently. Therefore, upgrade all clients again without compatibility mode after the server upgrade.

   - Select the **No, servers must also be updated before connection is possible** option to continue the installation without compatibility mode.

10. Click **Next**.

11. The **Encryption settings** dialog window opens.

    - Select the **Yes, change encryption settings** option to automatically change the encryption settings. Detailed information about this setting can be found **here**.
    - Select the **No, do not change any encryption settings** option to not change the encryption settings automatically.

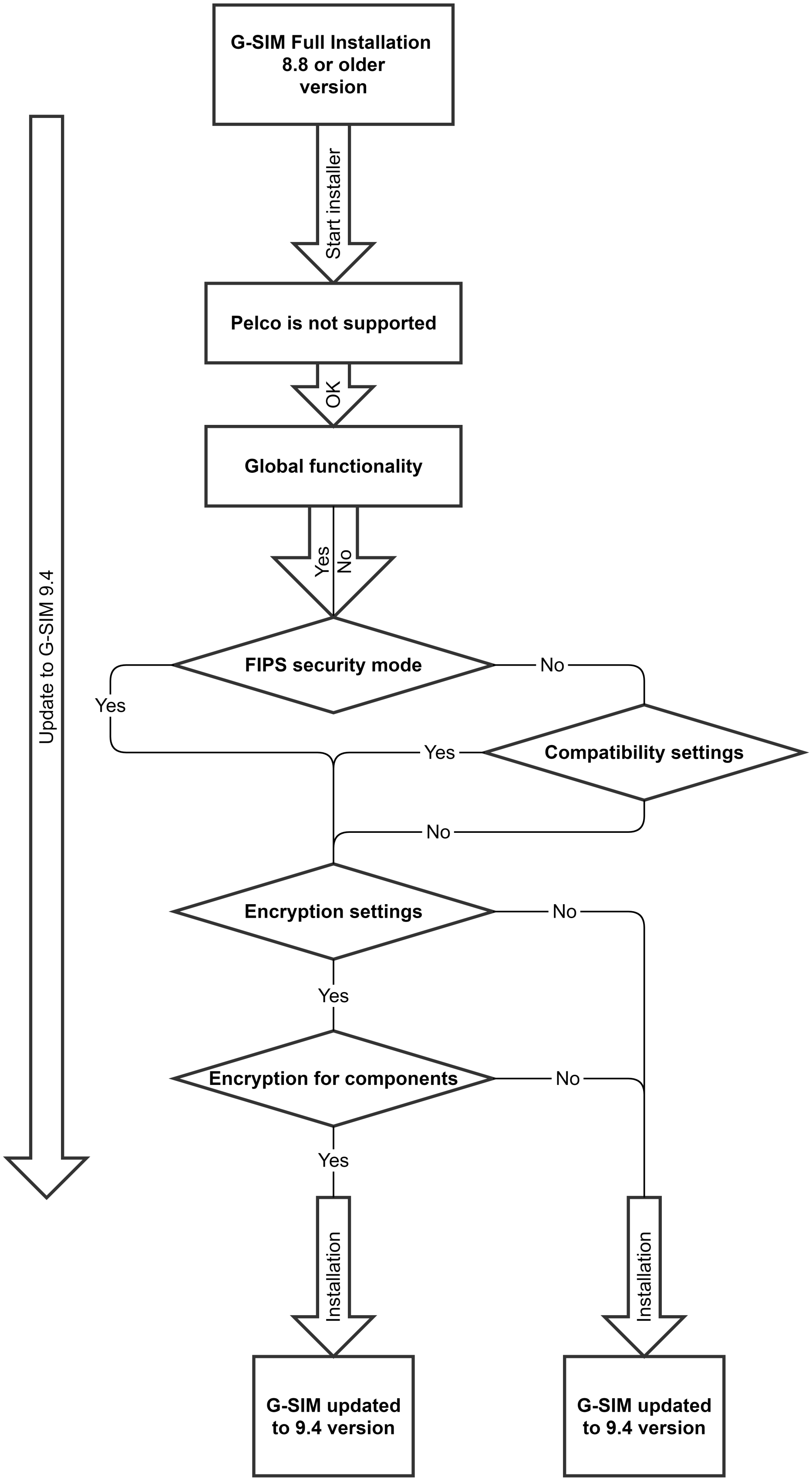
12. Click **Next**.

13. The **Encryption settings** dialog window opens.

    - Select the **Enable encryption for GSIM Server, Operator UI, Management Console, Health Agent** option to enable encryption for the system components.
    - Select the **Disable encryption for these components** option to disable encryption or the system components.

14. Start the installation.

    → The G-SIM server and the selected clients are upgraded to G-SIM version 9.4.


G-SIM Full Installation 8.8 or older version
Start installer
Pelco is not supported
OK
Global functionality
Yes
No
FIPS security mode
No
Yes
Compatibility settings
Yes
No
Encryption settings
No
Yes
Encryption for components
No
Yes
Installation
Installation
G-SIM updated to 9.4 version
G-SIM updated to 9.4 version
Update to G-SIM 9.4

Cluster Installation

The cluster installation of OpCon and server enables the upgrade of complex systems as well as the upgrade in a running operation by upgrading client and server separately from each other.

OpCon Installation

1. Start the Installer.
2. The note Please note that Pelco is not longer supported by GSIM appears. Click OK.

   ⓘ **As of G-SIM Version 9.2, the Pelco integration is no longer supported.**

3. In the Select Components dialog window, select Operator installation.
4. Click Next.
5. The Enhanced Security Mode Setting dialog window opens.
   - Select the Enable the enhanced security mode option to enable the enhanced security mode. Detailed information about this mode can be found here.

     ⓘ **If the FIPS mode is already enabled in the Window settings of your respective system, the mode is automatically enabled for G-SIM. The Enable the enhanced security mode option is then selected by default and grayed out.**

     ⚠ **IMPORTANT:** The compatibility towards older system versions is no longer possible in the enhanced security mode. All system components must be installed in FIPS mode, otherwise no connection between the server and the clients (operator or management console, health agent) is possible.

   - Do not select the Enable the enhanced security mode option to install G-SIM without the enhanced security mode.
6. Click Next.
7. The Compatibility settings dialog window opens.

If you enabled the enhanced security mode during installation, no compatibility mode is available for this installation.

- Select the Yes, install in compatibility mode option to allow the clients (Operator or Management Console, Health Agent) to connect to an older server (version below 9.2) without interrupting operation. Detailed information about this mode can be found **here**.

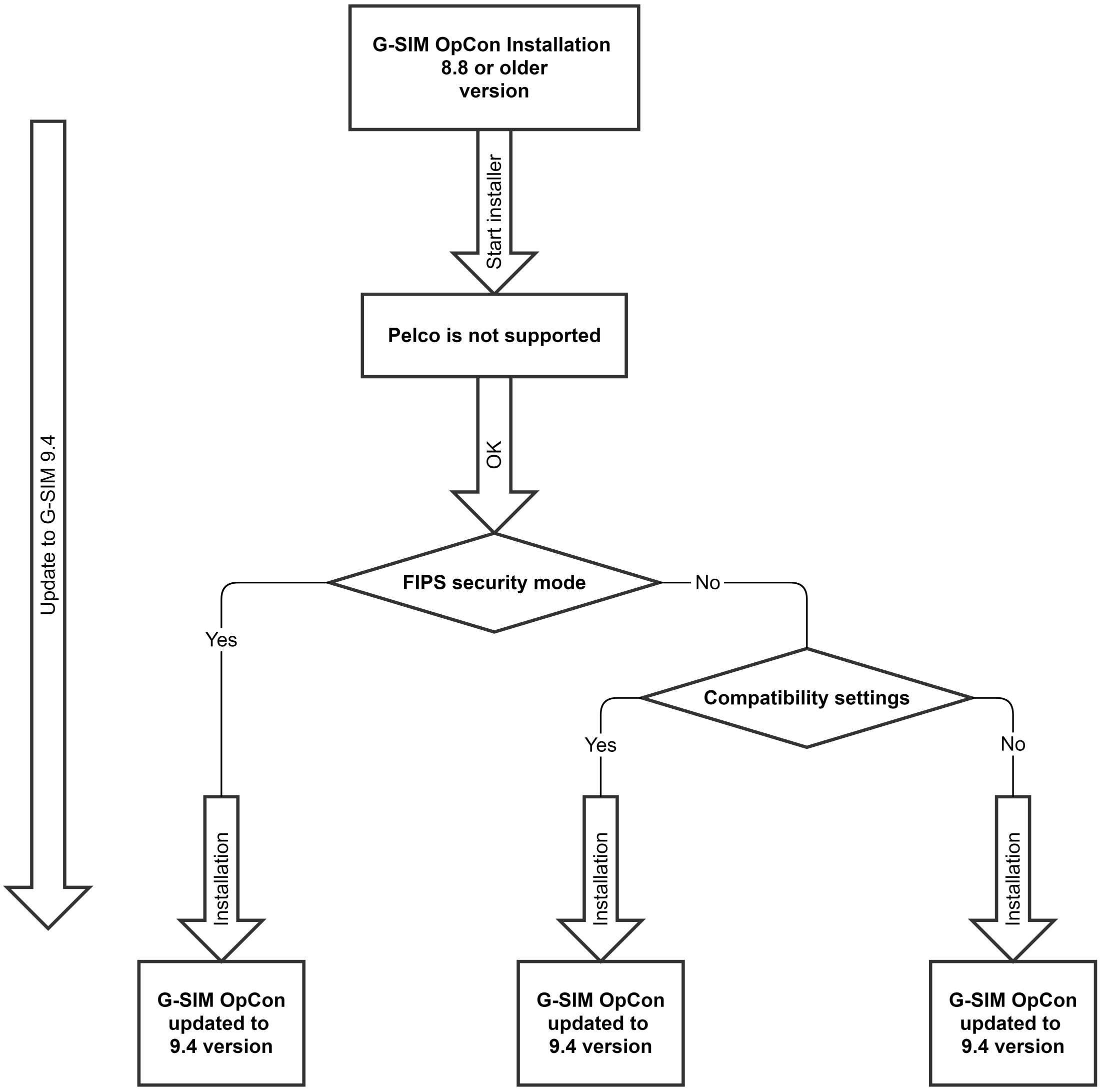
  > **IMPORTANT:** The compatibility mode is intended only for transition during system upgrade to avoid interruption of service. The clients should not run in compatibility mode for an extended period of time or permanently. Therefore, upgrade all clients again without compatibility mode after the server upgrade.

- Select the No, servers must also be updated before connection is possible option to continue the installation without compatibility mode.

8. Start the installation.

   → The OpCon is upgraded to G-SIM version 9.4.

To connect to a server with encryption of the system components activated, the option Use encrypted connection must be activated for the connection of OpCon and server in the OpCon startup settings.


G-SIM OpCon Installation 8.8 or older version
Start installer
Pelco is not supported
OK
FIPS security mode
Yes
No
Compatibility settings
Yes
No
Installation
Installation
Installation
G-SIM OpCon updated to 9.4 version
G-SIM OpCon updated to 9.4 version
G-SIM OpCon updated to 9.4 version
Update to G-SIM 9.4

Server Installation

1. Start the Installer.
2. The note **Please note that Pelco is not longer supported by GSIM** appears. Click **OK**.

   As of G-SIM Version 9.2, the Pelco integration is no longer supported.

3. In the **Select Components** dialog window, select **Server installation**.

4. Select the components you want to upgrade or install. By default, the existing components are selected.
5. Optionally, you can install G-SIM Global by selecting the **Global GSim Environment** component.
6. Click **Next**.
7. The **Enhanced Security Mode Setting** dialog window opens.
   - Select the **Enable the enhanced security mode** option to enable the enhanced security mode. Detailed information about this mode can be found **here**.

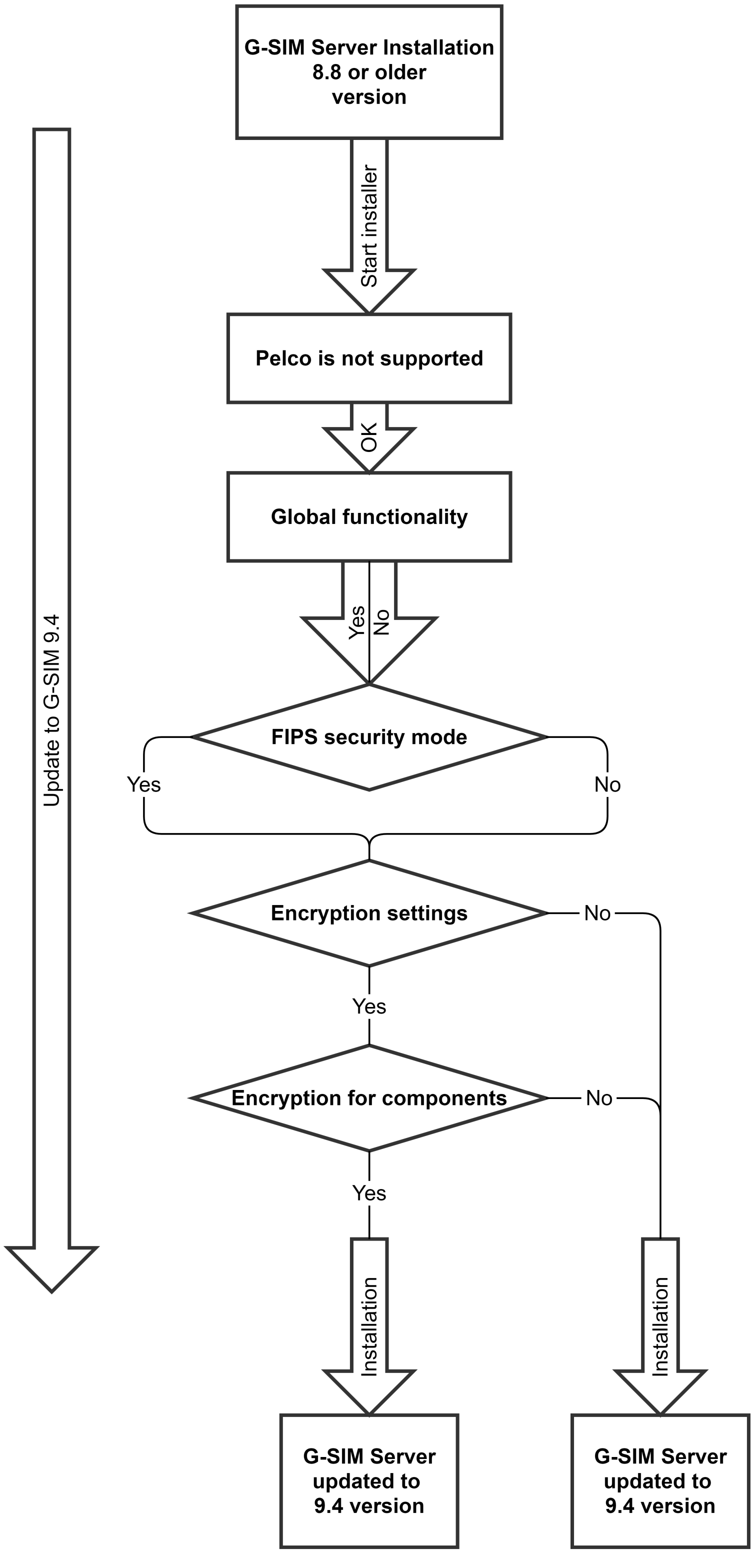
     If the FIPS mode is already enabled in the Window settings of your respective system, the mode is automatically enabled for G-SIM. The Enable the enhanced security mode option is then selected by default and grayed out.

     IMPORTANT: The compatibility towards older system versions is no longer possible in the enhanced security mode. All system components must be installed in FIPS mode, otherwise no connection between the server and the clients (operator or management console, health agent) is possible.

   - Do not select the **Enable the enhanced security mode** option to install G-SIM without the enhanced security mode.
8. Click **Next**.
9. The **Encryption settings** dialog window opens.
   - Select the **Yes, change encryption settings** option to automatically change the encryption settings. Detailed information about this setting can be found **here**.
   - Select the **No, do not change any encryption settings** option to not change the encryption settings automatically.
10. Click **Next**.
11. The **Encryption settings** dialog window opens.
    - Select the **Enable encryption for GSIM Server, Operator UI, Management Console, Health Agent** option to enable encryption for the system components.
    - Select the **Disable encryption for these components** option to disable encryption or the system components.

12. Start the installation.

    → The G-SIM server is upgraded to G-SIM version 9.4.

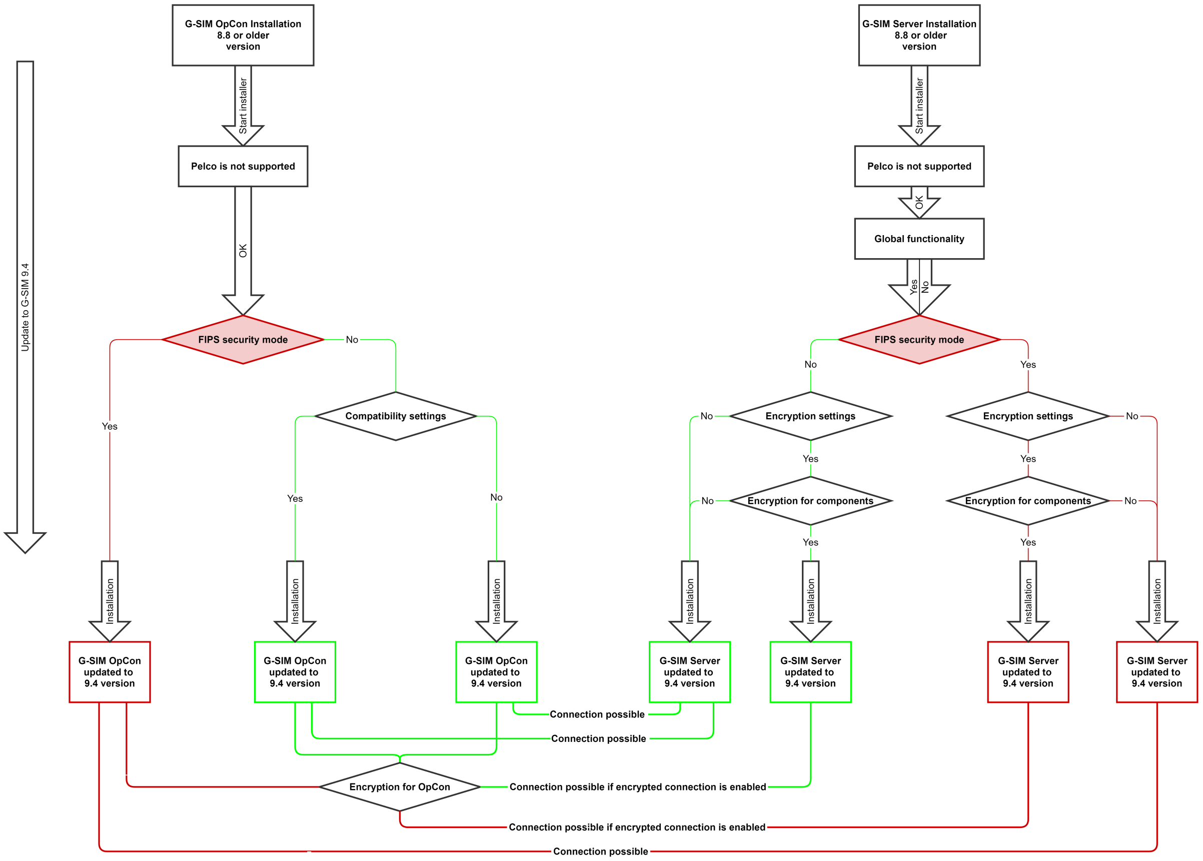

G-SIM Server Installation 8.8 or older version
Start installer
Pelco is not supported
OK
Global functionality
Yes
No
FIPS security mode
Yes
No
Encryption settings
No
Yes
Encryption for components
No
Yes
Installation
Installation
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
Update to G-SIM 9.4

Connections of OpCon and Server

The possible connections of OpCon and Server after upgrading to G-SIM version 9.4 depend on your selected settings during the respective installation.

Note:

- If the enhanced security mode is enabled on a component, all system components must be installed in FIPS-mode, otherwise no connection between the server and clients (operator or management console, health agent) is possible.
- To connect to a server with encryption of the system components activated, the option **Use encrypted connection** must be activated for the connection of OpCon and server in the OpCon startup settings.


G-SIM OpCon Installation 8.8 or older version
G-SIM Server Installation 8.8 or older version
Update to G-SIM 9.4
Start installer
Start installer
Pelco is not supported
Pelco is not supported
OK
OK
Global functionality
Yes
No
FIPS security mode
No
FIPS security mode
No
Yes
Yes
Compatibility settings
No
Encryption settings
Encryption settings
No
Yes
Yes
Yes
No
No
Encryption for components
Encryption for components
No
Yes
Yes
Installation
Installation
Installation
Installation
Installation
Installation
Installation
G-SIM OpCon updated to 9.4 version
G-SIM OpCon updated to 9.4 version
G-SIM OpCon updated to 9.4 version
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
Connection possible
Connection possible
Encryption for OpCon
Connection possible if encrypted connection is enabled
Connection possible if encrypted connection is enabled
Connection possible

Upgrade 9.2 or newer to 9.4

Requirements

- Before upgrading, create a backup of all SQL databases and G-SIM setup and verify that the backup restore works properly.
- Check the required system requirements.
- Check the validity of your upgrade license.

Note

A system with a control server is no longer supported as of G-SIM version 9.2. You can now use the global function that allows all servers to communicate directly with each other.

- The servers are equal and communicate directly with each other. There is no hierarchy with a "main server" (unlike the control server with sub-servers).
- All administrators can access all servers. The reason for this is that users and restrictions are mapped and synchronized throughout the system. For example, an administrator from site A can log on to site B and have the same rights.
- For the operator, there are no changes compared to a system with one control server. You can still apply restrictions to individual sites. If required, you can also view the information of several sites here.

Full Installation

The full installation upgrades the entire system, i.e. the G-SIM server and the selected clients, in one step.

1. Start the Installer.
2. In the **Select Components** dialog window, select **Full installation**.
3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Optionally, you can install G-SIM Global by selecting the **Global GSim Environment** component.
5. Click **Next**.

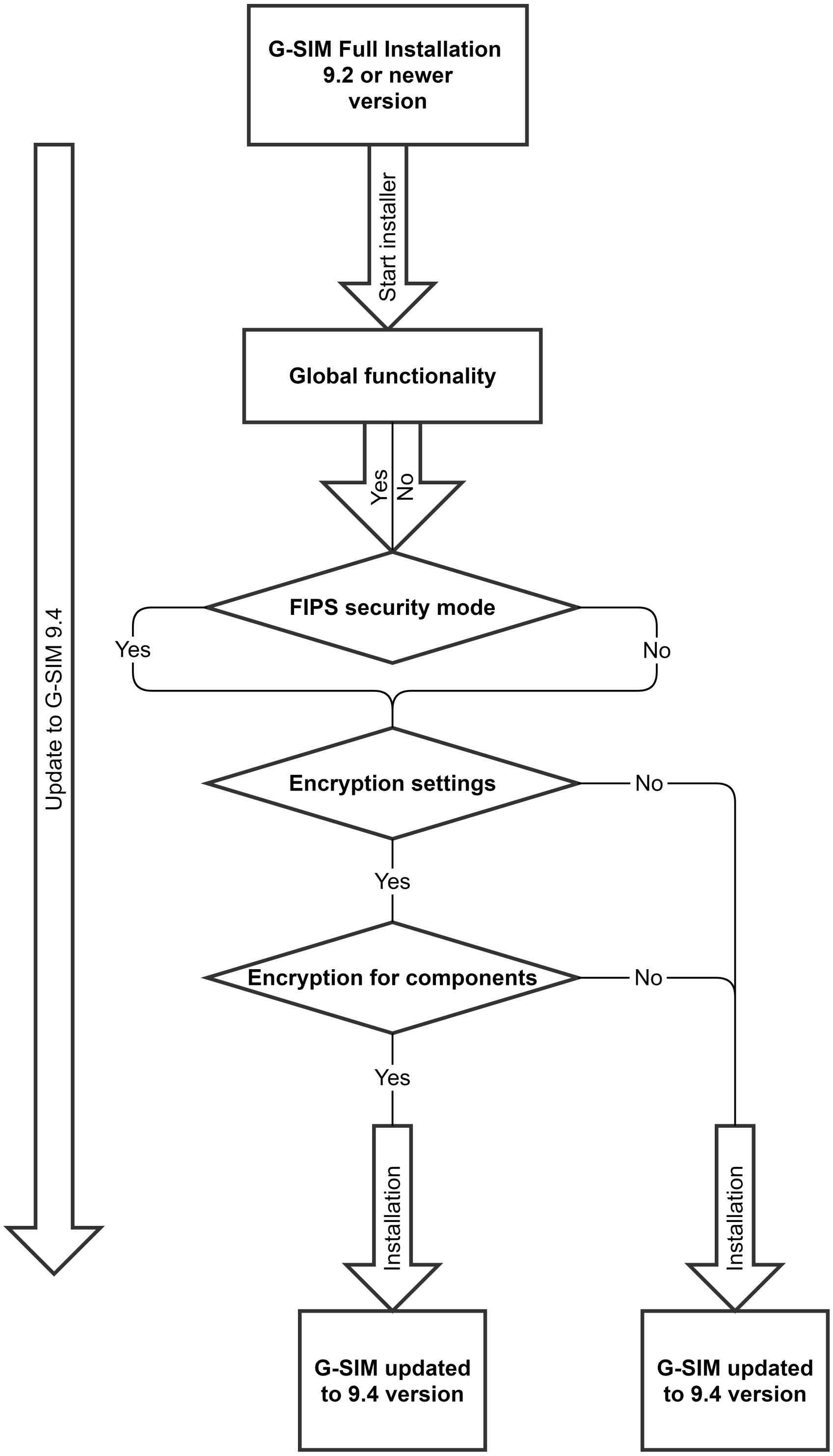
6. The Enhanced Security Mode Setting dialog window opens.
    - Select the Enable the enhanced security mode option to enable the enhanced security mode. Detailed information about this mode can be found **here**.

      If the FIPS mode is already enabled in the Window settings of your respective system, the mode is automatically enabled for G-SIM. The Enable the enhanced security mode option is then selected by default and grayed out.

      IMPORTANT: The compatibility towards older system versions is no longer possible in the enhanced security mode. All system components must be installed in FIPS mode, otherwise no connection between the server and the clients (operator or management console, health agent) is possible.

    - Do not select the Enable the enhanced security mode option to install G-SIM without the enhanced security mode.
7. Click Next.
8. The Encryption settings dialog window opens.
    - Select the Yes, change encryption settings option to automatically change the encryption settings. Detailed information about this setting can be found **here**.
    - Select the No, do not change any encryption settings option to not change the encryption settings automatically.
9. Click Next.
10. The Encryption settings dialog window opens.
    - Select the Enable encryption for GSIM Server, Operator UI, Management Console, Health Agent option to enable encryption for the system components.
    - Select the Disable encryption for these components option to disable encryption or the system components.
11. Start the installation.

    → The G-SIM server and the selected clients are upgraded to G-SIM version 9.4.


G-SIM Full Installation 9.2 or newer version
Start installer
Global functionality
Yes
No
FIPS security mode
Yes
No
Encryption settings
No
Yes
Encryption for components
No
Yes
Installation
Installation
G-SIM updated to 9.4 version
G-SIM updated to 9.4 version
Update to G-SIM 9.4

Cluster Installation

The cluster installation of OpCon and server enables the upgrade of complex systems as well as the upgrade in a running operation by upgrading client and server separately from each other.

OpCon Installation

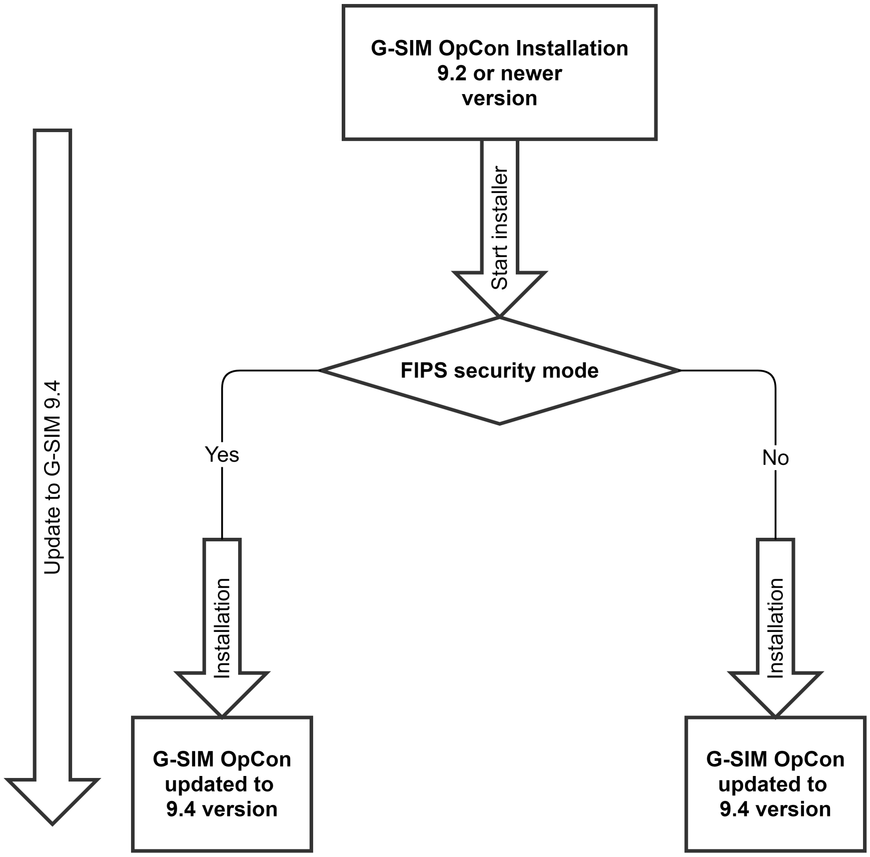
1. Start the Installer.
2. In the **Select Components** dialog window, select **Operator installation**.
3. Click **Next**.
4. The **Enhanced Security Mode Setting** dialog window opens.
   - Select the **Enable the enhanced security mode** option to enable the enhanced security mode. Detailed information about this mode can be found **here**.

     ⓘ **If the FIPS mode is already enabled in the Window settings of your respective system, the mode is automatically enabled for G-SIM. The Enable the enhanced security mode option is then selected by default and grayed out.**

     ⚠ **IMPORTANT:** The compatibility towards older system versions is no longer possible in the enhanced security mode. All system components must be installed in FIPS mode, otherwise no connection between the server and the clients (operator or management console, health agent) is possible.
   - Do not select the **Enable the enhanced security mode** option to install G-SIM without the enhanced security mode.
5. Start the installation.

   → The OpCon is upgraded to G-SIM version 9.4.

   ⓘ **To connect to a server with encryption of the system components activated, the option Use encrypted connection must be activated for the connection of OpCon and server in the OpCon startup settings.**


G-SIM OpCon Installation 9.2 or newer version
Start installer
FIPS security mode
Yes
No
Installation
Installation
G-SIM OpCon updated to 9.4 version
G-SIM OpCon updated to 9.4 version
Update to G-SIM 9.4

Server Installation

1. Start the Installer.
2. In the **Select Components** dialog window, select **Server installation**.
3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Optionally, you can install G-SIM Global by selecting the **Global GSim Environment** component.
5. Click **Next**.
6. The **Enhanced Security Mode Setting** dialog window opens.

- Select the Enable the enhanced security mode option to enable the enhanced security mode. Detailed information about this mode can be found **here**.

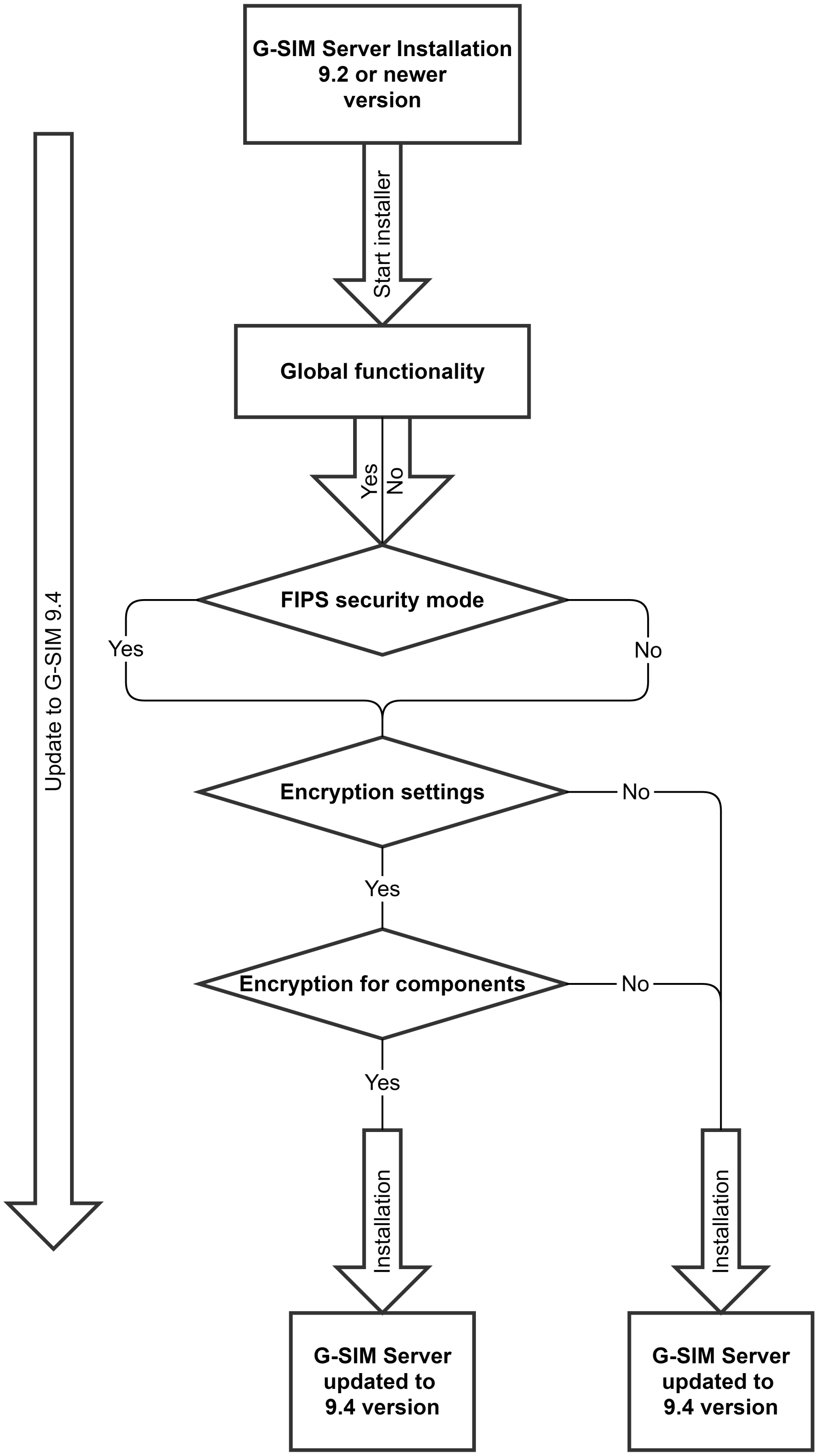
  ⓘ **If the FIPS mode is already enabled in the Window settings of your respective system, the mode is automatically enabled for G-SIM. The Enable the enhanced security mode option is then selected by default and grayed out.**

  ⚠ **IMPORTANT:** The compatibility towards older system versions is no longer possible in the enhanced security mode. All system components must be installed in FIPS mode, otherwise no connection between the server and the clients (operator or management console, health agent) is possible.

- Do not select the Enable the enhanced security mode option to install G-SIM without the enhanced security mode.

7. Click Next.
8. The Encryption settings dialog window opens.
   - Select the Yes, change encryption settings option to automatically change the encryption settings. Detailed information about this setting can be found **here**.
   - Select the No, do not change any encryption settings option to not change the encryption settings automatically.
9. Click Next.
10. The Encryption settings dialog window opens.
    - Select the Enable encryption for GSIM Server, Operator UI, Management Console, Health Agent option to enable encryption for the system components.
    - Select the Disable encryption for these components option to disable encryption or the system components.
11. Start the installation.

    → The G-SIM server is upgraded to G-SIM version 9.4.

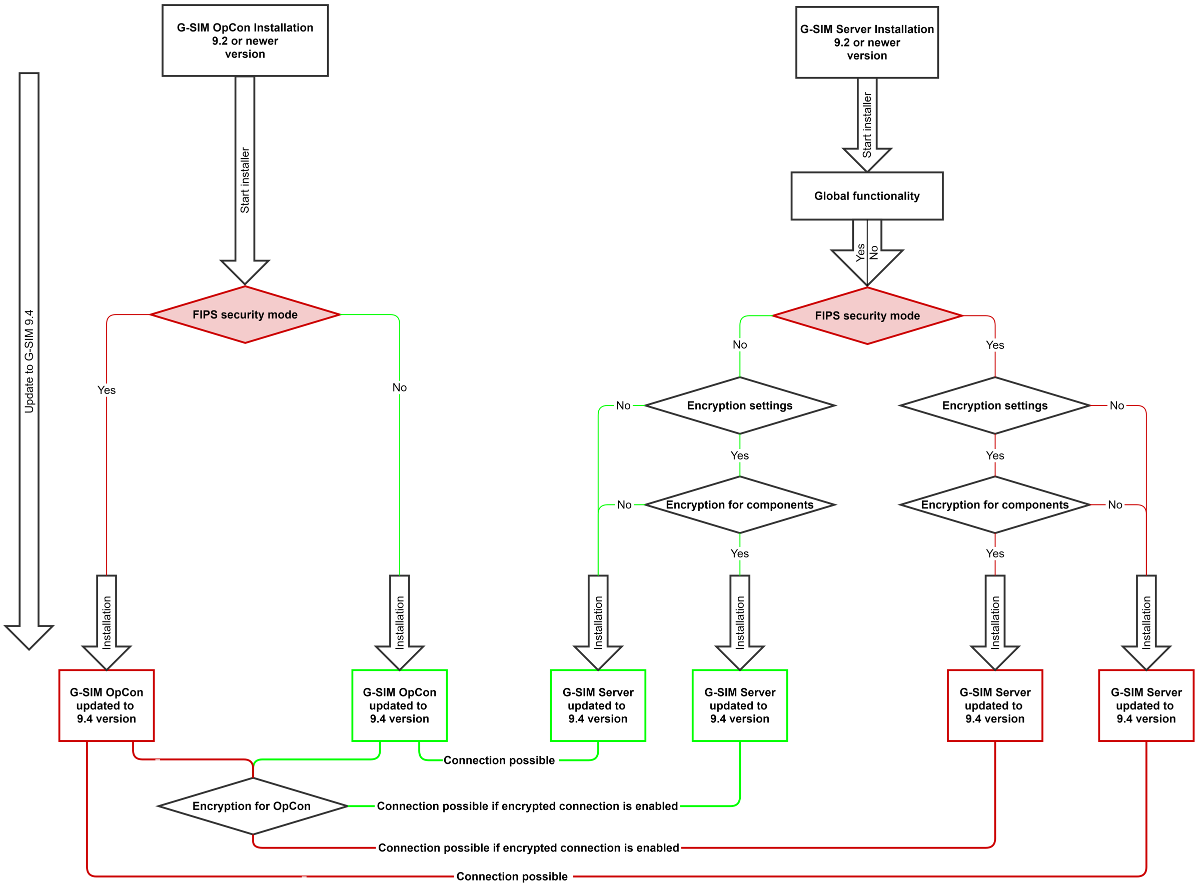

G-SIM Server Installation 9.2 or newer version
Start installer
Global functionality
Yes
No
FIPS security mode
Yes
No
Encryption settings
No
Yes
Encryption for components
No
Yes
Installation
Installation
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
Update to G-SIM 9.4

Connections of OpCon and Server

The possible connections of OpCon and Server after upgrading to G-SIM version 9.4 depend on your selected settings during the respective installation.

Note:

- If the enhanced security mode is enabled on a component, all system components must be installed in FIPS-mode, otherwise no connection between the server and clients (operator or management console, health agent) is possible.
- To connect to a server with encryption of the system components activated, the option **Use encrypted connection** must be activated for the connection of OpCon and server in the OpCon startup settings.


G-SIM OpCon Installation 9.2 or newer version
G-SIM Server Installation 9.2 or newer version
Update to G-SIM 9.4
Start installer
Start installer
Global functionality
Yes
No
FIPS security mode
Yes
No
FIPS security mode
No
Yes
No
Encryption settings
Encryption settings
No
Yes
Yes
No
Encryption for components
Encryption for components
No
Yes
Yes
Installation
Installation
Installation
Installation
Installation
Installation
G-SIM OpCon updated to 9.4 version
G-SIM OpCon updated to 9.4 version
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
G-SIM Server updated to 9.4 version
Connection possible
Encryption for OpCon
Connection possible if encrypted connection is enabled
Connection possible if encrypted connection is enabled
Connection possible

Upgrade 9.3 to 9.4

With version G-SIM 9.3 the use of FQDN as local server identity was introduced. This means that it is no longer possible to connect an OpCon of version 9.3 or newer to a G-SIM server older than version 8.8.

To establish the connection and upgrade to version 9.4 without interrupting operations, you must first upgrade the server and OpCon to version 9.3. In the next step, you can then upgrade to version 9.4.

How to proceed

1. Start the installer for the G-SIM 9.3 version.
2. In the **Select Components** dialog window, select **Operator installation**.
3. Note the **Installation Modes** required for this upgrade.
4. Start the installer.

   → The OpCon is upgraded to version 9.3.
5. Start the installer again for the G-SIM 9.3 version.
6. In the **Select Components** dialog window, select **Server installation**.
7. Note the **Installation Modes** required for this upgrade.
8. Start the installer.

   → The G-SIM server is upgraded to version 9.3.
9. Perform the upgrade to version 9.4. See **Upgrade 9.2 or newer to 9.4**.

Upgrade 9.4 to 10

With version G-SIM 10, the use of the security-related functions Enhanced Security Mode (FIPS), Change Communication Protocol and Encryption Settings is introduced. These installation modes are automatically installed with the upgrade to G-SIM 10.

⚠ **IMPORTANT:** Backward compatibility of G-SIM servers and clients is no longer possible. Downgrading from version 10 to a previous version may damage your setup. Therefore, make sure to create a backup of your setup before you start the upgrade!

ⓘ **To establish the connection and upgrade to version 10 without interrupting operation, you must first update the G-SIM server to version 9.4.2. In the next step, you can then upgrade the clients to version 10 and then upgrade the server to version 10 as well.**

Limitations

- Clients are no longer able to connect to older servers.
- Server and client must both be upgraded to version 10. There is no longer the possibility to use a hybrid / mixed environment with different versions.
- Every system component must have the same version.
- Upgrade to the major version 10 is only possible from 9.4 and 9.4.1.

Requirements

- G-SIM server and clients have the version 9.4.1.

  ⓘ **An upgrade to first version 9.4.2 and then to version 10 is only possible with version 9.4.1. G-SIM server and clients must be updated to version 9.4.1!**

- When updating to version 9.4.2, you must enable the following installation modes:
  - Compatibility Mode - Enabled
  - Encryption Settings - Enabled
  - Encryption Settings for Components - Enabled
  - Enhanced Security Mode (FIPS) - Depending on previous installation

Note

- Before upgrading, create a backup of all SQL databases and G-SIM setup and verify that the backup restore works properly.
- Check the required system requirements.
- Check the validity of your upgrade license.

Standard Installation

ⓘ **If the Enhanced Security Mode (FIPS) has already been activated in your system during a previous update, you can upgrade your system directly to version 10 and skip step 1.**

Step 1 - Update the Server to Version 9.4.2

1. Start the installer for G-SIM 9.4.2 version.
2. In the Select Components dialog window, select Server installation or Full installation.
3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Optionally, you can install G-SIM Global by selecting the Global GSim Environment component.
5. Click Next.
6. The Enhanced Security Mode Setting dialog window opens.
7. Do not select the Enable the enhanced security mode option to install G-SIM without the enhanced security mode.

   ⚠ **IMPORTANT:** If the FIPS mode is not yet activated in your system, the mode should not be activated for the update to 9.4.2!

8. Click Next.
9. The Compatibility settings dialog window opens.
10. Select the Yes, install in compatibility mode option.
11. The Encryption settings dialog window opens.
12. Select the Yes, change encryption settings option.

    ⚠ **IMPORTANT:** If you do not select this option, connection problems between server and clients may occur.

13. Click Next.
14. The Encryption settings dialog window opens.

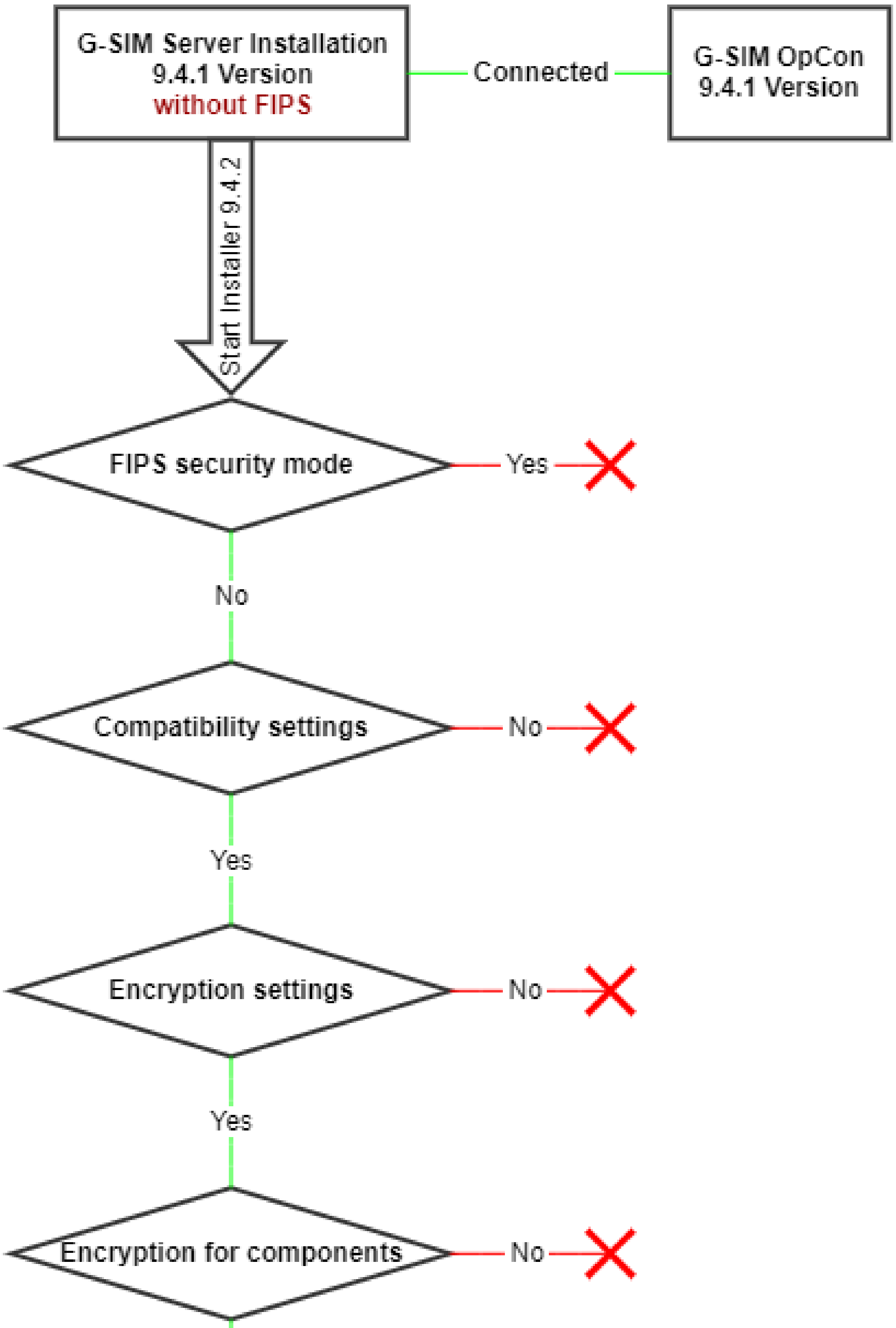
15. Select the Enable encryption for GSIM Server, Operator UI, Management Console, Health Agent option to enable encryption for the system components.

    ⚠ **IMPORTANT:** If you do not select this option, connection problems between server and clients may occur.

16. Start the installation.

→ The G-SIM server and the selected clients are upgraded to G-SIM version 9.4.2.

Step 1 -
Update Server to 9.4.2 Version



Step 2 - Upgrade the Clients to Version 10

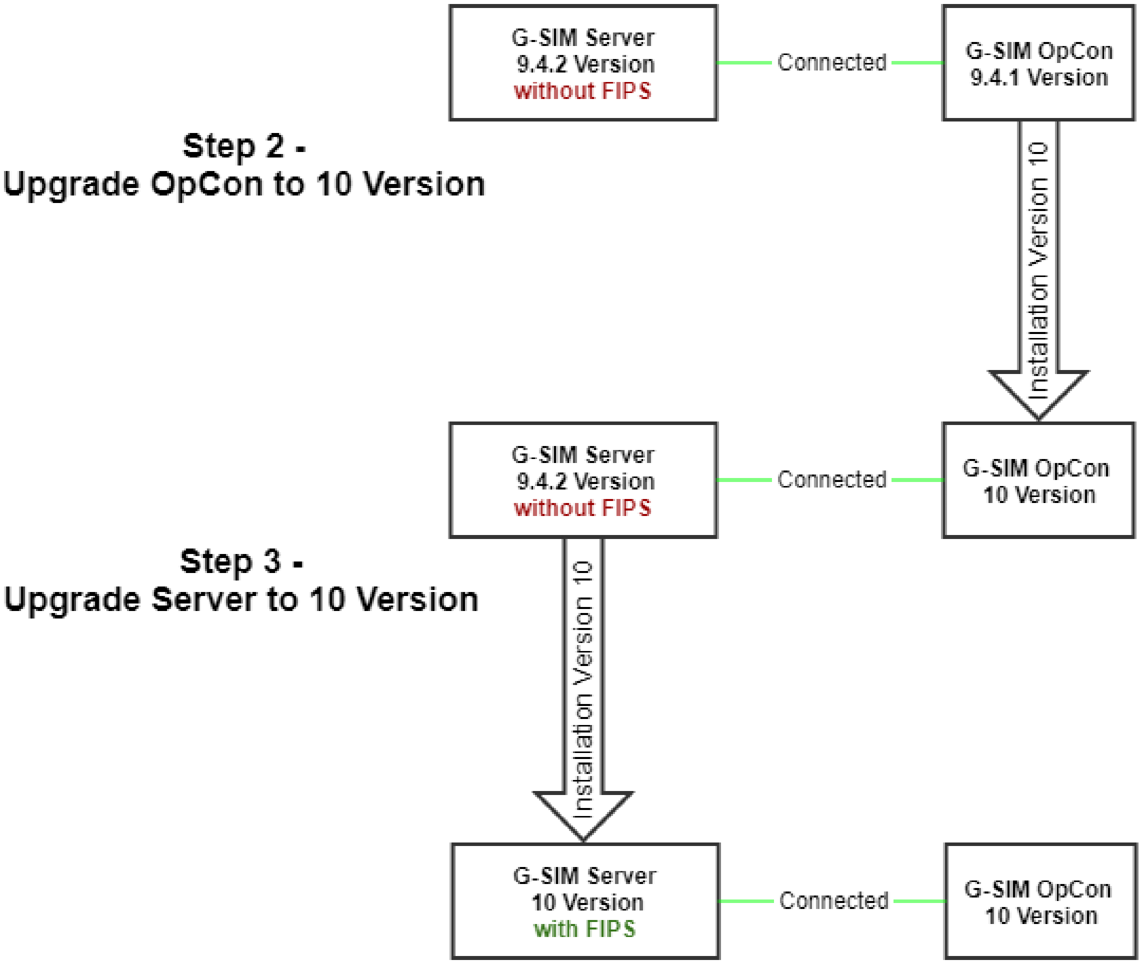
1. Start the installer for the G-SIM 10 version.
2. In the **Select Components** dialog window, select **Operator installation**.
3. Click **Next**.
4. Start the installation.

→ The clients are upgraded to G-SIM version 10.

Step 3 - Upgrade the Server to Version 10

1. Start the installer for the G-SIM 10 version.
2. In the **Select Components** dialog window, select **Server installation** or **Full installation**.
3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Click **Next**.
5. Start the installation.

→ The server is upgraded to G-SIM version 10.



Cluster Installation

If the Enhanced Security Mode (FIPS) has already been activated in your system during a previous update, you can upgrade your system directly to version 10 and skip step 1.

Step 1 - Update the Secondary Server to Version 9.4.2

1. Start the installer for G-SIM 9.4.2 version.
2. In the **Select Components** dialog window, select **Server installation** or **Full installation**.

3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Optionally, you can install G-SIM Global by selecting the **Global GSim Environment** component.
5. Click **Next**.
6. The **Enhanced Security Mode Setting** dialog window opens.
7. Do not select the **Enable the enhanced security mode** option to install G-SIM without the enhanced security mode.

   > ⚠ **IMPORTANT:** If the FIPS mode is not yet activated in your system, the mode should not be activated for the update to 9.4.2!

8. Click **Next**.
9. The **Compatibility settings** dialog window opens.
10. Select the **Yes, install in compatibility mode** option.
11. The **Encryption settings** dialog window opens.
12. Select the **Yes, change encryption settings** option.

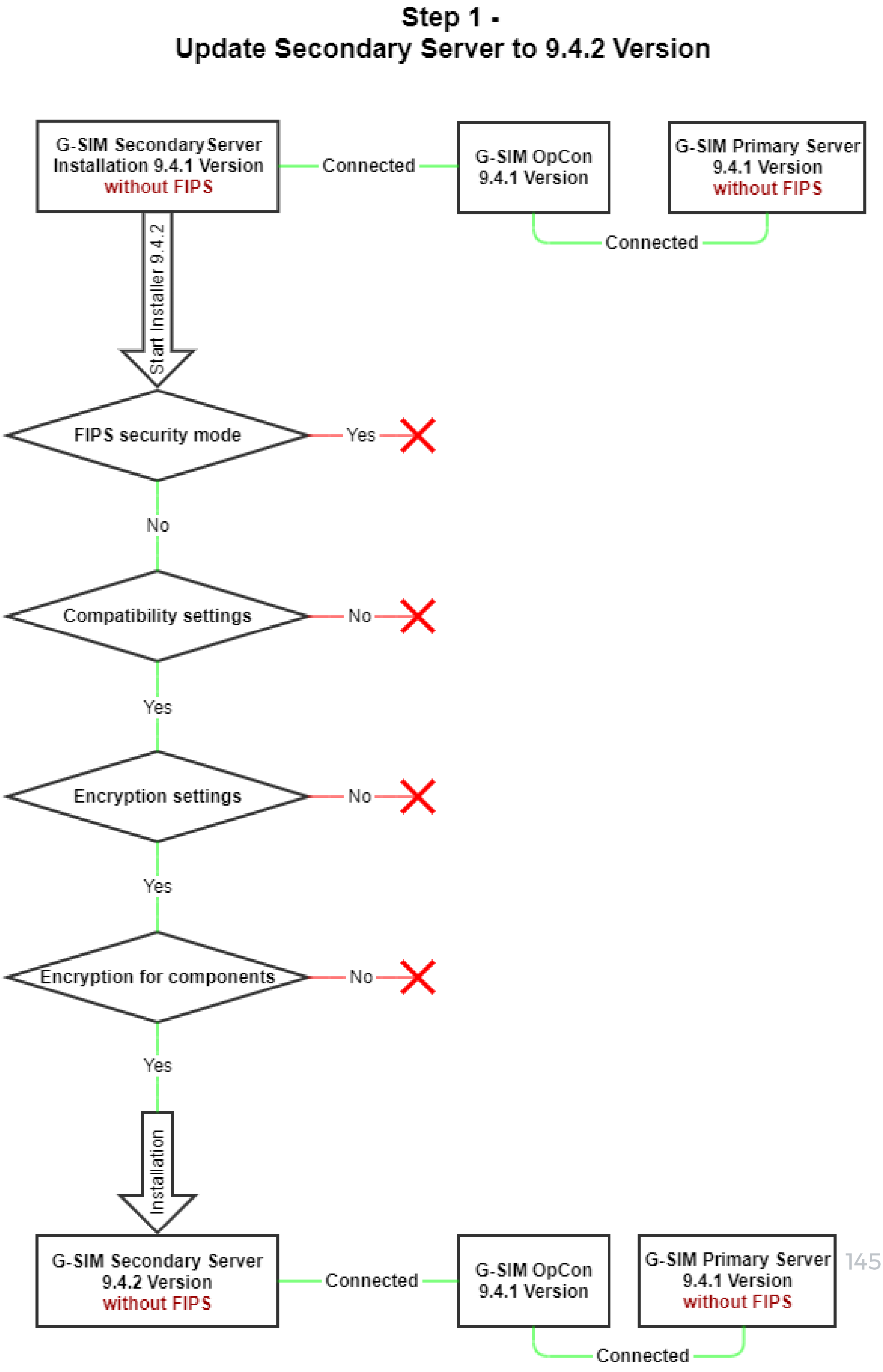
    > ⚠ **IMPORTANT:** If you do not select this option, connection problems between server and clients may occur.

13. Click **Next**.
14. The **Encryption settings** dialog window opens.
15. Select the **Enable encryption for GSIM Server, Operator UI, Management Console, Health Agent** option to enable encryption for the system components.

    > ⚠ **IMPORTANT:** If you do not select this option, connection problems between server and clients may occur.

16. Start the installation.

→ The G-SIM server and the selected clients are upgraded to G-SIM version 9.4.2.


Step 1 -
Update Secondary Server to 9.4.2 Version
G-SIM Secondary Server Installation 9.4.1 Version without FIPS
Connected
G-SIM OpCon 9.4.1 Version
G-SIM Primary Server 9.4.1 Version without FIPS
Connected
Start Installer 9.4.2
FIPS security mode
Yes
No
Compatibility settings
No
Yes
Encryption settings
No
Yes
Encryption for components
No
Yes
Installation
G-SIM Secondary Server 9.4.2 Version without FIPS
Connected
G-SIM OpCon 9.4.1 Version
G-SIM Primary Server 9.4.1 Version without FIPS
Connected

Step 2 - Stop the Primary Server

Stop the Primary Server.

→ The clients establish a new connection to the Secondary Server.

Step 3 - Upgrade the Clients to Version 10

1. Start the installer for the G-SIM 10 version.
2. In the **Select Components** dialog window, select **Operator installation**.
3. Click **Next**.
4. Start the installation.

→ The clients are upgraded to G-SIM version 10. The clients establish a new connection to the Secondary Server after client restart.

Step 4 - Upgrade the Primary Server to Version 10

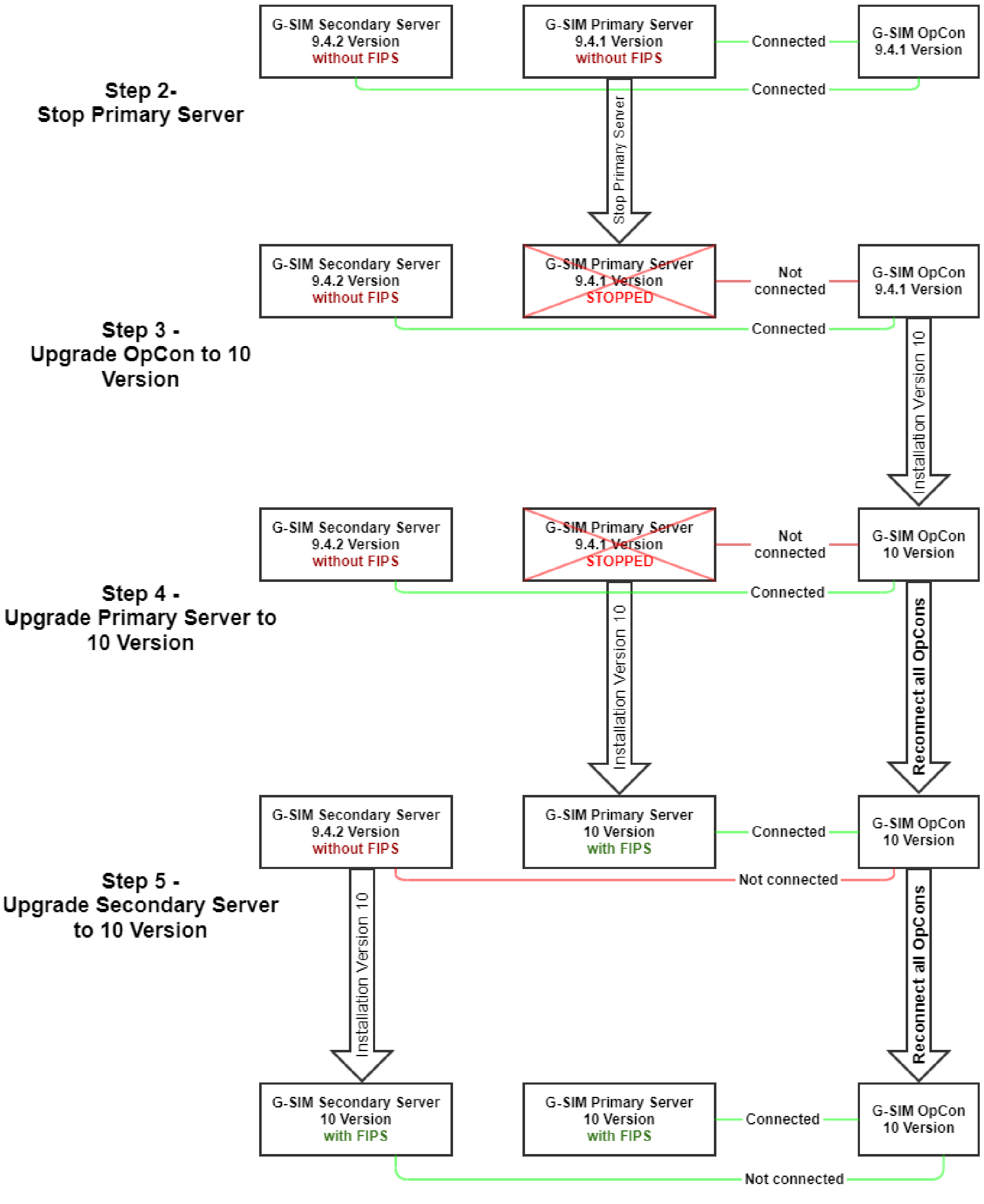
1. Start the installer for the G-SIM 10 version.
2. In the **Select Components** dialog window, select **Server installation** or **Full installation**.
3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Click **Next**.
5. Start the installation.

→ The primary server is upgraded to G-SIM version 10. The clients establish a new connection to the Primary Server after client restart.

Step 5 - Upgrade the Secondary Server to Version 10

1. Start the installer for the G-SIM 10 version.
2. In the **Select Components** dialog window, select **Server installation** or **Full installation**.
3. Select the components you want to upgrade or install. By default, the existing components are selected.
4. Click **Next**.
5. Start the installation.

→ The secondary server is upgraded to G-SIM version 10.



Upgrade to 10.x

If the system is already on version 10, any future update comprises starting the installer and following the steps.

ⓘ **Saving your setup and creating a backup of the SQL database before you start. The backup will be helpful if you need to return to your previous version. If you have completed the backup, you can start updating your system.**

Standard Installation

Update the Clients

Firstly, you should update all G-SIM clients (operator consoles).

1. Start the installer.
2. Accept the License Agreement and click Next.
3. In the Select Destination Location dialog window, select the install destination and click Next.
4. In the Select Components dialog window, select which components you want to install. The installer automatically selects any previously installed components. Click Next.
5. In the Ready to Install dialog window, click Install to continue with the installation.
6. Click on Finish once the installation is complete.

Now, you can start your operator console (OpCon) and connect to the server that still has the older version.

ⓘ **Using mixed version operation should only be done temporarily. You should also update the server to the same version as the clients.**

ⓘ **G-SIM OpCon is only backward compatible, not forward compatible. Clients with a newer version of G-SIM can connect to an older G-SIM server version. However, a server with two or more versions older than the clients can lead to unexpected problems.**

Update the Server

After updating all clients, you can update the server.

1. Start the installer.
2. Accept the **License Agreement** and click **Next**.
3. In the **Select Destination Location** dialog window, select the install destination and click **Next**.
4. In the **Select Components** dialog window, select which components you want to install. The installer automatically selects any previously installed components. Click **Next**.
5. In the **Ready to Install** dialog window, click **Install** to continue with the installation.
6. Click on **Finish** once the installation is complete.

ℹ **The installation will break connections between the G-SIM server and OpCons. New OpCon connections are only possible once the G-SIM server starts again. OpCons which are already connected will run in a restricted mode. Any cameras in viewers will stay in the mode they were in before the server stopped. After the server is updated, all OpCons reconnect automatically and exit this restricted mode.**

ℹ **Any agents in your environment that do not run on the same hardware as the server must be updated separately.**

ℹ **If the G-SIM SQL database is on a different machine than the G-SIM server, stop the server before updating SQL Express (see** Upgrade SQL Server**). We also recommend having DebugView running before starting the server to check for SQL errors.**

Cluster Installation

Update the Clients

Firstly, you should update all G-SIM clients (operator consoles).

1. Start the installer.
2. Accept the **License Agreement** and click **Next**.
3. In the **Select Destination Location** dialog window, select the install destination and click **Next**.

4. In the Select Components dialog window, select which components you want to install. The installer automatically selects any previously installed components. Click Next.
5. In the Ready to Install dialog window, click Install to continue with the installation.
6. Click on Finish once the installation is complete.

Now, you can start your operator console (OpCon) and connect to the server that still has the older version.

ⓘ **Using mixed version operation should only be done temporarily. You should also update the server to the same version as the clients.**

ⓘ **G-SIM OpCon is only backward compatible, not forward compatible. Clients with a newer version of G-SIM can connect to an older G-SIM server version. However, a server with two or more versions older than the clients can lead to unexpected problems.**

Update the Secondary Server

After updating all clients, you can update the servers.

ⓘ **We always recommend updating the secondary server first.**

1. Start the installer.
2. Accept the License Agreement and click Next.
3. In the Select Destination Location dialog window, select the install destination and click Next.
4. In the Select Components dialog window, select which components you want to install. The installer automatically selects any previously installed components. Click Next.
5. In the Ready to Install dialog window, click Install to continue with the installation.
6. Click on Finish once the installation is complete.
7. Wait until the secondary server has started again and synchronization between both servers is complete.

ⓘ **If the G-SIM SQL database is on a different machine than the secondary G-SIM server, stop the G-SIM secondary server before updating SQL Express (see** Upgrade SQL Server**). After updating, start the**

G-SIM secondary server and wait for synchronization to finish. We also recommend having DebugView running before starting the server to check for SQL errors.

Update the Primary Server

1. Start the installer
2. Accept the License Agreement.
3. In the Select Destination Location dialog window, select the install destination and click Next.
4. In the Select Components dialog window, select which components you want to install. The installer automatically selects any previously installed components. Click Next.
5. In the Ready to Install dialog window, click Install to continue with the installation.
6. Click on Finish once the installation is complete.
7. Wait until the primary server has started again and synchronization between both servers is complete.

If the G-SIM SQL database is on a different machine than the primary G-SIM server, stop the G-SIM primary server before updating SQL Express (see Upgrade SQL Server). After updating, start the G-SIM primary server and wait for synchronization to finish. We also recommend having DebugView running before starting the server to check for SQL errors.

Any agents in your environment that do not run on the same hardware as the servers must be updated separately.

Upgrade SQL Server

If the G-SIM SQL database is on a different machine than the G-SIM server, stop the server before updating SQL Express. We also recommend having DebugView running before starting the server to check for SQL errors.

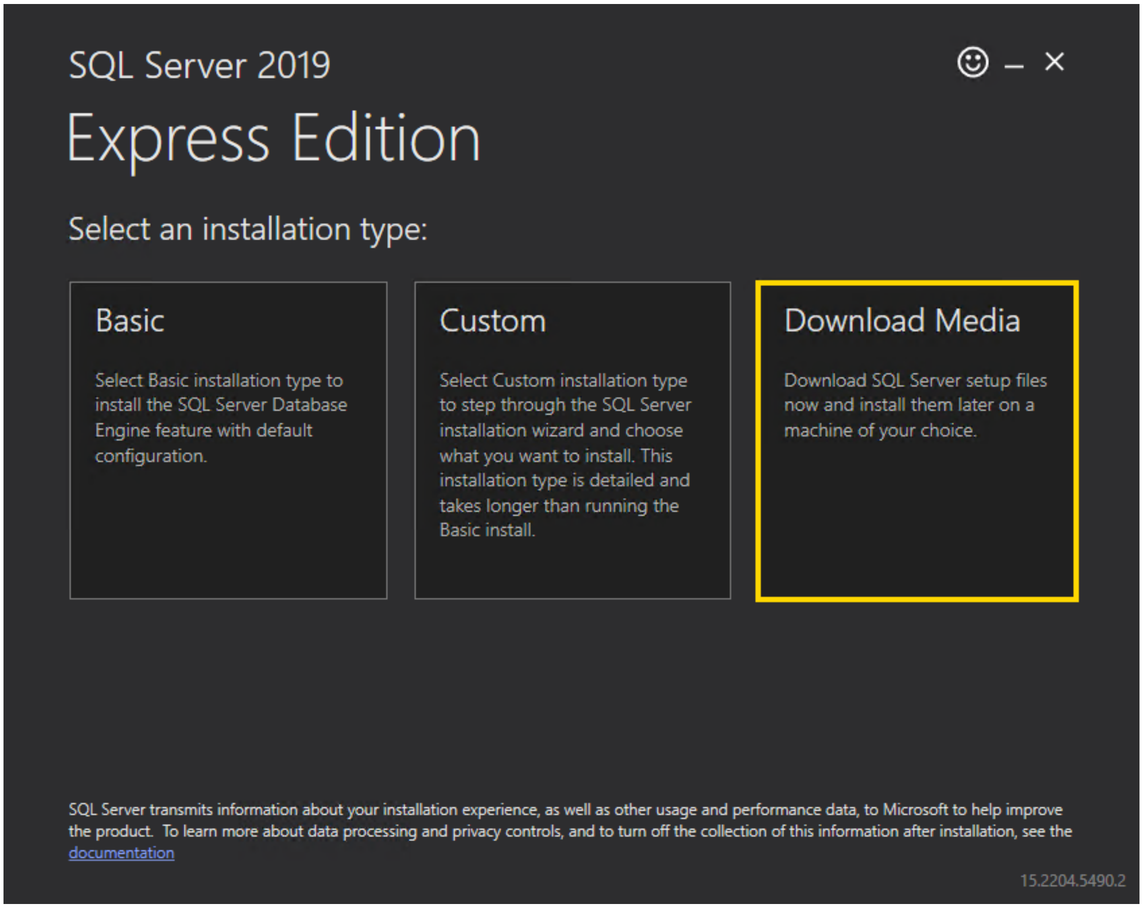
Upgrade SQL Server 2014 to 2019

SQL Server 2019 is supported starting from G-SIM version 9.3.0.

If the G-SIM SQL database is on a different machine than the G-SIM server, stop the server before updating SQL Express. We also recommend having DebugView running before starting the server to check for SQL errors.

How to upgrade the SQL Server 2014 to 2019:

1. Download the SQL Server 2019 Express from the Microsoft website (see here).
2. Run the downloaded file SQL2019-SSEI-Expr.exe.
3. In the Select an installation type dialog window, select Download Media.



SQL Server 2019

Express Edition

Select an installation type:

Basic

Select Basic installation type to install the SQL Server Database Engine feature with default configuration.

Custom

Select Custom installation type to step through the SQL Server installation wizard and choose what you want to install. This installation type is detailed and takes longer than running the Basic install.

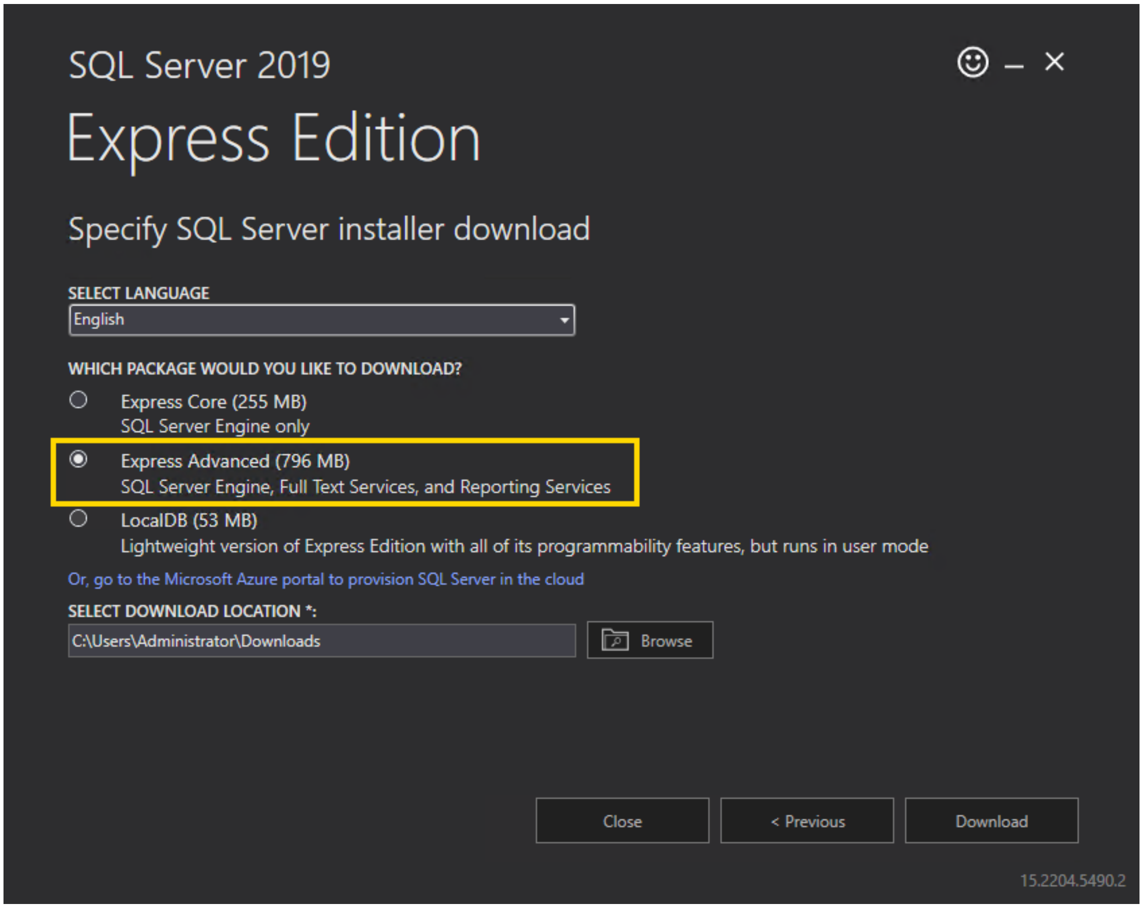
Download Media

Download SQL Server setup files now and install them later on a machine of your choice.

SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation

15.2204.5490.2

4. In the Specify SQL Server installer download dialog window, select the Express Advanced option for the download package and specify the language and the download location for the installer. Click Download.



SQL Server 2019

Express Edition

Specify SQL Server installer download

SELECT LANGUAGE

English

WHICH PACKAGE WOULD YOU LIKE TO DOWNLOAD?

○ Express Core (255 MB)
SQL Server Engine only

● Express Advanced (796 MB)
SQL Server Engine, Full Text Services, and Reporting Services

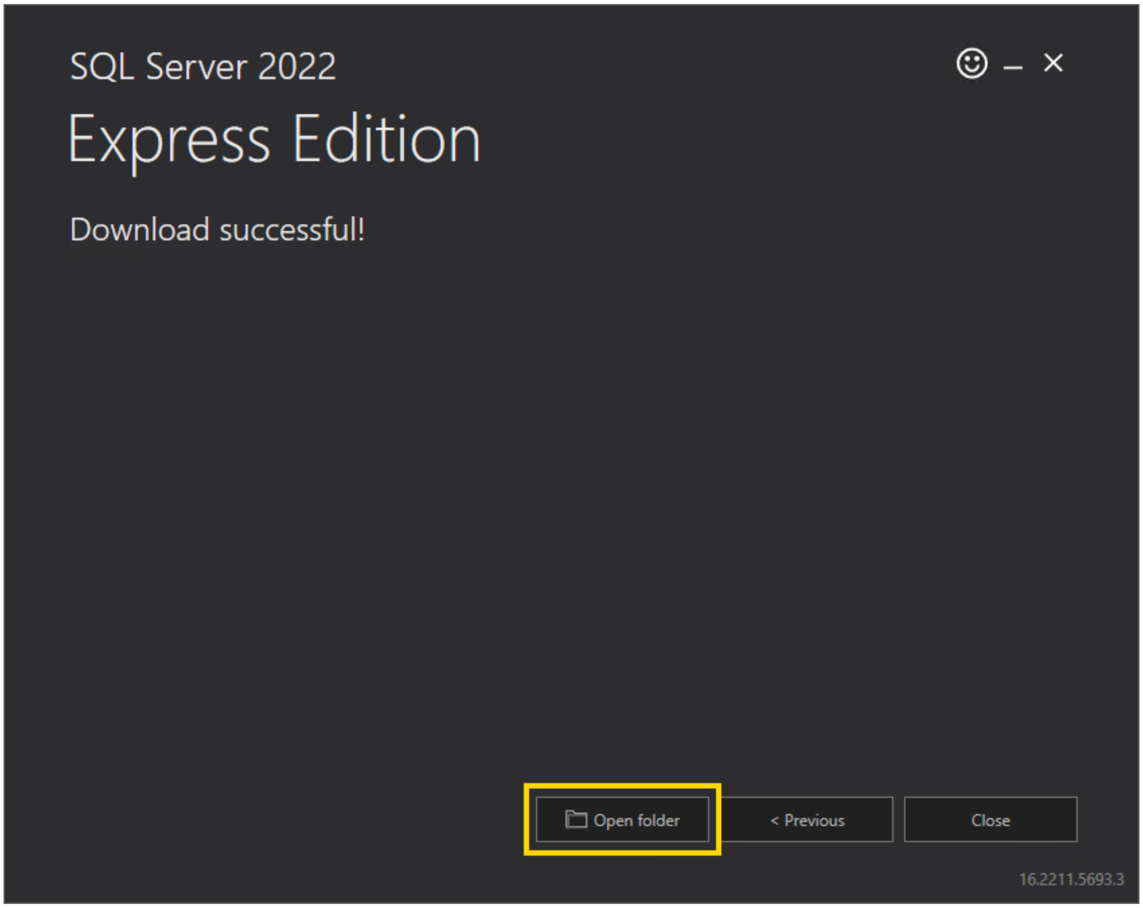
○ LocalDB (53 MB)
Lightweight version of Express Edition with all of its programmability features, but runs in user mode

Or, go to the Microsoft Azure portal to provision SQL Server in the cloud

SELECT DOWNLOAD LOCATION *:

C:\Users\Administrator\Downloads

5. In the **Download successful!** dialog window, click **Open folder**.



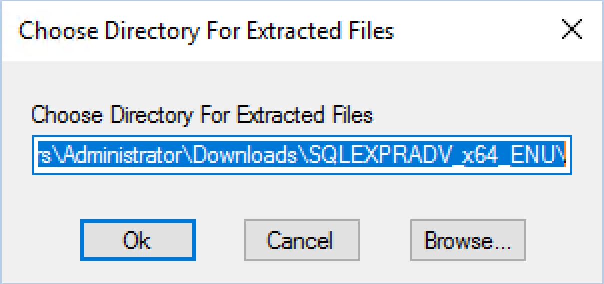
SQL Server 2022

Express Edition

Download successful!

6. Run the downloaded file **SQLEXPRADV_x64_ENU.exe**.

7. In the **Choose Directory For Extracted Files** dialog window, select the directory in which the installation files are to be extracted. Click **Ok**.

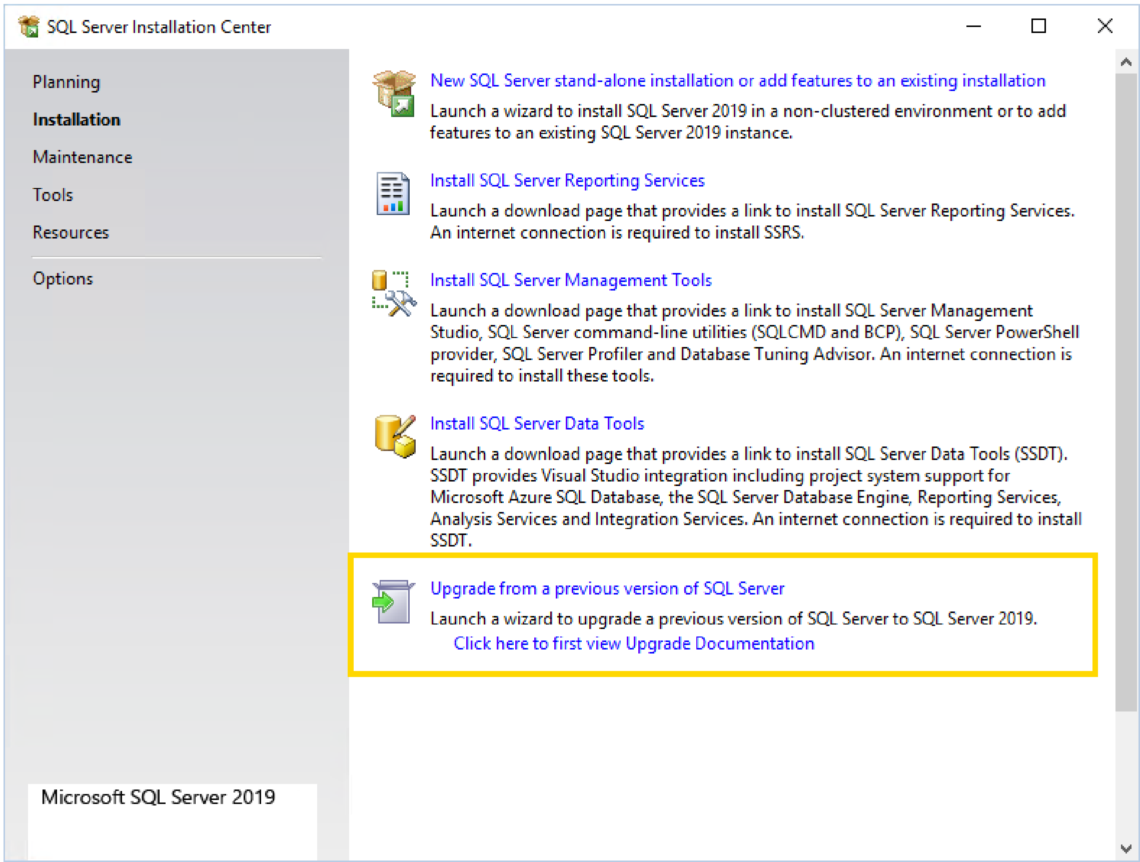


Choose Directory For Extracted Files

Choose Directory For Extracted Files

rs\Administrator\Downloads\SQLEXPRADV_x64_ENU\

8. In the **SQL Server Installation Center** dialog window, select **Upgrade from a previous version of SQL Server**. If the Installation Center does not start automatically, run the **setup.exe** file from the extracted files.



New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2019 in a non-clustered environment or to add features to an existing SQL Server 2019 instance.

Install SQL Server Reporting Services

Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.

Install SQL Server Management Tools

Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

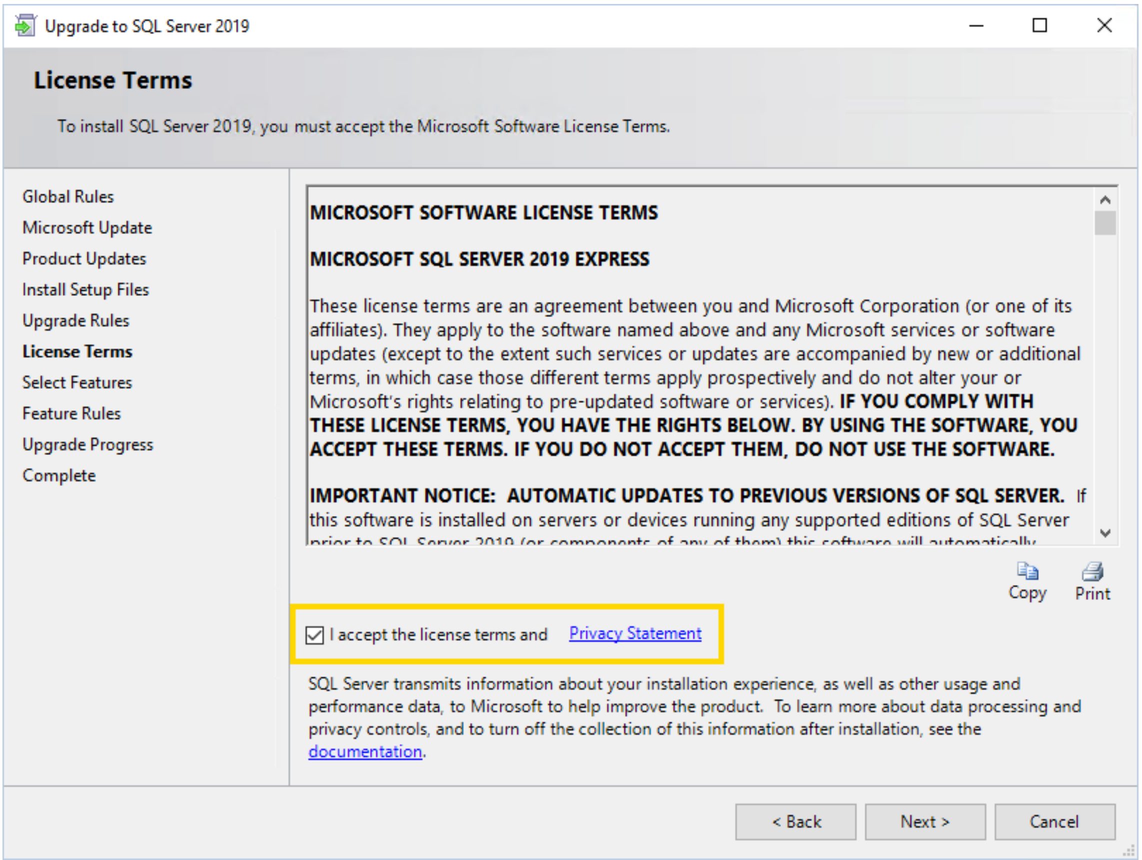
Install SQL Server Data Tools

Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

Upgrade from a previous version of SQL Server

Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019.
Click here to first view Upgrade Documentation

9. In the **License Terms** dialog window, select the **I accept the license terms and Privacy Statement** check box and click **Next**.



Upgrade to SQL Server 2019

License Terms

To install SQL Server 2019, you must accept the Microsoft Software License Terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2019 EXPRESS

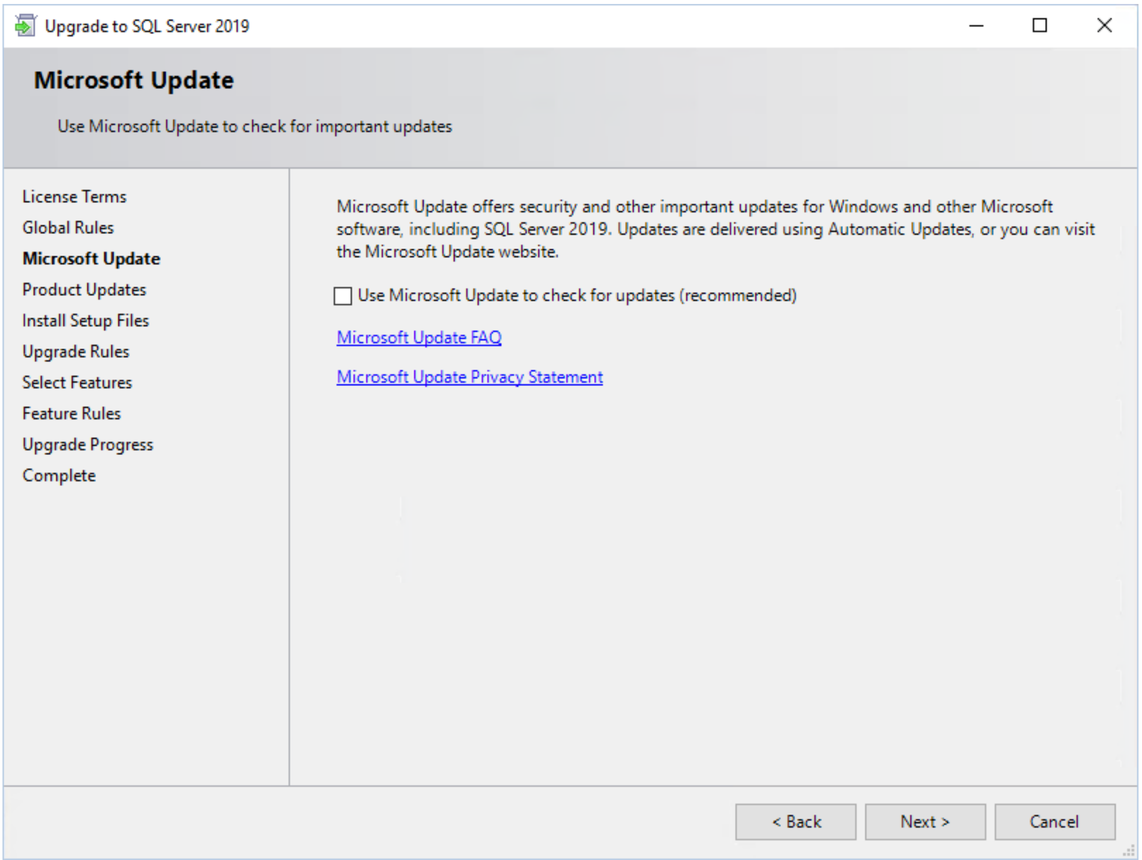
These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to the software named above and any Microsoft services or software updates (except to the extent such services or updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter your or Microsoft's rights relating to pre-updated software or services). **IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.**

IMPORTANT NOTICE: AUTOMATIC UPDATES TO PREVIOUS VERSIONS OF SQL SERVER. If this software is installed on servers or devices running any supported editions of SQL Server prior to SQL Server 2019 (or components of any of them) this software will automatically

☑ I accept the license terms and Privacy Statement

SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.

10. In the **Microsoft Update** dialog window, you do not have to select the check box. Click **Next**.



Upgrade to SQL Server 2019

Microsoft Update

Use Microsoft Update to check for important updates

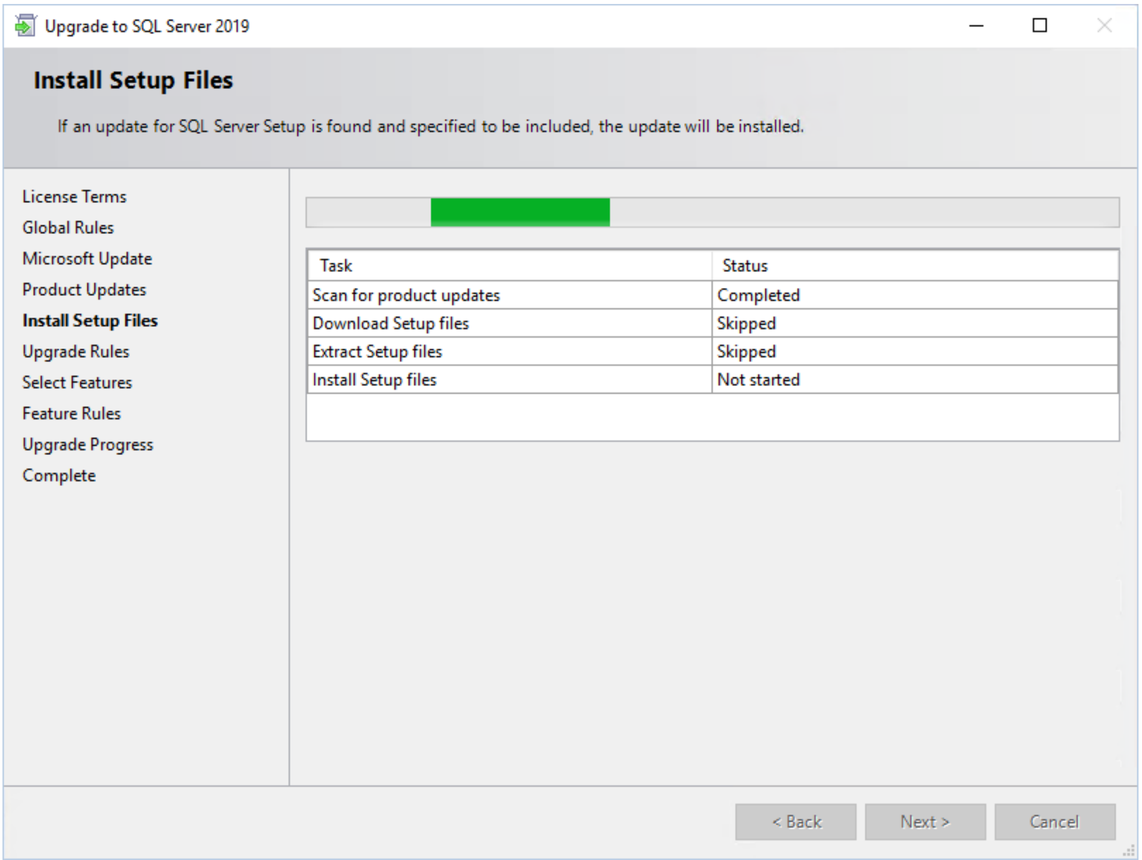
Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2019. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.

□ Use Microsoft Update to check for updates (recommended)

Microsoft Update FAQ

Microsoft Update Privacy Statement

11. In the **Install Setup Files** dialog window, click **Next** when the installation is completed.

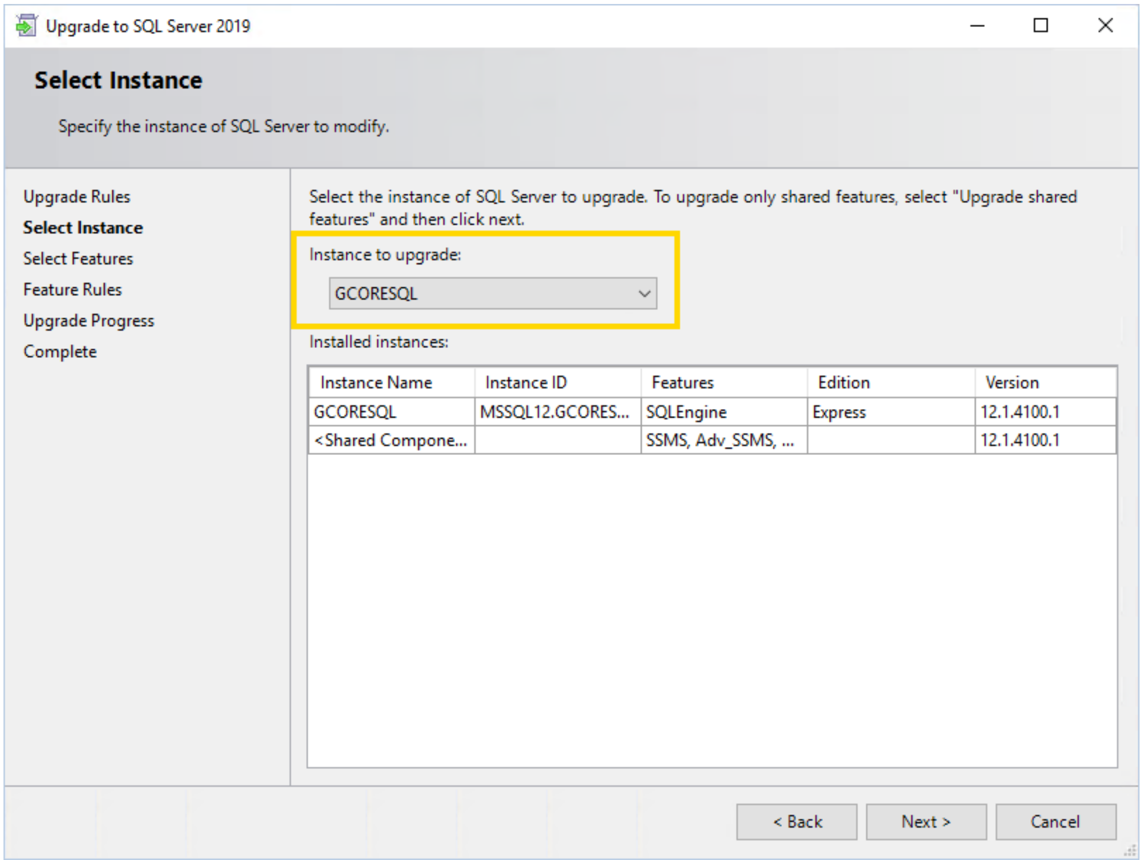


Install Setup Files

If an update for SQL Server Setup is found and specified to be included, the update will be installed.

Task	Status
Scan for product updates	Completed
Download Setup files	Skipped
Extract Setup files	Skipped
Install Setup files	Not started

12. In the **Select Instance** dialog window, select the instance to upgrade and click **Next**.



Select Instance

Specify the instance of SQL Server to modify.

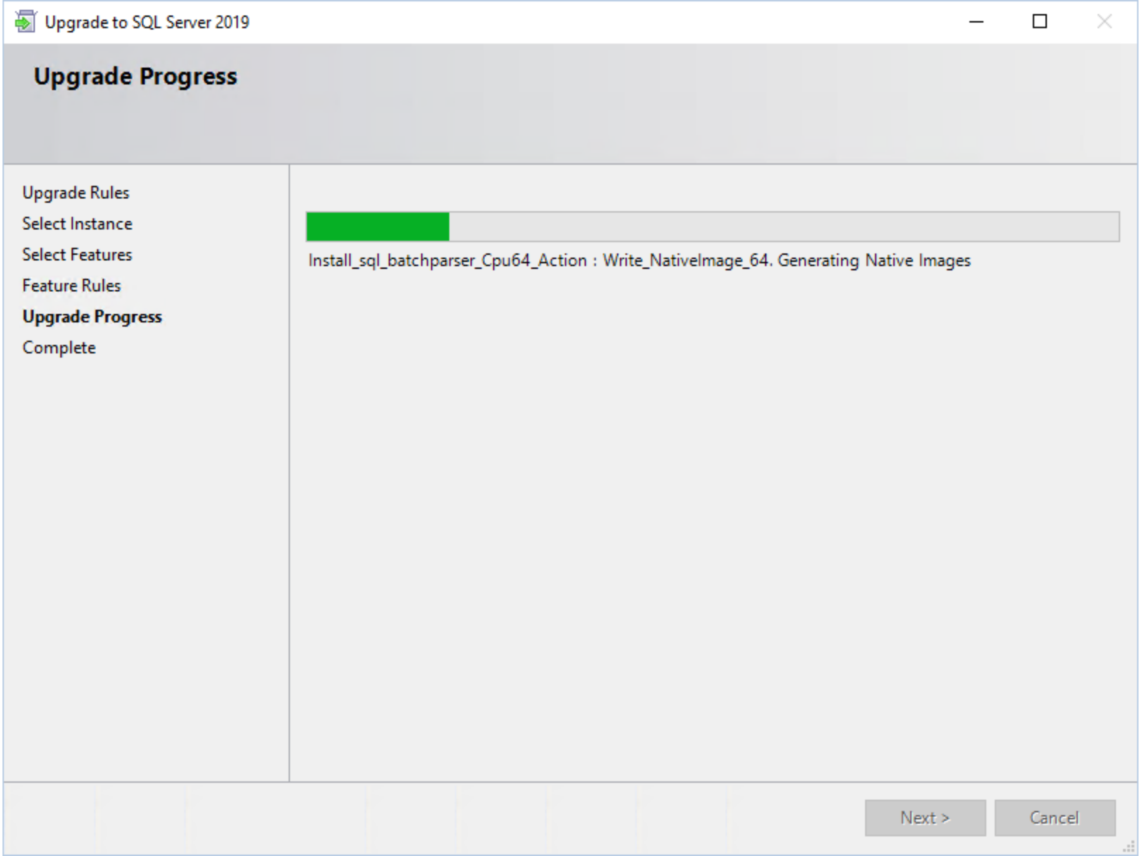
Select the instance of SQL Server to upgrade. To upgrade only shared features, select "Upgrade shared features" and then click next.

Instance to upgrade: GCORESQL

Installed instances:

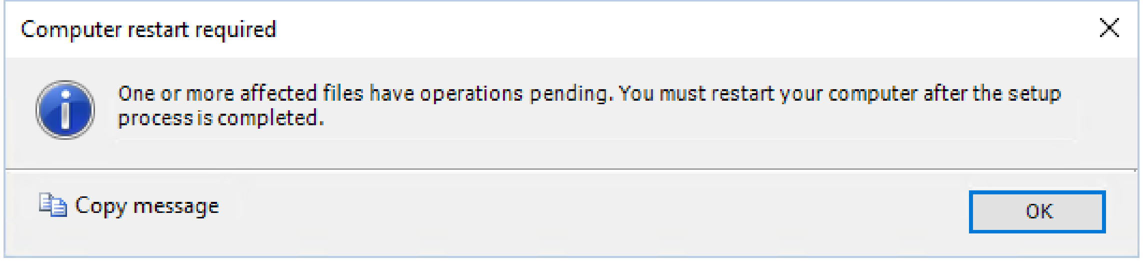
Instance Name	Instance ID	Features	Edition	Version
GCORESQL	MSSQL12.GCORES...	SQLEngine	Express	12.1.4100.1
<Shared Compone...		SSMS, Adv_SSMS, ...		12.1.4100.1

13. In the **Upgrade Progress** dialog window, click **Next** when the upgrade progress is completed.



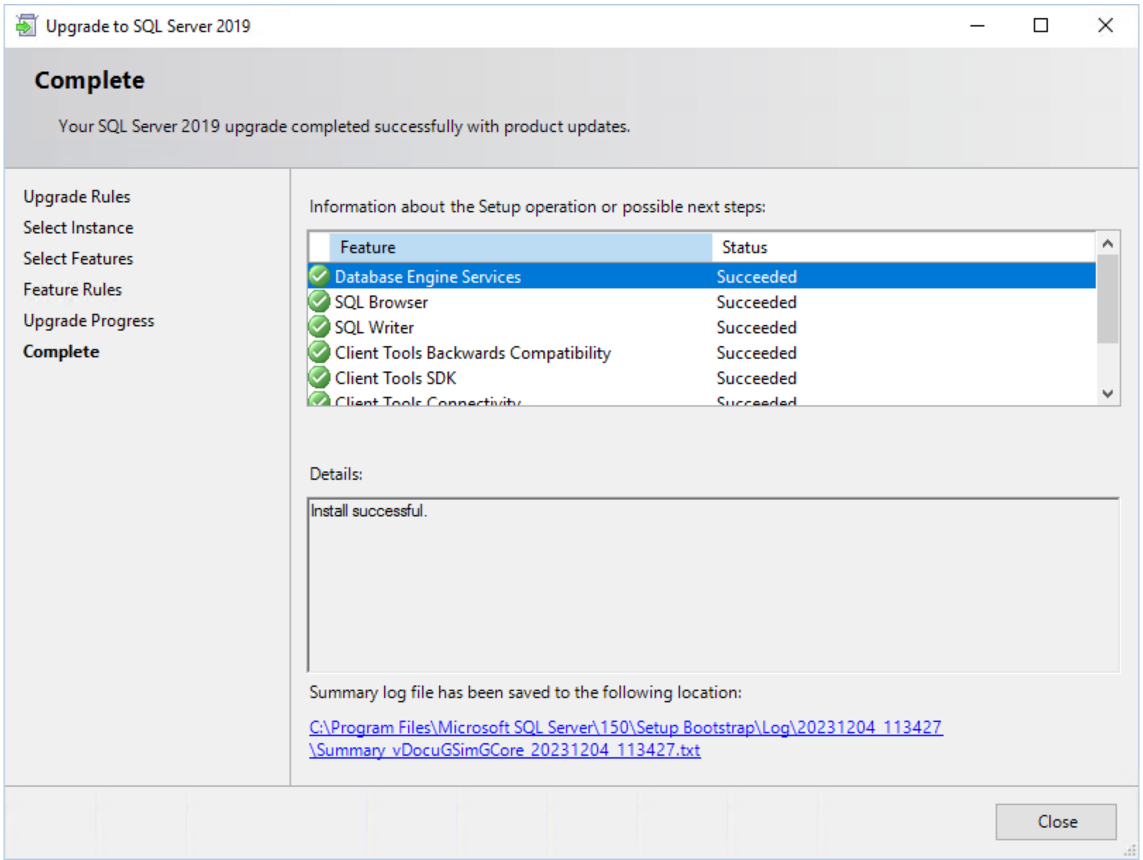
Install_sql_batchparser_Cpu64_Action : Write_NativeImage_64. Generating Native Images

14. Confirm the message **Computer restart required** with **OK**.



One or more affected files have operations pending. You must restart your computer after the setup process is completed.

15. In the **Complete** dialog window, click **Close**. The upgrade completed successfully.



Your SQL Server 2019 upgrade completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
Database Engine Services	Succeeded
SQL Browser	Succeeded
SQL Writer	Succeeded
Client Tools Backwards Compatibility	Succeeded
Client Tools SDK	Succeeded
Client Tools Connectivity	Succeeded

Details:

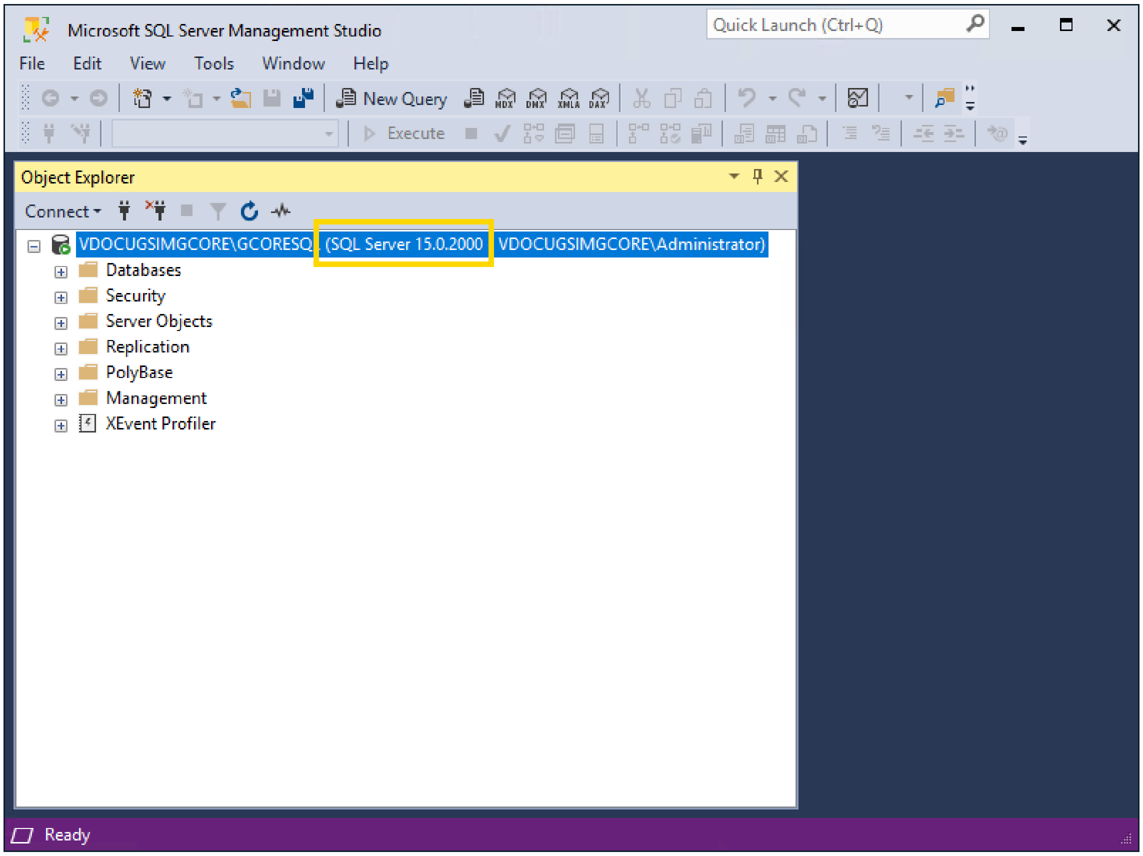
Install successful.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20231204_113427
\Summary_vDocuGSimGCore_20231204_113427.txt

16. Restart your computer.

17. You can check the version of your SQL Server in the **Microsoft SQL Server Management Studio**. Version 15.x is SQL Server 2019. You may need to install the tool manually, you can find the download file on the Microsoft website.



Next, install the latest cumulative security update for SQL Server 2019 to bring your server up to date and close possible security gaps (see Cumulative Update for SQL Server**).**

Upgrade SQL Server 2019 to 2022

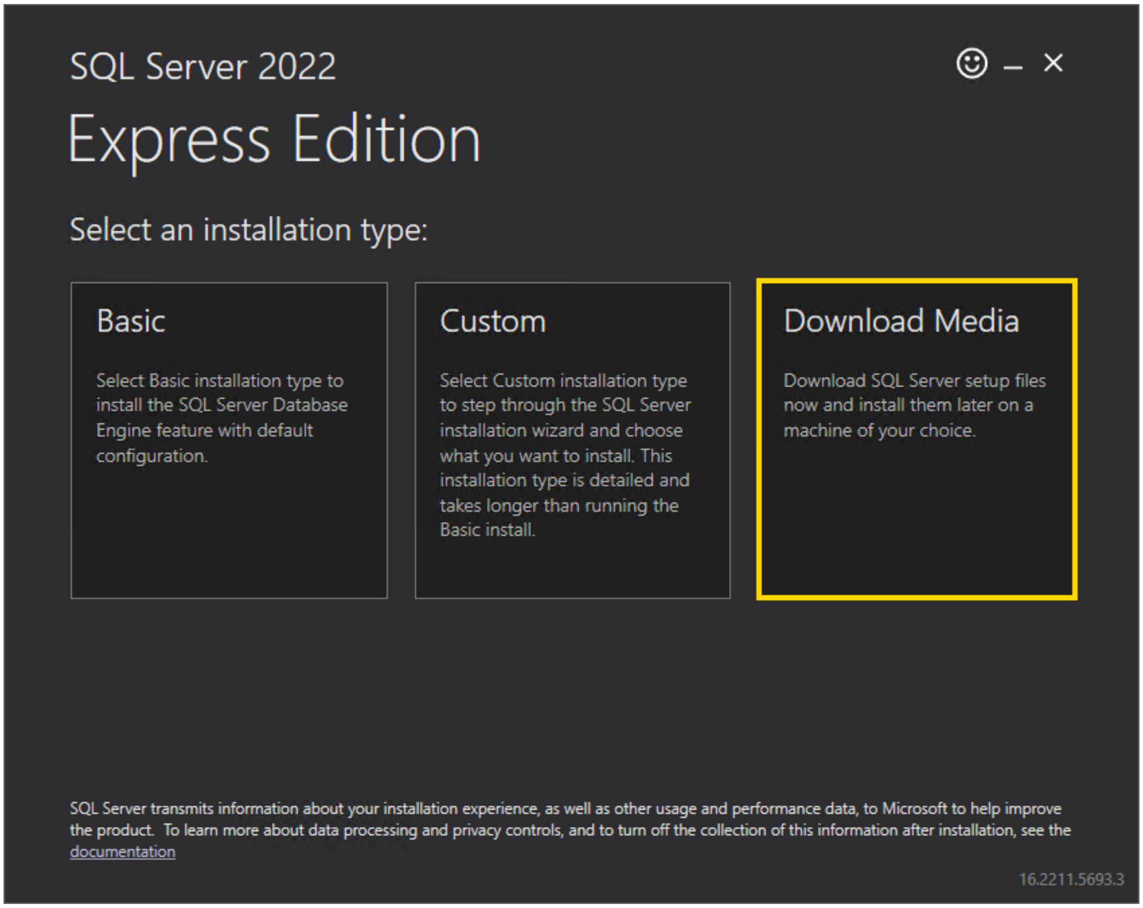
SQL Server 2022 is supported starting from G-SIM version 11.0.

If the G-SIM SQL database is on a different machine than the G-SIM server, stop the server before updating SQL Express. We also recommend having DebugView running before starting the server to check for SQL errors.

How to upgrade the SQL Server 2019 to 2022:

1. Download the **SQL Server 2022 Express** from the Microsoft website (see **here**).
2. Run the downloaded file **SQL2022-SSEI-Expr.exe**.

3. In the **Select an installation type** dialog window, select **Download Media**.



SQL Server 2022

Express Edition

Select an installation type:

Basic

Select Basic installation type to install the SQL Server Database Engine feature with default configuration.

Custom

Select Custom installation type to step through the SQL Server installation wizard and choose what you want to install. This installation type is detailed and takes longer than running the Basic install.

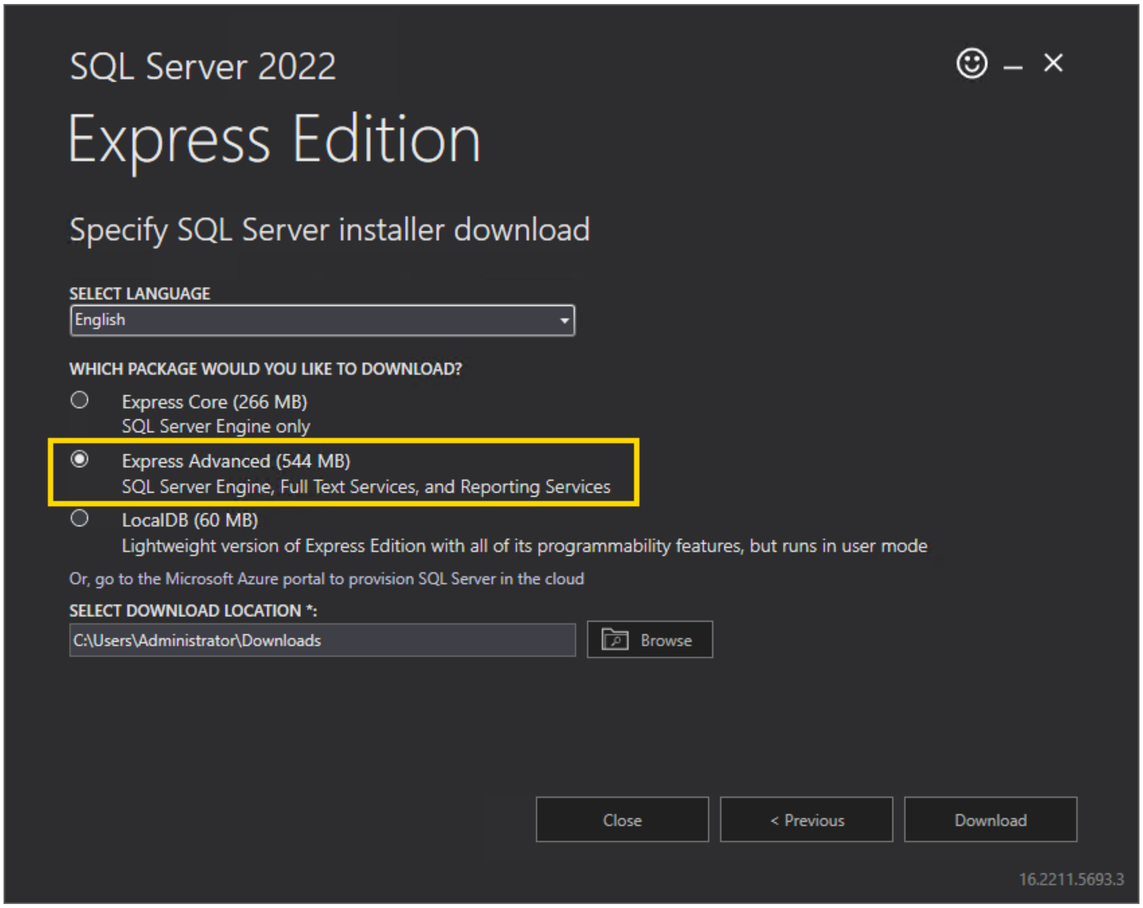
Download Media

Download SQL Server setup files now and install them later on a machine of your choice.

SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation

16.2211.5693.3

4. In the **Specify SQL Server installer download** dialog window, select the **Express Advanced** option for the download package and specify the language and the download location for the installer. Click **Download**.



SQL Server 2022

Express Edition

Specify SQL Server installer download

SELECT LANGUAGE: English

WHICH PACKAGE WOULD YOU LIKE TO DOWNLOAD?

○ Express Core (266 MB)
SQL Server Engine only

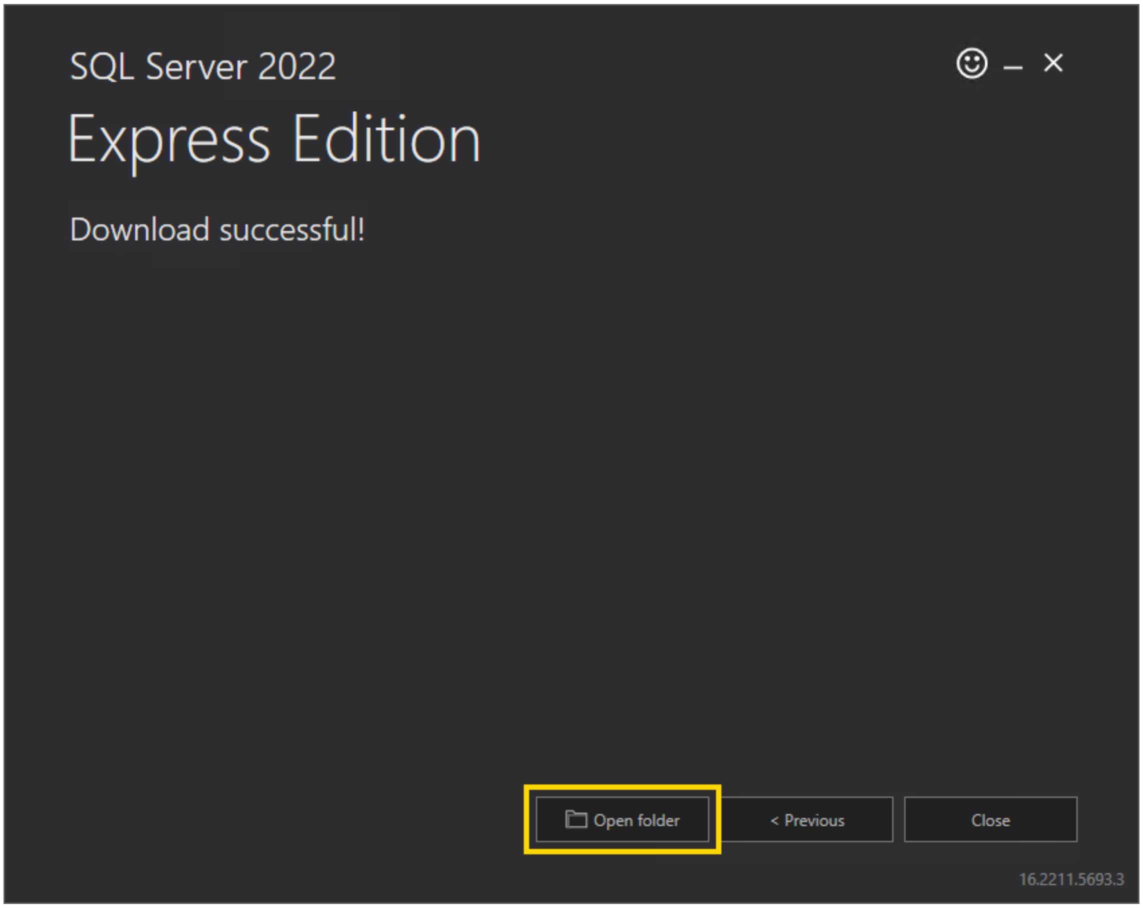
● Express Advanced (544 MB)
SQL Server Engine, Full Text Services, and Reporting Services

○ LocalDB (60 MB)
Lightweight version of Express Edition with all of its programmability features, but runs in user mode

Or, go to the Microsoft Azure portal to provision SQL Server in the cloud

SELECT DOWNLOAD LOCATION *: C:\Users\Administrator\Downloads

5. In the **Download successful!** dialog window, click **Open folder**.

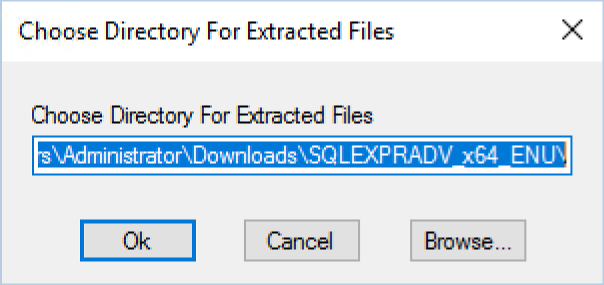

SQL Server 2022

Express Edition

Download successful!

6. Run the downloaded file **SQLEXPRADV_x64_ENU.exe**.

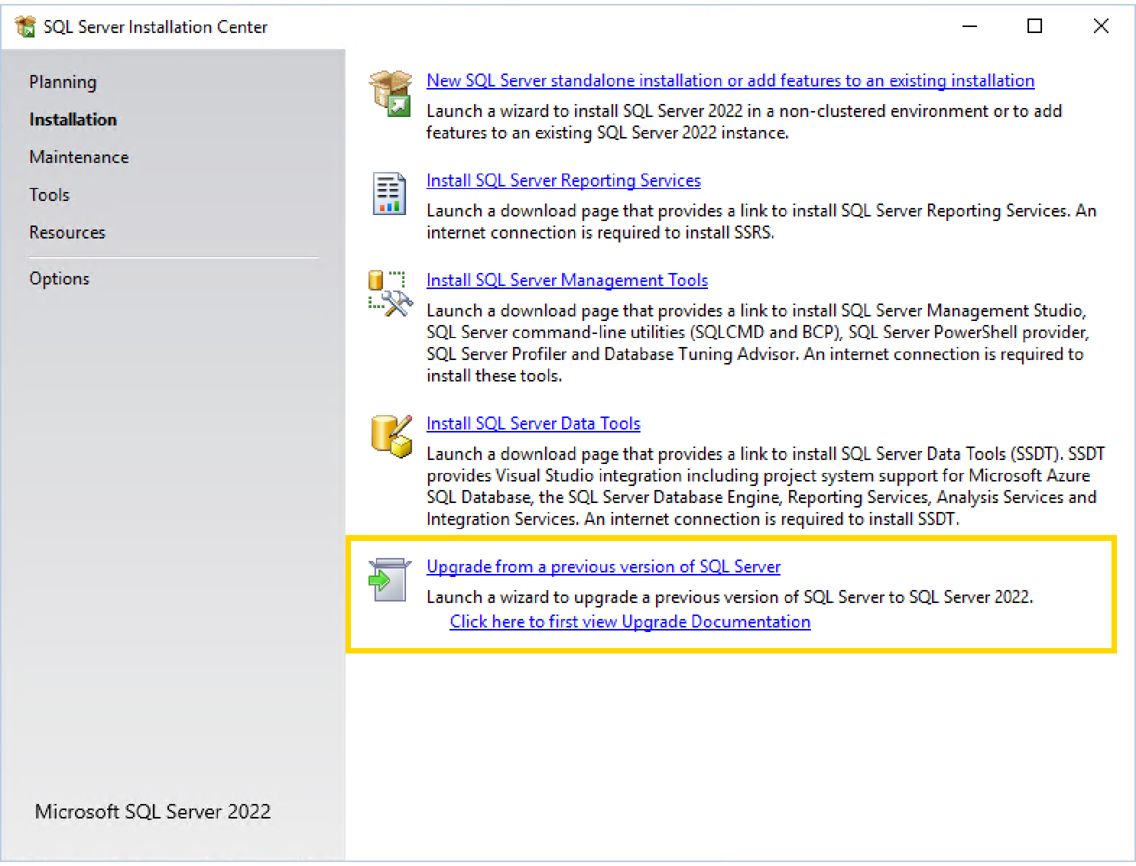
7. In the **Choose Directory For Extracted Files** dialog window, select the directory in which the installation files are to be extracted. Click **Ok**.


Choose Directory For Extracted Files

Choose Directory For Extracted Files

rs\Administrator\Downloads\SQLEXPRADV_x64_ENU\

8. In the **SQL Server Installation Center** dialog window, select **Upgrade from a previous version of SQL Server**. If the Installation Center does not start automatically, run the **setup.exe** file from the extracted files.



New SQL Server standalone installation or add features to an existing installation

Launch a wizard to install SQL Server 2022 in a non-clustered environment or to add features to an existing SQL Server 2022 instance.

Install SQL Server Reporting Services

Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.

Install SQL Server Management Tools

Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

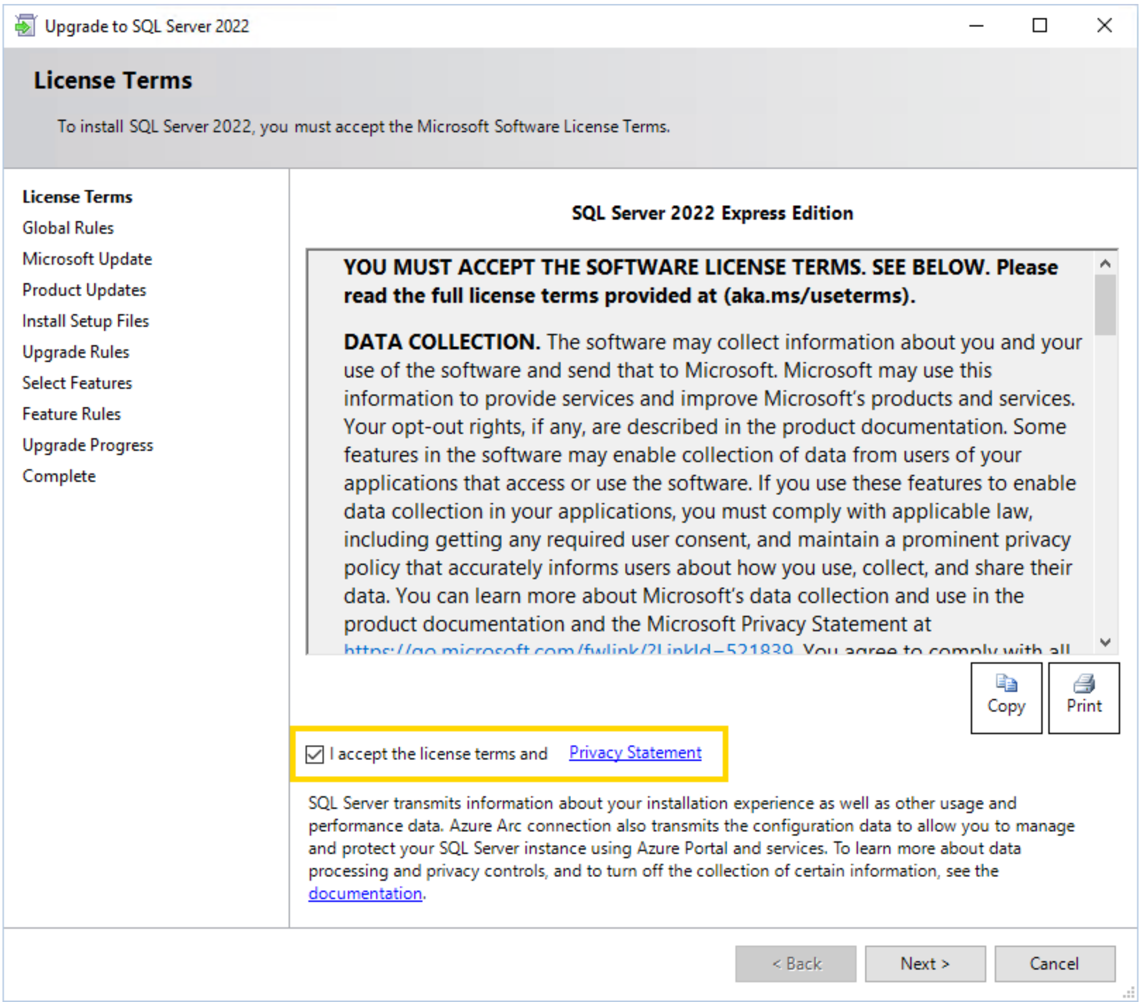
Install SQL Server Data Tools

Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

Upgrade from a previous version of SQL Server

Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2022.
Click here to first view Upgrade Documentation

9. In the **License Terms** dialog window, select the **I accept the license terms and Privacy Statement** check box and click **Next**.



License Terms

To install SQL Server 2022, you must accept the Microsoft Software License Terms.

SQL Server 2022 Express Edition

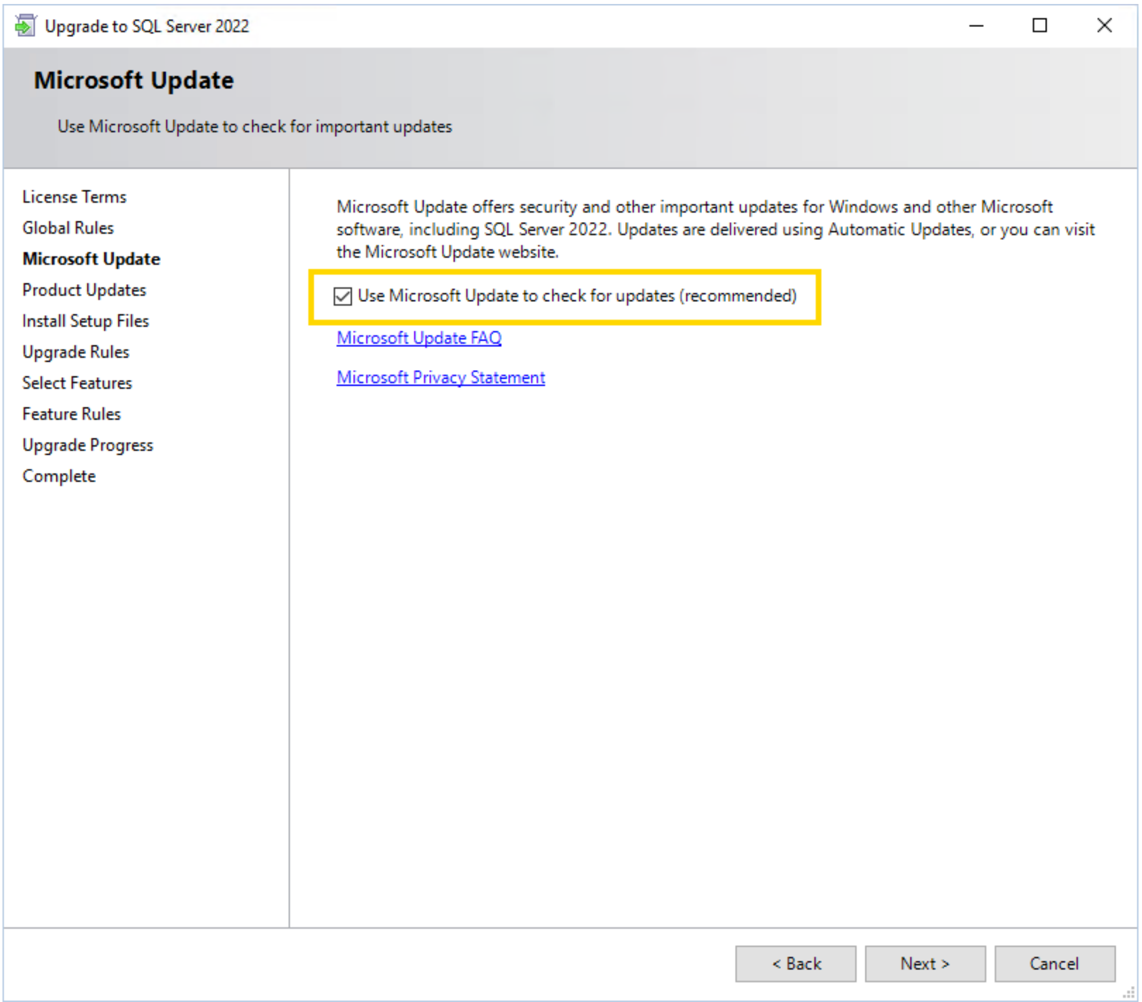
YOU MUST ACCEPT THE SOFTWARE LICENSE TERMS. SEE BELOW. Please read the full license terms provided at (aka.ms/useterms).

DATA COLLECTION. The software may collect information about you and your use of the software and send that to Microsoft. Microsoft may use this information to provide services and improve Microsoft's products and services. Your opt-out rights, if any, are described in the product documentation. Some features in the software may enable collection of data from users of your applications that access or use the software. If you use these features to enable data collection in your applications, you must comply with applicable law, including getting any required user consent, and maintain a prominent privacy policy that accurately informs users about how you use, collect, and share their data. You can learn more about Microsoft's data collection and use in the product documentation and the Microsoft Privacy Statement at https://go.microsoft.com/fwlink/?LinkId=521839. You agree to comply with all

☑ I accept the license terms and Privacy Statement

SQL Server transmits information about your installation experience as well as other usage and performance data. Azure Arc connection also transmits the configuration data to allow you to manage and protect your SQL Server instance using Azure Portal and services. To learn more about data processing and privacy controls, and to turn off the collection of certain information, see the documentation.

10. In the **Microsoft Update** dialog window, select the **Use Microsoft Update to check for updates** check box and click **Next**.



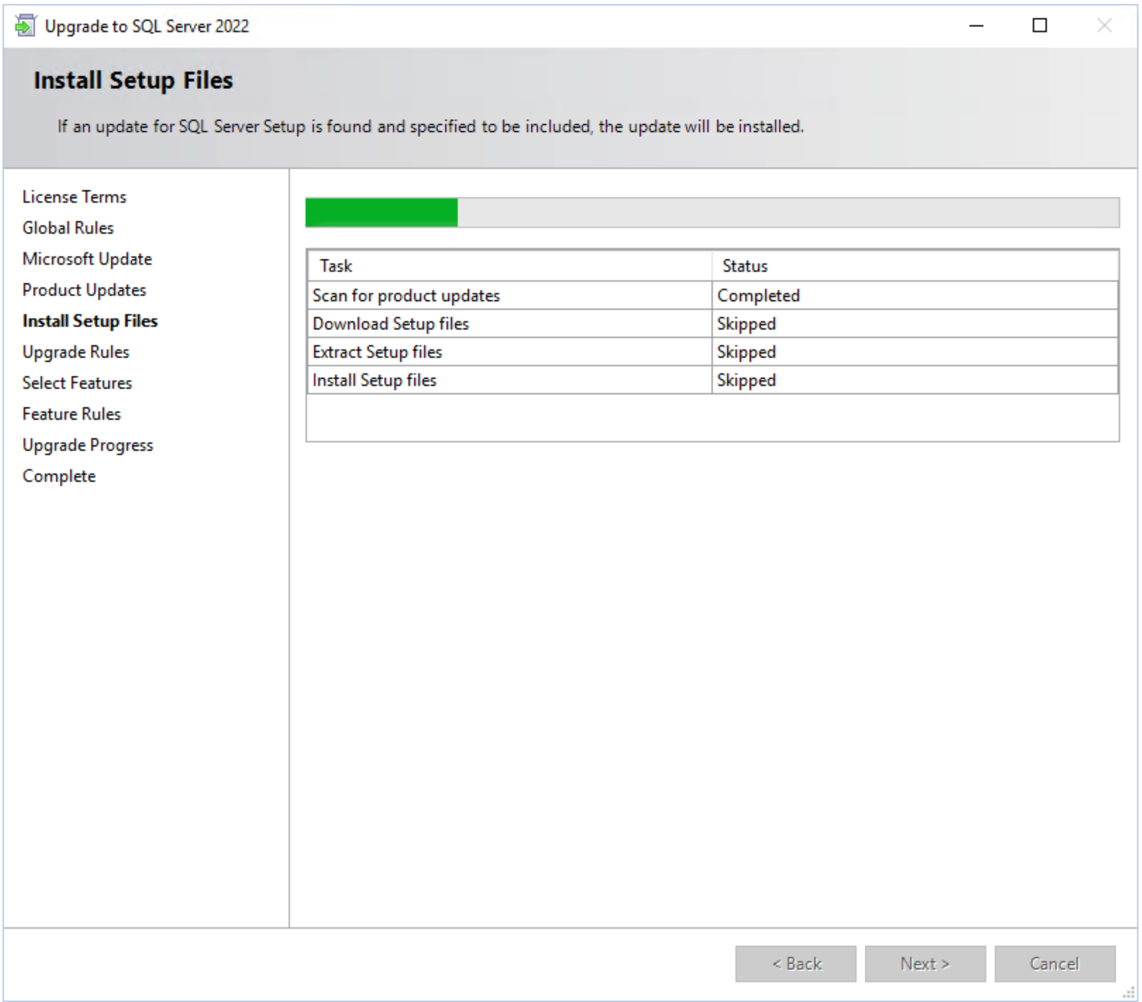
Microsoft Update

Use Microsoft Update to check for important updates

Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2022. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.

☑ Use Microsoft Update to check for updates (recommended)

11. In the **Install Setup Files** dialog window, click **Next** when the installation is completed.

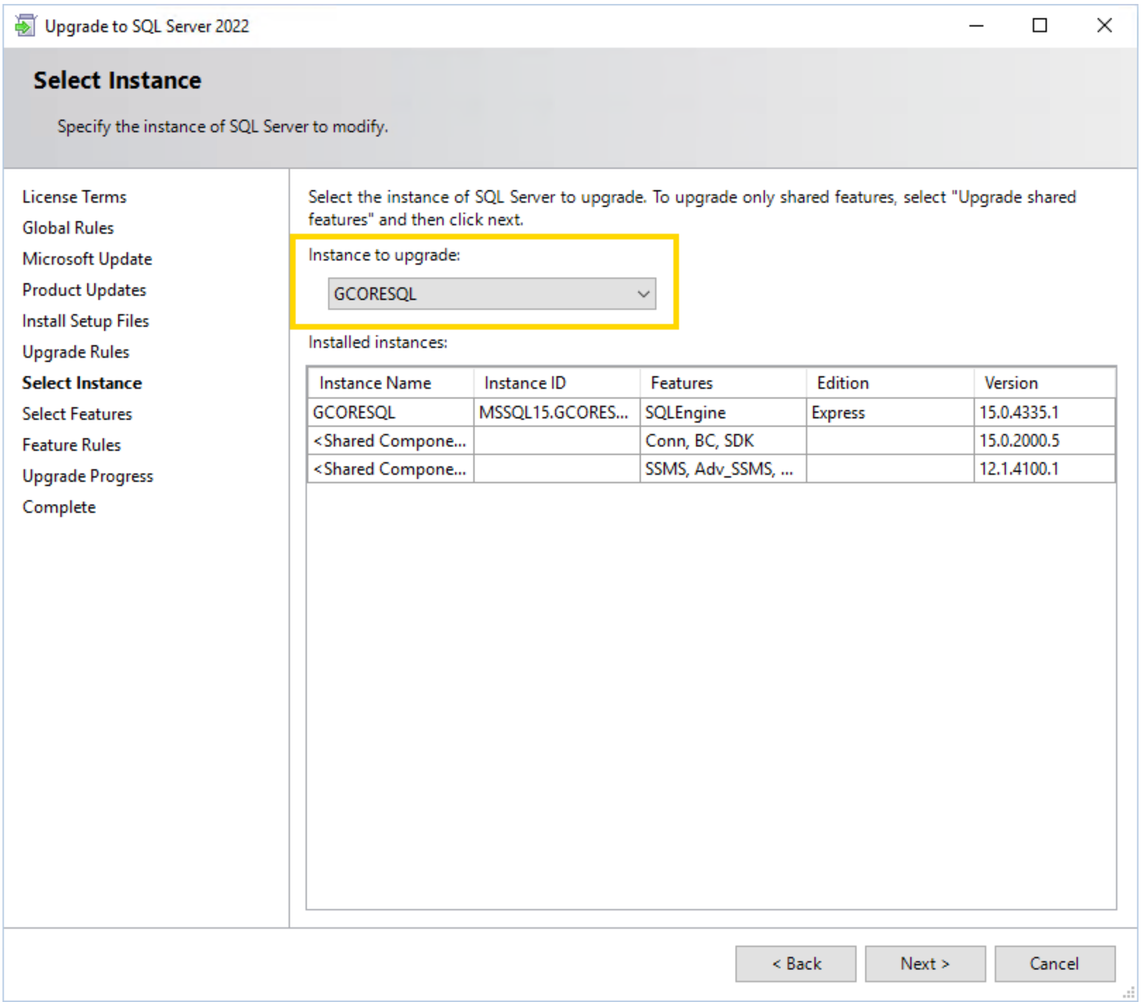


Install Setup Files

If an update for SQL Server Setup is found and specified to be included, the update will be installed.

Task	Status
Scan for product updates	Completed
Download Setup files	Skipped
Extract Setup files	Skipped
Install Setup files	Skipped

12. In the **Select Instance** dialog window, select the instance to upgrade and click **Next**.



Select Instance

Specify the instance of SQL Server to modify.

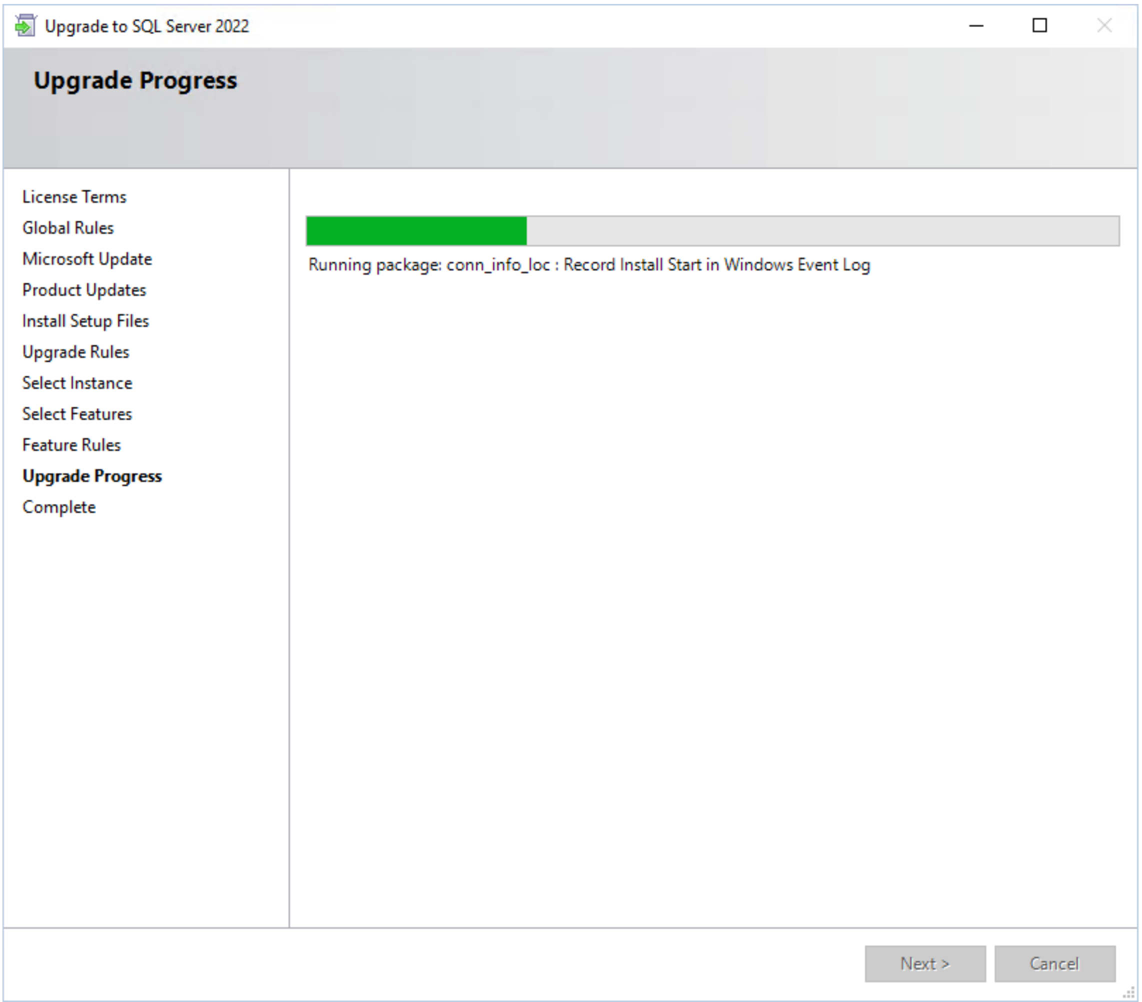
Select the instance of SQL Server to upgrade. To upgrade only shared features, select "Upgrade shared features" and then click next.

Instance to upgrade: GCORESQL

Installed instances:

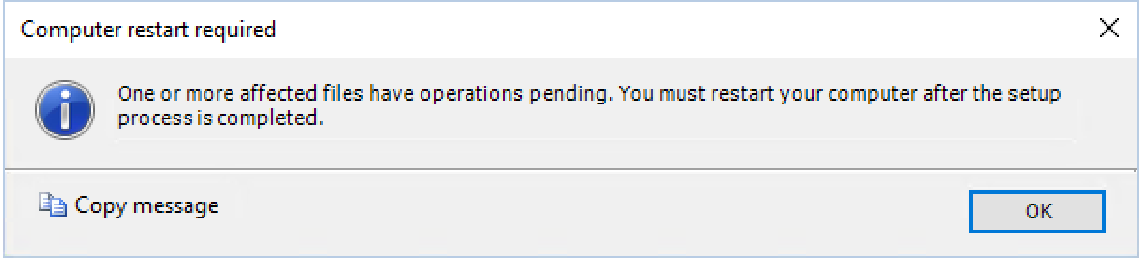
Instance Name	Instance ID	Features	Edition	Version
GCORESQL	MSSQL15.GCORES...	SQLEngine	Express	15.0.4335.1
<Shared Compone...		Conn, BC, SDK		15.0.2000.5
<Shared Compone...		SSMS, Adv_SSMS, ...		12.1.4100.1

13. In the **Upgrade Progress** dialog window, click **Next** when the upgrade progress is completed.



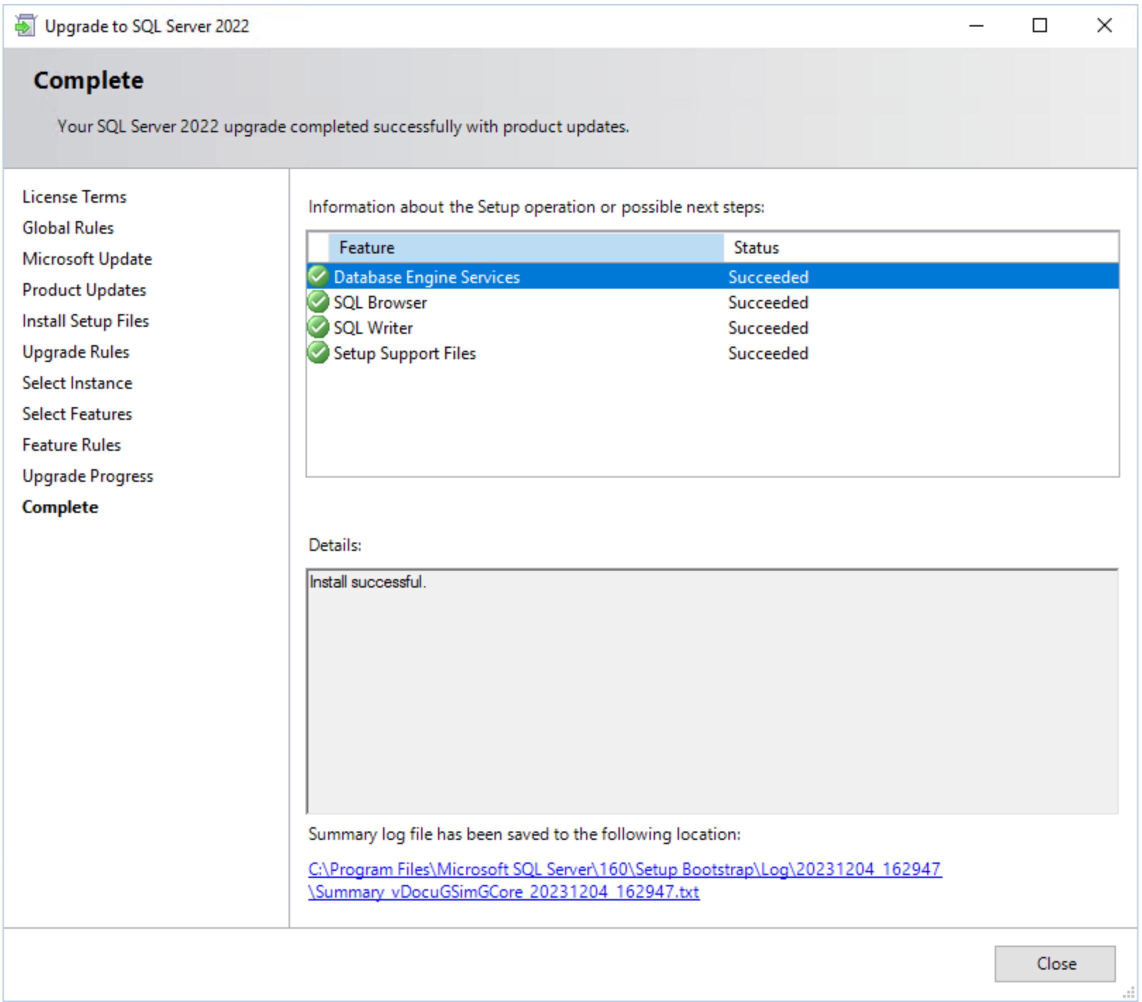
Running package: conn_info_loc : Record Install Start in Windows Event Log

14. Confirm the message **Computer restart required** with **OK**.



One or more affected files have operations pending. You must restart your computer after the setup process is completed.

15. In the **Complete** dialog window, click **Close**. The upgrade completed successfully.



Complete

Your SQL Server 2022 upgrade completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
✓ Database Engine Services	Succeeded
✓ SQL Browser	Succeeded
✓ SQL Writer	Succeeded
✓ Setup Support Files	Succeeded

Details:

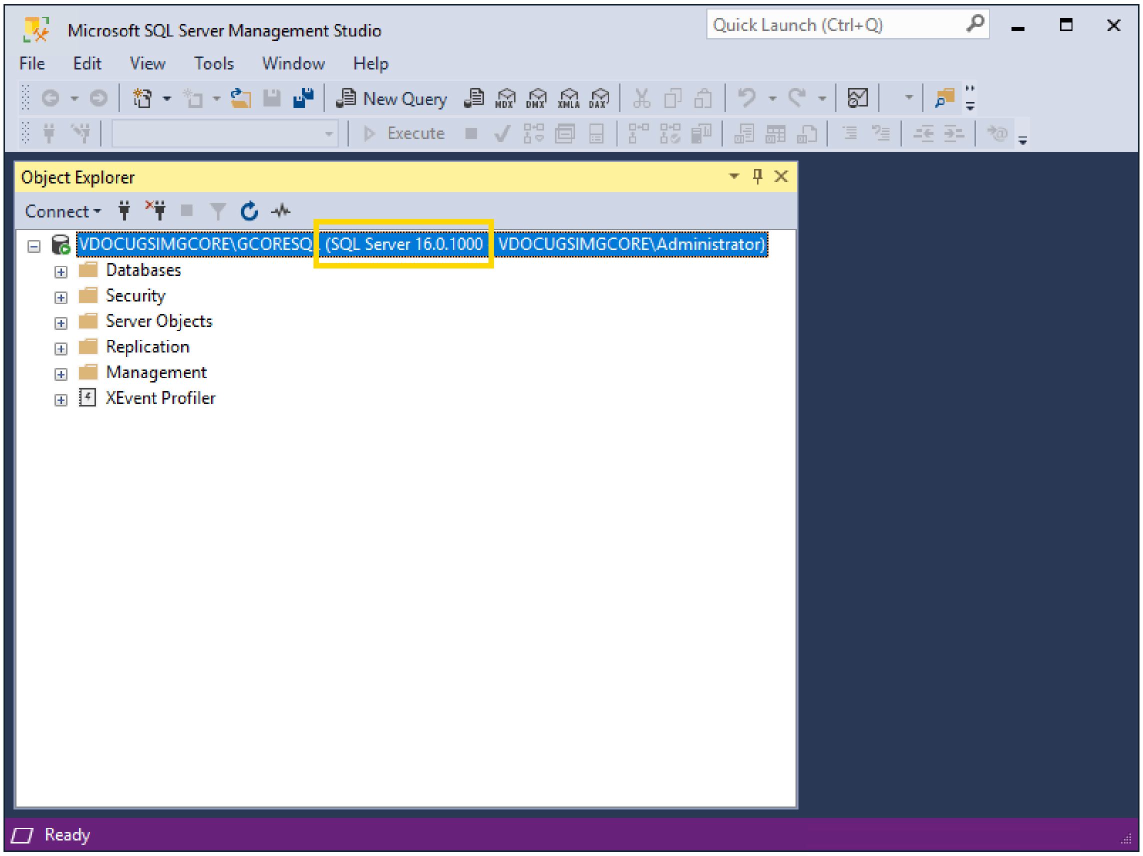
Install successful.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\160\Setup Bootstrap\Log\20231204_162947
\Summary_vDocuGSimGCore_20231204_162947.txt

16. Restart your computer.

17. You can check the version of your SQL Server in the **Microsoft SQL Server Management Studio**. Version 16.x is SQL Server 2022. You may need to install the tool manually, you can find the download file on the Microsoft website.


Microsoft SQL Server Management Studio
Quick Launch (Ctrl+Q)
File Edit View Tools Window Help
New Query
Execute
Object Explorer
Connect
VDOCUGSIMGCORE\GCORESQ (SQL Server 16.0.1000 VDOCUGSIMGCORE\Administrator)
Databases
Security
Server Objects
Replication
Management
XEvent Profiler
Ready

Next, install the latest cumulative security update for SQL Server 2022 to bring your server up to date and close possible security gaps (see Cumulative Update for SQL Server**).**

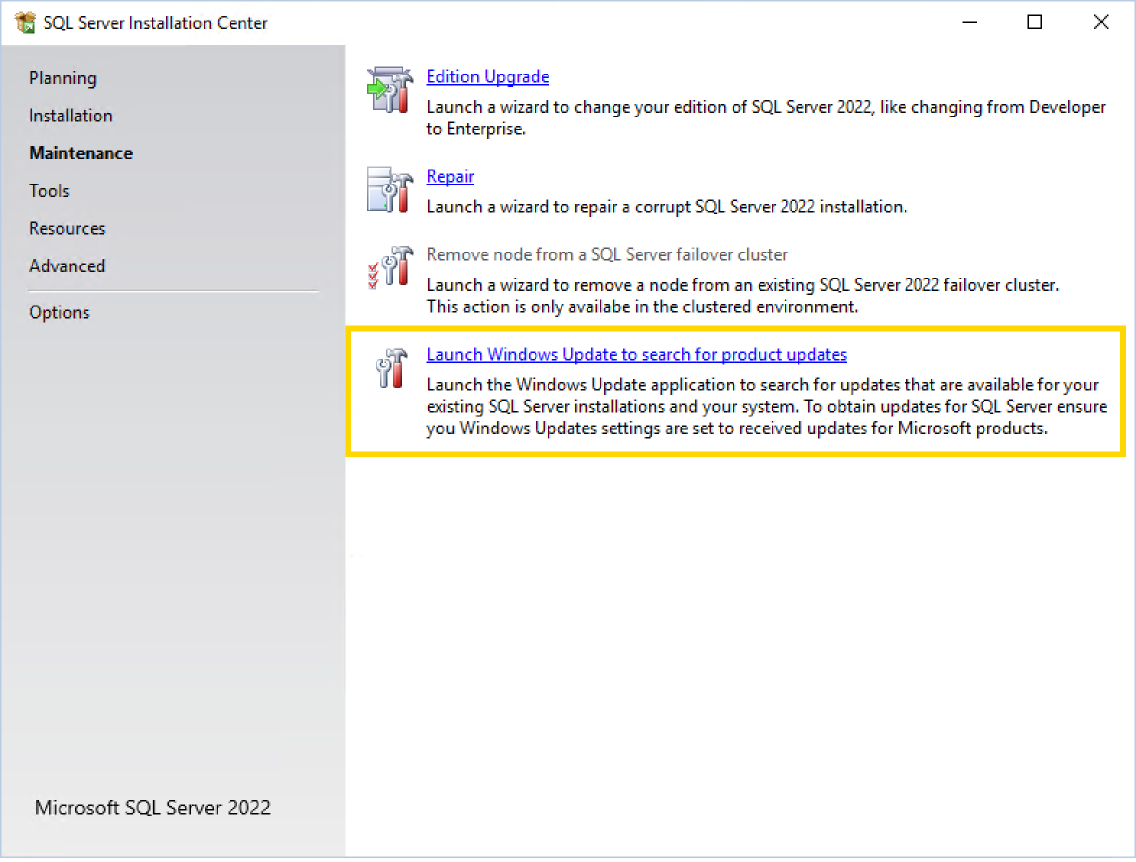
Cumulative Update for SQL Server

Install the latest cumulative security update for your SQL Server version to bring your server up to date and close possible security gaps.

How to install the latest cumulative update for your SQL Server:

1. Open the SQL Server Installation Center.

2. Open the Maintenance tab and select Launch Windows Update to search for product updates. An internet connection is required.



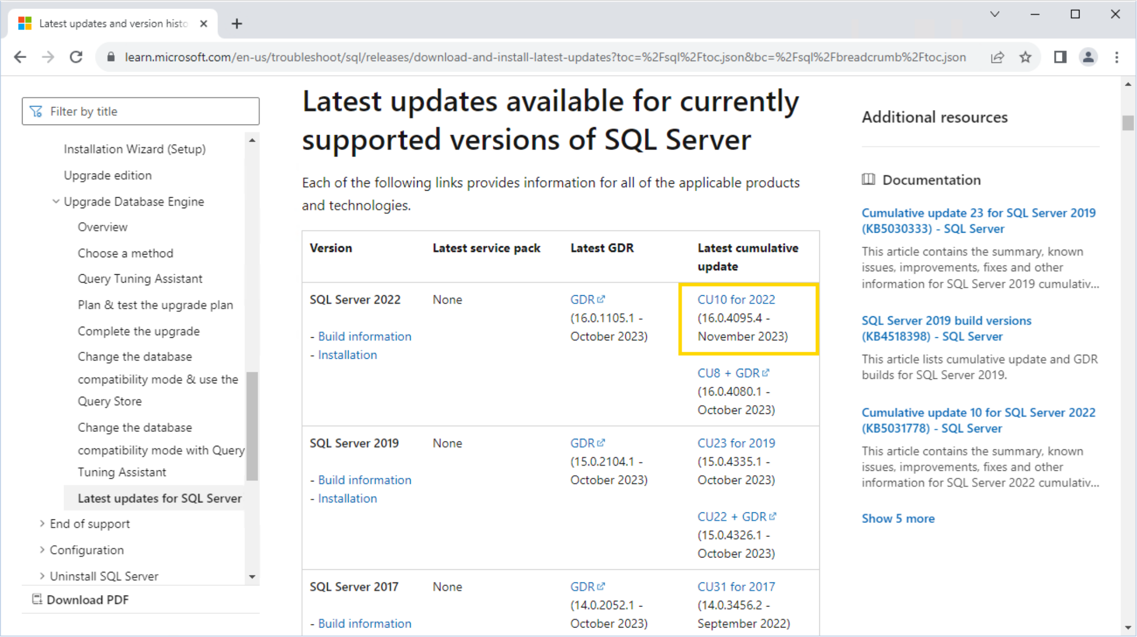
Edition Upgrade
Launch a wizard to change your edition of SQL Server 2022, like changing from Developer to Enterprise.

Repair
Launch a wizard to repair a corrupt SQL Server 2022 installation.

Remove node from a SQL Server failover cluster
Launch a wizard to remove a node from an existing SQL Server 2022 failover cluster. This action is only availabe in the clustered environment.

Launch Windows Update to search for product updates
Launch the Windows Update application to search for updates that are available for your existing SQL Server installations and your system. To obtain updates for SQL Server ensure you Windows Updates settings are set to received updates for Microsoft products.

3. The Microsoft website opens. Select the latest cumulative update for the your SQL Server from the table in the **Latest updates available for currently supported versions of SQL Server** section.


Latest updates and version histo
learn.microsoft.com/en-us/troubleshoot/sql/releases/download-and-install-latest-updates?toc=%2Fsql%2Ftoc.json&bc=%2Fsql%2Fbreadcrumb%2Ftoc.json
Filter by title
Installation Wizard (Setup)
Upgrade edition
Upgrade Database Engine
Overview
Choose a method
Query Tuning Assistant
Plan & test the upgrade plan
Complete the upgrade
Change the database compatibility mode & use the Query Store
Change the database compatibility mode with Query Tuning Assistant
Latest updates for SQL Server
End of support
Configuration
Uninstall SQL Server
Download PDF

Latest updates available for currently supported versions of SQL Server

Each of the following links provides information for all of the applicable products and technologies.

Version	Latest service pack	Latest GDR	Latest cumulative update
SQL Server 2022 - Build information - Installation	None	GDR (16.0.1105.1 - October 2023)	CU10 for 2022 (16.0.4095.4 - November 2023) CU8 + GDR (16.0.4080.1 - October 2023)
SQL Server 2019 - Build information - Installation	None	GDR (15.0.2104.1 - October 2023)	CU23 for 2019 (15.0.4335.1 - October 2023) CU22 + GDR (15.0.4326.1 - October 2023)
SQL Server 2017 - Build information	None	GDR (14.0.2052.1 - October 2023)	CU31 for 2017 (14.0.3456.2 - September 2022)

Additional resources

Documentation

Cumulative update 23 for SQL Server 2019 (KB5030333) - SQL Server

This article contains the summary, known issues, improvements, fixes and other information for SQL Server 2019 cumulativ...

SQL Server 2019 build versions (KB4518398) - SQL Server

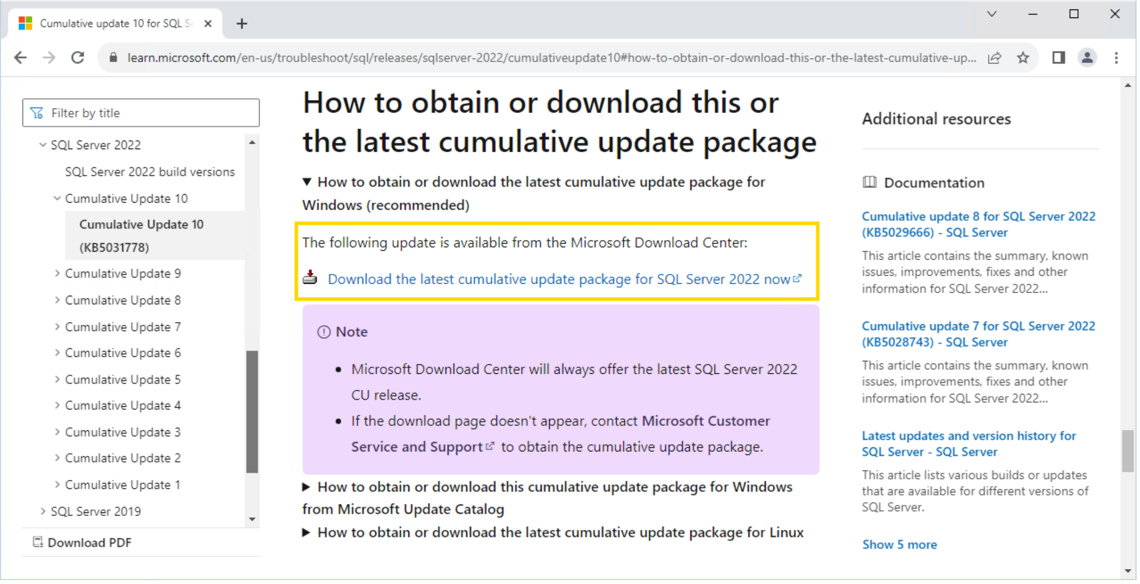
This article lists cumulative update and GDR builds for SQL Server 2019.

Cumulative update 10 for SQL Server 2022 (KB5031778) - SQL Server

This article contains the summary, known issues, improvements, fixes and other information for SQL Server 2022 cumulativ...

Show 5 more

4. The website of the selected update opens. Click the download link in the **How to obtain or download this or the latest cumulative update package** section.



How to obtain or download this or the latest cumulative update package

▼ How to obtain or download the latest cumulative update package for Windows (recommended)

The following update is available from the Microsoft Download Center:

Download the latest cumulative update package for SQL Server 2022 now

ⓘ Note

- Microsoft Download Center will always offer the latest SQL Server 2022 CU release.
- If the download page doesn't appear, contact Microsoft Customer Service and Support to obtain the cumulative update package.

▶ How to obtain or download this cumulative update package for Windows from Microsoft Update Catalog

▶ How to obtain or download the latest cumulative update package for Linux

Additional resources

Documentation

Cumulative update 8 for SQL Server 2022 (KB5029666) - SQL Server

This article contains the summary, known issues, improvements, fixes and other information for SQL Server 2022...

Cumulative update 7 for SQL Server 2022 (KB5028743) - SQL Server

This article contains the summary, known issues, improvements, fixes and other information for SQL Server 2022...

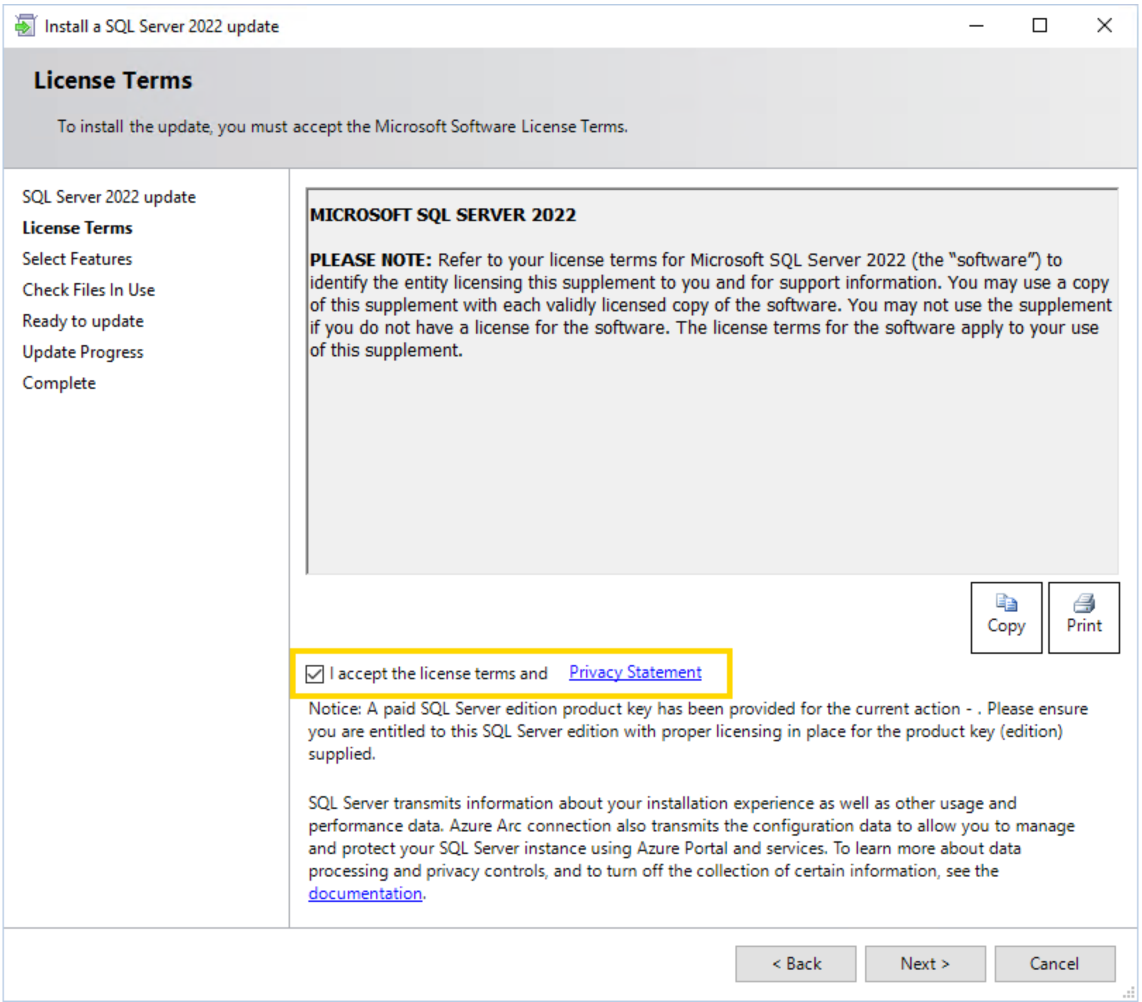
Latest updates and version history for SQL Server - SQL Server

This article lists various builds or updates that are available for different versions of SQL Server.

Show 5 more

5. The website for downloading the update package opens. Select the language and click on **Download**.
6. Run the downloaded file.

7. In the **License Terms** dialog window, select the **I accept the license terms and Privacy Statement** check box and click **Next**.



License Terms

To install the update, you must accept the Microsoft Software License Terms.

MICROSOFT SQL SERVER 2022

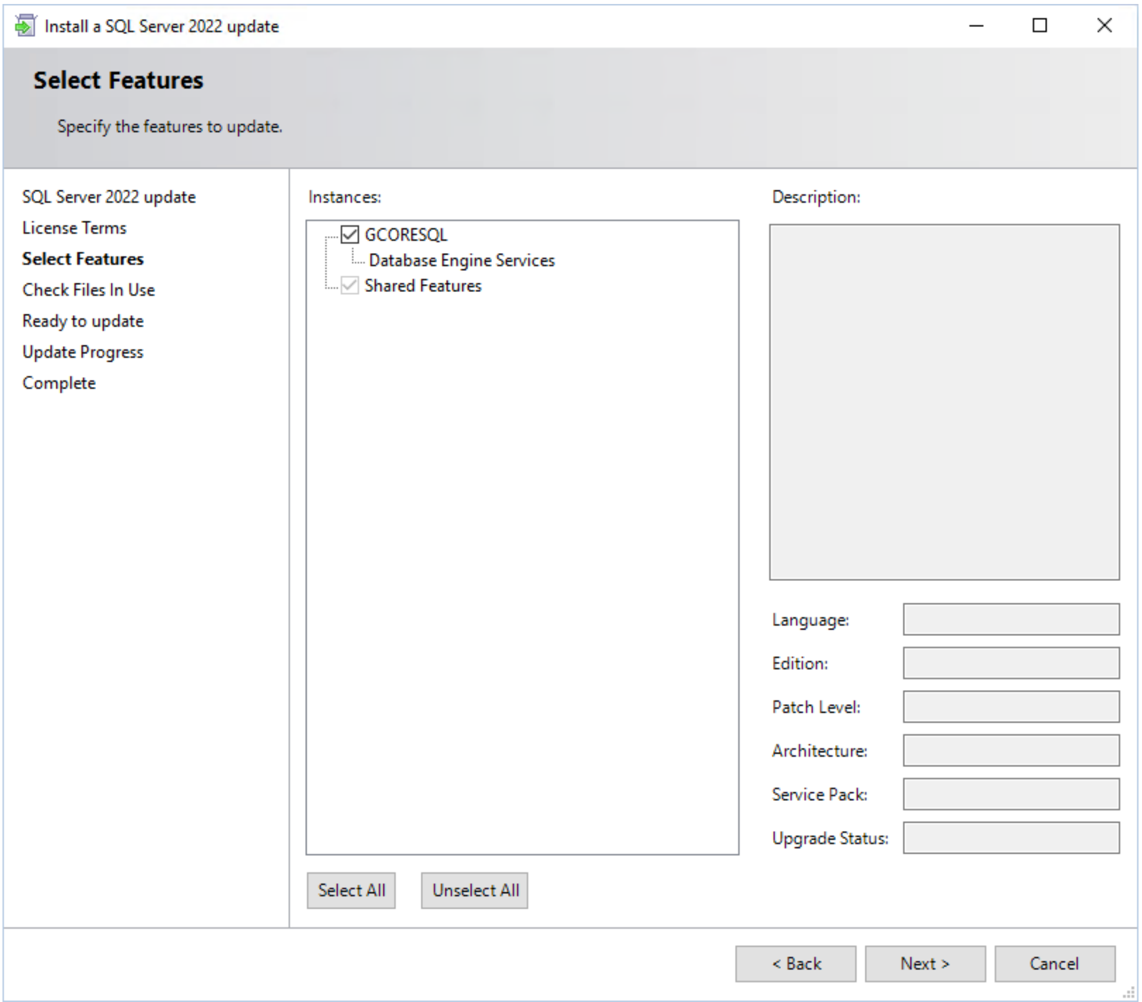
PLEASE NOTE: Refer to your license terms for Microsoft SQL Server 2022 (the "software") to identify the entity licensing this supplement to you and for support information. You may use a copy of this supplement with each validly licensed copy of the software. You may not use the supplement if you do not have a license for the software. The license terms for the software apply to your use of this supplement.

☑ I accept the license terms and Privacy Statement

Notice: A paid SQL Server edition product key has been provided for the current action - . Please ensure you are entitled to this SQL Server edition with proper licensing in place for the product key (edition) supplied.

SQL Server transmits information about your installation experience as well as other usage and performance data. Azure Arc connection also transmits the configuration data to allow you to manage and protect your SQL Server instance using Azure Portal and services. To learn more about data processing and privacy controls, and to turn off the collection of certain information, see the documentation.

8. In the **Select Features** dialog window, click **Next**.



Install a SQL Server 2022 update

Select Features

Specify the features to update.

SQL Server 2022 update
License Terms
Select Features
Check Files In Use
Ready to update
Update Progress
Complete

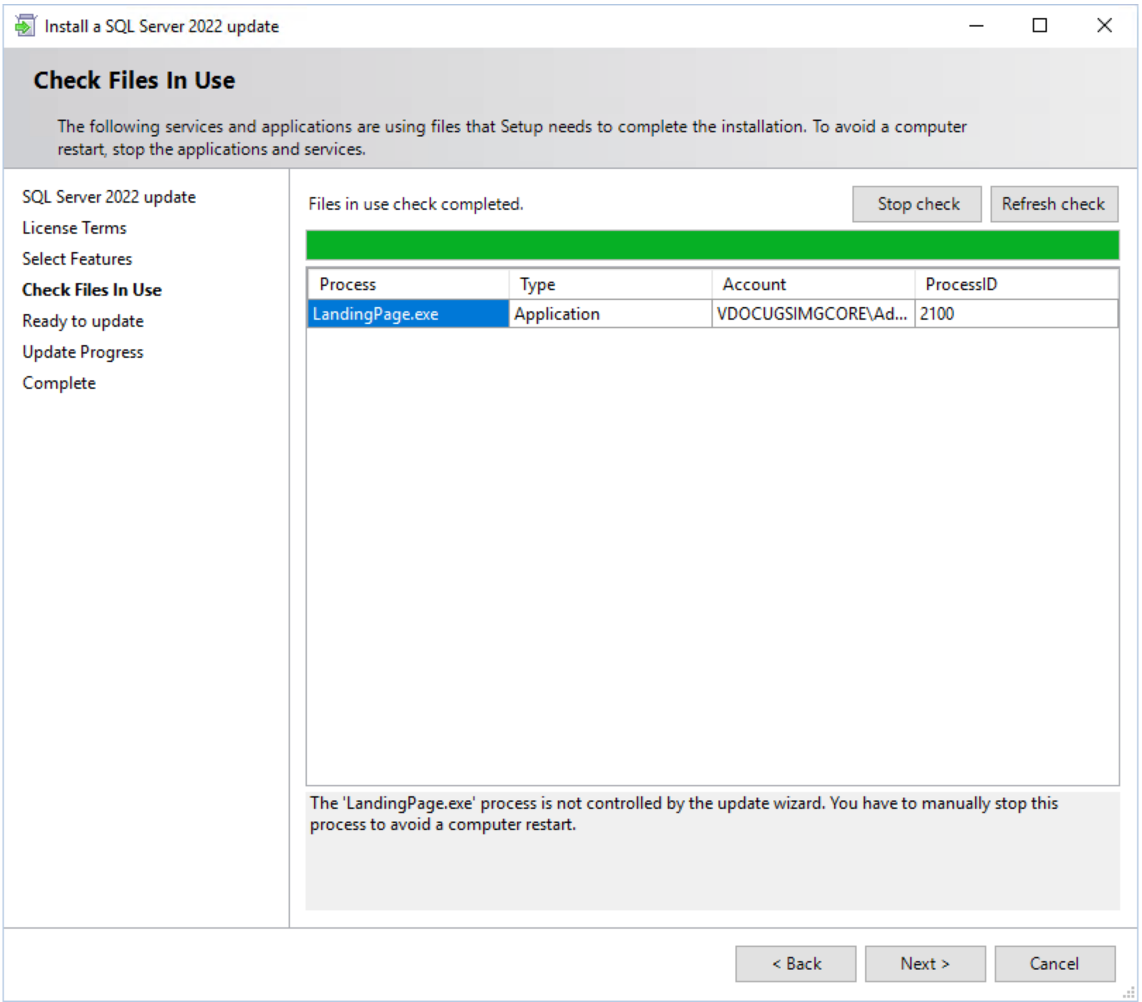
Instances:

☑ GCORESQL
Database Engine Services
☑ Shared Features

Description:

Language:
Edition:
Patch Level:
Architecture:
Service Pack:
Upgrade Status:

9. In the **Check Files In Use** dialog window, click **Next** when the check is completed.



Check Files In Use

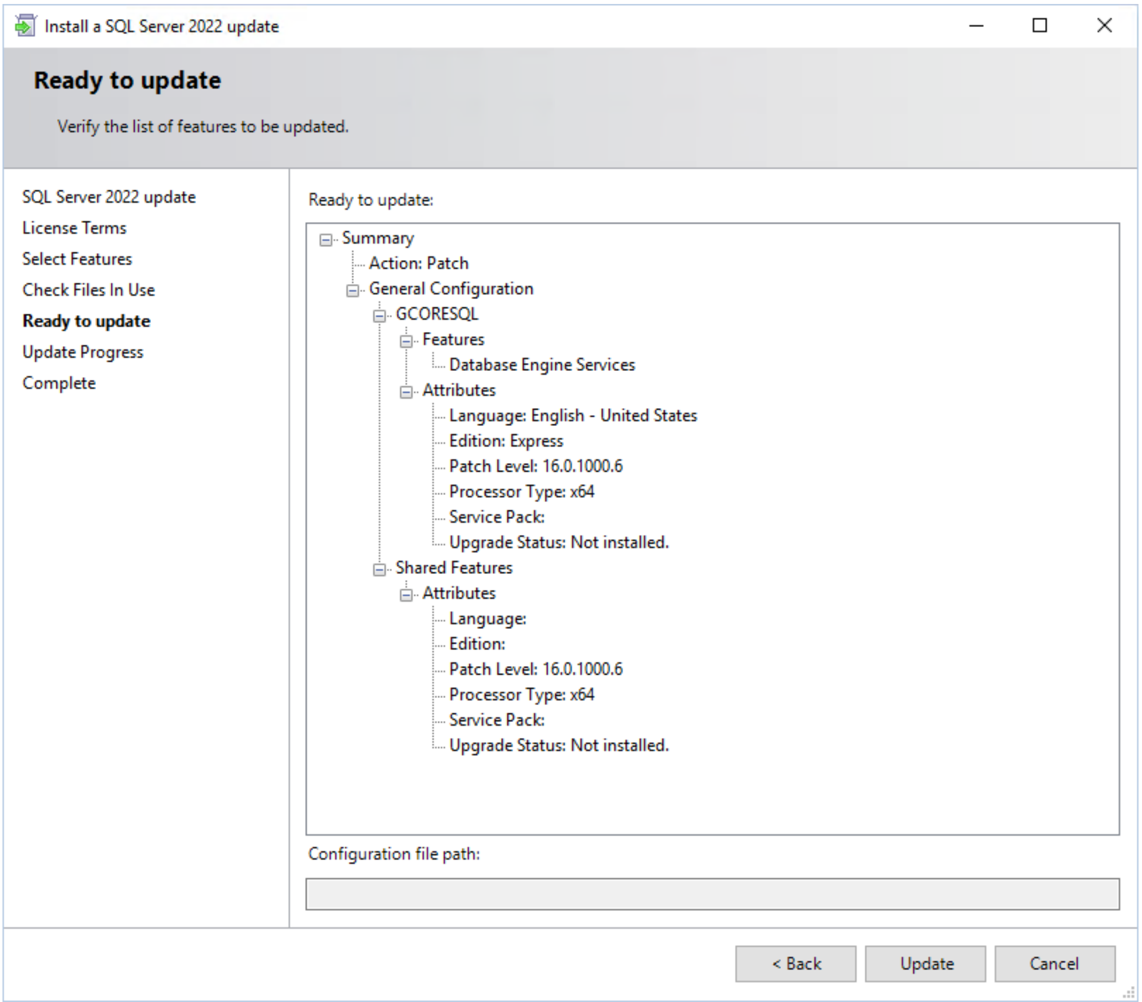
The following services and applications are using files that Setup needs to complete the installation. To avoid a computer restart, stop the applications and services.

Files in use check completed.

Process	Type	Account	ProcessID
LandingPage.exe	Application	VDOCUGSIMGCORE\Ad...	2100

The 'LandingPage.exe' process is not controlled by the update wizard. You have to manually stop this process to avoid a computer restart.

10. In the **Ready to update** dialog window click **Update**.



Ready to update

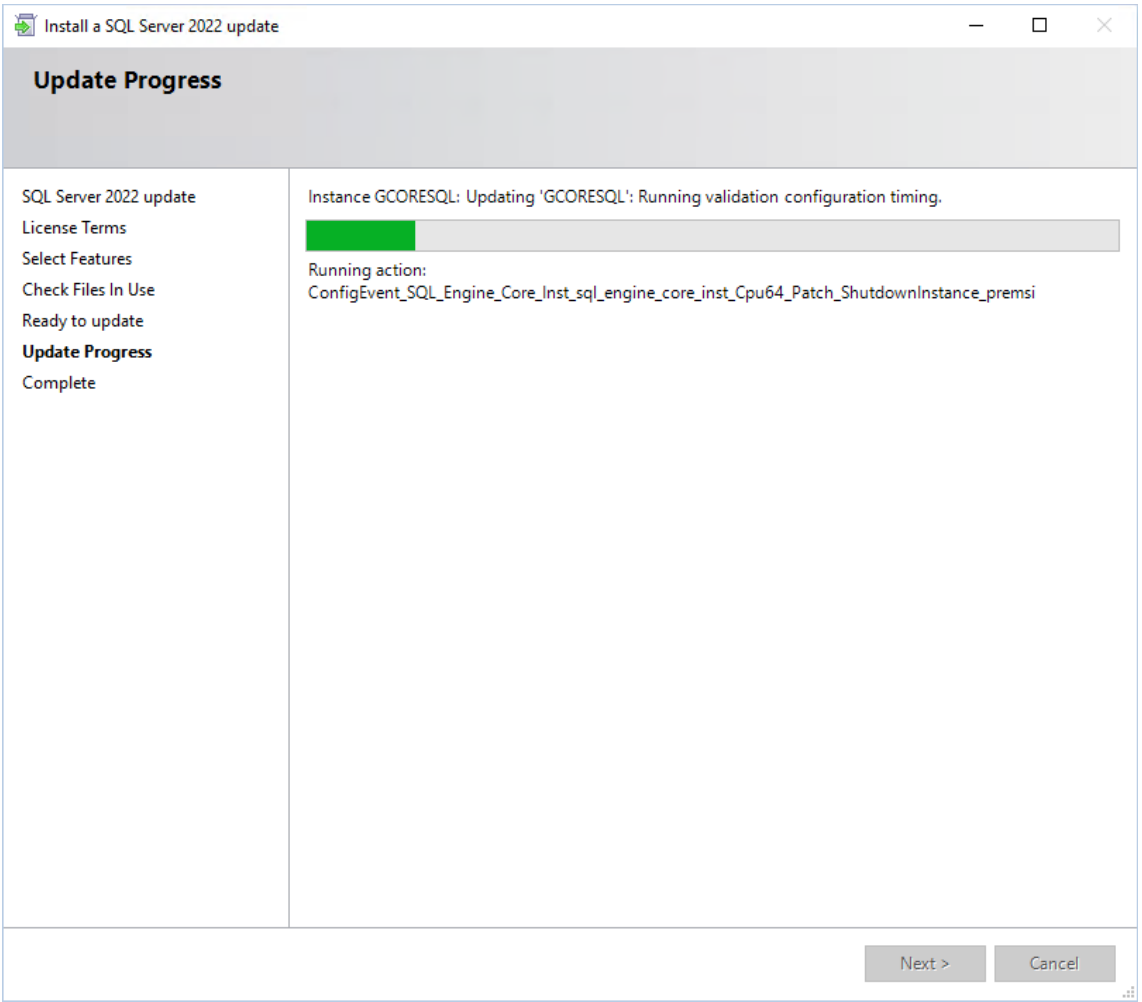
Verify the list of features to be updated.

Ready to update:

```
Summary
  Action: Patch
  General Configuration
    GCORESQL
      Features
        Database Engine Services
      Attributes
        Language: English - United States
        Edition: Express
        Patch Level: 16.0.1000.6
        Processor Type: x64
        Service Pack:
        Upgrade Status: Not installed.
    Shared Features
      Attributes
        Language:
        Edition:
        Patch Level: 16.0.1000.6
        Processor Type: x64
        Service Pack:
        Upgrade Status: Not installed.
```

Configuration file path:

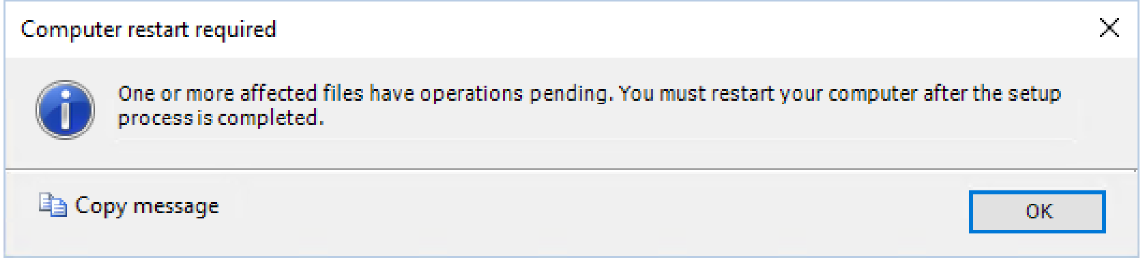
11. In the **Update Progress** dialog window, click **Next** when the update progress is completed.



Instance GCORESQL: Updating 'GCORESQL': Running validation configuration timing.

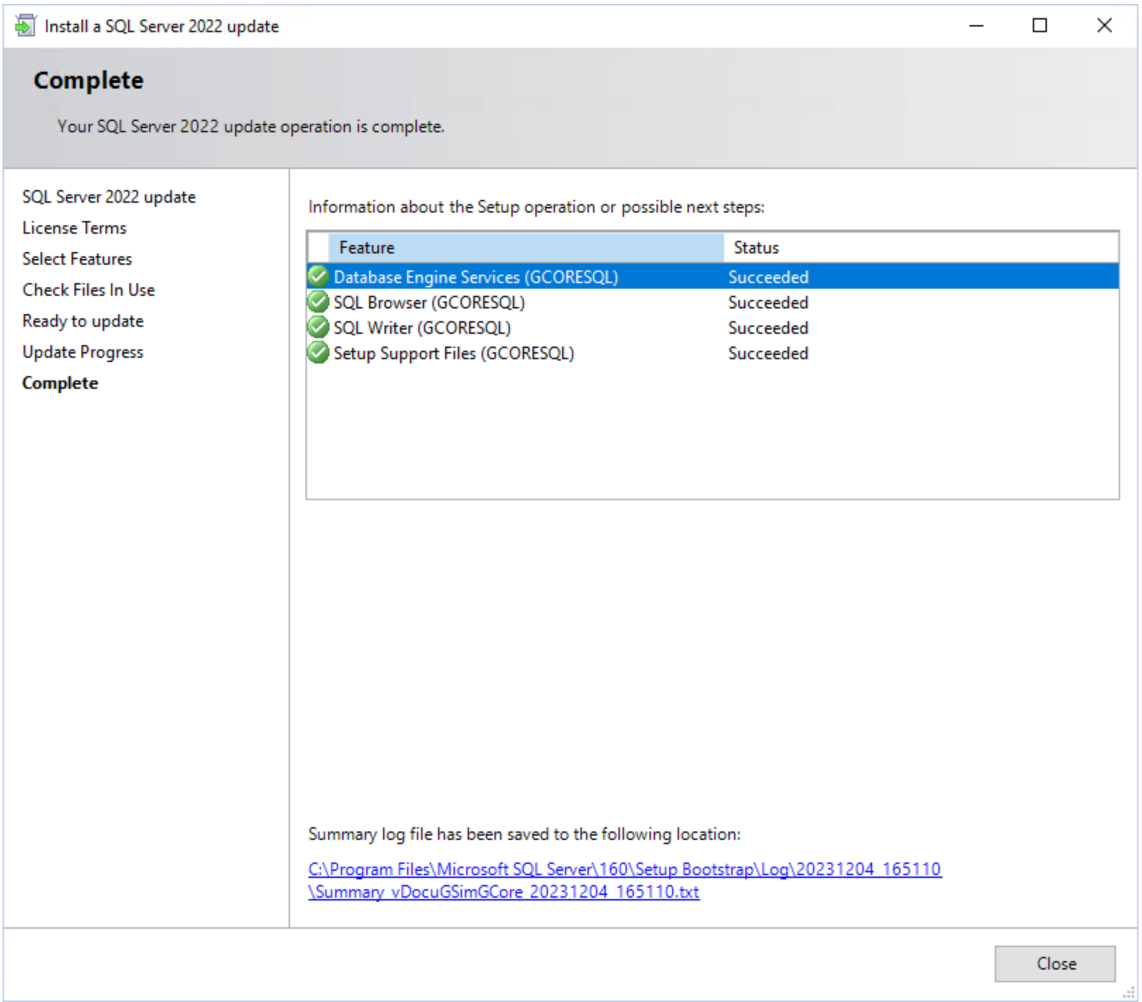
Running action:
ConfigEvent_SQL_Engine_Core_Inst_sql_engine_core_inst_Cpu64_Patch_ShutdownInstance_premsi

12. Confirm the message **Computer restart required** with **OK**.



One or more affected files have operations pending. You must restart your computer after the setup process is completed.

13. In the **Complete** dialog window, click **Close**. The update completed successfully.



Complete

Your SQL Server 2022 update operation is complete.

Information about the Setup operation or possible next steps:

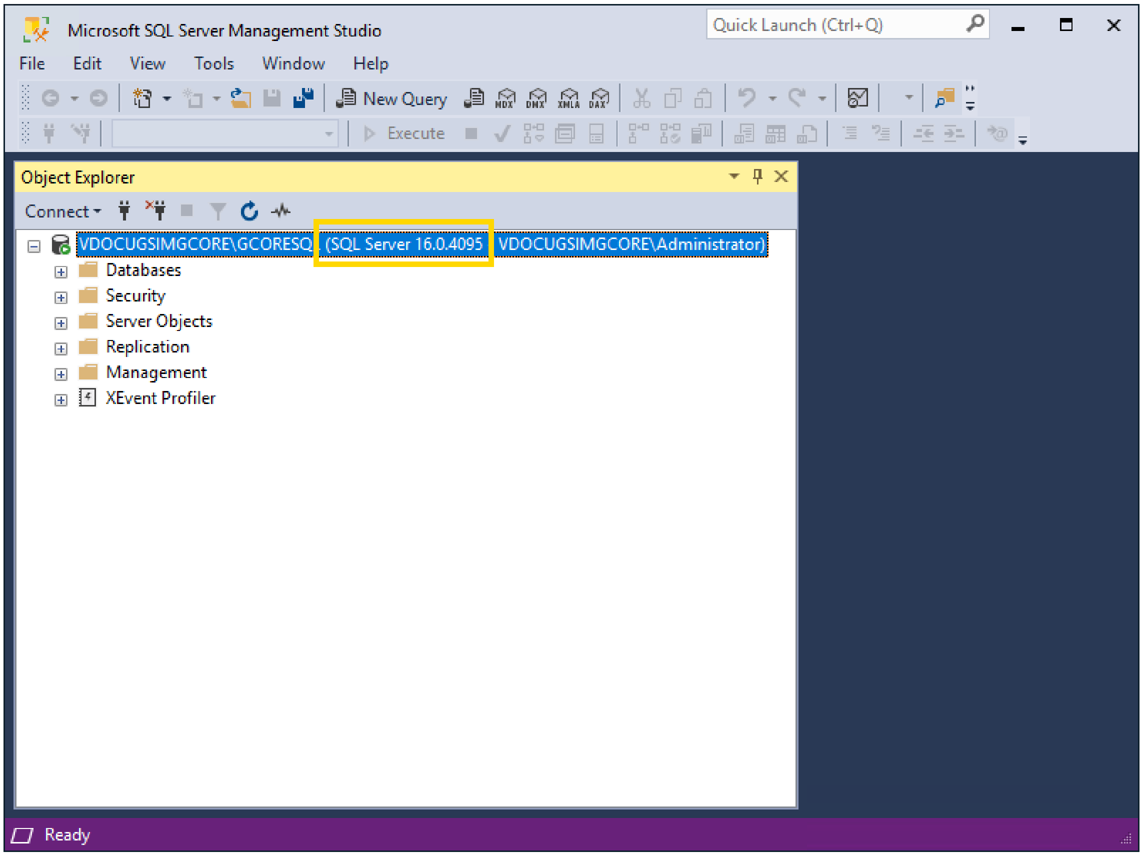
Feature	Status
✓ Database Engine Services (GCORESQL)	Succeeded
✓ SQL Browser (GCORESQL)	Succeeded
✓ SQL Writer (GCORESQL)	Succeeded
✓ Setup Support Files (GCORESQL)	Succeeded

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\160\Setup Bootstrap\Log\20231204_165110
\Summary_vDocuGSimGCore_20231204_165110.txt

14. Restart your computer.

15. You can check the version of your SQL Server in the **Microsoft SQL Management Studio**.



VDOCUGSIMGCORE\GCORESQ (SQL Server 16.0.4095 VDOCUGSIMGCORE\Administrator)

- Databases
- Security
- Server Objects
- Replication
- Management
- XEvent Profiler

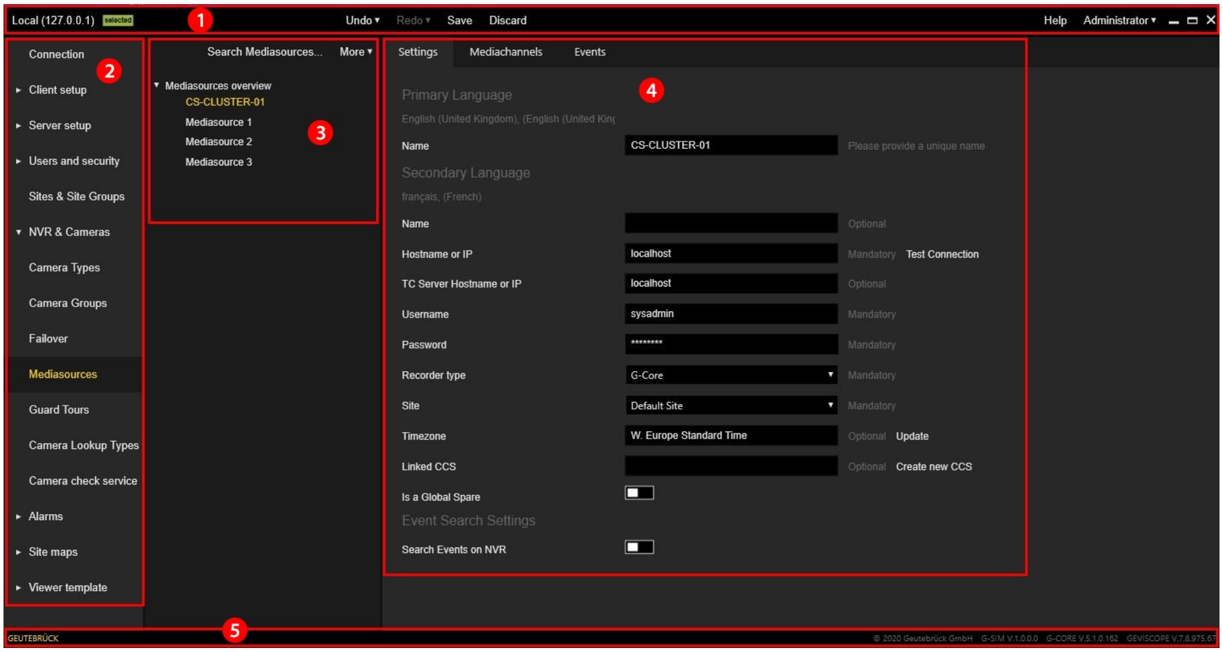
Management Console

The Management Console (ManCon) is used to manage all resources, functions, users and their authorizations in real time. Instant plausibility checks, multiple administrator access and simultaneous connections to several G-SIM servers support the efficient configuration of the system.

Main Window Layout

The Management Console (ManCon) window is divided into the following parts:

- 1 **Title Bar**
- 2 **Main Menu**
- 3 **List of Configurable Elements**
- 4 **Settings of the Selected Configurable Element**
- 5 **Status Bar**



Primary Language
English (United Kingdom), (English (United King

Name	CS-CLUSTER-01	Please provide a unique name

Secondary Language
français, (French)

Name		Optional
Hostname or IP	localhost	Mandatory
TC Server Hostname or IP	localhost	Optional
Username	sysadmin	Mandatory
Password	********	Mandatory
Recorder type	G-Core	Mandatory
Site	Default Site	Mandatory
Timezone	W. Europe Standard Time	Optional
Linked CCS		Optional
Is a Global Spare	☐	

Event Search Settings

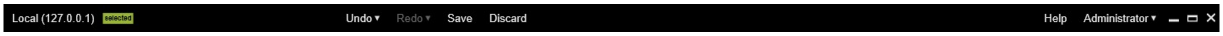
Search Events on NVR	☐

© 2020 Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67

Title Bar

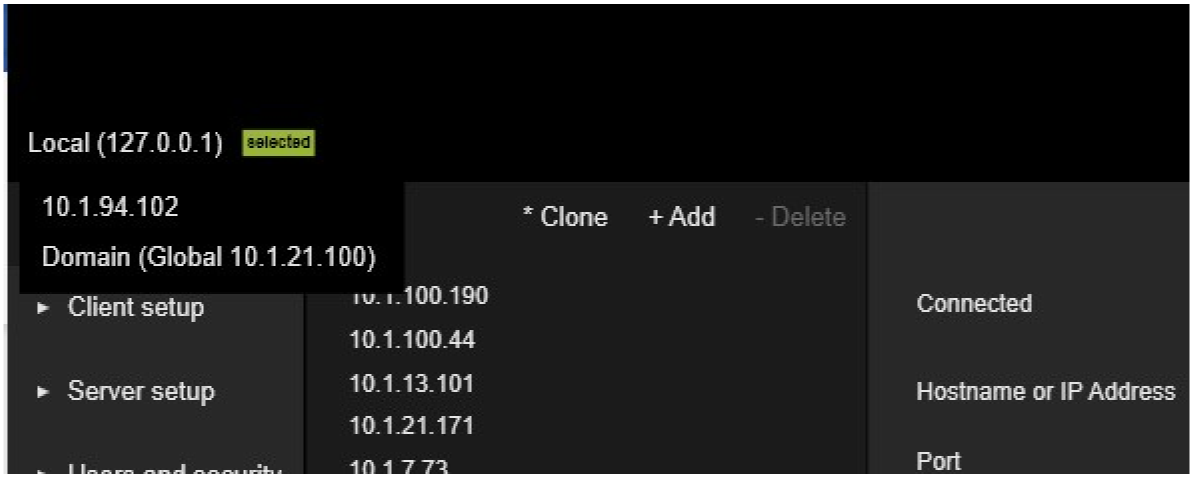
The title bar contains the following menu items:

- List of the connected G-SIM servers
- Undo / Redo
- Save
- Discard
- Help
- Administrator



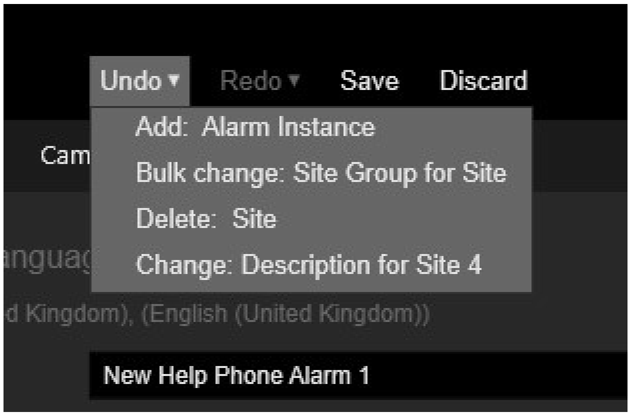
List of the Connected G-SIM Servers

The Management Console supports multiple connections to the different G-SIM severs at the same time. Only one connection can be active at a time. The active connection is displayed in the title bar and marked with a green **Selected** label. All administrator actions are applied to the active connection.

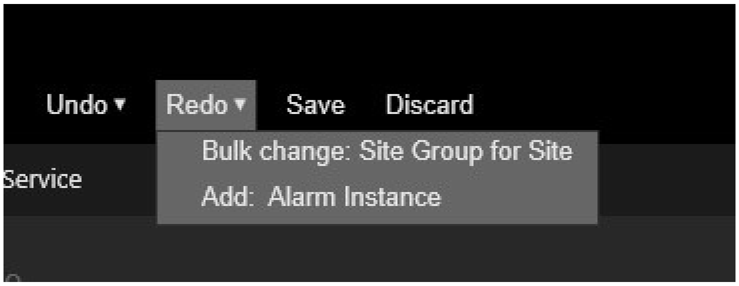


Undo / Redo

The last 100 changes are stored in the **Undo list**.


Undo ▾
Redo ▾
Save
Discard
Add: Alarm Instance
Bulk change: Site Group for Site
Delete: Site
Change: Description for Site 4
Cam
anguag
d Kingdom), (English (United Kingdom))
New Help Phone Alarm 1

If the administrator performs undo for some changes, those changes are moved to the **Redo list** and can be performed again.



Save

The **Save** button is active if the setup of the active connection has changes and no validation errors have occurred. Press the **Save** button to save the setup on the G-SIM server.

Discard

The **Discard** button is active if the setup of the active connection has changes. Press the **Discard** button to discard all changes made when setting up the active connection. This operation cannot be undone.

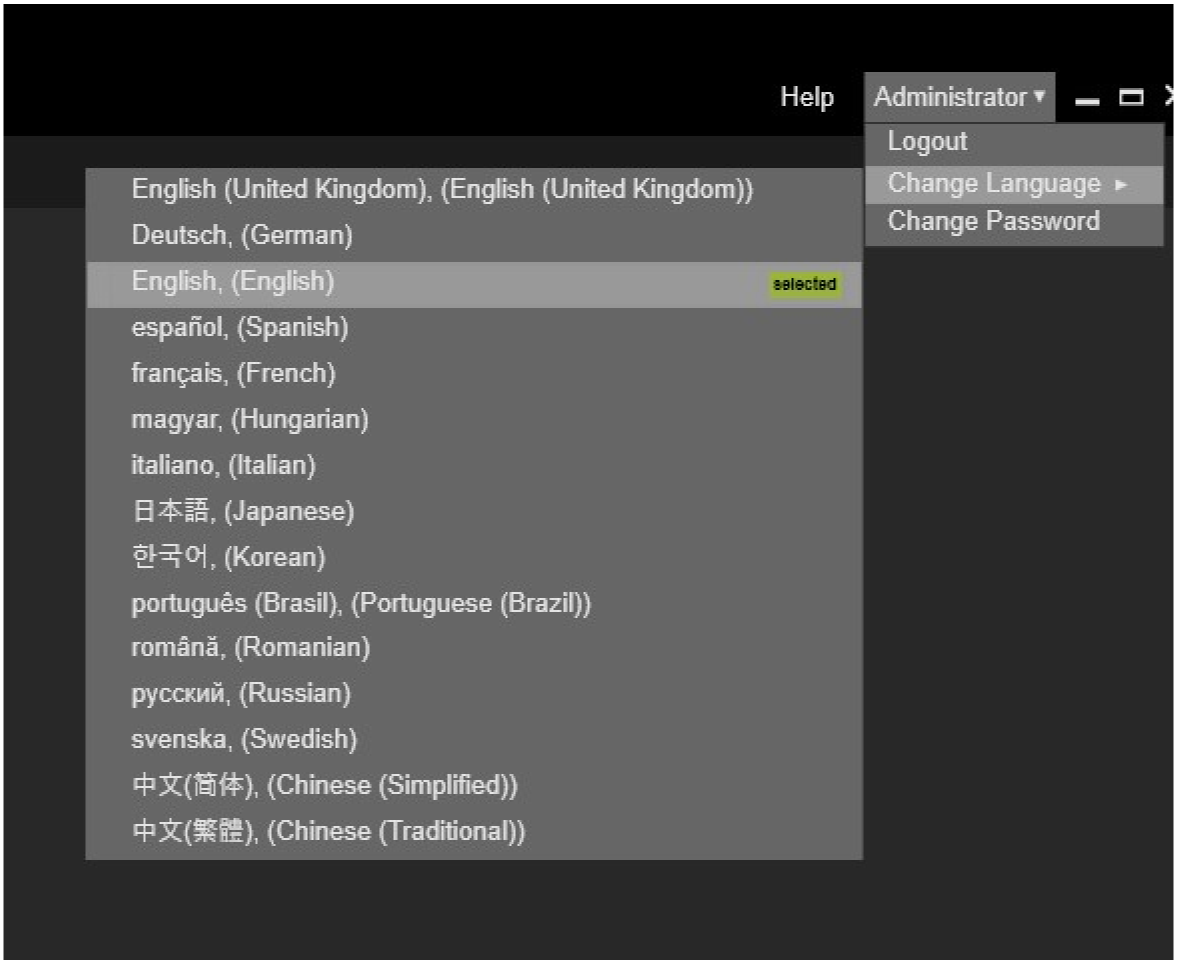
Help

Displays help for the Management Console.

Administrator

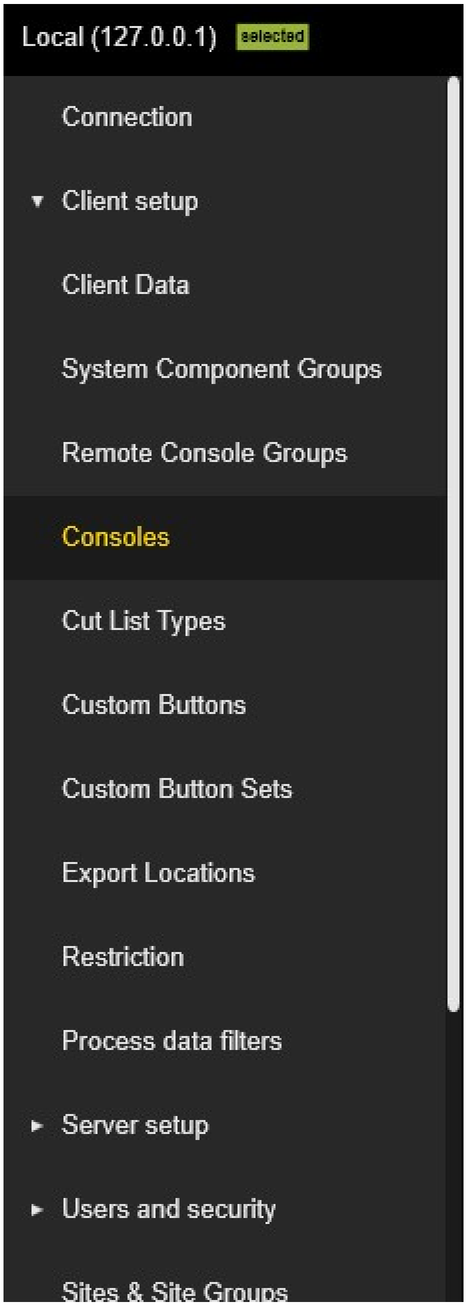
Displays the current users menu. It contains the following submenu items:

Submenu Item	Description
Logout	Closes the active connection. The Management Console will automatically set the active connection to the next connection from the list of the connected G-SIM servers, if available.
Change Language	The administrator can change the language of the Management Console user interface.
Change Password	The administrator can change the password.



Main Menu

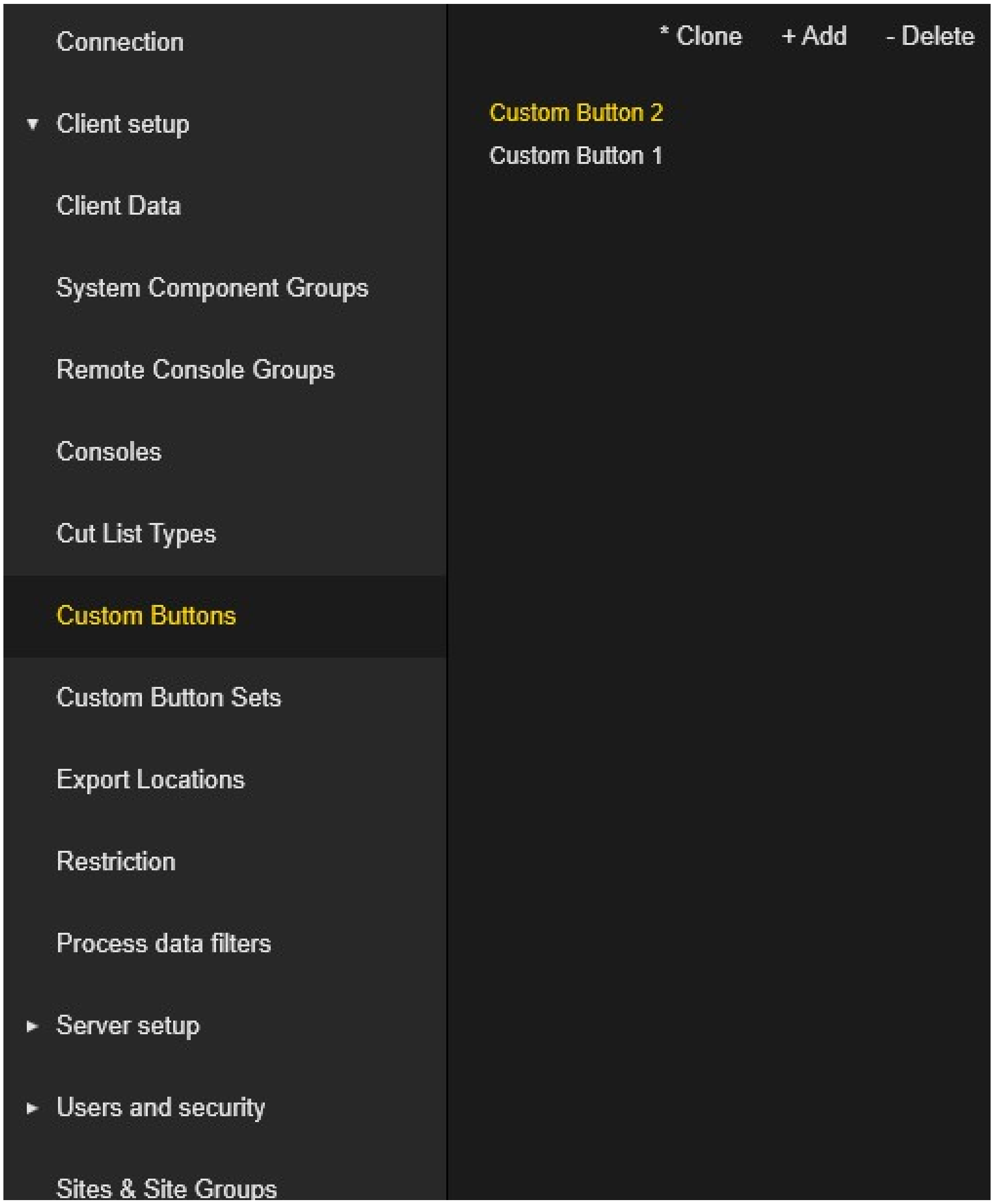
The administrator can select menu item to view and edit specific setup settings. The selected menu item is marked with yellow color. Some menu items can be disabled due to missing licenses. The main menu can be shown or hidden with the shortcuts **Ctrl + D** and **Ctrl + E**. The main menu items, except the **connection** menu item, are disabled until a connection to the G-SIM server is established.



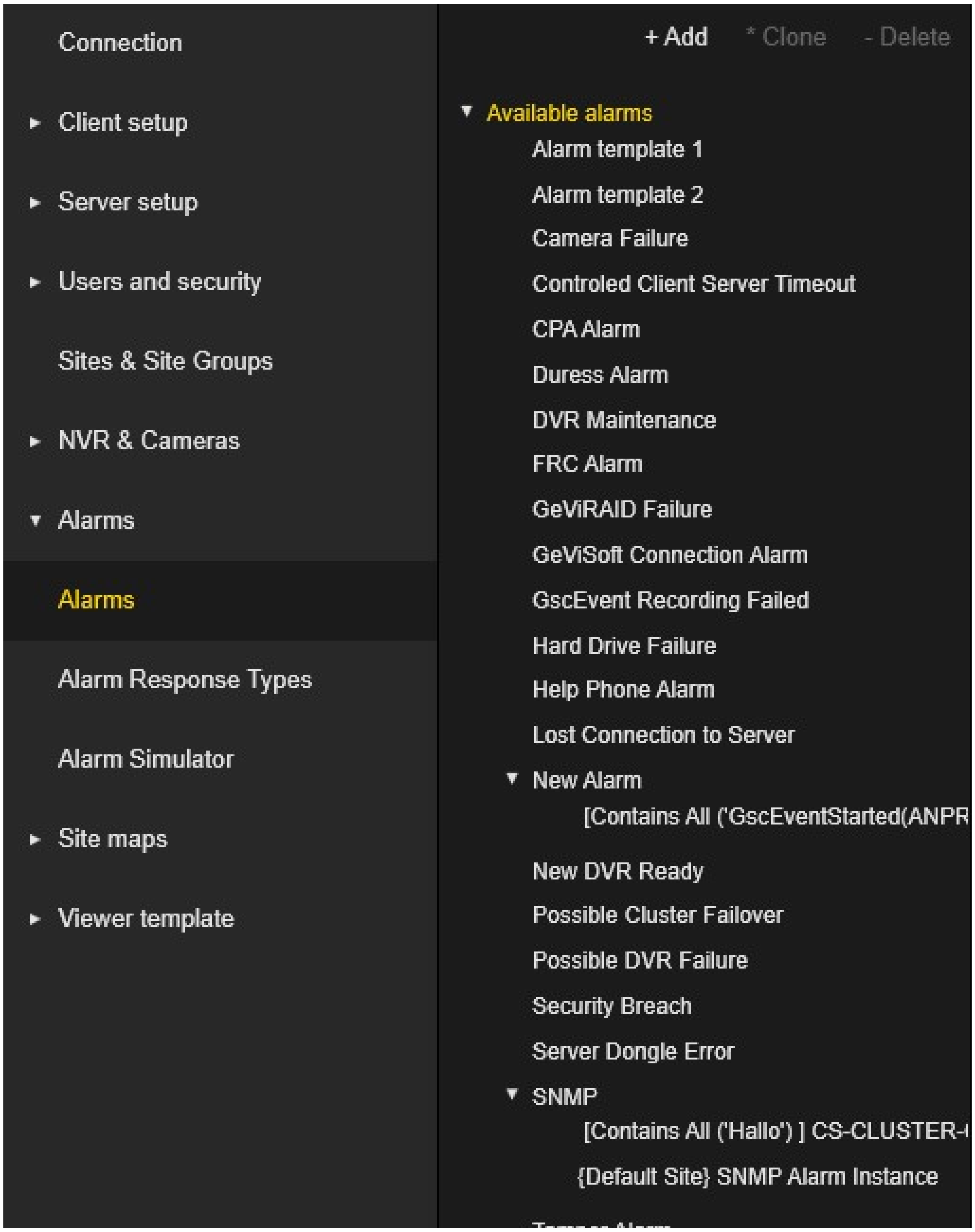
List of Configurable Elements

The configurable elements of the current menu item are organized in a list or a tree view. Selected elements are marked with yellow color. In general, more than one element can be selected.

Organization in a list:

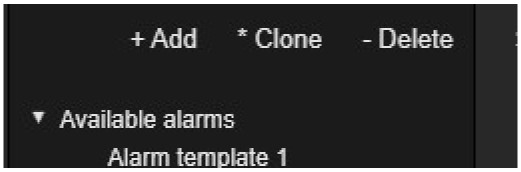


Organization in a tree view:



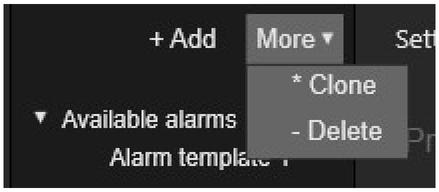
- Available alarms
  - Alarm template 1
  - Alarm template 2
  - Camera Failure
  - Controled Client Server Timeout
  - CPA Alarm
  - Duress Alarm
  - DVR Maintenance
  - FRC Alarm
  - GeViRAID Failure
  - GeViSoft Connection Alarm
  - GscEvent Recording Failed
  - Hard Drive Failure
  - Help Phone Alarm
  - Lost Connection to Server
  - New Alarm
    - [Contains All ('GscEventStarted(ANPR
  - New DVR Ready
  - Possible Cluster Failover
  - Possible DVR Failure
  - Security Breach
  - Server Dongle Error
  - SNMP
    - [Contains All ('Hallo')] CS-CLUSTER-
    - {Default Site} SNMP Alarm Instance
  - Tamper Alarm

In general, the list of configurable elements has a toolbar with the **+ Add**, *** Clone** and **Delete** buttons.



- Available alarms
  - Alarm template 1

Some configurable elements have other buttons or hide standard buttons. If the list of configurable elements is not wide enough to include all buttons, all buttons except **+ Add** are moved to the **More** pop-up menu.



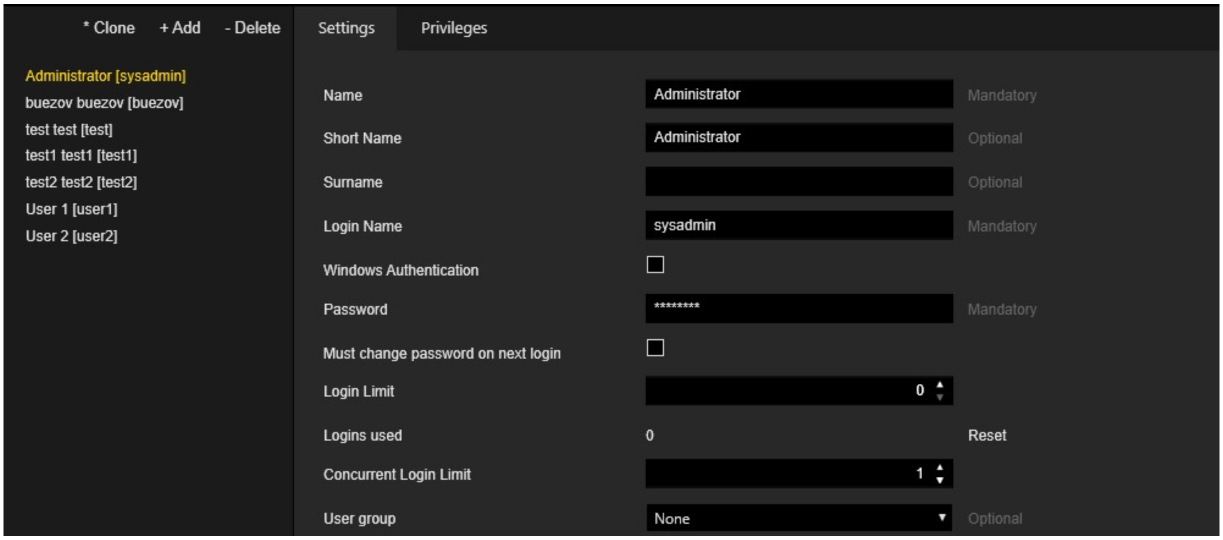
The buttons on the tool bar buttons perform the following actions:

Button	Description
+ Add	Creates a new configurable element. The shortcut `Ctrl` + `V` can be used for this action.
* Clone	Creates a copy of the currently selected configurable element. The shortcut `Ctrl` + `C` can be used for this action.
- Delete	Deletes the currently selected configurable elements. The shortcut `Ctrl` + `X` can be used for this action.

For the configurable elements that use the organization in a tree view, the shortcut `Ctr` + `T` can be used to collapse or expand all tree elements.

Settings of the Selected Configurable Element

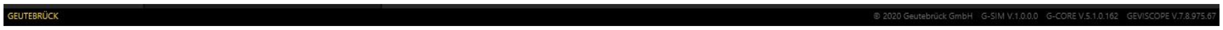
Contains settings of the selected configurable element(s). The visualization of this part is specific to the configurable element type. For example, the users settings part is shown in the following Figure. If more than one configurable element is selected, the administrator can change specific settings for all selected elements. The set of settings that can be edited with multiselect is specific to the configurable element type.



Name: Administrator (Mandatory)
Short Name: Administrator (Optional)
Surname: (Optional)
Login Name: sysadmin (Mandatory)
Windows Authentication: □
Password: ******** (Mandatory)
Must change password on next login: □
Login Limit: 0
Logins used: 0
Concurrent Login Limit: 1
User group: None (Optional)

Status Bar

The status bar contains the Geutebrück logo and information about the current versions of G-SIM, G-Core and GeViScope.

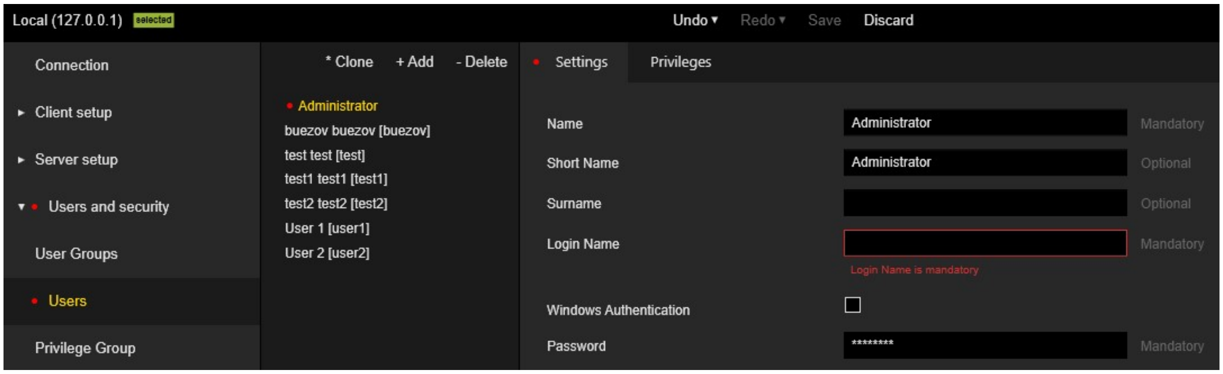


© 2020 Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67

Notifications

Validation

The Management Console performs the validation of the setup. Setup with validation errors cannot be saved. Main menu items and their configurable elements that have validation errors are marked with red dots. Controls that contain invalid settings are marked with red frames and notes with error descriptions. Tab pages that contain controls with invalid settings are marked with red dots.

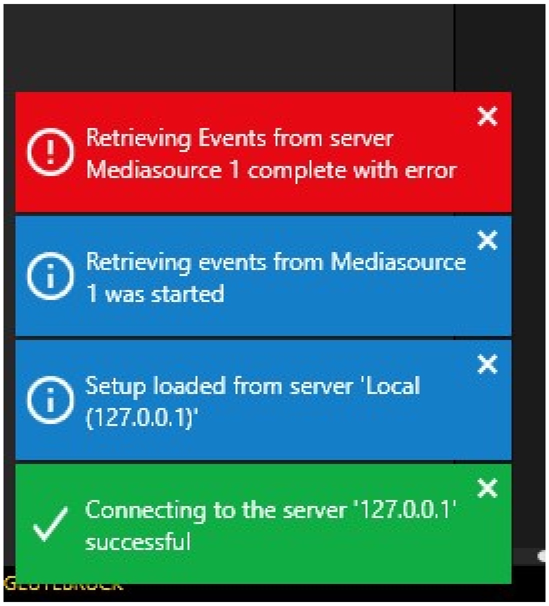


Name: Administrator (Mandatory)
Short Name: Administrator (Optional)
Surname: (Optional)
Login Name: (Mandatory)
Login Name is mandatory
Windows Authentication: □
Password: ******** (Mandatory)

Pop-up Notifications

The Management Console uses pop-up notifications to inform the administrator about events that occur. The type of pop-up notification is displayed in color.

Color	Description
Blue	Is used for the information events.
Red	Is used for errors.
Green	Is used for actions that have been performed successfully.



Retrieving Events from server Mediasource 1 complete with error

Retrieving events from Mediasource 1 was started

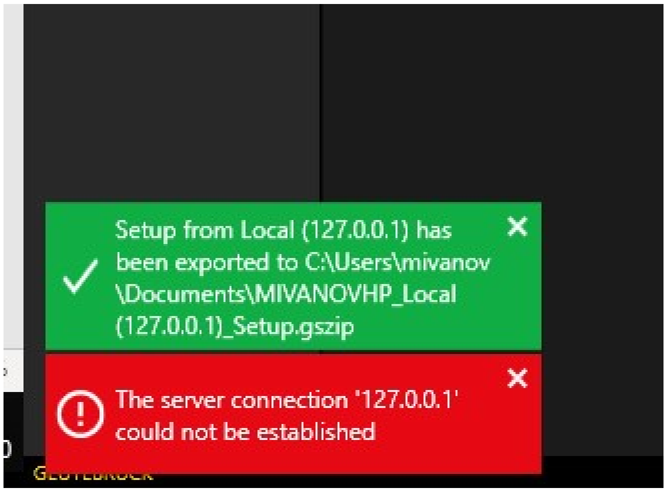
Setup loaded from server 'Local (127.0.0.1)'

Connecting to the server '127.0.0.1' successful

The notification will automatically close after 10 seconds. To prevent this, the administrator can move the mouse over the notification. The notification can be closed manually using the cross button.

Lost Connection

If the connection to the G-SIM server is lost and the setup contains changes, the setup is automatically exported.

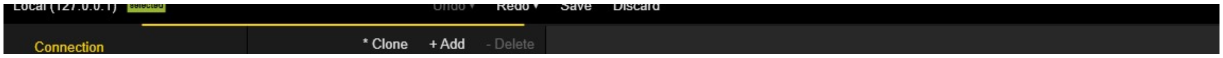


Setup from Local (127.0.0.1) has been exported to C:\Users\mivanov\Documents\MIVANOVHP_Local (127.0.0.1)_Setup.gszip

The server connection '127.0.0.1' could not be established

Long-Term Operations

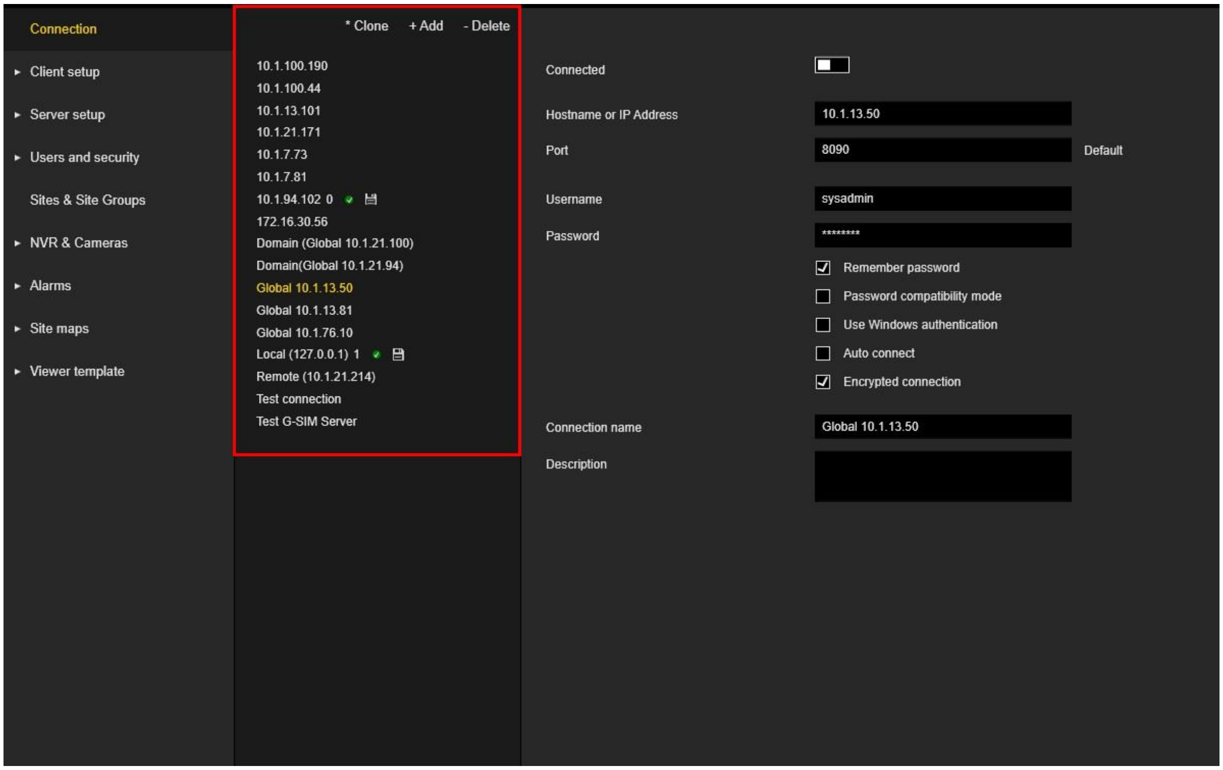
If a long-term operation (e.g. import / export setup) is running, a progress bar is displayed.



Connection

List of Connections

The list of connections contains existing connections to the G-SIM servers. Connection records that are connected to G-SIM servers are marked with a green check icon. Connection records that have unsaved changes are marked with a diskette icon.



Connected

Hostname or IP Address: 10.1.13.50

Port: 8090 Default

Username: sysadmin

Password: ********

☑ Remember password

□ Password compatibility mode

□ Use Windows authentication

□ Auto connect

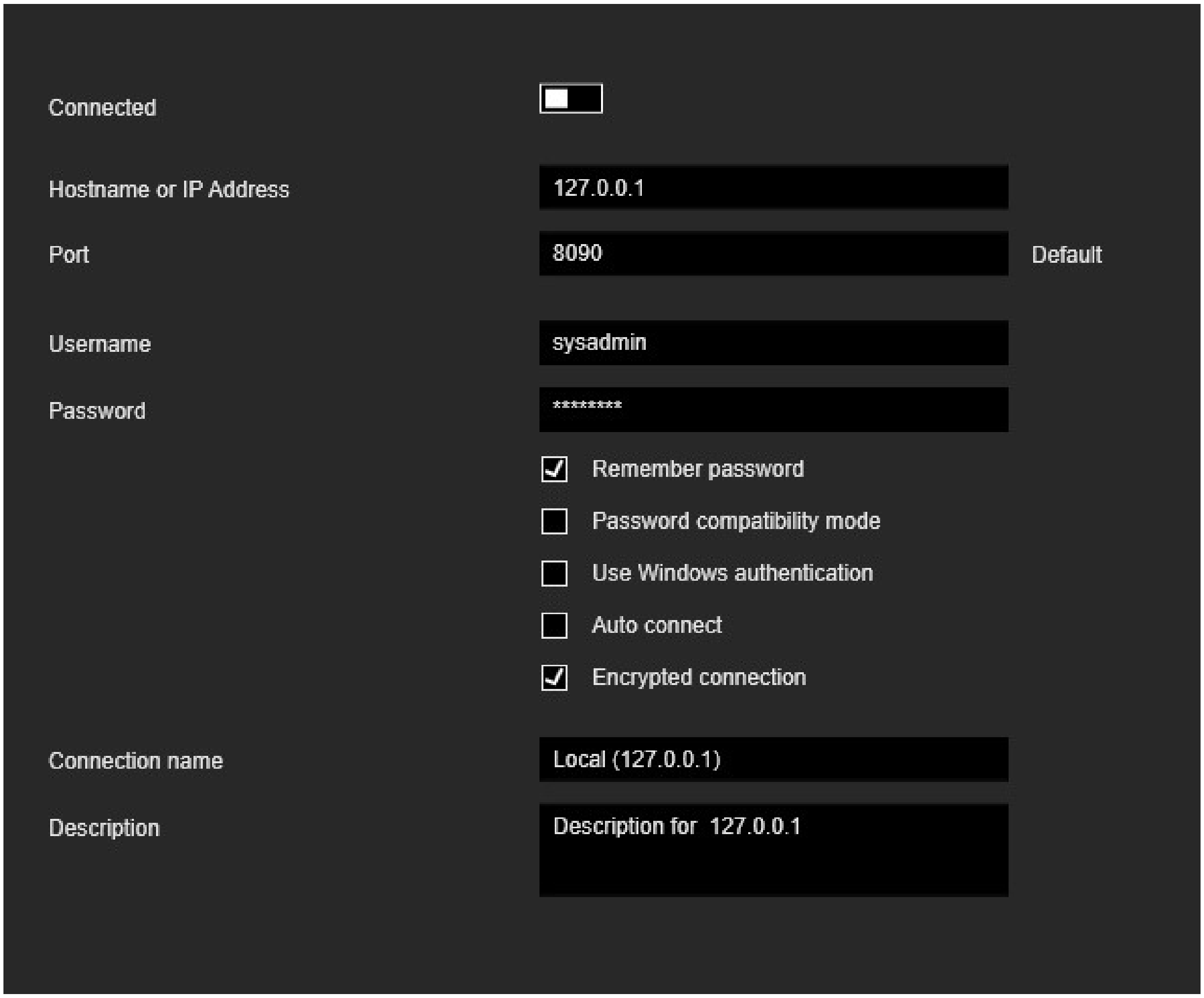
☑ Encrypted connection

Connection name: Global 10.1.13.50

Description

Connection View

The **Connection** view contains settings of the selected connection.



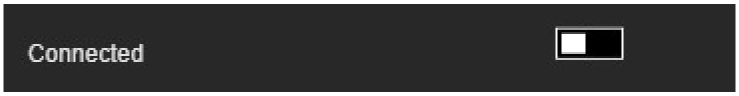
Connected		
Hostname or IP Address	127.0.0.1	
Port	8090	Default
Username	sysadmin	
Password	********	
	☑ Remember password	
	□ Password compatibility mode	
	□ Use Windows authentication	
	□ Auto connect	
	☑ Encrypted connection	
Connection name	Local (127.0.0.1)	
Description	Description for 127.0.0.1	

Setting	Description
Hostname or IP Address	Contains the address of the G-SIM server. This field is mandatory.
Port	Contains the port of the G-SIM server. This field is mandatory. Click the **Default** button to reset port to the default value.
Username	Contains the name of the G-SIM user.
Password	Contains the password of the G-SIM user.
Remember password	Select this checkbox to save the password.

Setting	Description
Password compatibility mode	Select this checkbox for connection to the old G-SIM server (<V8).
Use Windows authentication	Select this checkbox to use Windows user as G-SIM users. G-SIM user should be configured for this mode.
Auto connect	Select this checkbox to automatically connect to the G-SIM server when the Management Console starts.
Encrypted connection	Select this checkbox to encrypt the connection between the Management Console and the G-SIM server. G-SIM server should use the same setting to be able to establish the connection.
Connection name	Contains the name of the connection. This name will be used in the list of connections and list of the connected G-SIM servers.
Description	Description for the connection.

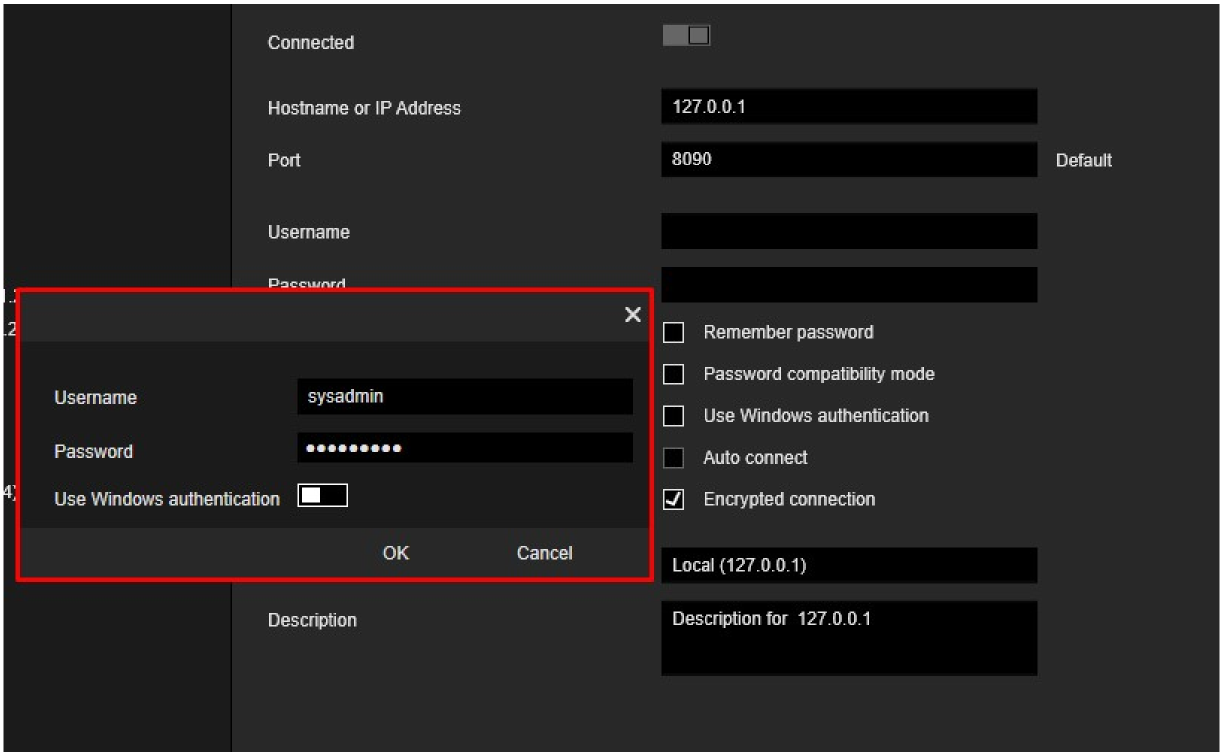
Connect / Disconnect to the G-SIM Server

If the connection view has no validation errors, the **Connected** slider button is enabled.



The administrator can click the slider to establish the connection to the G-SIM server.

If the **Remember password** check box is not selected, a dialog box for entering connection information appears.



Connected

Hostname or IP Address: 127.0.0.1

Port: 8090 Default

Username

Password

Username: sysadmin

Password: ••••••••••

Use Windows authentication

☐ Remember password

☐ Password compatibility mode

☐ Use Windows authentication

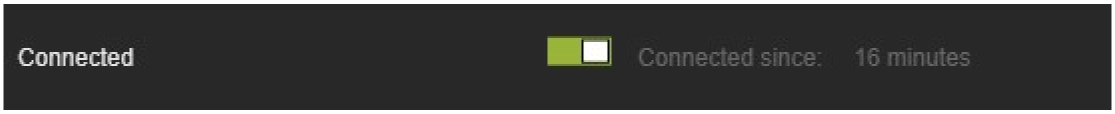
☐ Auto connect

☑ Encrypted connection

Local (127.0.0.1)

Description: Description for 127.0.0.1

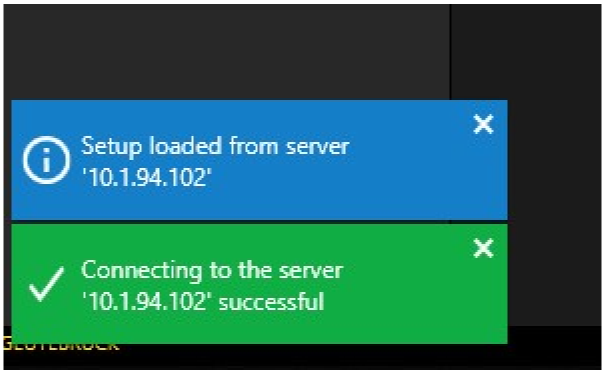
If the connection to the G-SIM server is established successfully, the slider button changes its state to active, the label **Connected since** and the time specification appears are displayed.



Connected

Connected since: 16 minutes

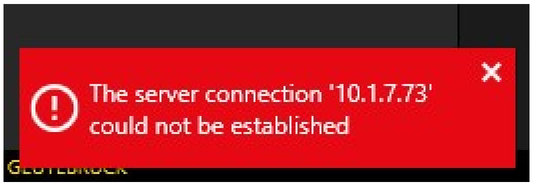
Pop-up notifications are also displayed.



Setup loaded from server '10.1.94.102'

Connecting to the server '10.1.94.102' successful

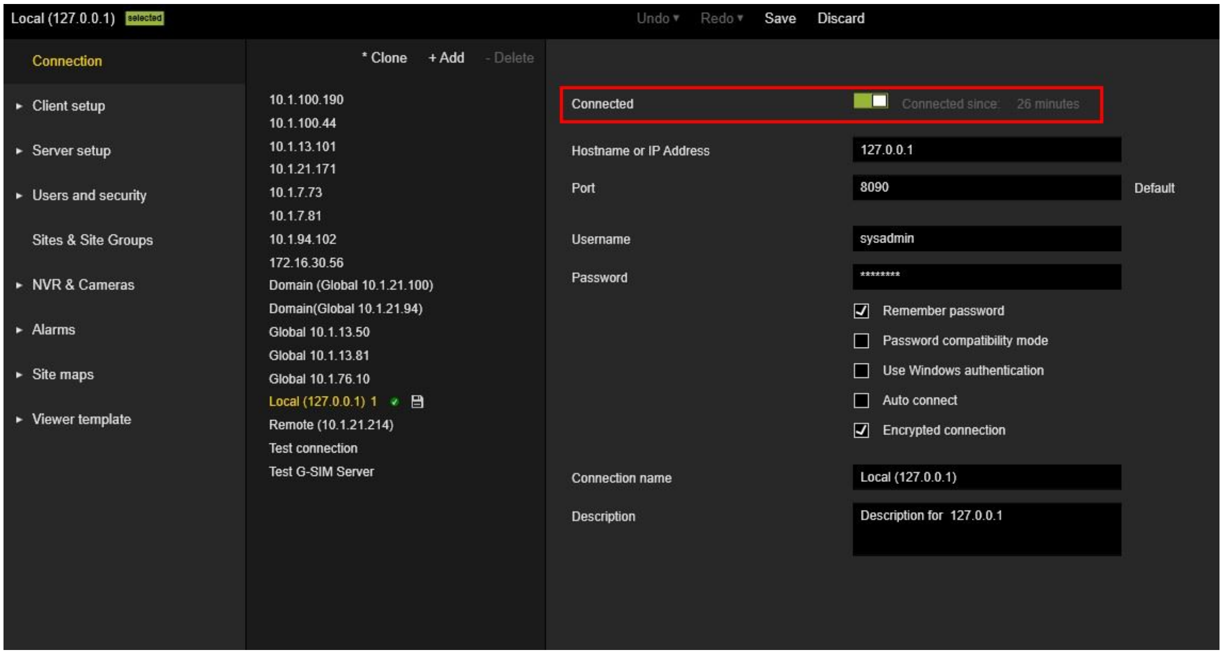
If the connection to the G-SIM server cannot be established, the slider button is inactive and a pop-up notification with an error message is displayed.



The server connection '10.1.7.73' could not be established

After the connection to the G-SIM server is established, the connection settings are not editable.

The main menu items, except the connection item, are only enabled when a connection to the G-SIM server exists.



10.1.100.190
10.1.100.44
10.1.13.101
10.1.21.171
10.1.7.73
10.1.7.81
10.1.94.102
172.16.30.56
Domain (Global 10.1.21.100)
Domain(Global 10.1.21.94)
Global 10.1.13.50
Global 10.1.13.81
Global 10.1.76.10
Local (127.0.0.1) 1 ✓
Remote (10.1.21.214)
Test connection
Test G-SIM Server

Connected 🟩 Connected since: 26 minutes

Hostname or IP Address: 127.0.0.1

Port: 8090 Default

Username: sysadmin

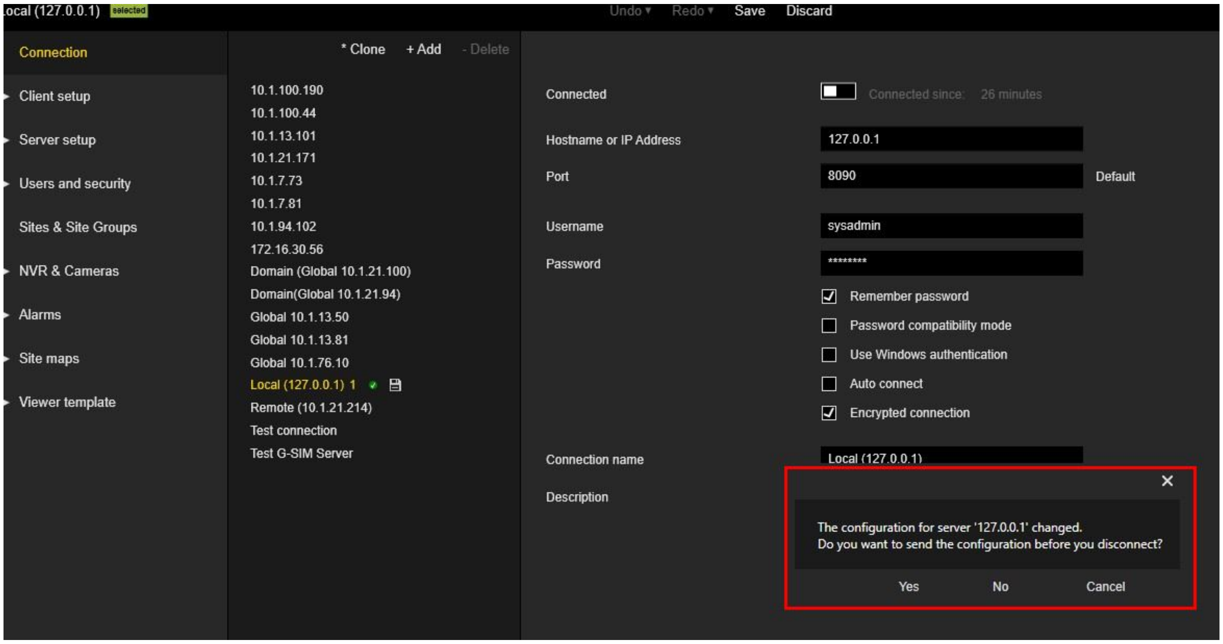
Password: ********

☑ Remember password
□ Password compatibility mode
□ Use Windows authentication
□ Auto connect
☑ Encrypted connection

Connection name: Local (127.0.0.1)

Description: Description for 127.0.0.1

If the administrator tries to close the connection with unsaved changes, a message box appears.



10.1.100.190
10.1.100.44
10.1.13.101
10.1.21.171
10.1.7.73
10.1.7.81
10.1.94.102
172.16.30.56
Domain (Global 10.1.21.100)
Domain(Global 10.1.21.94)
Global 10.1.13.50
Global 10.1.13.81
Global 10.1.76.10
Local (127.0.0.1) 1
Remote (10.1.21.214)
Test connection
Test G-SIM Server

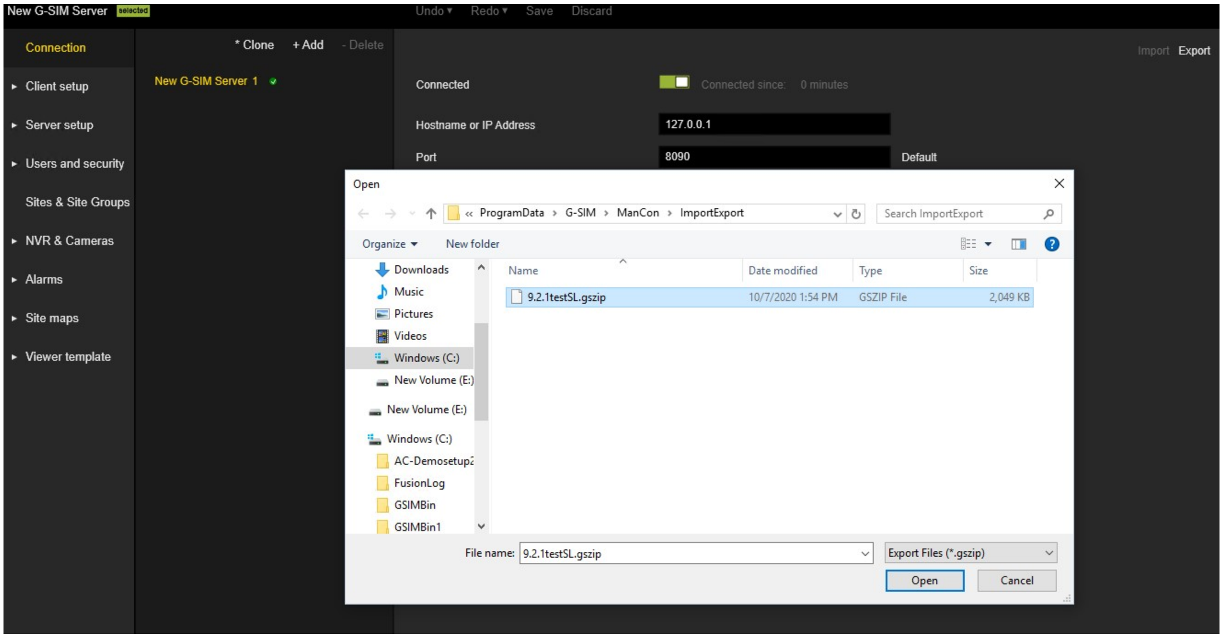
Connected: Connected since: 26 minutes
Hostname or IP Address: 127.0.0.1
Port: 8090 Default
Username: sysadmin
Password: ********
☑ Remember password
☐ Password compatibility mode
☐ Use Windows authentication
☐ Auto connect
☑ Encrypted connection
Connection name: Local (127.0.0.1)
Description

The configuration for server '127.0.0.1' changed.
Do you want to send the configuration before you disconnect?

Export / Import G-SIM Setup

After the connection to the G-SIM server is established, the **Import** and **Export** buttons are enabled.

To import setup, the administrator should select an existing file with G-SIM setup.



New G-SIM Server 1

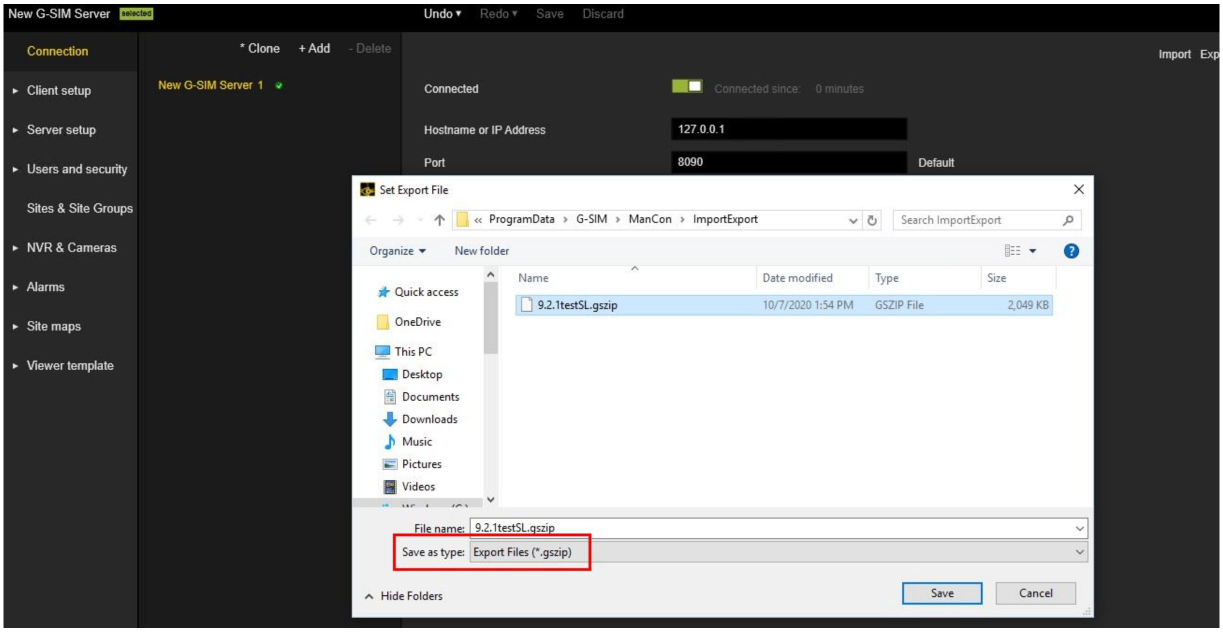
Connected: Connected since: 0 minutes
Hostname or IP Address: 127.0.0.1
Port: 8090 Default

« ProgramData › G-SIM › ManCon › ImportExport
Search ImportExport

Name	Date modified	Type	Size
9.2.1testSL.gszip	10/7/2020 1:54 PM	GSZIP File	2,049 KB

File name: 9.2.1testSL.gszip
Export Files (*.gszip)

To export the setup, the administrator should select the path where the file is created with the current G-SIM setup.



Connected — Connected since: 0 minutes

Hostname or IP Address: 127.0.0.1

Port: 8090 Default

Name	Date modified	Type	Size
9.2.1testSL.gszip	10/7/2020 1:54 PM	GSZIP File	2,049 KB

File name: 9.2.1testSL.gszip

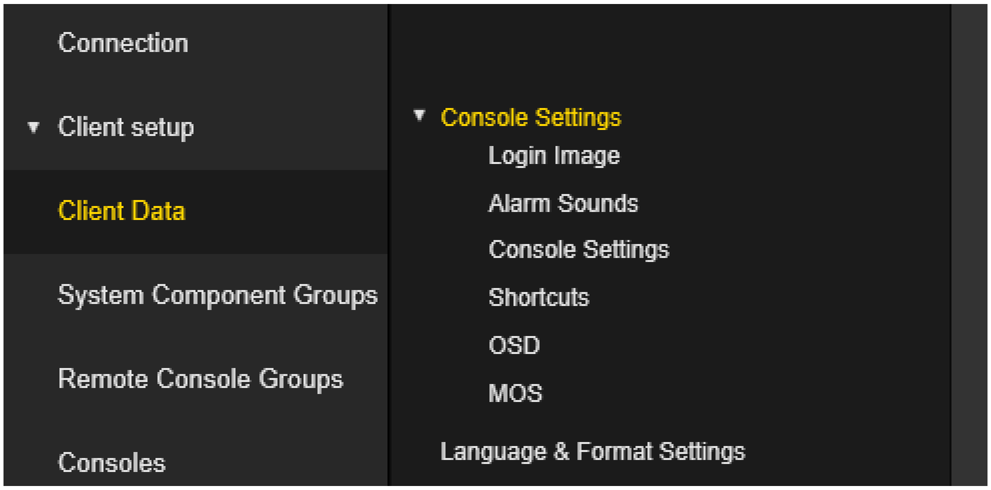
Save as type: Export Files (*.gszip)

IMPORTANT: In global environments, the import of an older setup that does not contain the current data state can lead to the deletion of data on other servers (e.g. users, groups, privileges..). Therefore the popup window **Attention! You are importing a setup into a global environment. The data might be older than the existing setup and could lead to deletion of data on other servers. Please verify if new data exists which will be overwritten! Do you really want to continue?** appears, where you have to click the **Continue** button to confirm this action.

Client Setup

Client Data

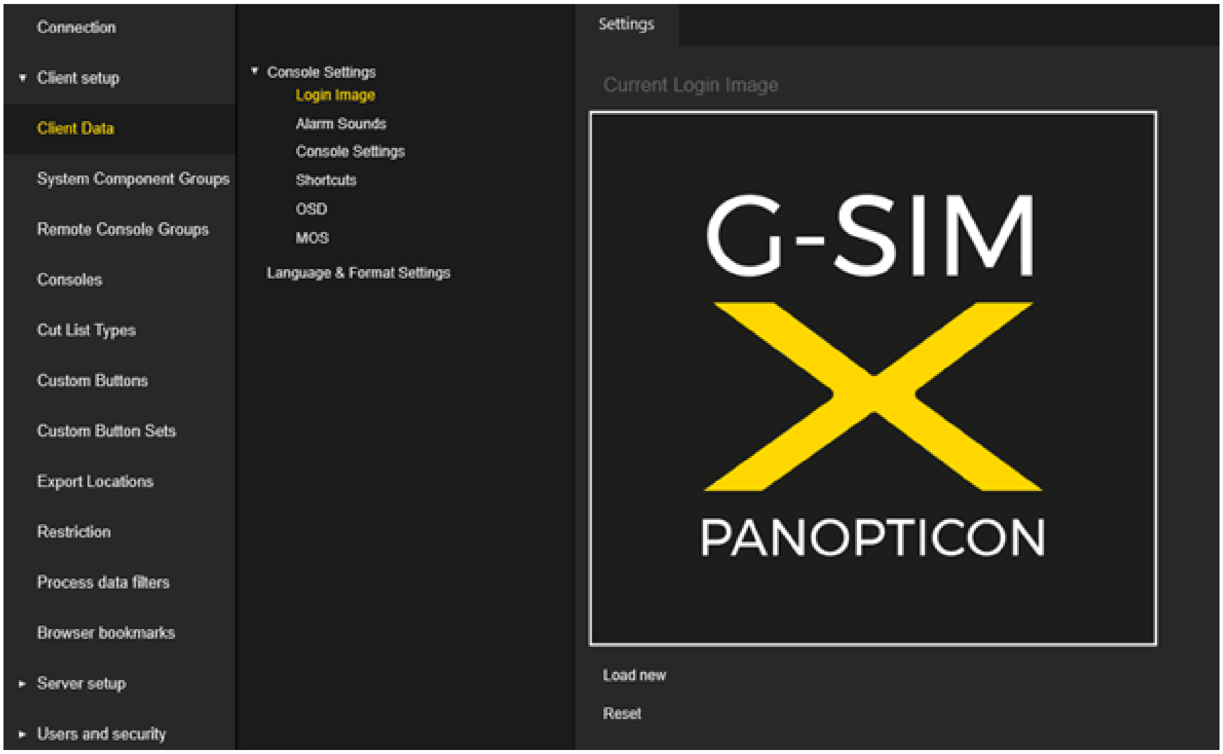
Client Data contains a set of settings that are used to customize the Operator Console.



Console Settings

Login Image

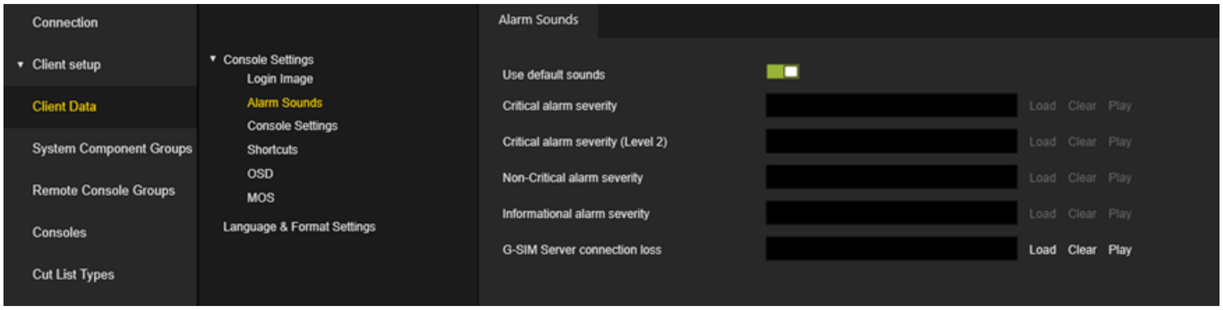
The administrator can configure the **Login Image** of the Operator Console.



- Click the **Load new** button to select the image file that will be used for the login image.
- Click the **Reset** button to set the default login image.

Alarm Sounds

The administrator can configure sounds to be played in the Operator Console when an alarm is received.



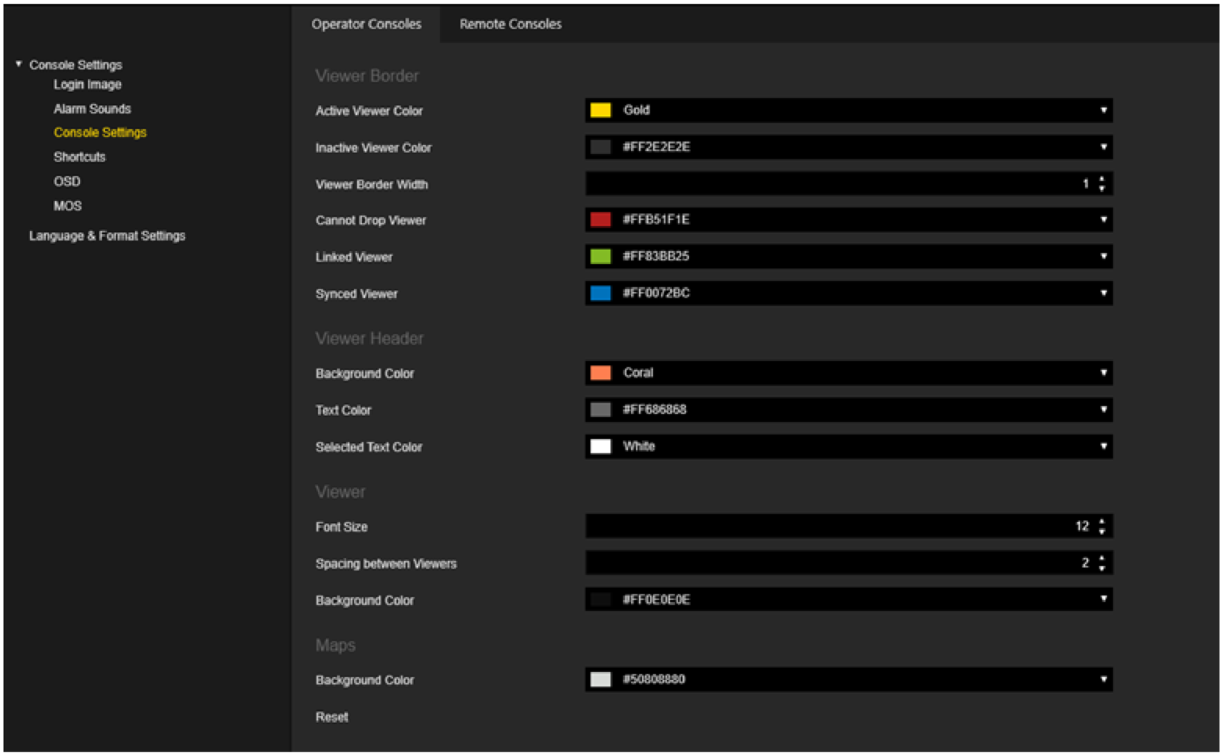
The **G-SIM Server connection loss** sound is used when the connection between the G-SIM server and the Operator Console is lost.

- Deactivate the **Used default sounds** slider to override the default sounds.
- Click the **Load** button to select the sound file to be used for the specific alarm. Only the WAV format is supported.
- Click the **Clear** button to remove the sound for the specific alarm.
- Click the **Play** button to check (hear) the sound for the specific alarm.

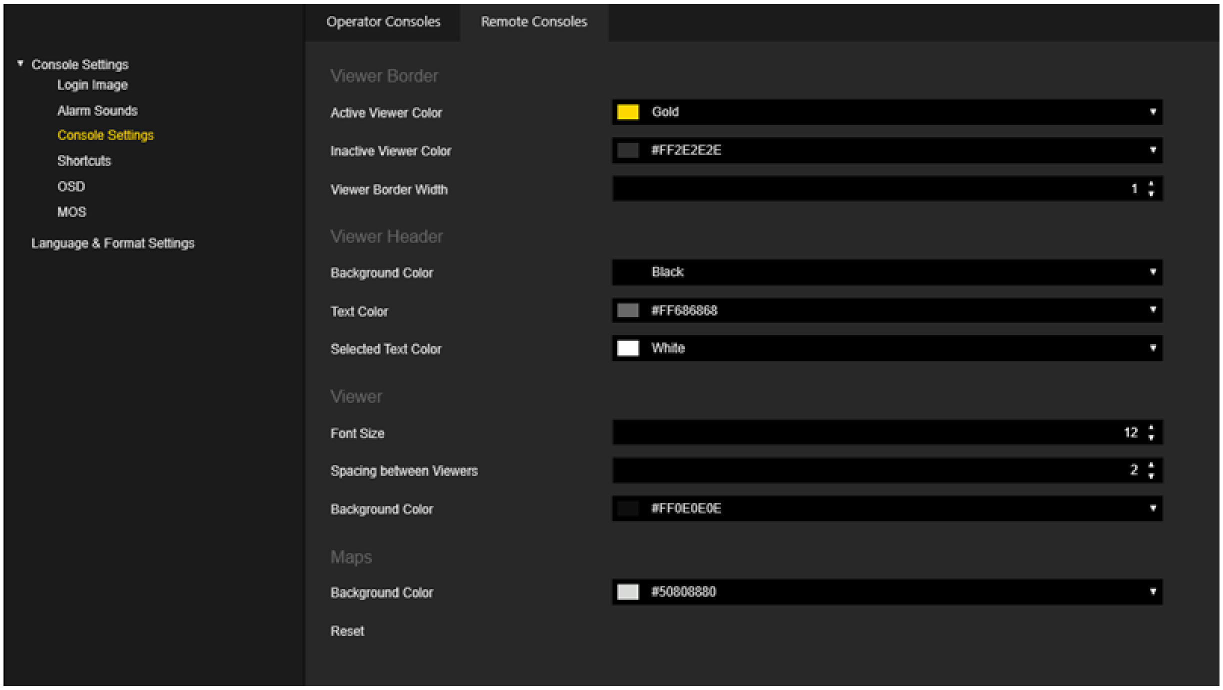
Alarm sounds can be overridden in the specific Alarm (see **Alarms**).

Console Settings

The administrator can configure visual settings that will be applied to the viewers in the **Operator Consoles** and **Remote Consoles**.



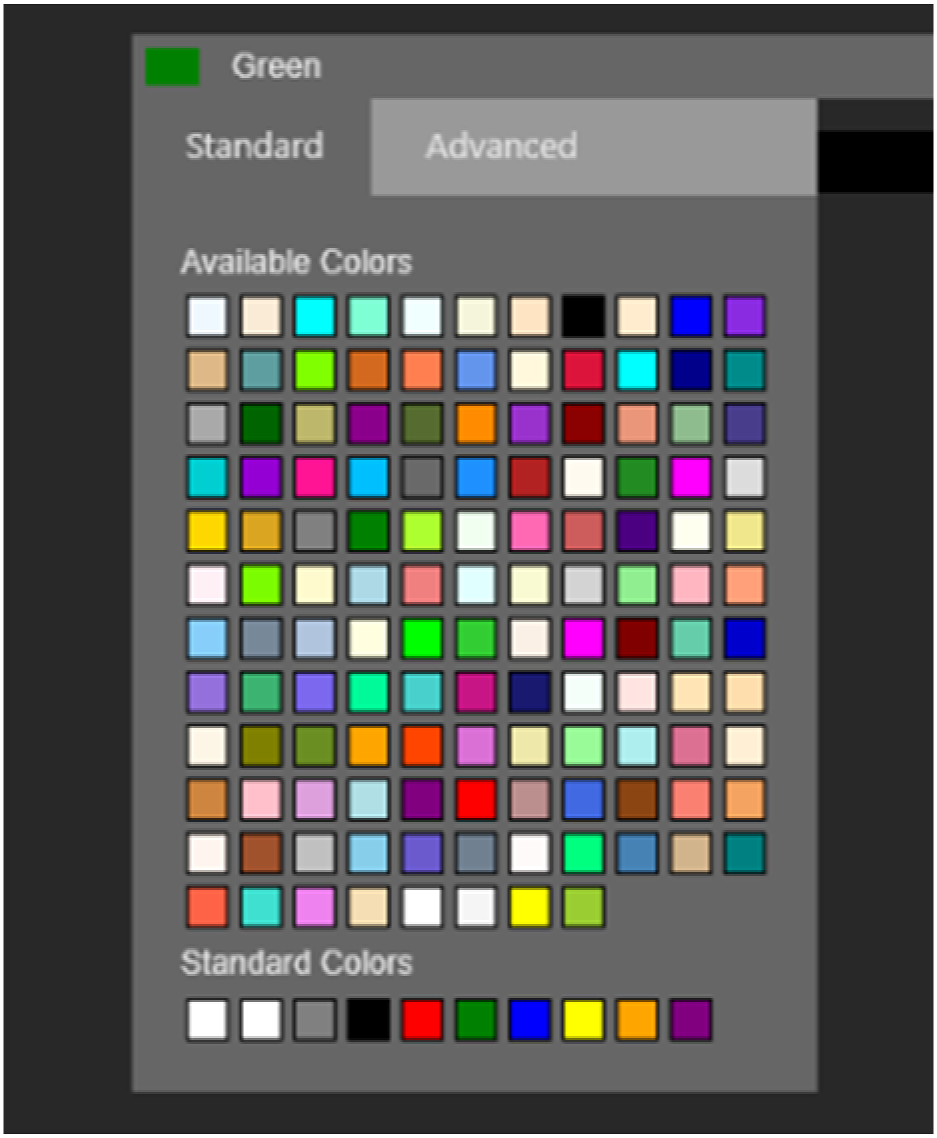
Viewer Border	
Active Viewer Color	Gold
Inactive Viewer Color	#FF2E2E2E
Viewer Border Width	1
Cannot Drop Viewer	#FFB51F1E
Linked Viewer	#FF83BB25
Synced Viewer	#FF0072BC
Viewer Header	
Background Color	Coral
Text Color	#FF686868
Selected Text Color	White
Viewer	
Font Size	12
Spacing between Viewers	2
Background Color	#FF0E0E0E
Maps	
Background Color	#50808880
Reset	



Viewer Border	
Active Viewer Color	Gold
Inactive Viewer Color	#FF2E2E2E
Viewer Border Width	1
Viewer Header	
Background Color	Black
Text Color	#FF686868
Selected Text Color	White
Viewer	
Font Size	12
Spacing between Viewers	2
Background Color	#FF0E0E0E
Maps	
Background Color	#50808880
Reset	

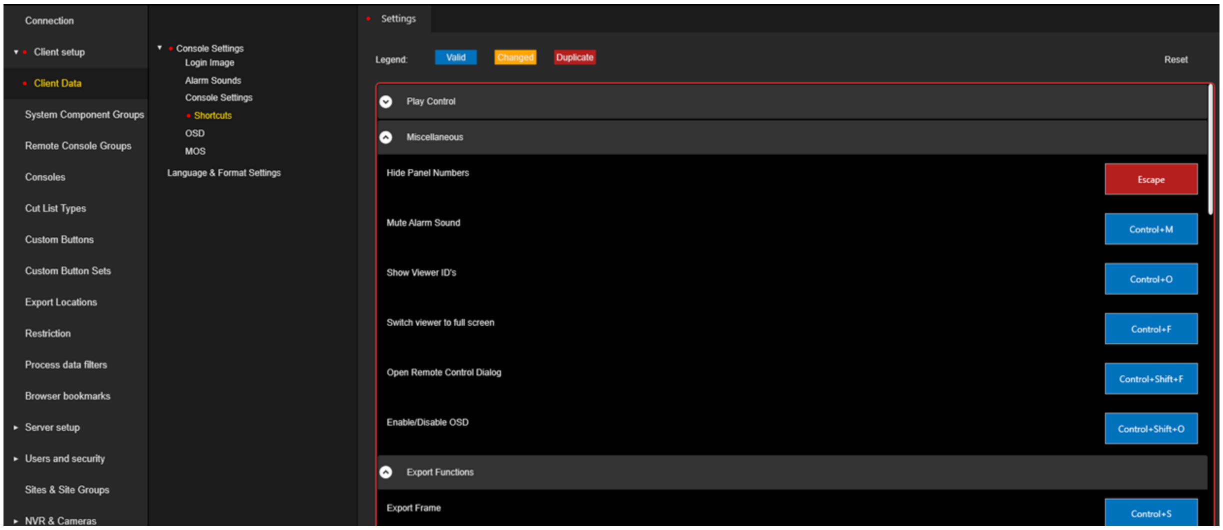
Click the **Reset** button to reset visual settings to the default values.

Specific colors can be selected by color selector control.



Shortcuts

The administrator can configure shortcuts to be used in the Operator Console to perform different actions.



Hide Panel Numbers: Escape

Mute Alarm Sound: Control+M

Show Viewer ID's: Control+O

Switch viewer to full screen: Control+F

Open Remote Control Dialog: Control+Shift+F

Enable/Disable OSD: Control+Shift+O

Export Frame: Control+S

The shortcuts are placed in the groups.

Click the rectangle of the shortcut and specify the key combination to be used for this shortcut.

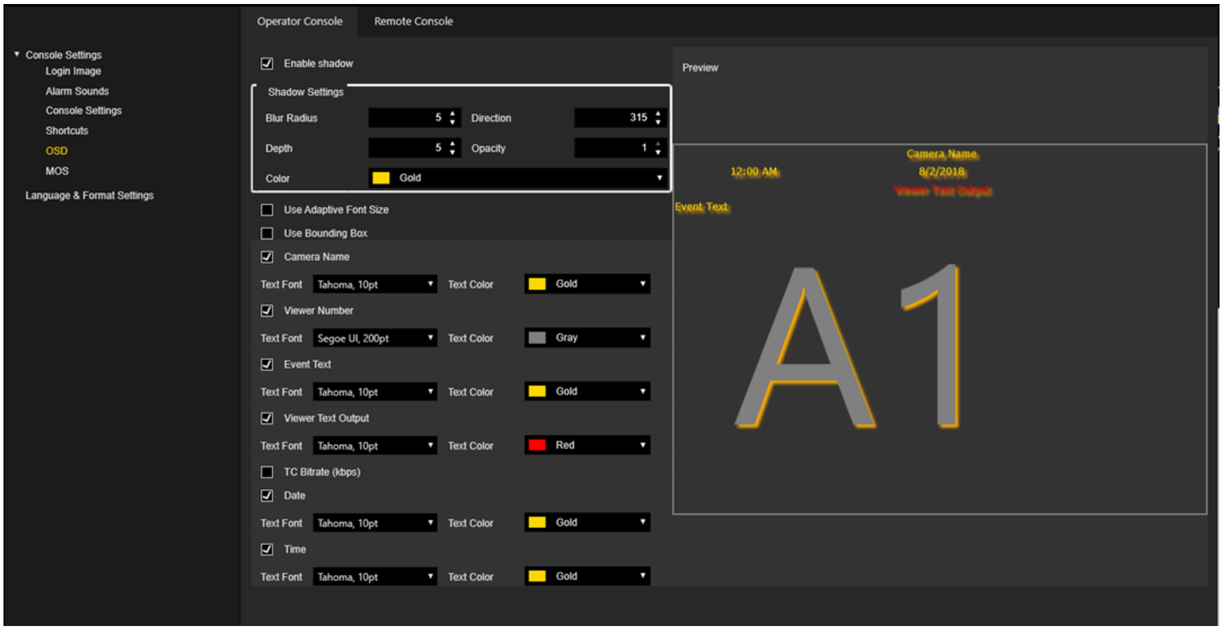
The shortcut state is displayed in color:

Color	Description
Red	Is used for shortcuts that use the same key combination.
Orange	Is used for shortcuts that have been recently changed by the administrator.
Blue	Is used to display valid and unchanged shortcuts.

Click the **Reset** button to reset the shortcut keys to default values.

OSD

The administrator can configure display parameters for different settings that can be displayed in the **Operator Console / Remote Console** viewers.



☑ Enable shadow

Shadow Settings

Blur Radius 5 Direction 315

Depth 5 Opacity 1

Color Gold

□ Use Adaptive Font Size

□ Use Bounding Box

☑ Camera Name

Text Font Tahoma, 10pt Text Color Gold

☑ Viewer Number

Text Font Segoe UI, 200pt Text Color Gray

☑ Event Text

Text Font Tahoma, 10pt Text Color Gold

☑ Viewer Text Output

Text Font Tahoma, 10pt Text Color Red

□ TC Bitrate (kbps)

☑ Date

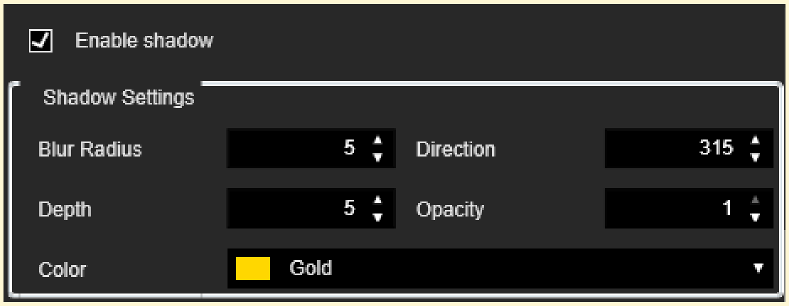
Text Font Tahoma, 10pt Text Color Gold

☑ Time

Text Font Tahoma, 10pt Text Color Gold

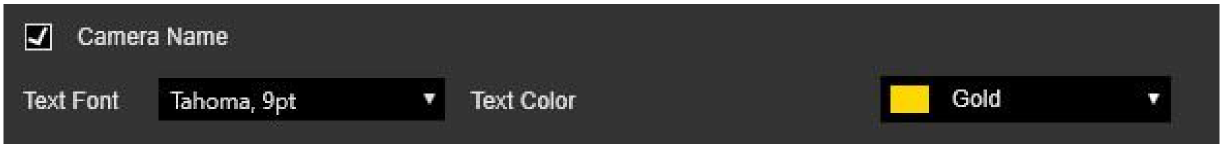
The **Operator Console** tab displays settings for the Operator Console. The **Remote Console** tab displays settings for the Remote Console. The sets of settings are the same for both console types.

The following settings can be configured:

Setting	Description
Shadow Settings	The administrator can configure the shadow parameters that will be applied to each visible text label.  ☑ Enable shadow Shadow Settings Blur Radius 5 Direction 315 Depth 5 Opacity 1 Color Gold
Use Bounding Box	Select this checkbox to draw a bounding box under each text label.
Camera Name	Configure settings for the **Camera Name** label.
Viewer	Configure settings for the **Viewer Number / Global Viewer Num-**

Setting	Description
Number	**ber** label.
Event Text	Configure settings for the **Event Text** label.
Viewer Text Output	Configure settings for the **Viewer Text Output** label.
TC Bitrate (kbps)	Configure settings for the **Transcoding Viewer Bitrate** label.
Date	Configure settings for the **Date** label.
Time	Configure settings for the **Time** label.

Each text label has the following configurable settings:



☑ Camera Name

Text Font: Tahoma, 9pt

Text Color: 🟨 Gold

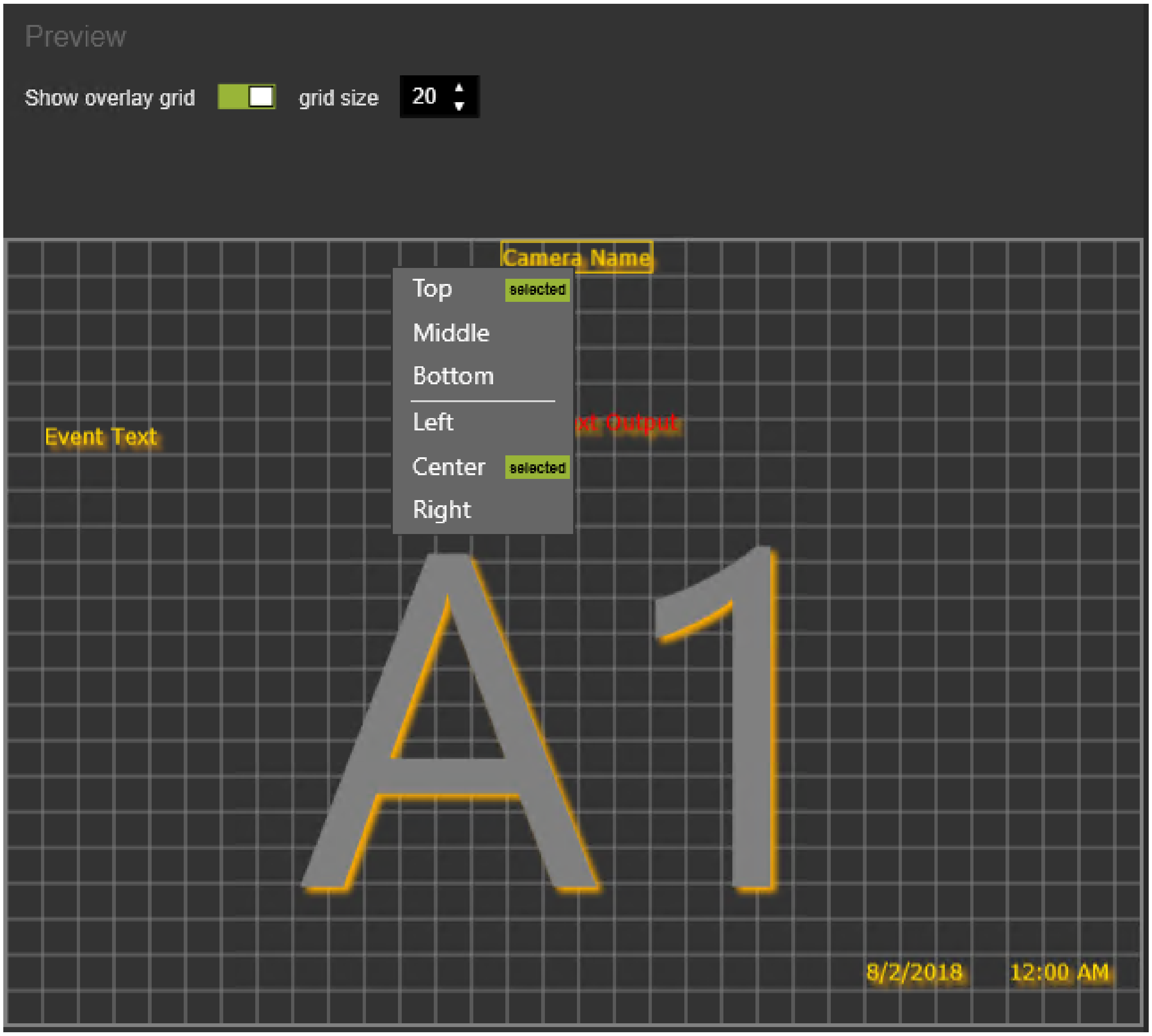
Setting	Description
Checkbox with label name	Select this checkbox to display the text label in the Viewer.
Text Font	Configure font parameters for the text label. **Note that the text font size is relative. It will be scaled according to the actual viewer height in the operator or remote console.**
Text Color	Configure color of the text label

The effects of the settings are displayed in the preview region.

- The position of the text label can be adjusted by dragging and dropping the respective label.
- Right-clicking in the preview region opens the context menu. This can be used to set the alignment of the text label.

Note that the operator or remote console can change the position of the text labels to avoid text overlapping.

- The Show overlay grid option can be used to simplify the positioning and alignment of text labels.



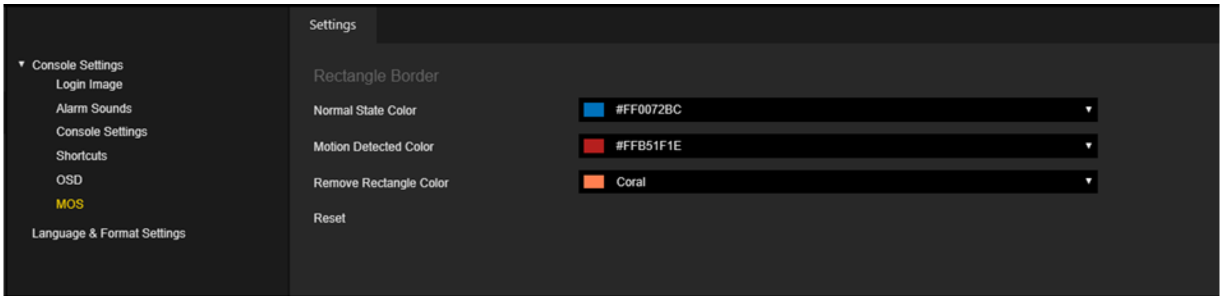
Preview

Show overlay grid: on

grid size: 20

MOS

The administrator can configure colors that will be used in the Operator Console to draw motion on the screen rectangle.



Settings

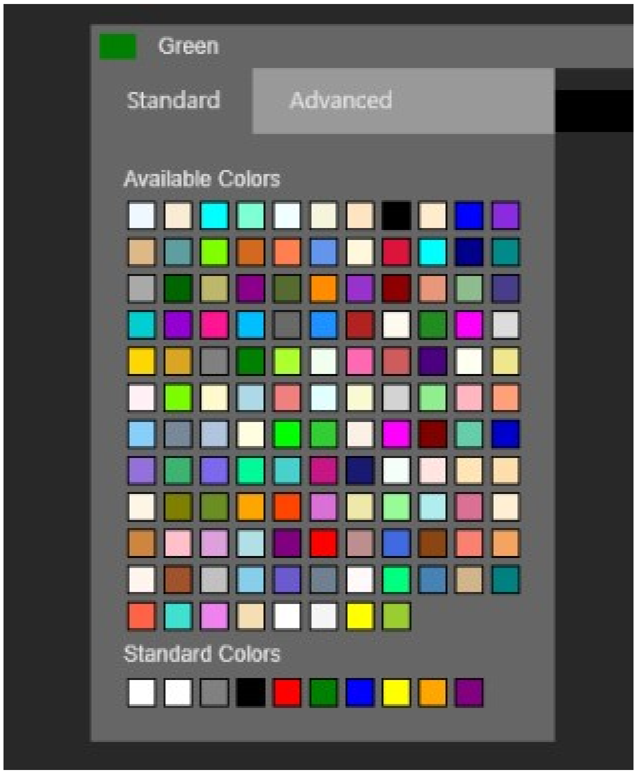
- Console Settings
  - Login Image
  - Alarm Sounds
  - Console Settings
  - Shortcuts
  - OSD
  - MOS
- Language & Format Settings

Rectangle Border

Normal State Color	🟦 #FF0072BC ▾
Motion Detected Color	🟥 #FFB51F1E ▾
Remove Rectangle Color	🟧 Coral ▾

Reset

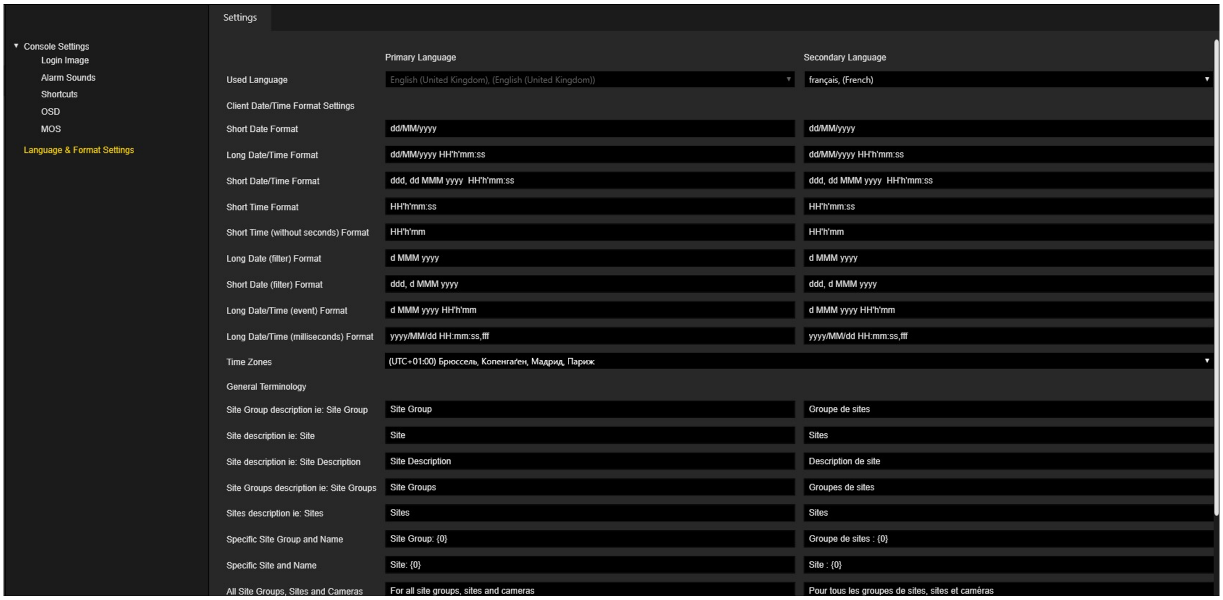
A specific color can be selected via the color selector control.



Click the **Reset** button to reset the colors to default values.

Language & Format Settings

The administrator can configure different settings that are used in the Operator Console user interface.



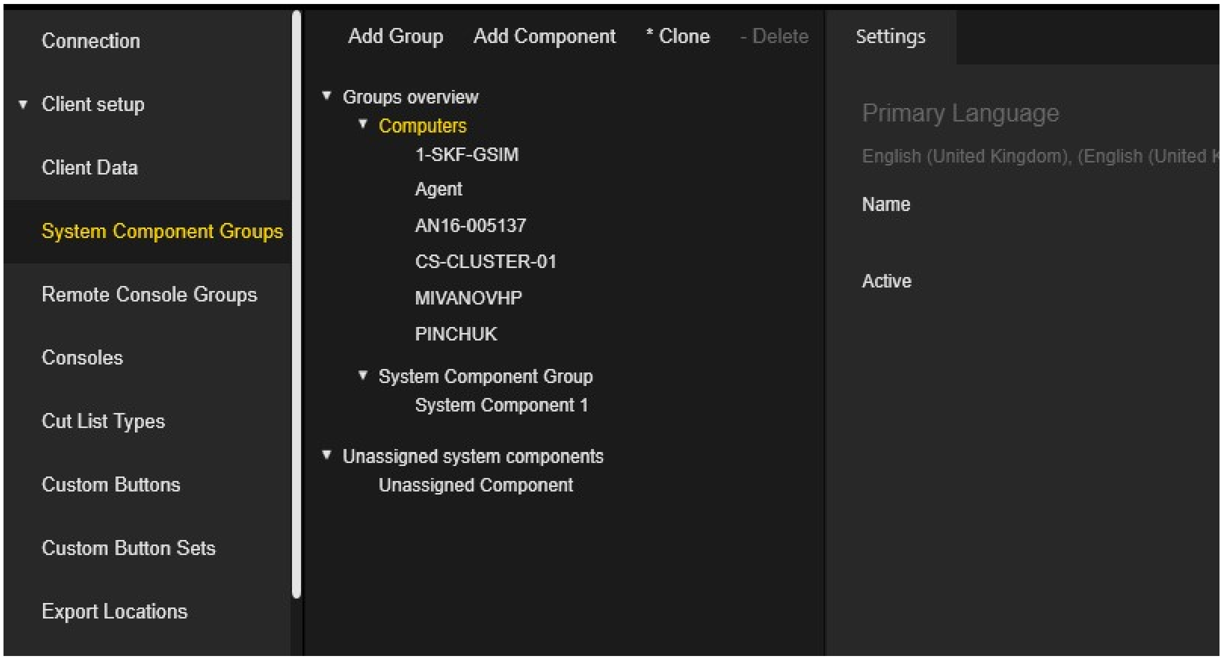
	Primary Language	Secondary Language
Used Language	English (United Kingdom), (English (United Kingdom))	français, (French)
Client Date/Time Format Settings		
Short Date Format	dd/MM/yyyy	dd/MM/yyyy
Long Date/Time Format	dd/MM/yyyy HH'h'mm:ss	dd/MM/yyyy HH'h'mm:ss
Short Date/Time Format	ddd, dd MMM yyyy HH'h'mm:ss	ddd, dd MMM yyyy HH'h'mm:ss
Short Time Format	HH'h'mm:ss	HH'h'mm:ss
Short Time (without seconds) Format	HH'h'mm	HH'h'mm
Long Date (filter) Format	d MMM yyyy	d MMM yyyy
Short Date (filter) Format	ddd, d MMM yyyy	ddd, d MMM yyyy
Long Date/Time (event) Format	d MMM yyyy HH'h'mm	d MMM yyyy HH'h'mm
Long Date/Time (milliseconds) Format	yyyy/MM/dd HH:mm:ss,fff	yyyy/MM/dd HH:mm:ss,fff
Time Zones	(UTC+01:00) Брюссель, Копенгаґен, Мадрид, Париж	
General Terminology		
Site Group description ie: Site Group	Site Group	Groupe de sites
Site description ie: Site	Site	Sites
Site description ie: Site Description	Site Description	Description de site
Site Groups description ie: Site Groups	Site Groups	Groupes de sites
Sites description ie: Sites	Sites	Sites
Specific Site Group and Name	Site Group: {0}	Groupe de sites : {0}
Specific Site and Name	Site: {0}	Site : {0}
All Site Groups, Sites and Cameras	For all site groups, sites and cameras	Pour tous les groupes de sites, sites et caméras

Each setting can be configured for primary and secondary language.

Click the **Set Default Values** button to reset the settings to default values.

System Component Groups

The **System Component Groups** view contains components that are organized in groups. The administrator can create groups and components inside groups. Components can be moved between groups using Drag & Drop.



Primary Language

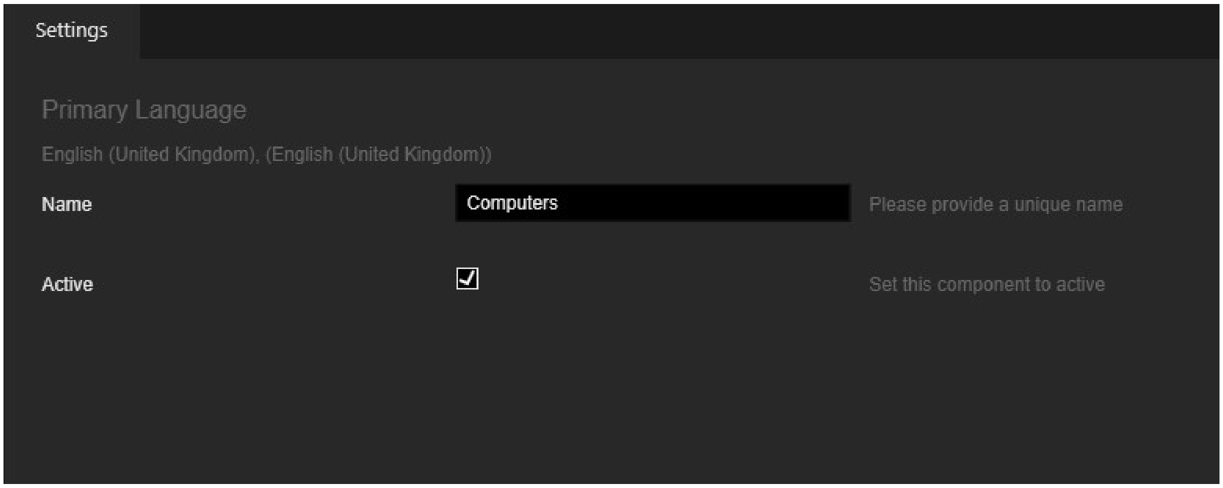
English (United Kingdom), (English (United K

Name

Active

System Group Settings

The administrator can configure the name of the groups and set **active** or **inactive** state for the group.



Settings

Primary Language

English (United Kingdom), (English (United Kingdom))

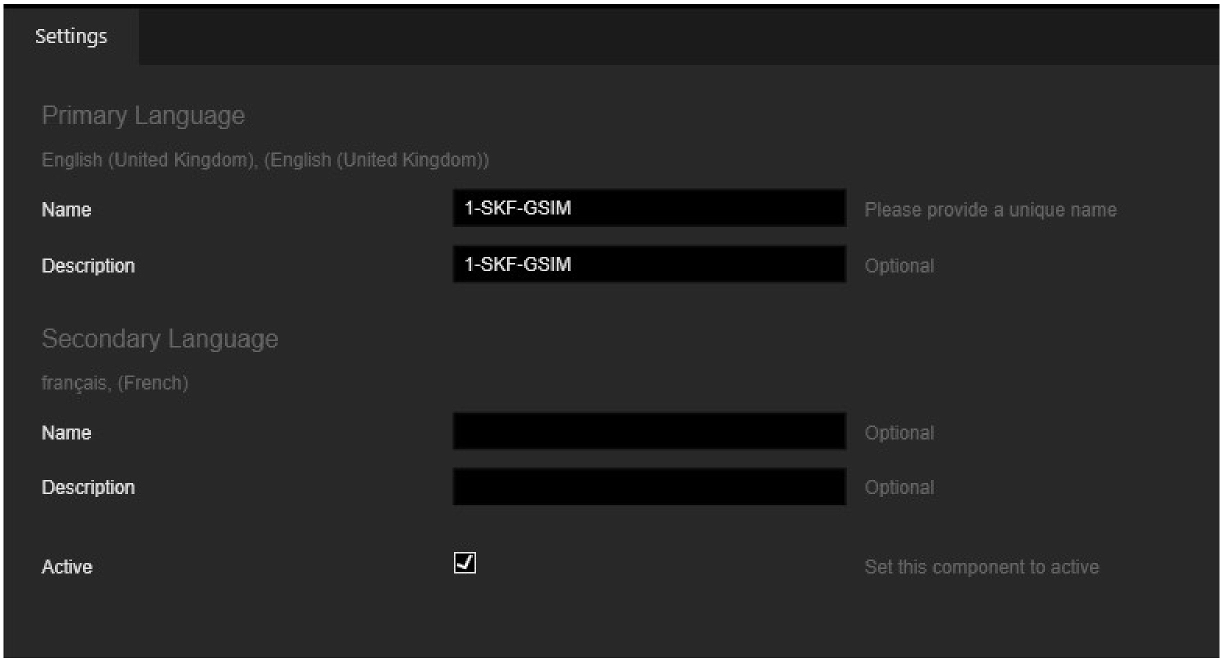
Name: Computers — Please provide a unique name

Active: ☑ — Set this component to active

When client application tries to connect to the G-SIM server for the first time, a component with the client's computer name is automatically created and added to the **Computers** system group.

System Component Settings

The administrator can configure **Name** and **Description** of the component for the primary and secondary languages and set the **active** or **inactive** state for the component.



Settings

Primary Language

English (United Kingdom), (English (United Kingdom))

Name: 1-SKF-GSIM — Please provide a unique name

Description: 1-SKF-GSIM — Optional

Secondary Language

français, (French)

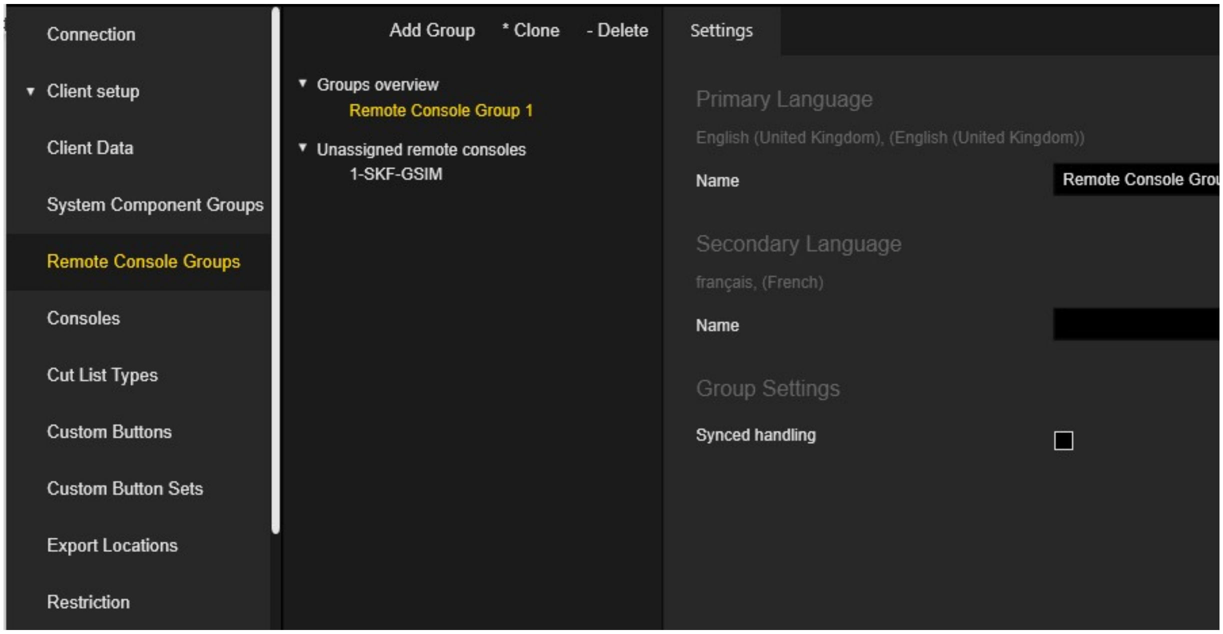
Name: — Optional

Description: — Optional

Active ☑ — Set this component to active

Remote Console Groups

The administrator can create groups and assign existing remote consoles to the groups. Remote consoles can be moved between groups using Drag & Drop.



Groups overview
- Remote Console Group 1

Unassigned remote consoles
- 1-SKF-GSIM

Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Remote Console Grou

Secondary Language

français, (French)

Name:

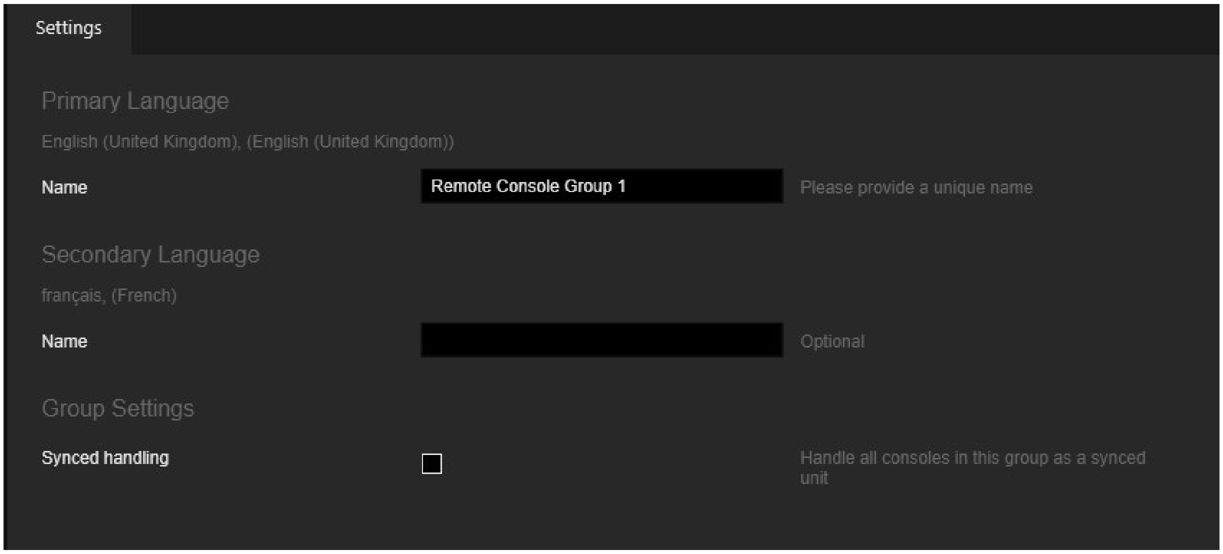
Group Settings

Synced handling □

Settings

The administrator can configure the group name for both the primary and secondary languages.

The administrator can select the **Synced handling** option to handle all remote consoles in this group as a single unit. When this option is selected, what is done with one remote console in this group will be done with all of them.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Remote Console Group 1 — Please provide a unique name

Secondary Language

français, (French)

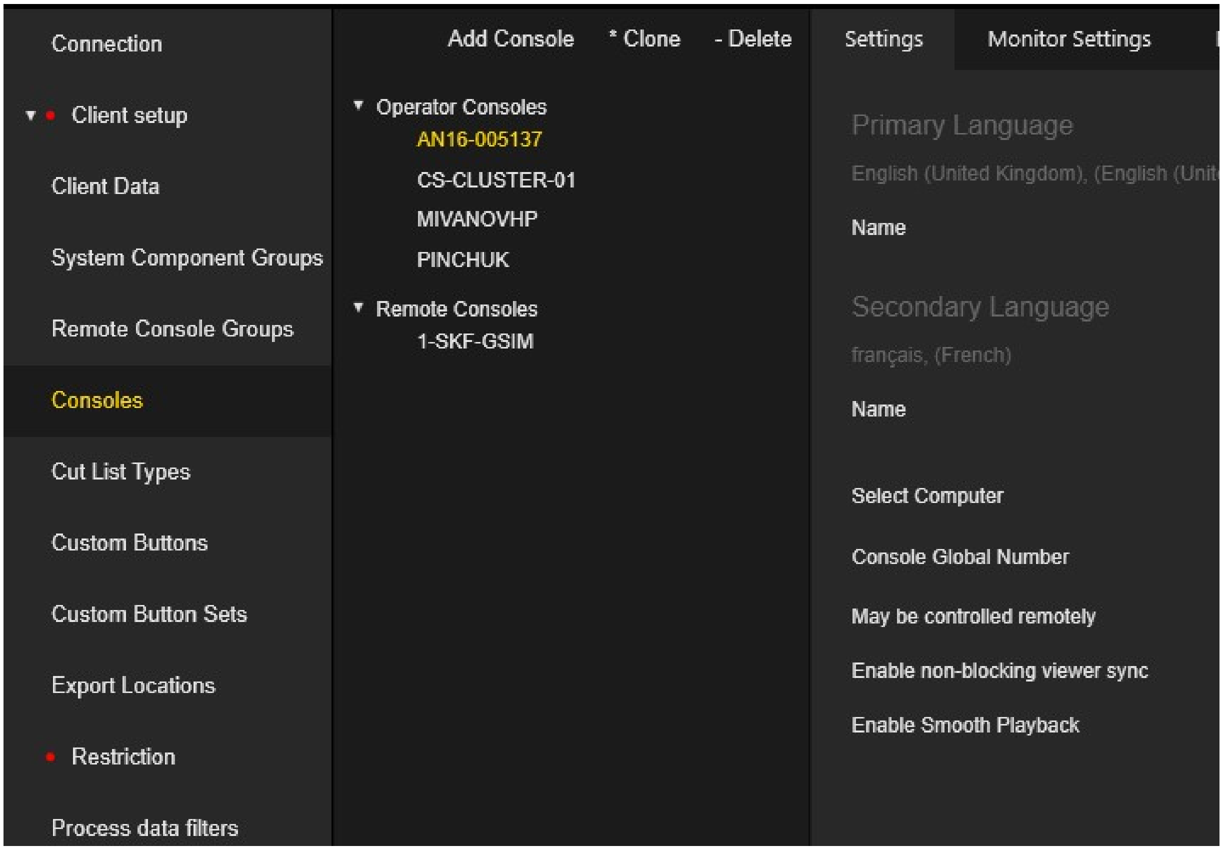
Name: — Optional

Group Settings

Synced handling □ — Handle all consoles in this group as a synced unit

Consoles

The administrator can create consoles and move them between the types **Operator Consoles** and **Remote Consoles** using Drag & Drop.



When the Operator Console tries to connect to the G-SIM server for the first time, a record with the client’s computer name is automatically created and added to Operator Consoles.

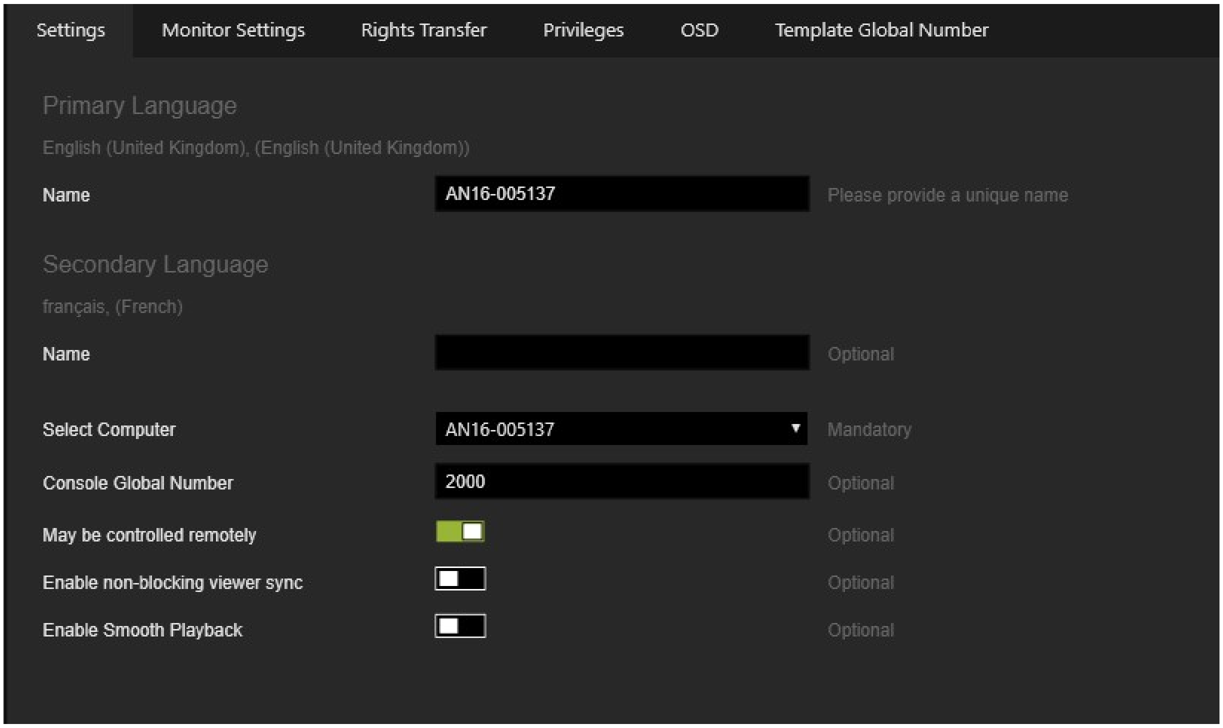
Operator Console Settings

Operator Consoles are the face of G-SIM as far as the operators are concerned. Here they interact with the interconnected system of cameras, NVRs, storage, rules and more.

The Consoles settings are grouped in tabs.

Settings

The administrator can configure the following settings:



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: AN16-005137 — Please provide a unique name

Secondary Language

français, (French)

Name: — Optional

Select Computer: AN16-005137 ▾ — Mandatory

Console Global Number: 2000 — Optional

May be controlled remotely: ● — Optional

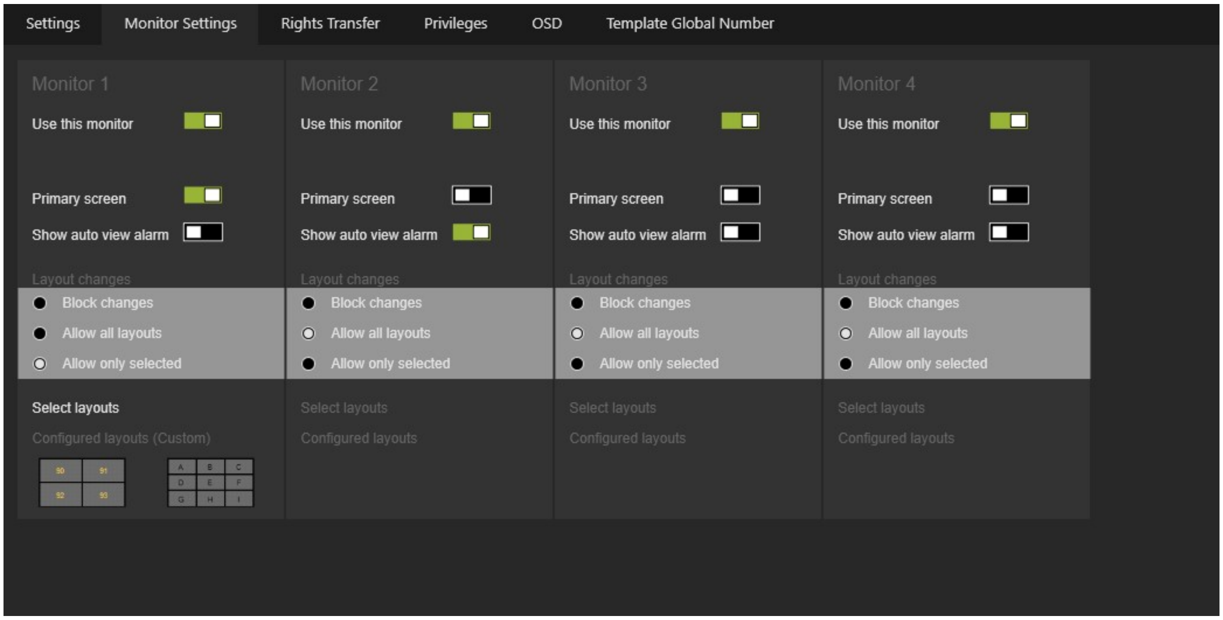
Enable non-blocking viewer sync: ○ — Optional

Enable Smooth Playback: ○ — Optional

Setting	Description
Name	Name of the console in the primary and secondary languages.
Select Computer	Name of the computer where the Operator Console is installed. The selection list is populated from the System Component Group **Computers**.
Console Global Number	This number is used in Remote Console Actions to identify the Operator Console.
May be controlled remotely	Possibility to allow remote users with the correct rights to control this Operator Console remotely while another user is logged in.
Enable non-blocking sync	Activate this slider to enable non-blocking sync in the video viewers of this Operator Console.
Enable Smooth Playback	Activate this slider to enable smooth playback in the video viewers of this Operator Console.

Monitor Settings

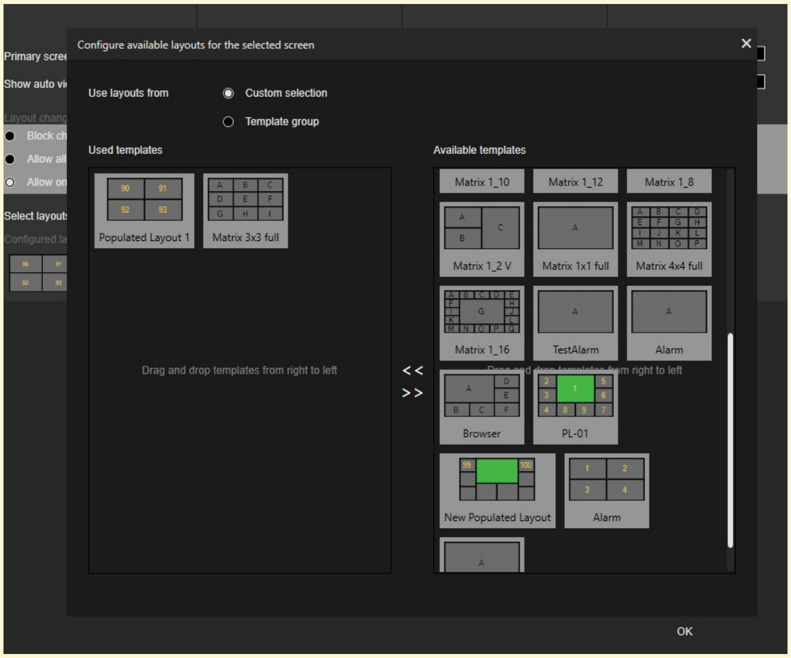
The administrator can configure up to four monitors that can be used in the specific Operator Console.



Monitor 1	Monitor 2	Monitor 3	Monitor 4
Use this monitor ☑	Use this monitor ☑	Use this monitor ☑	Use this monitor ☑
Primary screen ☑	Primary screen ☐	Primary screen ☐	Primary screen ☐
Show auto view alarm ☐	Show auto view alarm ☑	Show auto view alarm ☐	Show auto view alarm ☐
Layout changes	Layout changes	Layout changes	Layout changes
● Block changes	● Block changes	● Block changes	● Block changes
● Allow all layouts	○ Allow all layouts	○ Allow all layouts	○ Allow all layouts
○ Allow only selected	● Allow only selected	● Allow only selected	● Allow only selected
Select layouts	Select layouts	Select layouts	Select layouts
Configured layouts (Custom)	Configured layouts	Configured layouts	Configured layouts

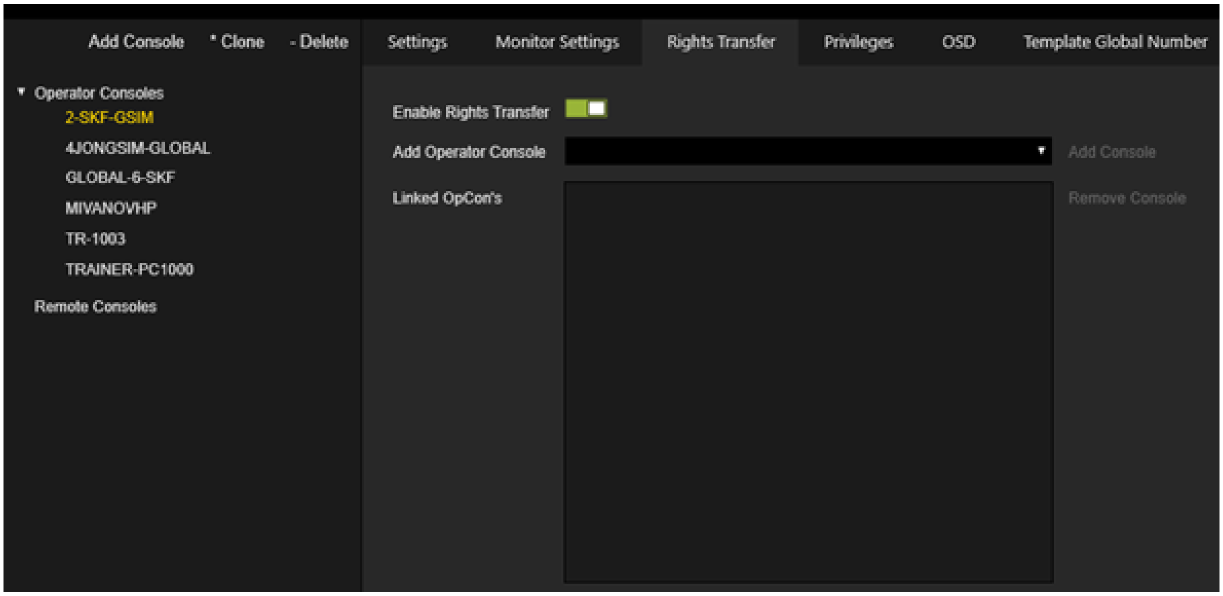
Each monitor has the same set of settings:

Settings	Description
Use this monitor	Activate this slider to use this monitor in the specific Operator Console.
Primary screen	Activate this slider to use this monitor as the primary monitor in the specific Operator Console. Only one monitor can be marked as **Primary Screen**.
Show auto view alarm	Activate this slider to use this monitor for display auto view alarms in the specific Operator Console. Only one monitor can be marked as **Show auto view alarm**. If no monitor is marked with **Show auto view alarm**, the primary monitor is used for the auto view alarms.
Layout changes:	

Settings	Description
Block changes	Select to disable users to switch the layouts on this monitor in the specific Operator Console.
Allow all layouts	Select to allow the user to choose any configuration layout in the specific Operator Console.
Allow only selected	The administrator can select a list of the layouts that can be used on this monitor by the user of the specific Operator Console.  Configure available layouts for the selected screen Use layouts from ● Custom selection ○ Template group Used templates: Populated Layout 1, Matrix 3x3 full Available templates Drag and drop templates from right to left Matrix 1_10 Matrix 1_12 Matrix 1_8 Matrix 1_2 V Matrix 1x1 full Matrix 4x4 full Matrix 1_16 TestAlarm Alarm Browser PL-01 New Populated Layout Alarm << >> OK

Rights Transfer

The **Rights Transfer** setting refers to the ability of the console to be started in the auto-login mode.

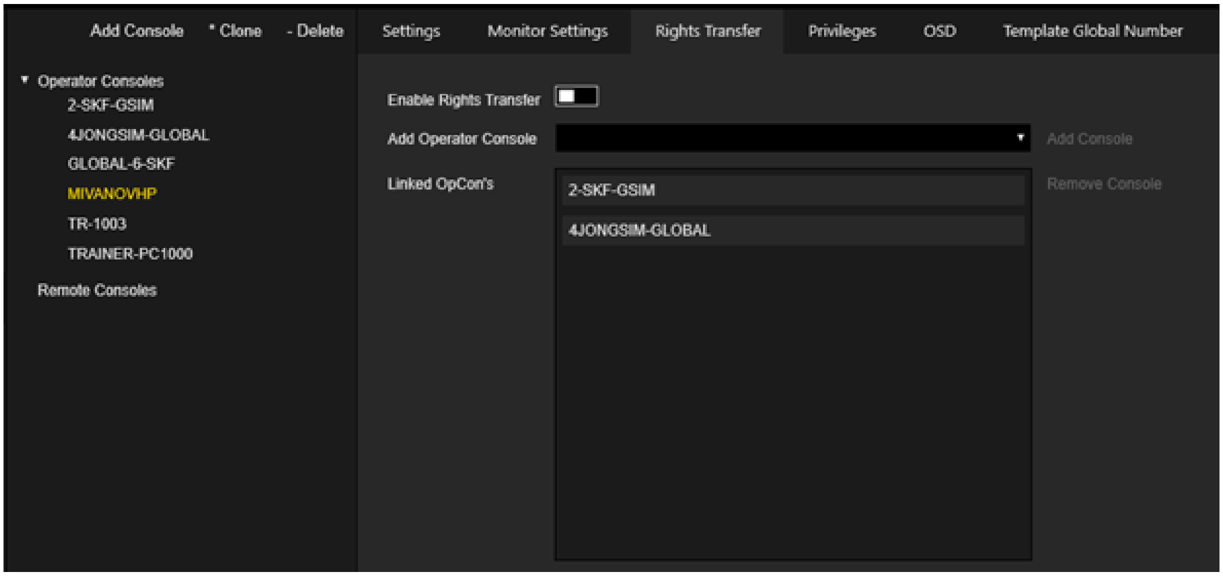


Enable Rights Transfer ●

Add Operator Console

Linked OpCon's

The **Linked OpCon’s** list contains consoles that can be controlled from the current console.



Enable Rights Transfer ○

Add Operator Console

Linked OpCon's
- 2-SKF-GSIM
- 4JONGSIM-GLOBAL

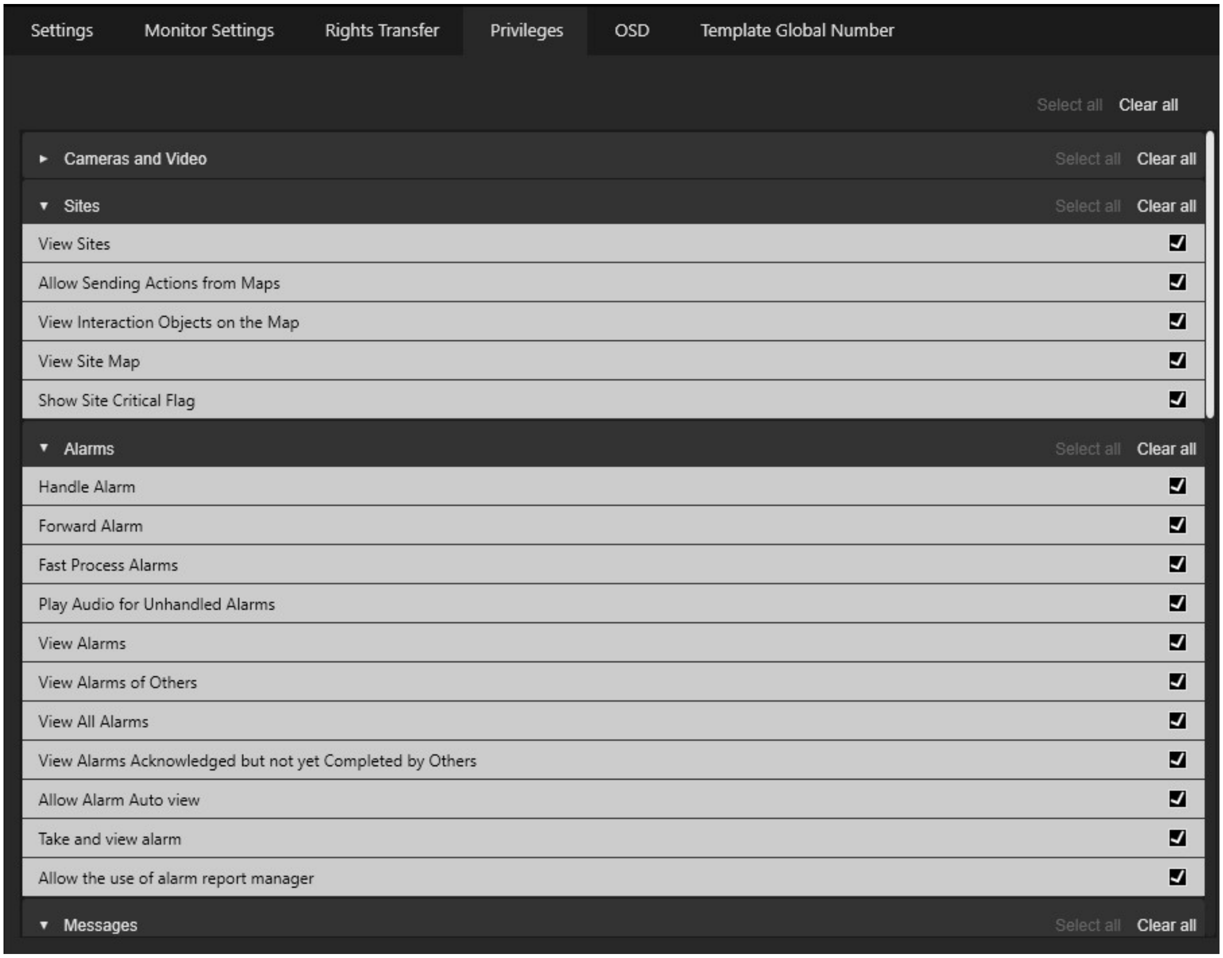
The administrator can add the Operator Console to the **Linked OpCon’s** list or remove the Operator Console from this list.

Note that console can only be controlled if it is started in the auto-login mode and the **May be controlled remotely** setting is activated. The user of the controlling console can manage all cameras etc. of the linked consoles that are in auto-login mode.

In the example above, the user of the MIVANOVHP console can control the 2-SKF-GSIM console if the 2-SKF-GSIM console is started in the auto-login mode.

Privileges

The administrator can configure the privileges of the specific Operator Console. If no privilege is selected, the specific Operator Console has all rights. The Console privileges can be overridden by the User / User Group privileges. The privileges are organized in groups. The administrator can use Select all and Clear all buttons to set / revoke all privileges in the group with one click. The administrator can hold the mouse cursor under the privilege to display a detailed description.



View Sites ☑
Allow Sending Actions from Maps ☑
View Interaction Objects on the Map ☑
View Site Map ☑
Show Site Critical Flag ☑

Handle Alarm ☑
Forward Alarm ☑
Fast Process Alarms ☑
Play Audio for Unhandled Alarms ☑
View Alarms ☑
View Alarms of Others ☑
View All Alarms ☑
View Alarms Acknowledged but not yet Completed by Others ☑
Allow Alarm Auto view ☑
Take and view alarm ☑
Allow the use of alarm report manager ☑

Overriding of default Privileges

There are separate sets of privileges for consoles and users.

Even for the Remote Console (ReCon) a virtual, but not visible user is created . This user has all privileges except Override Console Restrictions and Override Default Privileges.

When Operator Console or ReCon connects to G-SIM Server a combination of the console and user privileges is used to determine user's result rights. The user's privileges will be used if Override Default Privileges is selected.

If Override Default Privileges is NOT selected and the console has NO privileges set, the user’s privileges will be used.

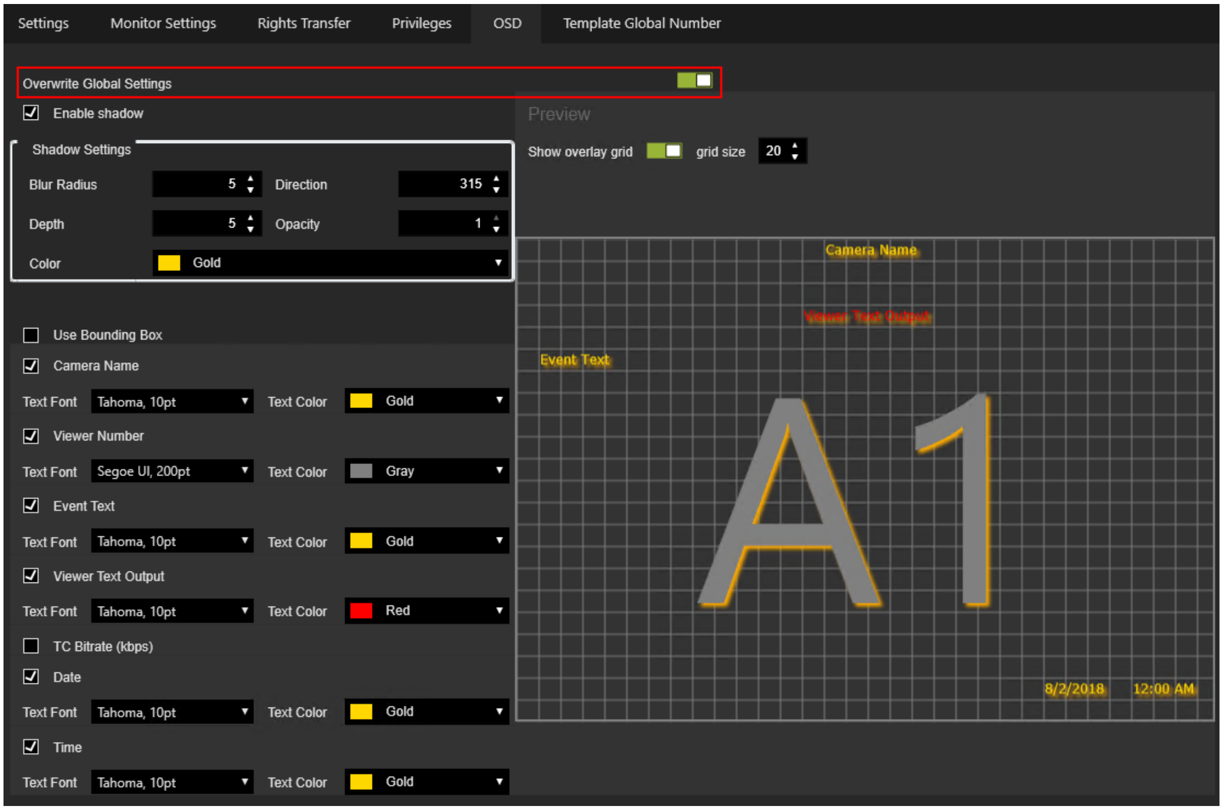
If Override Default Privileges is NOT selected and the console has privileges set, only the privileges where both, the console and the user privileges are selected, will be used.

There is no mechanism in the Management Console to determine connected users and from which consoles they are currently connected to show the current combination of users and consoles privileges.

The Management Console operates with Server Setup. Therefore it is stable ans independent from temporary states like connected users or consoles.

OSD

The administrator can override the default OSD settings for the specific Operator Console. See **OSD** for a detailed description of the OSD settings.



Overwrite Global Settings

☑ Enable shadow

Shadow Settings

Blur Radius 5 Direction 315

Depth 5 Opacity 1

Color 🟨 Gold

□ Use Bounding Box

☑ Camera Name

Text Font Tahoma, 10pt Text Color 🟨 Gold

☑ Viewer Number

Text Font Segoe UI, 200pt Text Color ⬜ Gray

☑ Event Text

Text Font Tahoma, 10pt Text Color 🟨 Gold

☑ Viewer Text Output

Text Font Tahoma, 10pt Text Color 🟥 Red

□ TC Bitrate (kbps)

☑ Date

Text Font Tahoma, 10pt Text Color 🟨 Gold

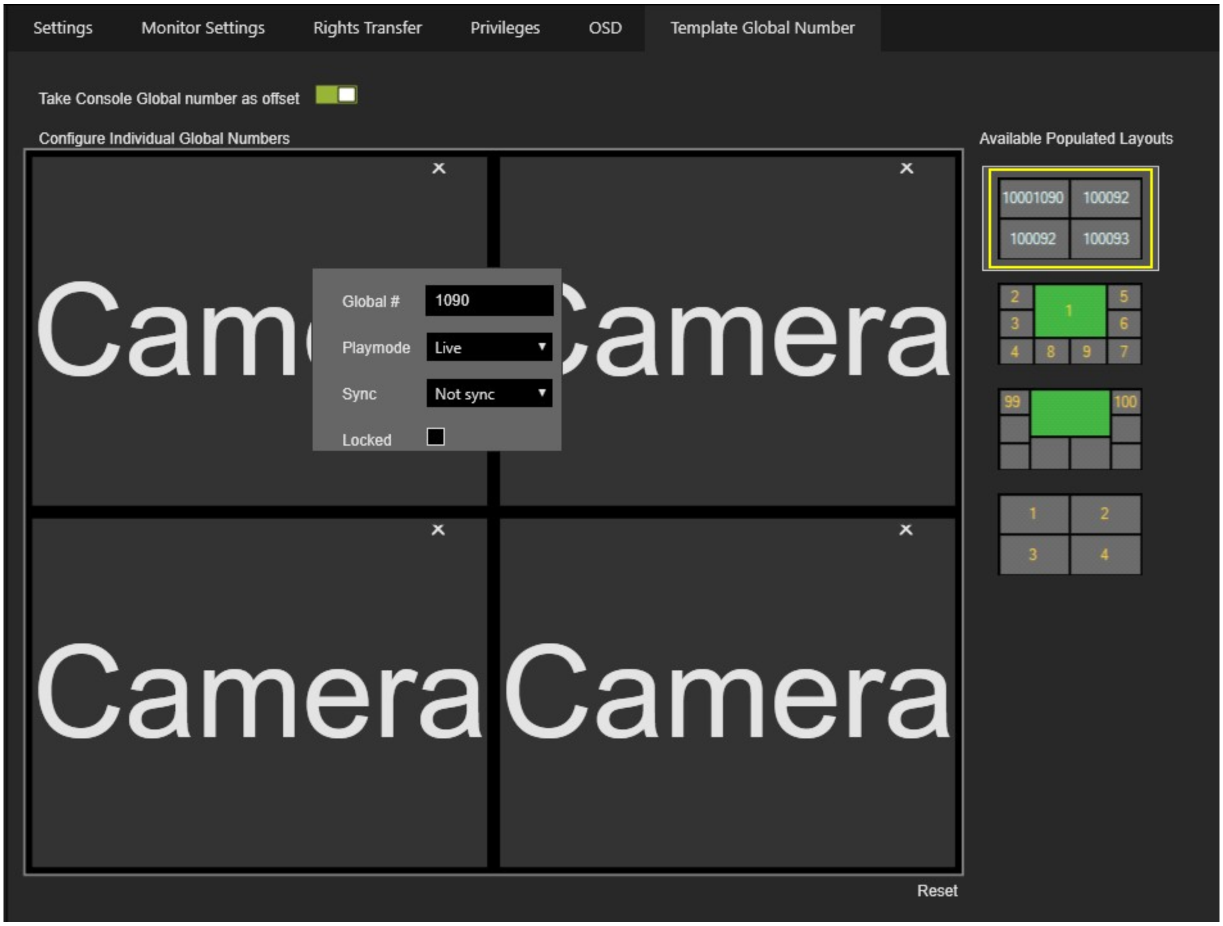
☑ Time

Text Font Tahoma, 10pt Text Color 🟨 Gold

Show overlay grid grid size 20

Template Global Number

The administrator can override the viewer global numbers of the populated layouts for the specific console. Viewer global numbers are used to identify the viewer in the remote viewer actions.



Take Console Global number as offset

Global # 1090

Playmode Live

Sync Not sync

Locked □

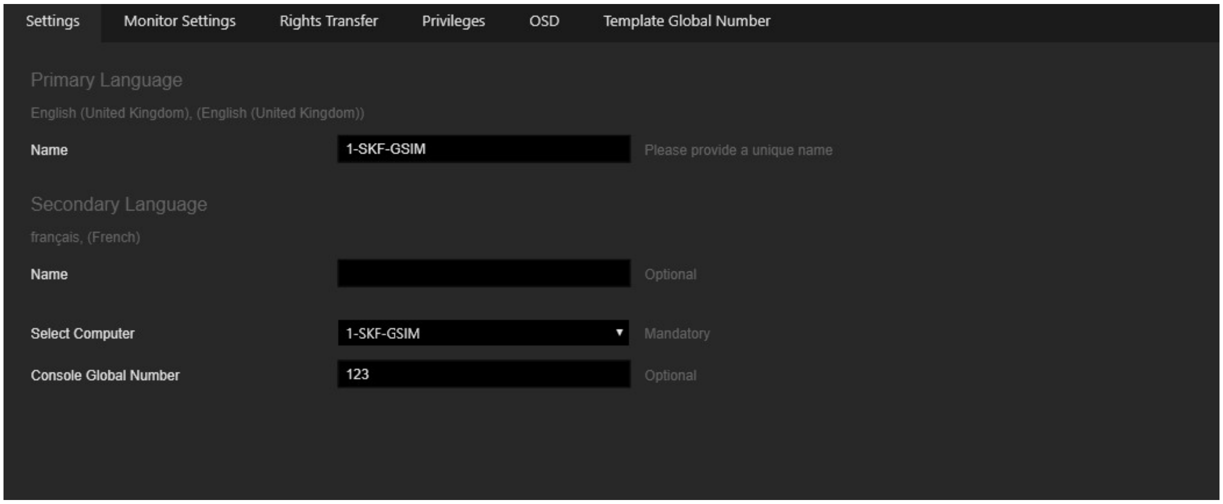
The administrator can select a specific populated layout on the right side and perform the following action:

- Select **Take Console Global number as offset** to add a non-zero Console Global number at the start of the Viewer Global number.
- Use the right-click context menu to configure the Viewer Global number for the specific Operator Console.
- Click the **Reset** button to discard the overriding of the Viewer Global numbers.

Remote Console Settings

Remote Consoles are just like Operator Consoles, with one glaring exception: they have no user interface. They are therefore remotely controlled by those who are authorized to do so. They are also the building blocks of video walls, which usually consist of a number of remote consoles that work in tandem. The content of each screen is determined by the normal G-SIM users (such as operators or supervisors) and the system rules, which may restrict some content, set some default content views, etc..

The remote console has a reduced set of the settings in comparison with the operator console:



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: 1-SKF-GSIM — Please provide a unique name

Secondary Language

français, (French)

Name: — Optional

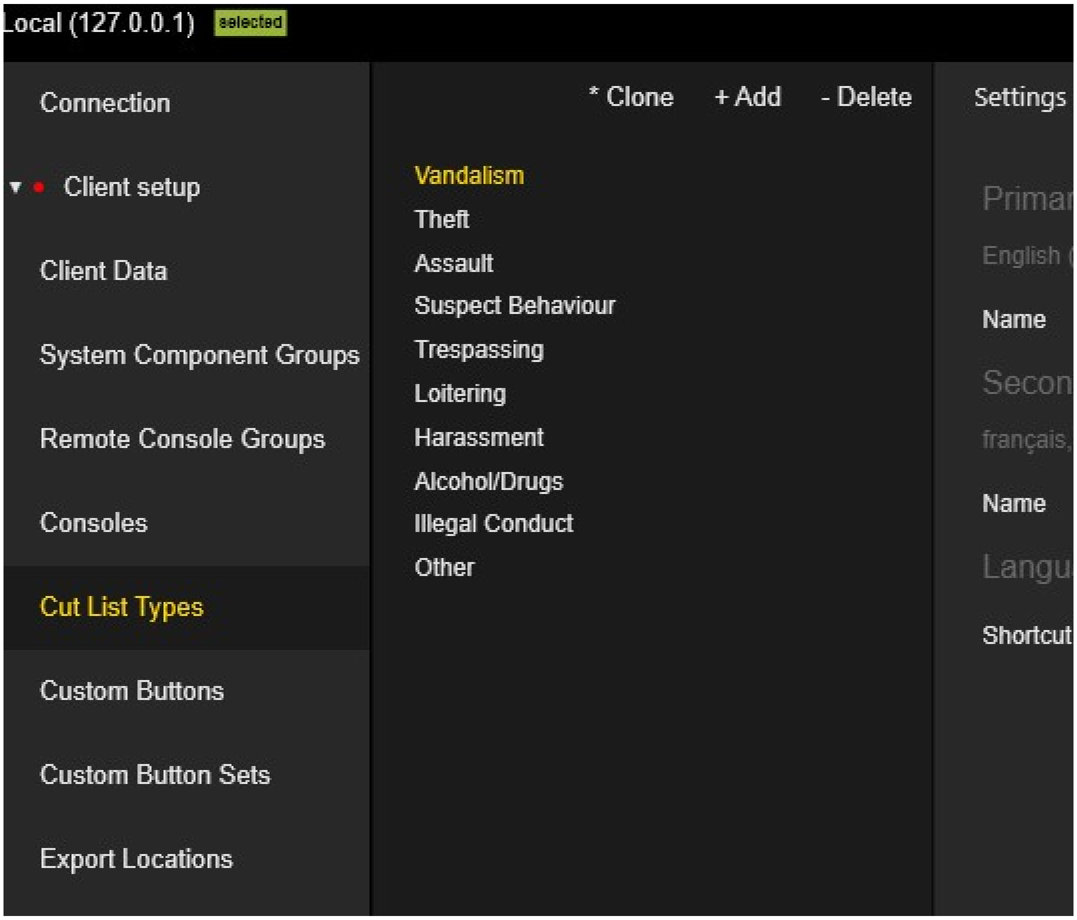
Select Computer: 1-SKF-GSIM — Mandatory

Console Global Number: 123 — Optional

For details, refer to **Operator Console Settings**.

Cut List Types

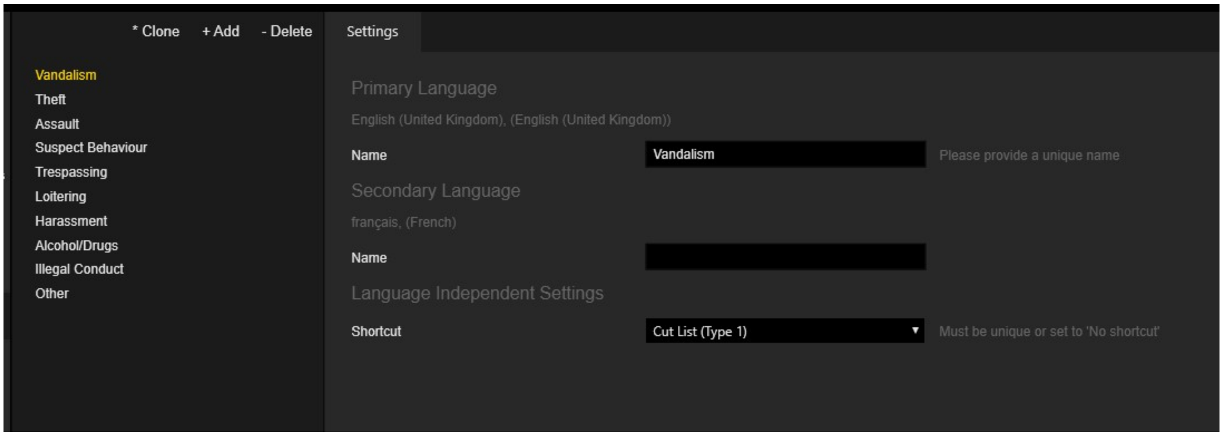
The Cut List Types view contains a list of the types which are used in the Operator Console´s cut lists. The default set of cut list types is created when G-SIM server is installed.



Settings

The administrator can configure the name of the cut list type for both the primary and secondary languages.

The administrator can select a shortcut to quickly create a cut list of the specific type in the Operator Console. The shortcut key that is used for the cut list type can be configured in the **Client Data Shortcuts View**.



Vandalism
Theft
Assault
Suspect Behaviour
Trespassing
Loitering
Harassment
Alcohol/Drugs
Illegal Conduct
Other

Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Vandalism — Please provide a unique name

Secondary Language

français, (French)

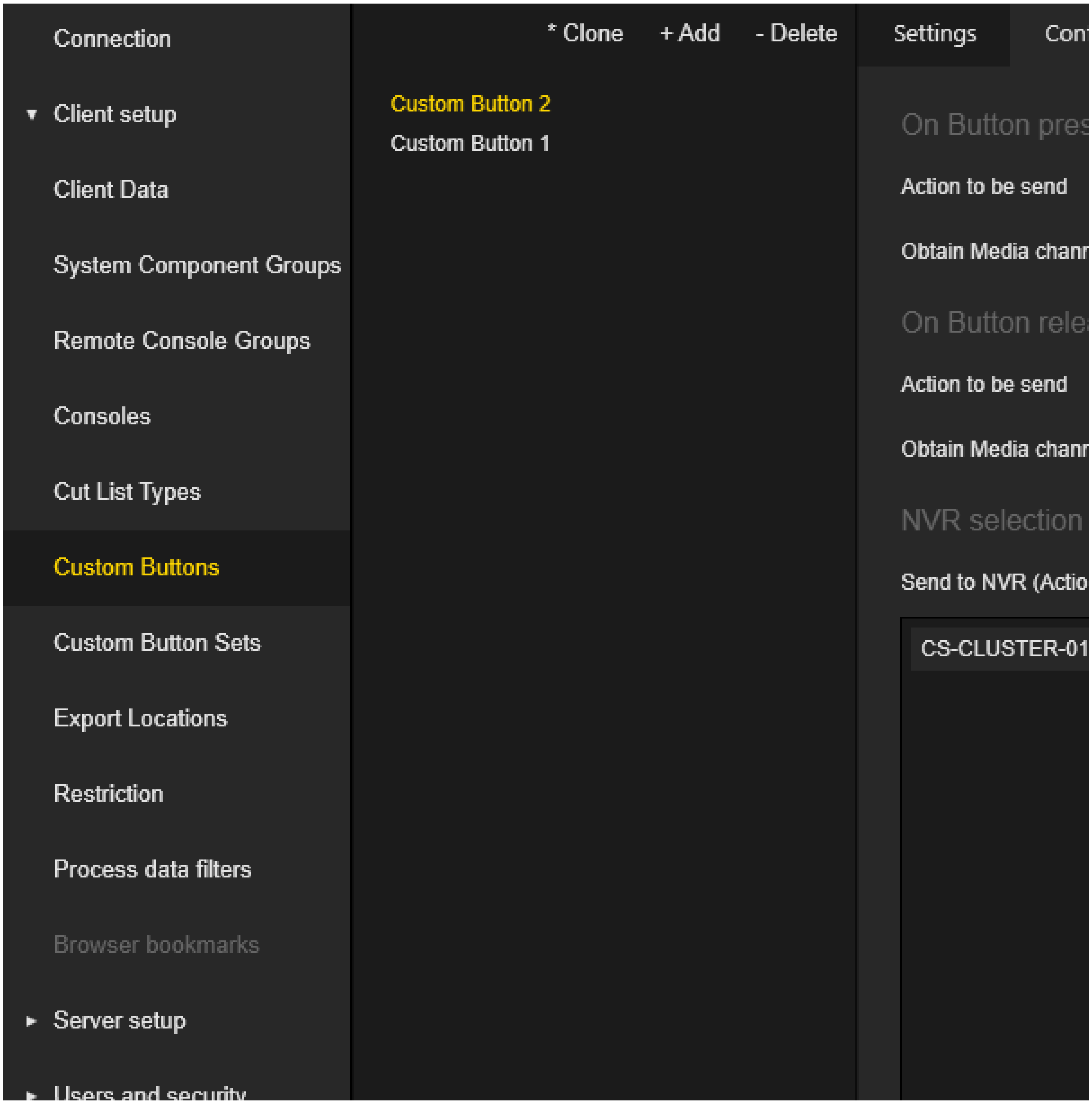
Name:

Language Independent Settings

Shortcut: Cut List (Type 1) ▾ — Must be unique or set to 'No shortcut'

Custom Buttons

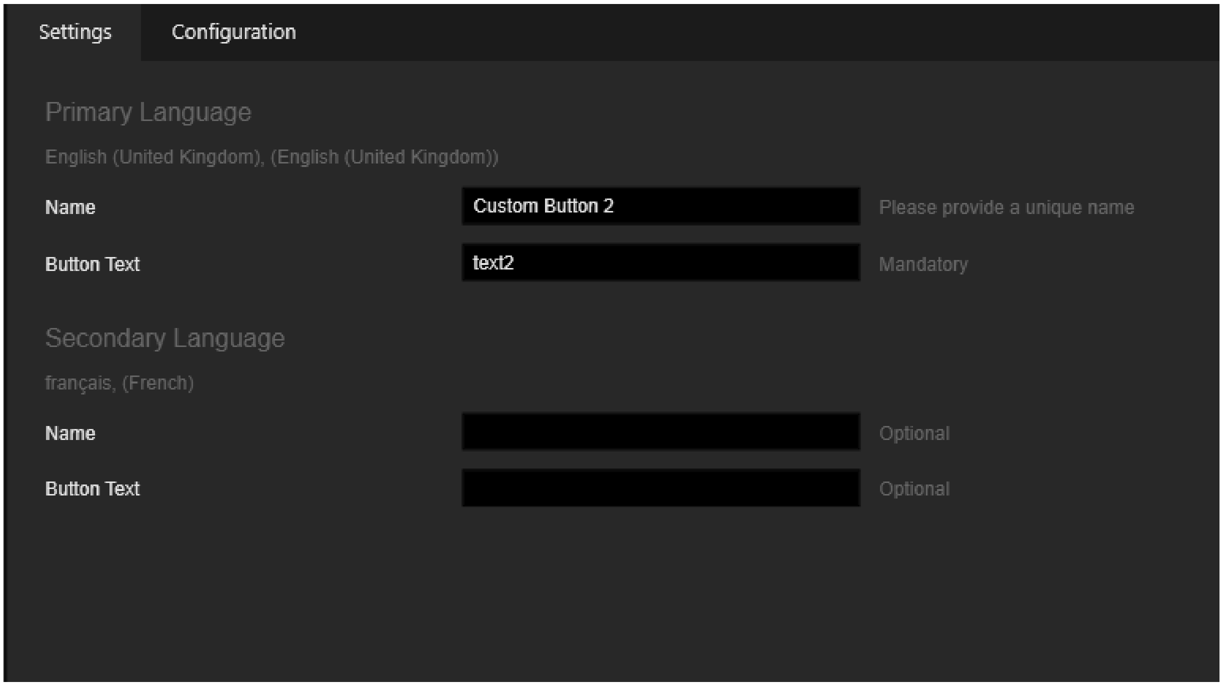
The **Custom Buttons** view contains a list of the custom buttons. Custom buttons, which are located in the **Custom Button Sets**, can be used in Operator Consoles to send actions to the NVRs.



The settings of the **Custom Buttons** are grouped in tabs.

Settings

The administrator can configure a **Name** and a **Button text** as a description for both the primary and secondary languages.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Custom Button 2 — Please provide a unique name

Button Text: text2 — Mandatory

Secondary Language

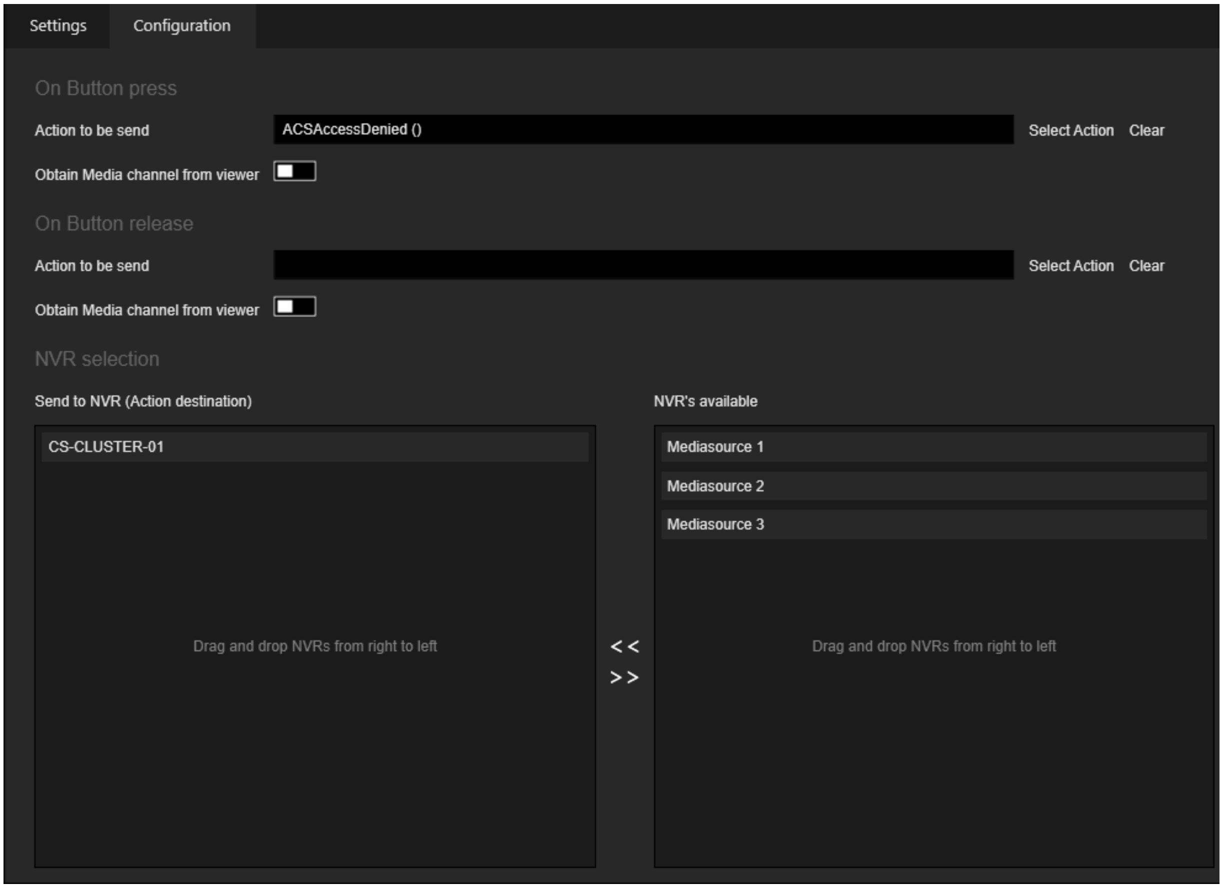
français, (French)

Name: — Optional

Button Text: — Optional

Configuration

The administrator can configure actions that will be sent when a button is pressed and released. The administrator can also select to which NVRs these actions are sent.



Settings | Configuration

On Button press

Action to be send: ACSAccessDenied ()

Obtain Media channel from viewer

On Button release

Action to be send:

Obtain Media channel from viewer

NVR selection

Send to NVR (Action destination)

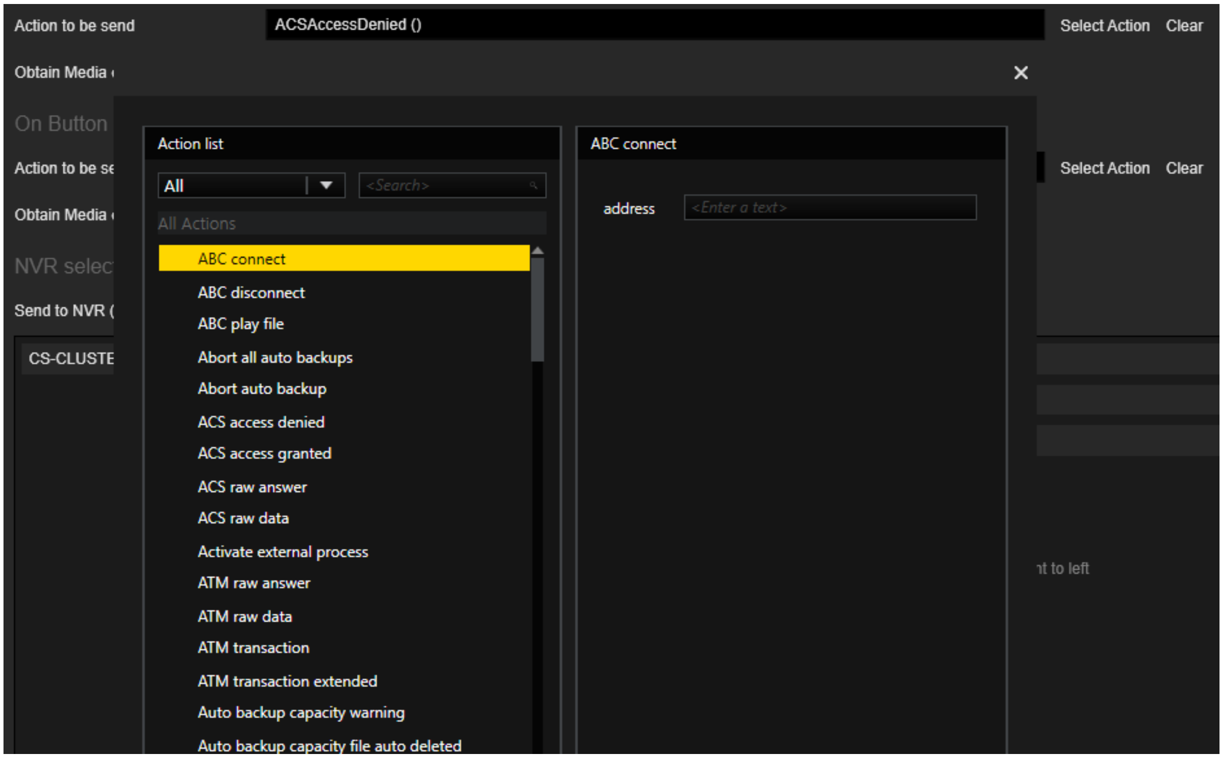
- CS-CLUSTER-01

NVR's available

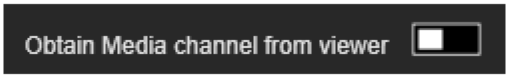
- Mediasource 1
- Mediasource 2
- Mediasource 3

Select Action
Clear
Select Action
Clear
Drag and drop NVRs from right to left
<<
>>
Drag and drop NVRs from right to left

Click the **Select Action** button to open the **Actions** dialog and select an action from the list. The action can also be entered directly into the associated text box.

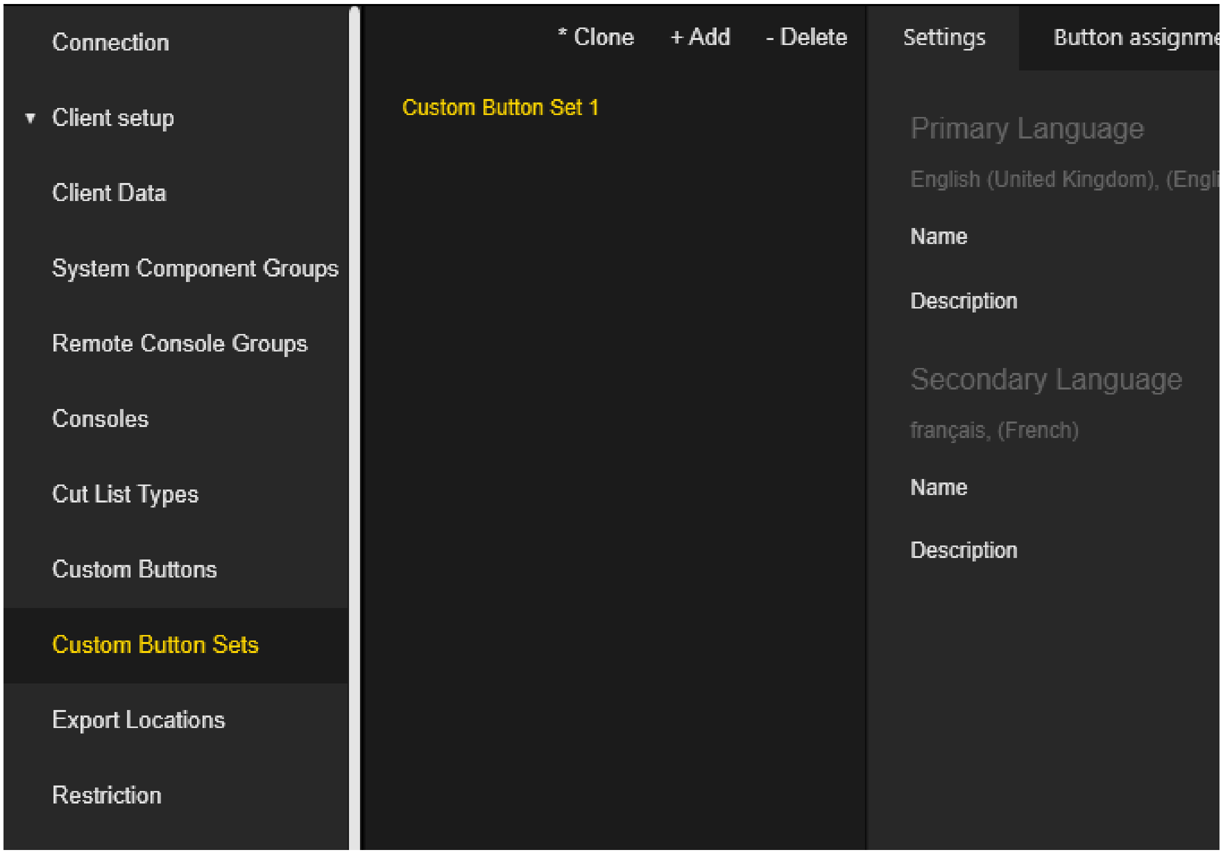


Activate the **Obtain Media channel from viewer** slider to send the action to the media channel which belongs to the active viewer. This allows the administrator to configure general actions.



Custom Button Sets

The **Custom Button Set** view contains a list of custom button sets. Buttons from the **Custom Button Sets** can be used in Operator Consoles to send actions to the NVRs.



Primary Language

English (United Kingdom), (Engli

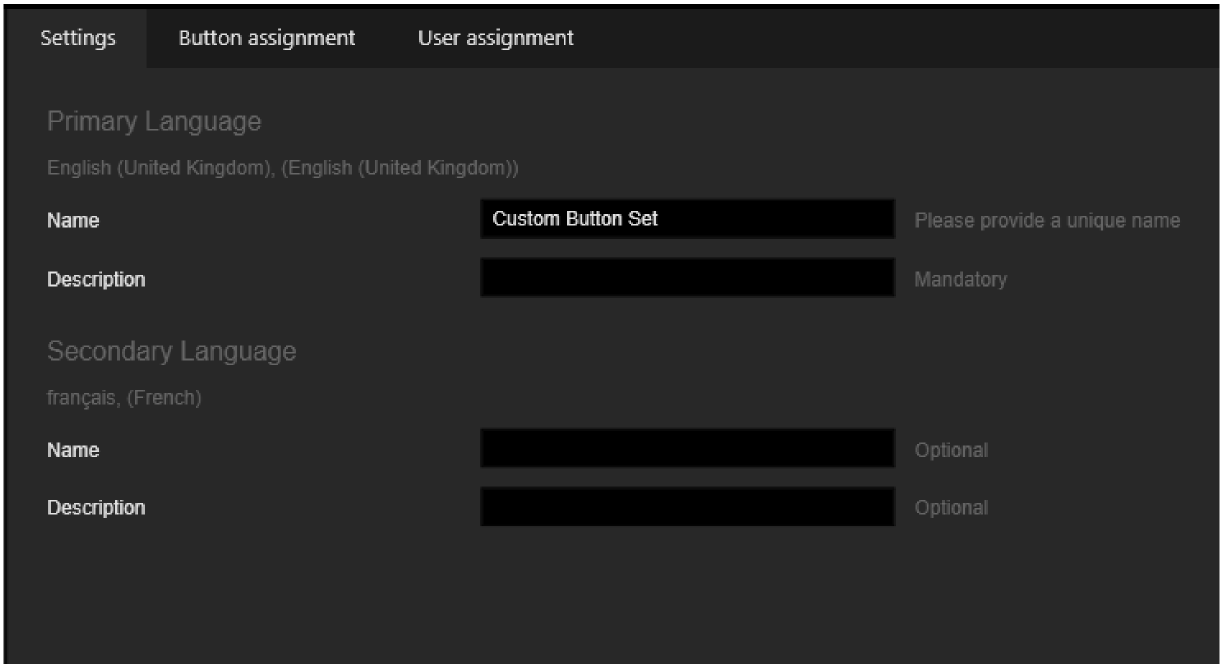
Secondary Language

français, (French)

The settings of the **Custom Button Sets** are grouped in tabs.

Settings

The administrator can configure the name and description for both the primary and secondary languages.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Custom Button Set — Please provide a unique name

Description: — Mandatory

Secondary Language

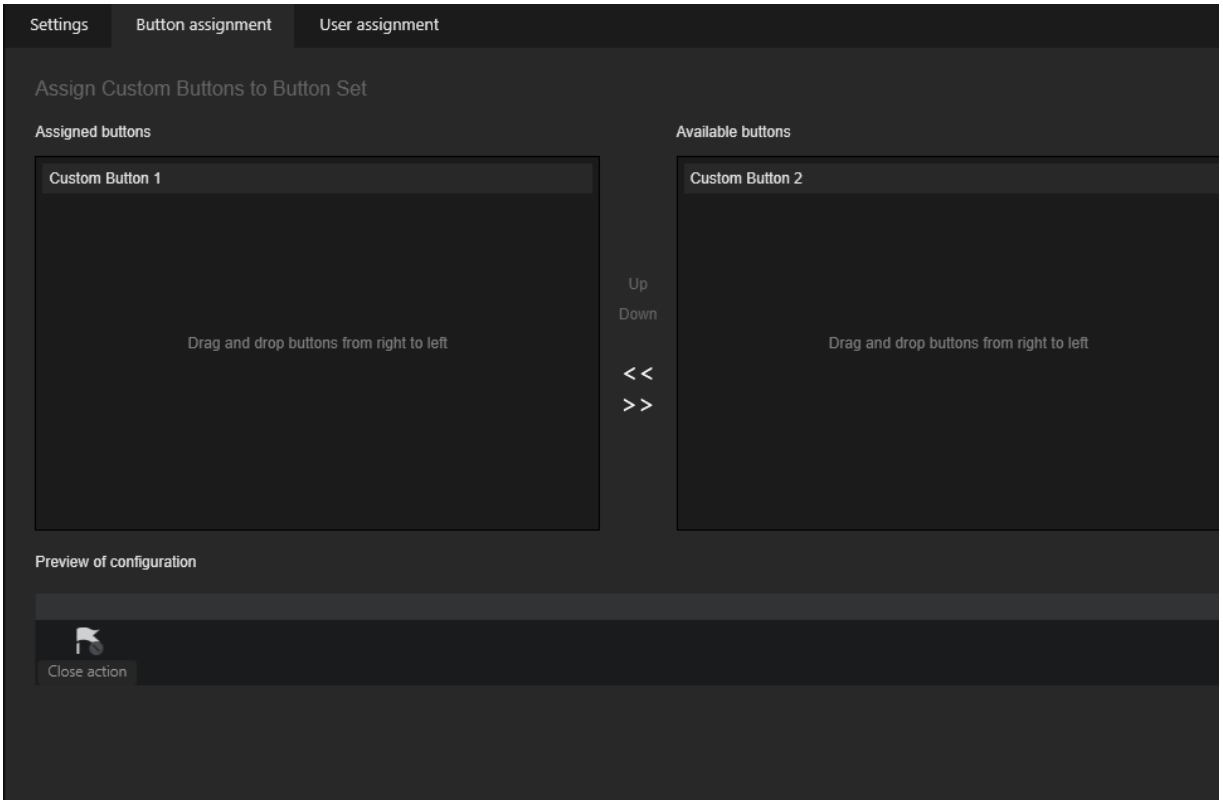
français, (French)

Name: — Optional

Description: — Optional

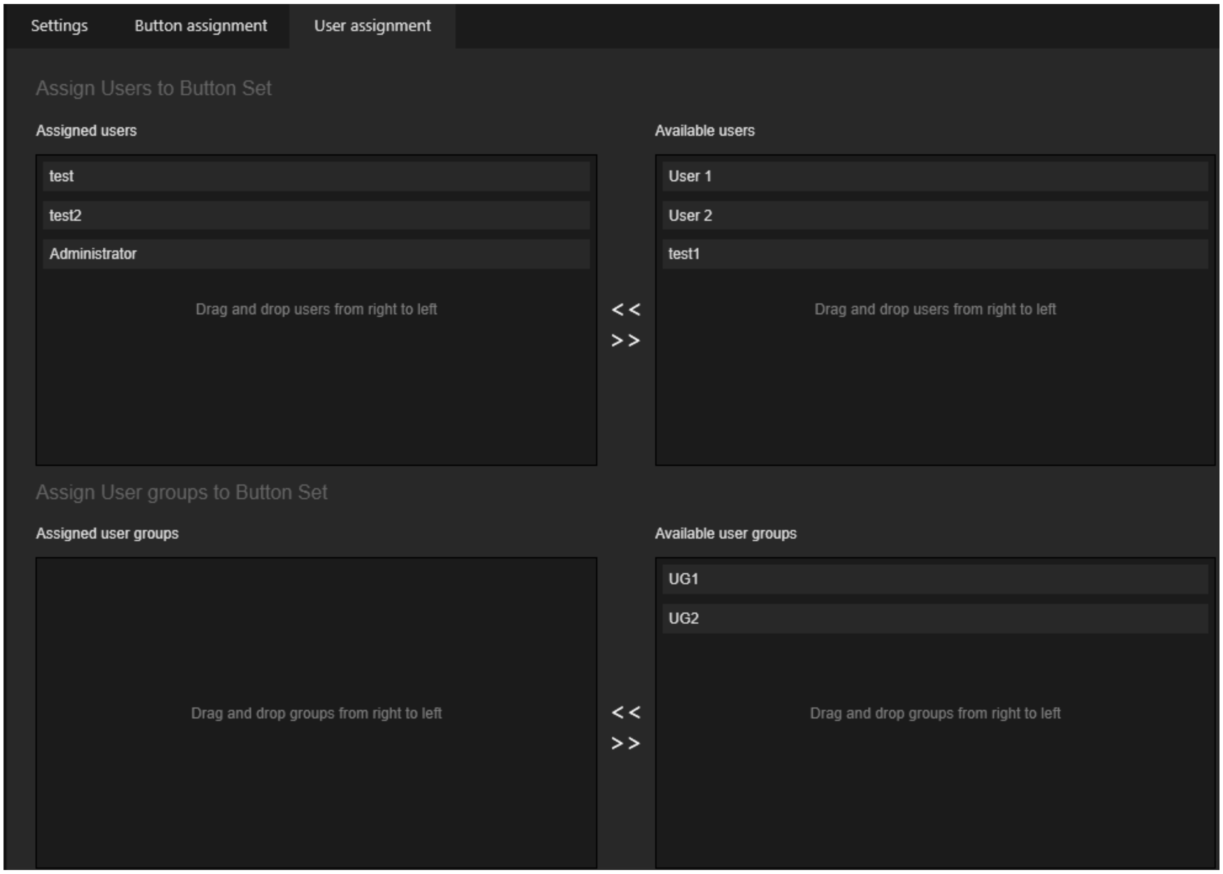
Button Assignment

The administrator can select which custom buttons will be placed in the custom button set. The order of the buttons can also be configured. The current configuration of the custom button set is displayed in the preview region.



User Assignment

The administrator can select users or user groups that are allowed to use specific custom buttons set on the Operator Consoles.


Settings
Button assignment
User assignment
<<
>>
Drag and drop users from right to left
Drag and drop groups from right to left

Assign Users to Button Set

Assigned users

test
test2
Administrator

Available users

User 1
User 2
test1

Assign User groups to Button Set

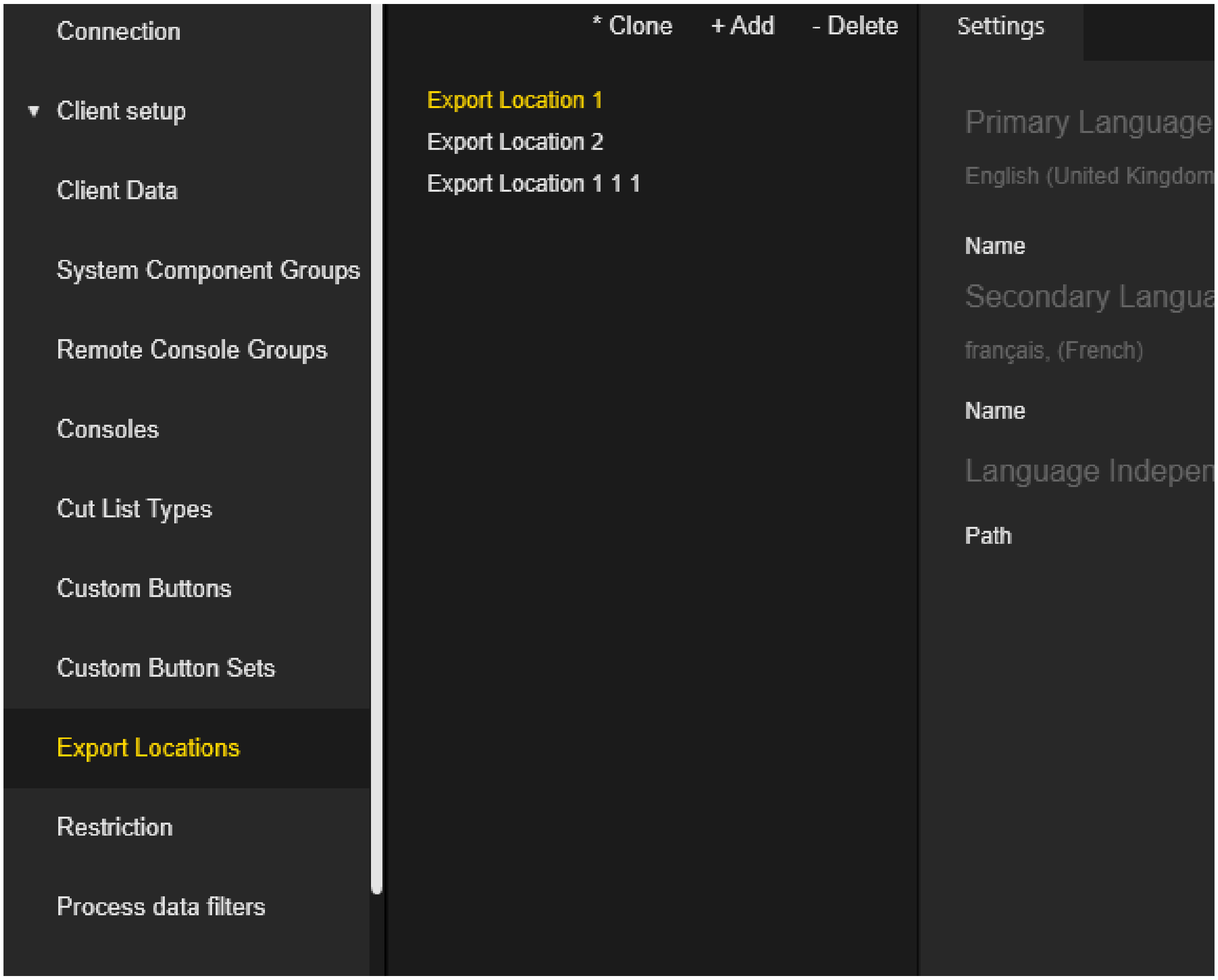
Assigned user groups

Available user groups

UG1
UG2

Export Locations

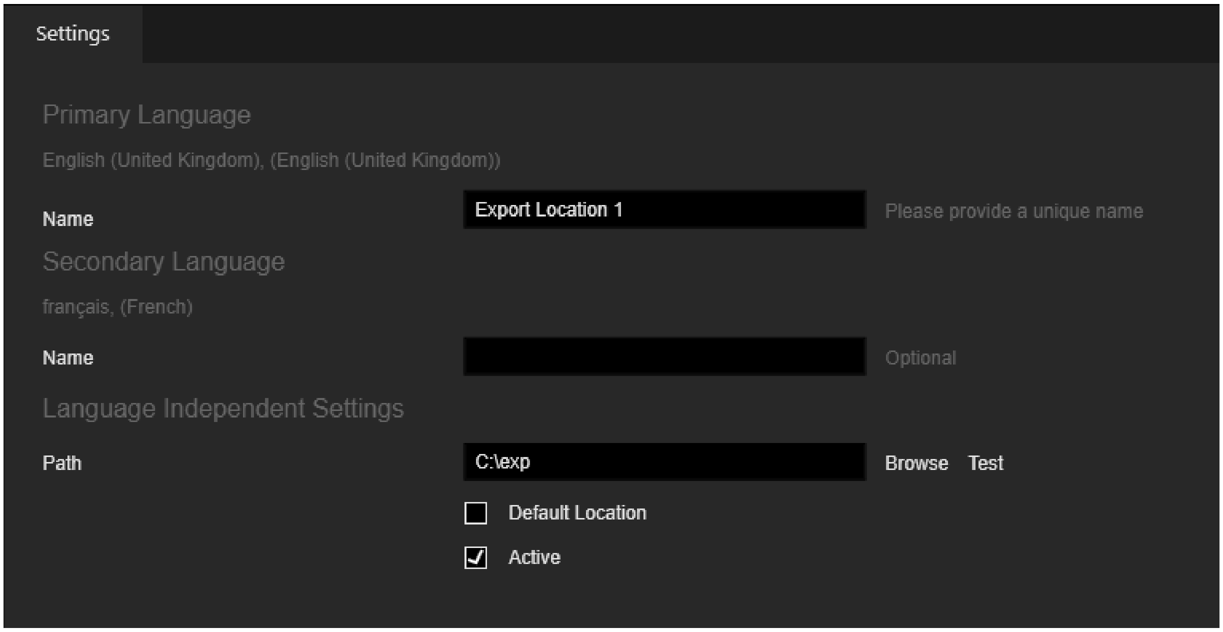
The **Export Locations** view contains a list of export locations that can be used in the Operator Console **Select export folder** dialog.



Settings

The administrator can configure the export location names for both the primary and secondary languages.

The location path can be entered manually or selected by clicking the **Browse** button. The administrator can check the validity of the path by clicking the **Test** button.



Settings

Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Export Location 1 — Please provide a unique name

Secondary Language

français, (French)

Name: — Optional

Language Independent Settings

Path: C:\exp — Browse Test

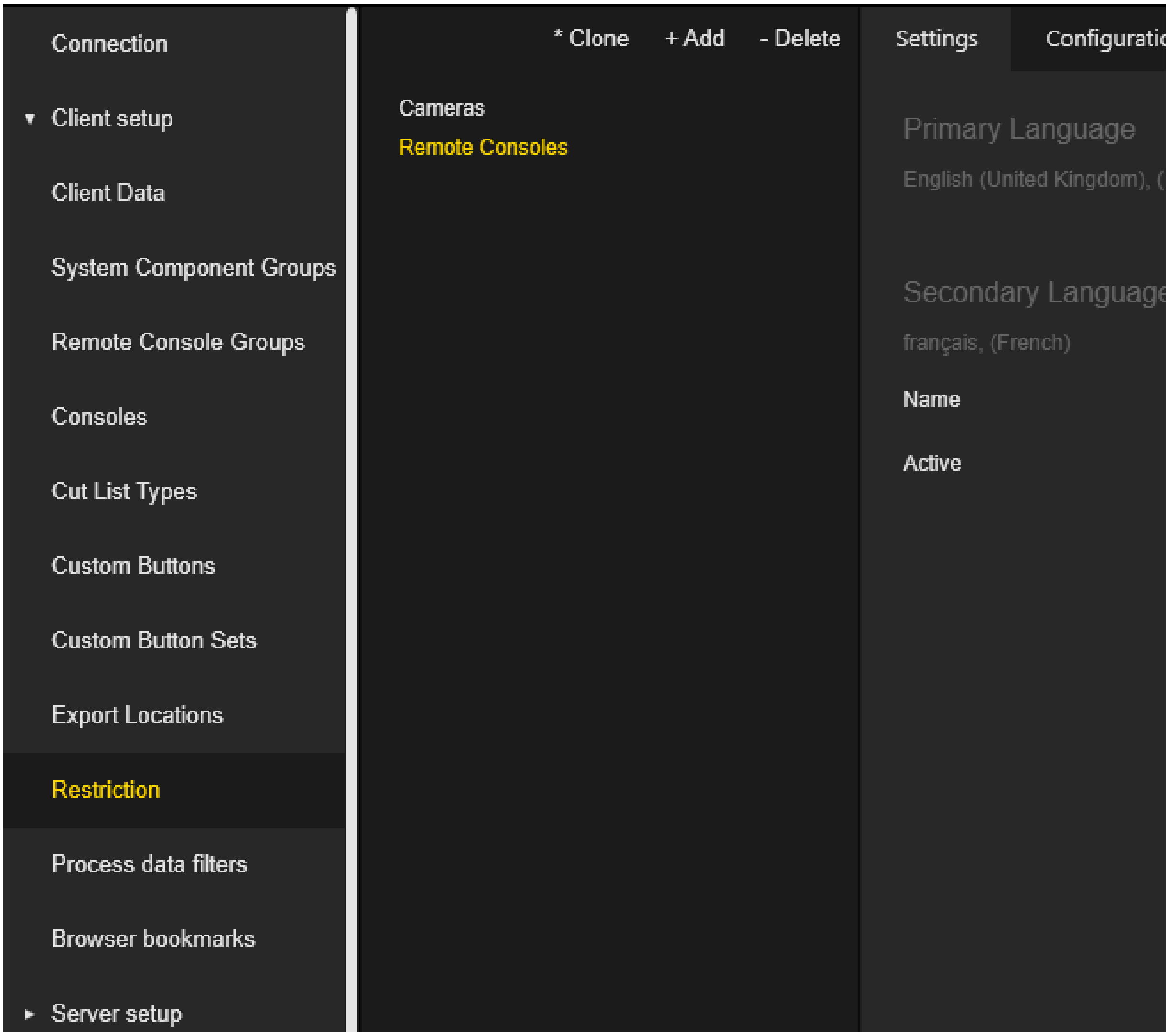
□ Default Location

☑ Active

- Select the **Default Location** checkbox to mark a specific export location as the default location. This default location will be selected by default in the Operator Console **Select export folder** dialog. Only one location can be marked as the default location.
- Select the **Active** checkbox to mark a specific export location as active or inactive. Only active locations are displayed in the Operator Console **Select export folder** dialog.

Restriction

The **Restriction** view contains a list of restrictions. Restrictions are further used to restrict or permit users, user groups, or consoles to use certain elements within your specific installation. It is typically used to prevent a specific operator to use certain cameras, to block the display of specific alarms on certain consoles, etc. Along with privileges, restrictions determine the rights of the user.



Primary Language

English (United Kingdom), (

Secondary Language

français, (French)

Name

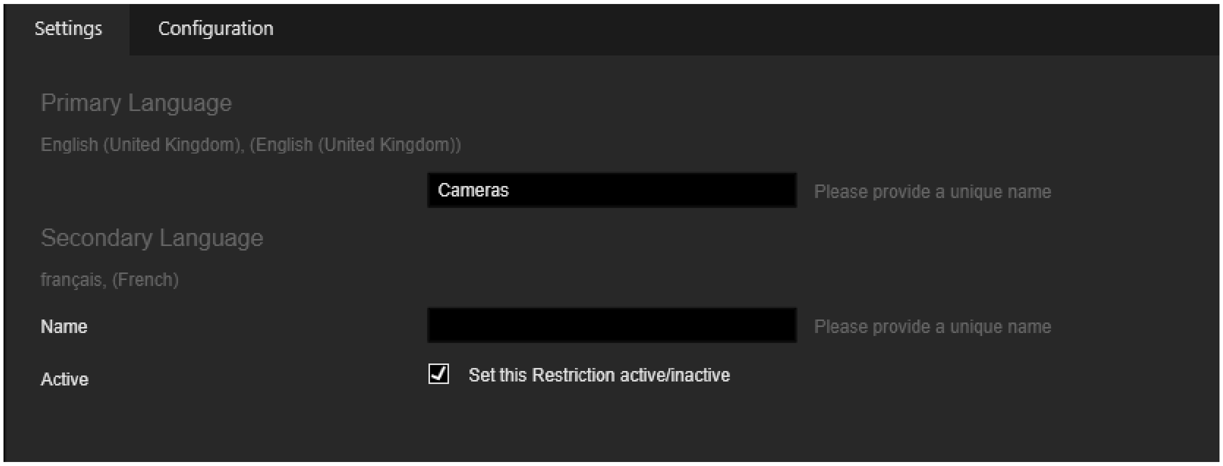
Active

The **Restriction** settings are grouped in tabs.

Settings

The administrator can configure names for both the primary and secondary languages.

The administrator can set the restriction to **active/inactive**. Only active restrictions are included in the account to determine the user rights.



Primary Language

English (United Kingdom), (English (United Kingdom))

Cameras — Please provide a unique name

Secondary Language

français, (French)

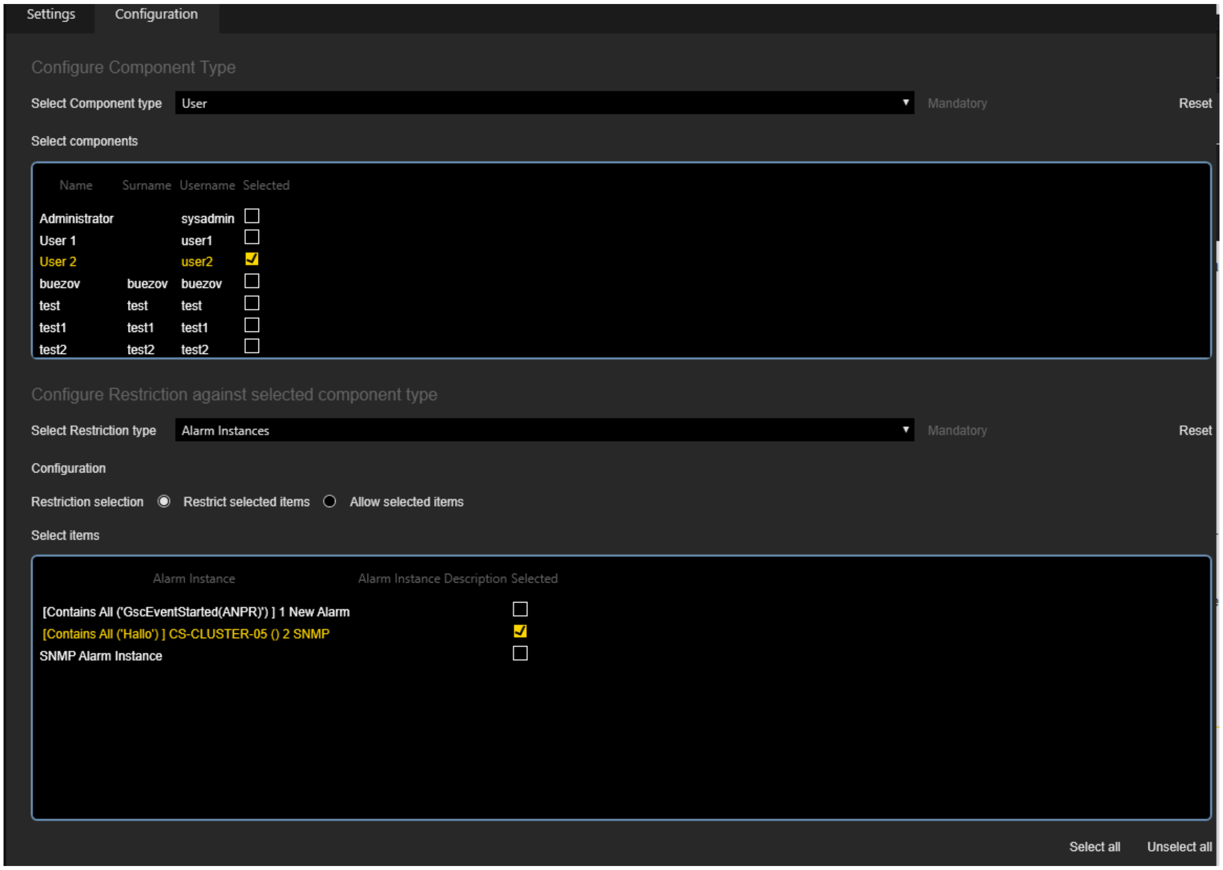
Name — Please provide a unique name

Active ☑ Set this Restriction active/inactive

Configuration

The **Configuration** tab contains two areas:

- Configure Component Type
- Configure Restriction against selected component type



Configure Component Type

Select Component type: User ▾ Mandatory Reset

Select components

Name	Surname	Username	Selected
Administrator		sysadmin	□
User 1		user1	□
User 2		user2	☑
buezov	buezov	buezov	□
test	test	test	□
test1	test1	test1	□
test2	test2	test2	□

Configure Restriction against selected component type

Select Restriction type: Alarm Instances ▾ Mandatory Reset

Configuration

Restriction selection ● Restrict selected items ○ Allow selected items

Select items

Alarm Instance	Alarm Instance Description	Selected
[Contains All ('GscEventStarted(ANPR)')] 1 New Alarm		□
[Contains All ('Hallo')] CS-CLUSTER-05 () 2 SNMP		☑
SNMP Alarm Instance		□

The buttons **Select all** and **Unselect all** can be used to select or unselect all items with one click. Click the **Reset** button to set the default restriction type.

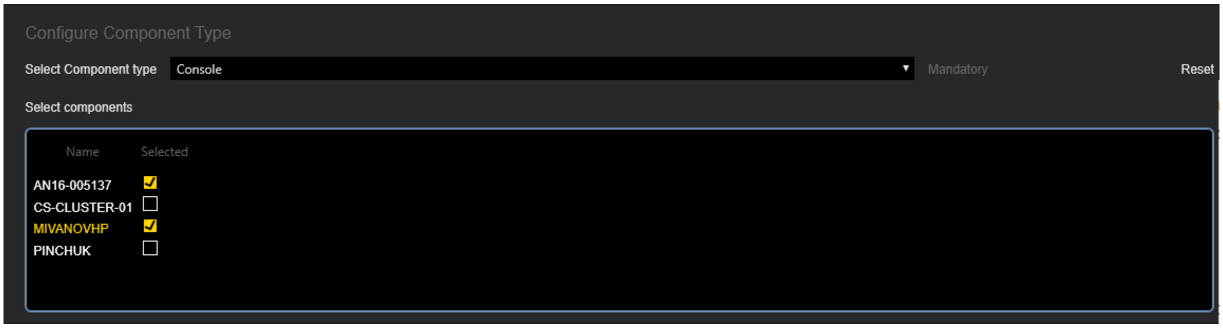
Configure Component Type

The administrator should select the component type to which the restrictions will be applied.

The following component types are available:

- Console
- High Resolution channels
- Privilege Groups
- Remote Consoles
- Transcoding Viewers
- User
- User Groups

When the component type is selected, the administrator can select items to which the restrictions will be applied.



Configure Component Type

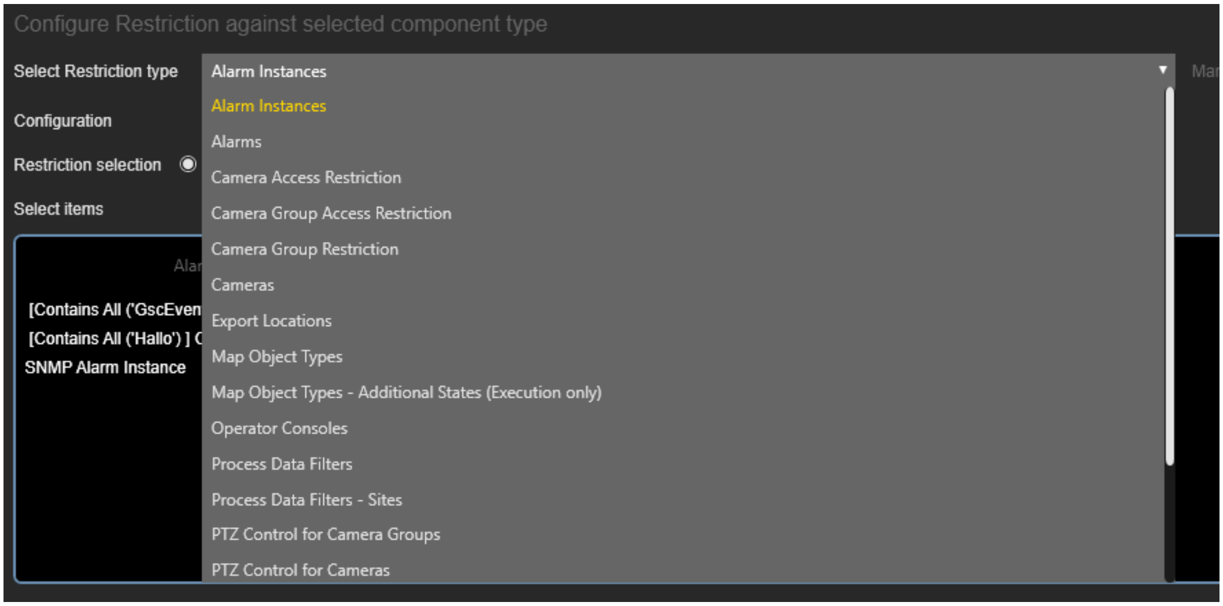
Select Component type: Console ▾ Mandatory

Select components

Name	Selected
AN16-005137	☑
CS-CLUSTER-01	□
MIVANOVHP	☑
PINCHUK	□

Configuring Restriction against selected component type

The administrator should select the restriction type.



Configure Restriction against selected component type

Select Restriction type: Alarm Instances

Configuration

Restriction selection ●

Select items

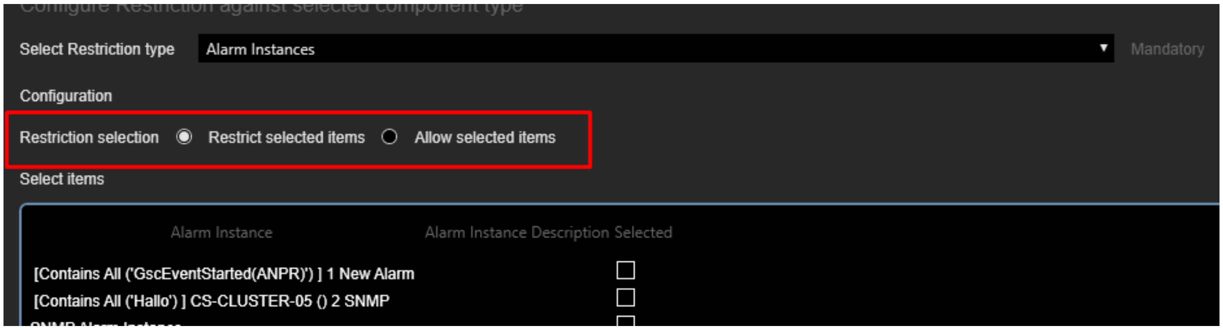
[Contains All ('GscEven

[Contains All ('Hallo')] C

SNMP Alarm Instance

Alarm Instances
Alarms
Camera Access Restriction
Camera Group Access Restriction
Camera Group Restriction
Cameras
Export Locations
Map Object Types
Map Object Types - Additional States (Execution only)
Operator Consoles
Process Data Filters
Process Data Filters - Sites
PTZ Control for Camera Groups
PTZ Control for Cameras
Mar
Alar

When the restriction type is selected, the administrator can select items to restrict or allow. Select the appropriate radio button on the **Restriction selection** group.



Configure Restriction against selected component type

Select Restriction type: Alarm Instances ▾ Mandatory

Configuration

Restriction selection ● Restrict selected items ○ Allow selected items

Select items

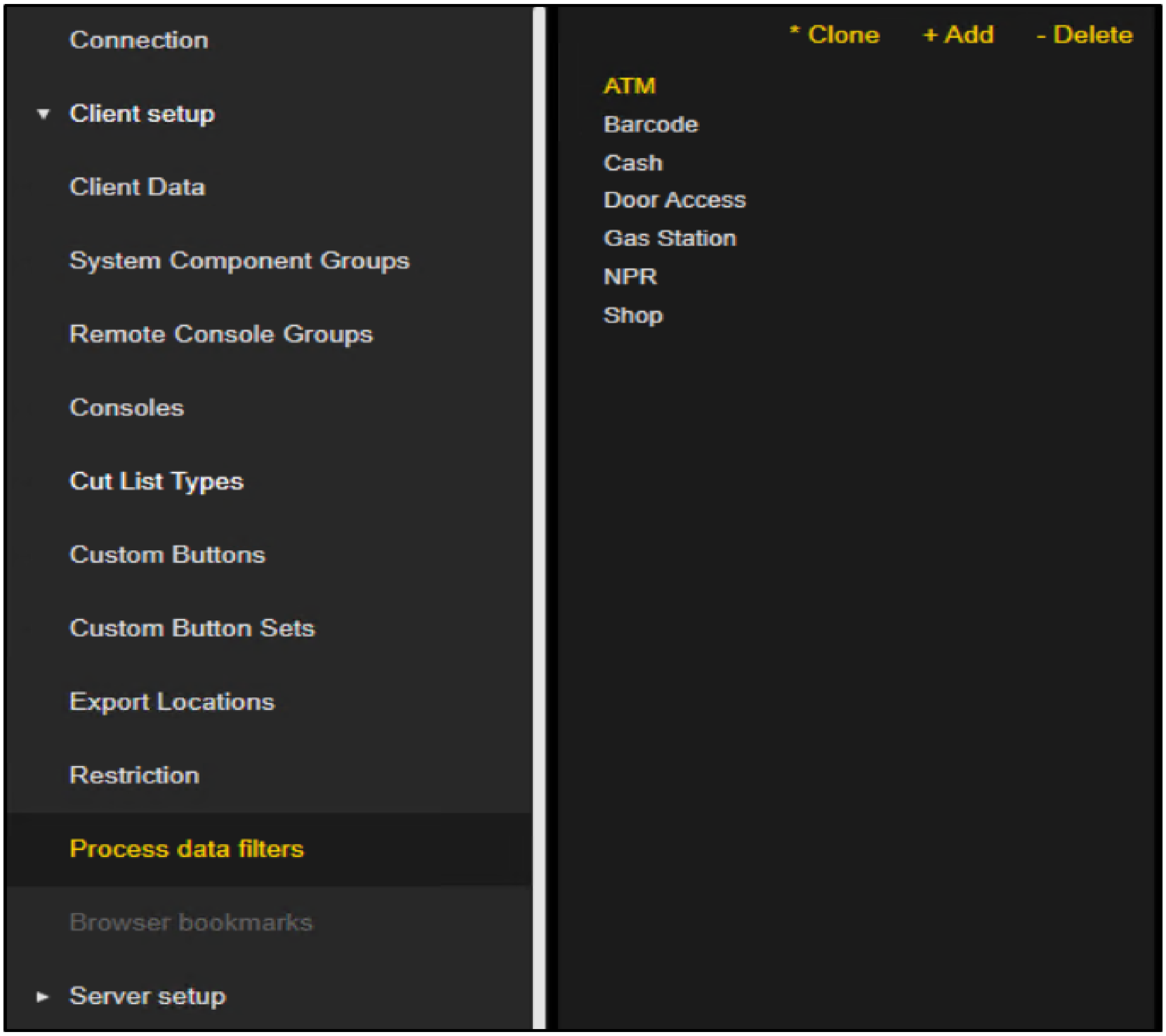
Alarm Instance	Alarm Instance Description	Selected
[Contains All ('GscEventStarted(ANPR)')] 1 New Alarm		□
[Contains All ('Hallo')] CS-CLUSTER-05 () 2 SNMP		□
SNMP Alarm Instance		□

If **Restrict selected items** is selected, the alarm instances selected in the area below will be hidden.

If **Allow selected items** is selected, the alarm instances selected in the area below will be shown.

Process Data Filters

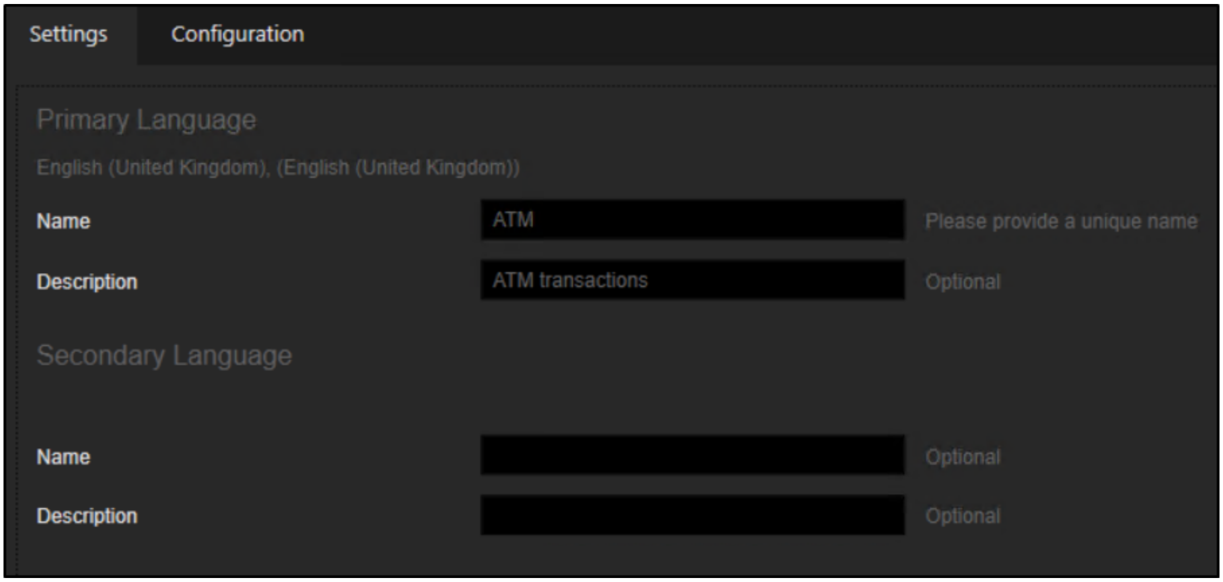
The **Process data filters** view contains process data filters that are used in the Operator Console to perform the process data search. The default set of the process data filters is created when the G-SIM server is installed.



The settings of the **Process data filters** are grouped in tabs.

Settings

Under the **Settings** tab you can configure **Name** and **Description** for both the primary and secondary languages.



Primary Language

English (United Kingdom), (English (United Kingdom))

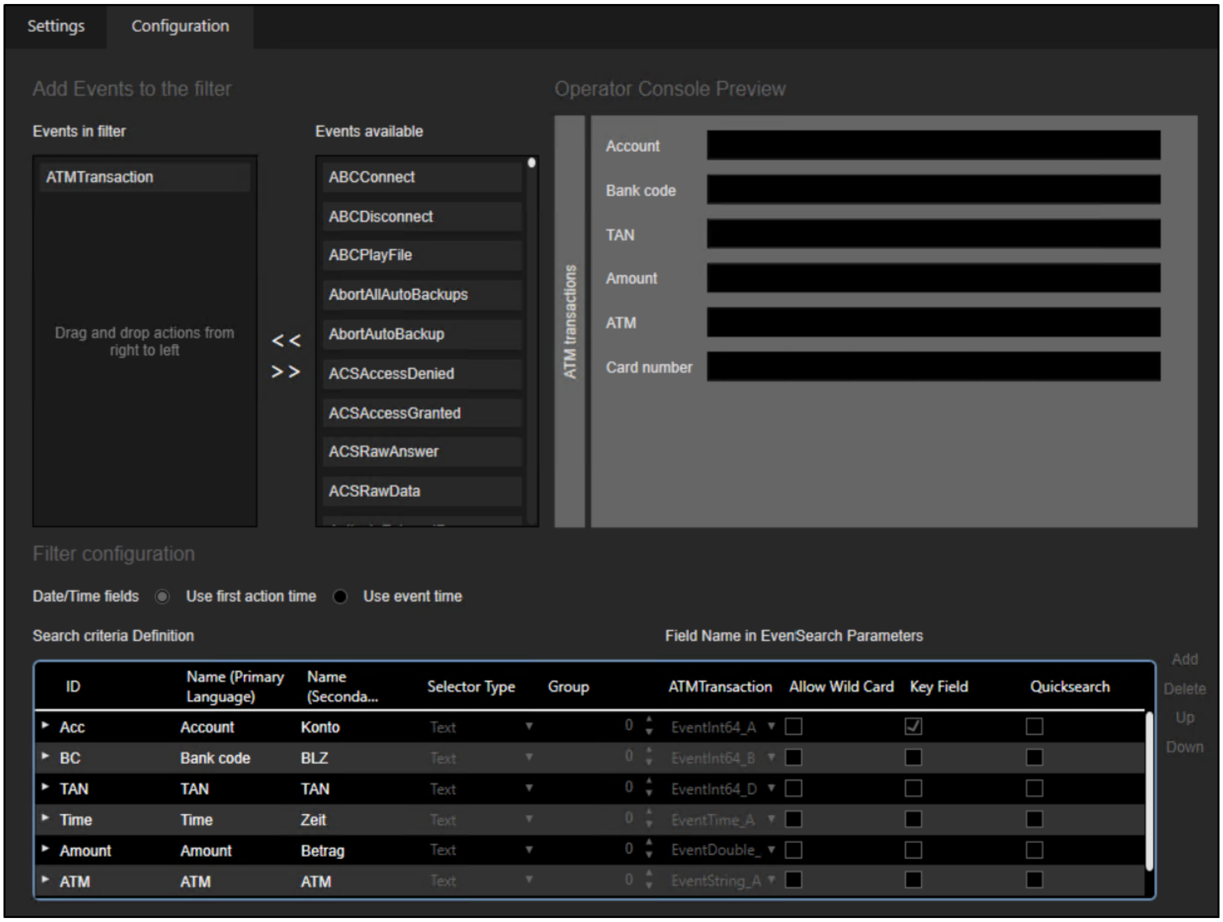
Name	ATM	Please provide a unique name
Description	ATM transactions	Optional

Secondary Language

Name		Optional
Description		Optional

Configuration

Under the **Configuration** tab you can select up to three event types to search with a specific process data filter.



Date/Time fields ○ Use first action time ● Use event time

Search criteria Definition

Field Name in EvenSearch Parameters

ID	Name (Primary Language)	Name (Seconda...	Selector Type	Group	ATMTransaction	Allow Wild Card	Key Field	Quicksearch
Acc	Account	Konto	Text	0	EventInt64_A	□	☑	□
BC	Bank code	BLZ	Text	0	EventInt64_B	□	□	□
TAN	TAN	TAN	Text	0	EventInt64_D	□	□	□
Time	Time	Zeit	Text	0	EventTime_A	□	□	□
Amount	Amount	Betrag	Text	0	EventDouble_	□	□	□
ATM	ATM	ATM	Text	0	EventString_A	□	□	□

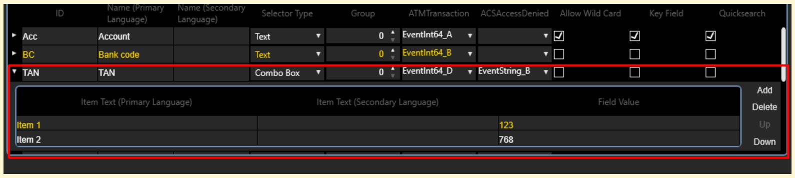
You can also create a **Search criteria Definition** list by using the **Add** and **Delete** buttons.

To order the search criteria definitions, use the **Up** and **Down** buttons.

Each **Search criteria Definition** contains the following set of fields:

Field	Description
ID	Identifier of the search criteria definition.
Name (Primary Language) / Name (Secondary Language)	Names of search criteria definitions for both primary and secondary languages.
Selector Type	The following types are available: • **Text**: Search criteria definitions will use a text box in

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
which you can type text to use as a filter.
<ul>
<li><b>Combo Box</b>: Search criteria definitions will use a combo box from which you can select predefined items. Predefined items can be added or removed using the <b>Add</b> and <b>Delete</b> buttons. Predefined items can be ordered using the <b>Up</b> and <b>Down</b> buttons.



<table>
<tr><th>ID</th><th>Name (Primary Language)</th><th>Name (Secondary Language)</th><th>Selector Type</th><th>Group</th><th>ATMTransaction</th><th>ACSAccessDenied</th><th>Allow Wild Card</th><th>Key Field</th><th>Quicksearch</th></tr>
<tr><td>Acc</td><td>Account</td><td></td><td>Text</td><td>0</td><td>EventInt64_A</td><td></td><td>☑</td><td>☑</td><td>☑</td></tr>
<tr><td>BC</td><td>Bank code</td><td></td><td>Text</td><td>0</td><td>EventInt64_B</td><td></td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>TAN</td><td>TAN</td><td></td><td>Combo Box</td><td>0</td><td>EventInt64_D</td><td>EventString_B</td><td>□</td><td>□</td><td>□</td></tr>
</table>

<table>
<tr><th>Item Text (Primary Language)</th><th>Item Text (Secondary Language)</th><th>Field Value</th></tr>
<tr><td>Item 1</td><td></td><td>123</td></tr>
<tr><td>Item 2</td><td></td><td>768</td></tr>
</table>

</li>
<li><b>Radio Button</b>: Search criteria definitions will use a set of predefined radio buttons from which you can select. It can be set up exactly like the combo box.</li>
<li><b>Display Only</b>: No interactive element will be provided to you, only the data of this field will be displayed.</li>
</ul>
</td></tr>
<tr><td>Group</td><td>Criteria with the same group value (greater than 0) are merged to groups. Grouped criteria receives name from the first item from the corresponding group.</td></tr>
<tr><td>ATMTransaction / ACSAccessDenied</td><td>Database column names in which event data are stored.</td></tr>
<tr><td>Allow Wild Card</td><td>Only applied to the <b>Text</b> selector type. If the checkbox is selected, you can either enter partial data or exact data for filtering. If the checkbox is not selected, you must enter exact data for filtering. More information on wild cards can be found under <b>Color Marking of Process Data</b>.</td></tr>
<tr><td>Key Field</td><td>The key field column is always displayed to you when it is selected. Only one search criteria definition can be marked as a key field. It is mandatory to enable a key field if <b>Use first action time</b> was chosen as date/time field.</td></tr>
<tr><td>Quicksearch</td><td>Only applied to the <b>Text</b> selector type. When using the Operator Console you can use quicksearch search criteria definitions to search for process data without having to open the process data search filter. Only one search criteria definition can be marked as a quicksearch.</td></tr>
</table>

You can see the configured process data filters in the preview area.

Customer User Actions

It is possible to use your own defined customer user actions in the G-SIM process data filters.

How to use customer user actions in process data filters:

1. Create an XML file and define the action. Detailed information on how to create a customer user action can be found in the **G-Core ATI**.

   The action code must be unique or else there is the possibility that actions will be overwritten.

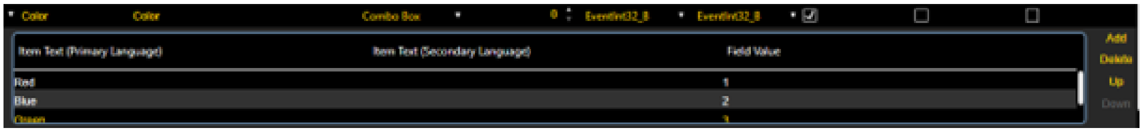
2. Save the XML file in the Management Console directory (`C:\Program Files\Geutebrueck\GSim\Management Console`).
3. Subscribe to the action from the media source. The action is visible in the events list when the Management Console is started.

   The action ID needs to be the same as the defined parameter name in the XML file.

How to filter custom enumerated values from XML file:

1. Add the parameter as a combo box.

2. Enter the values and the corresponding text fields (such as 1 = red, 2 = blue, etc.) manually to match the XML file.

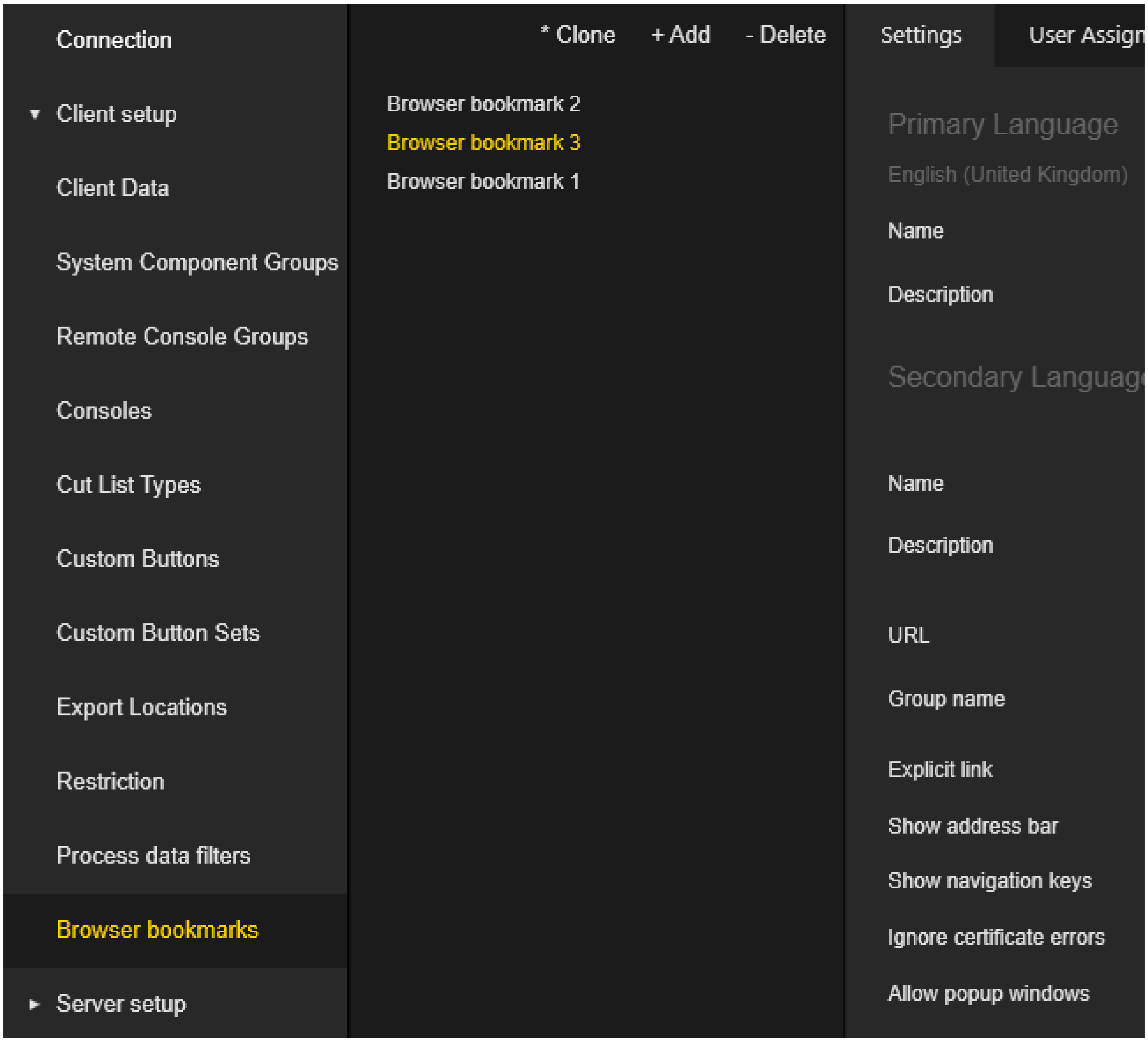


Color | Color | Combo Box | 0 | EventInt32_8 | EventInt32_8 | ☑ | □ | □

Item Text (Primary Language)	Item Text (Secondary Language)	Field Value
Red		1
Blue		2
Green		3

Browser Bookmarks

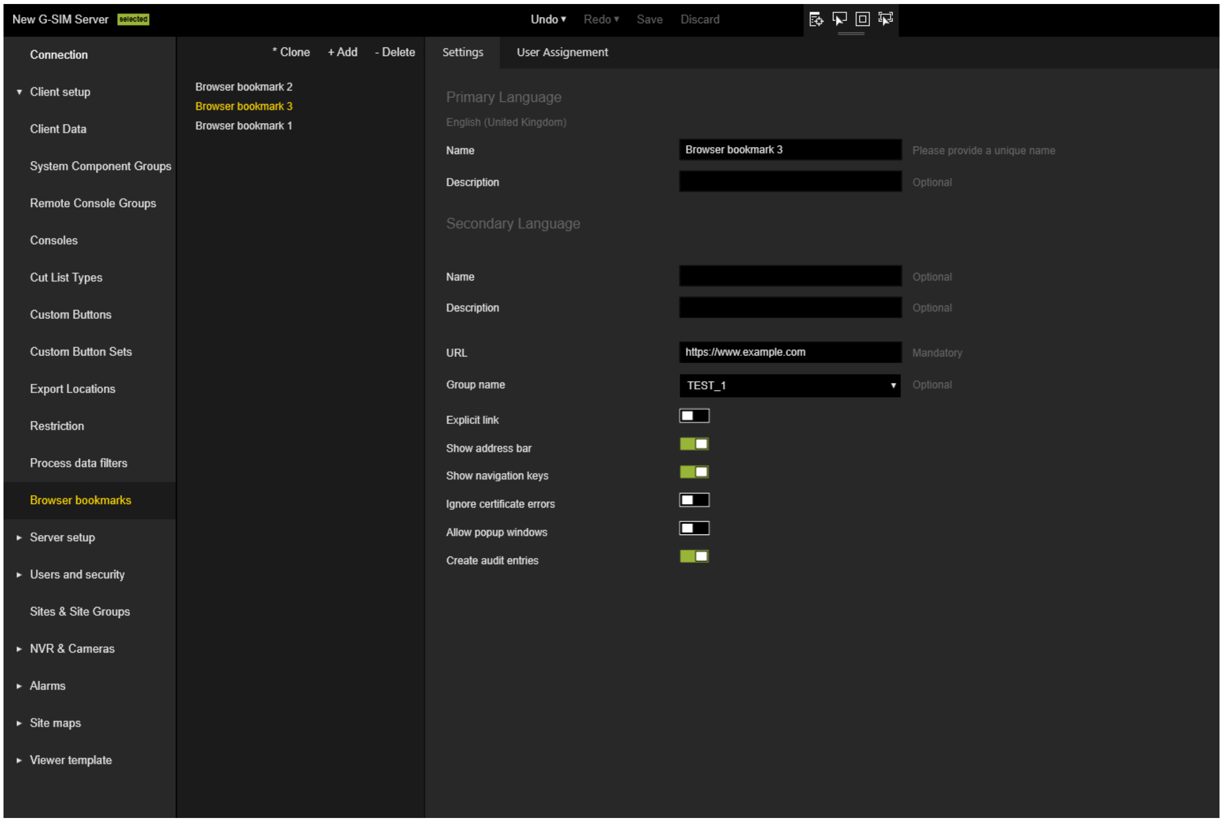
The **Browser bookmarks** menu allows to create, delete and configure browser bookmarks. Please note that this menu is not available in case there is no dongle with an appropriate option.



The settings of the **Browser bookmarks** are grouped in tabs.

Settings

The administrator can configure the following settings per bookmark:



Primary Language

English (United Kingdom)

Name	Browser bookmark 3	Please provide a unique name
Description		Optional

Secondary Language

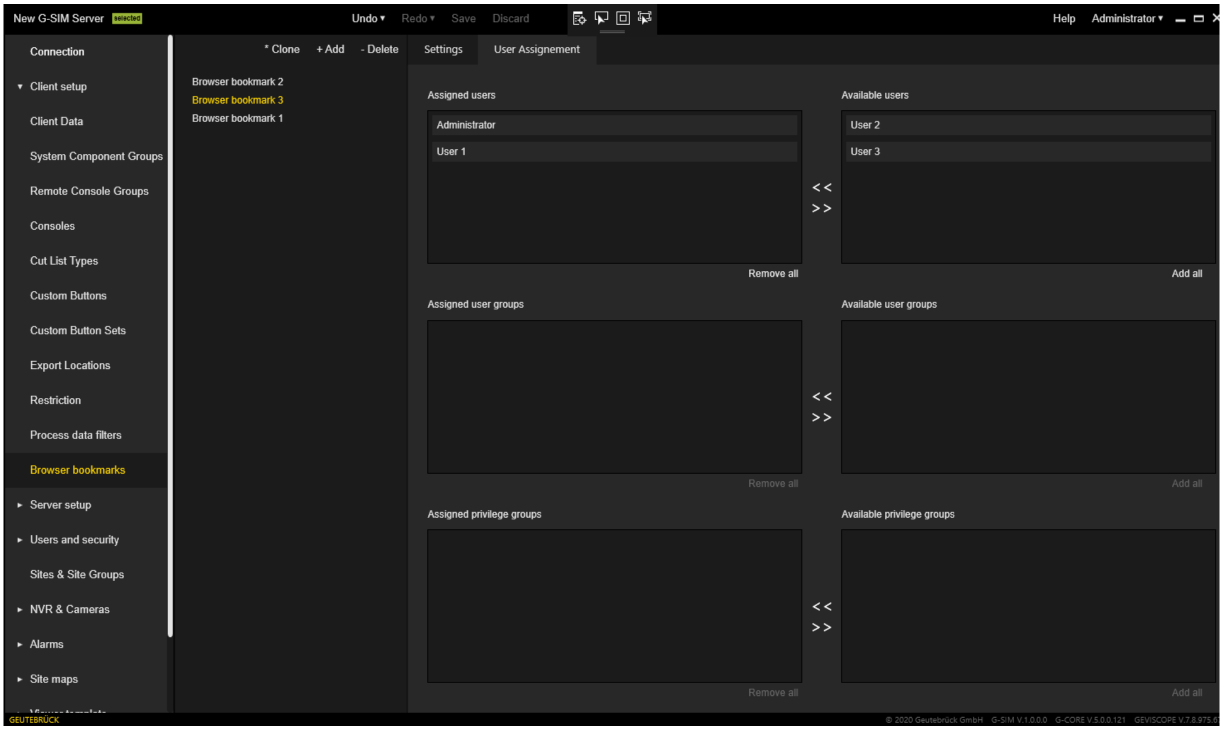
Name		Optional
Description		Optional
URL	https://www.example.com	Mandatory
Group name	TEST_1 ▾	Optional
Explicit link	○	
Show address bar	●	
Show navigation keys	●	
Ignore certificate errors	○	
Allow popup windows	○	
Create audit entries	●	

Settings	Description
Name	Browser bookmark name for both primary and secondary language.
Description	Browser bookmark description for both primary and secondary language.
URL	Specification of the corresponding URL.
Group name	Text tag that allows ordering and grouping in the Operator Console.
Explicit link	When activated, there is a strict binding to the exactly configured URL. If this is not activated, the user is also allowed to open other URLs by navigating or entering them in the address bar. → If **Explicit link** is activated, the options **Show address bar** and **Show navigation keys** are unchecked and disabled.

Settings	Description
Show address bar	Show or hide the address bar in the browser.
Show navigation keys	Show or hide the navigation keys
Ignore certificate errors (SSL certificates)	Can be set whether they are disregarded or mandatory.
Allow popup windows	Permission or restriction to open popup links.
Create audit entries	Set whether to audit the use of the bookmark and save in the audit log.

User Assignment

The **User Assignment** tab can configure which users / user groups / privilege groups have access to the selected bookmark.

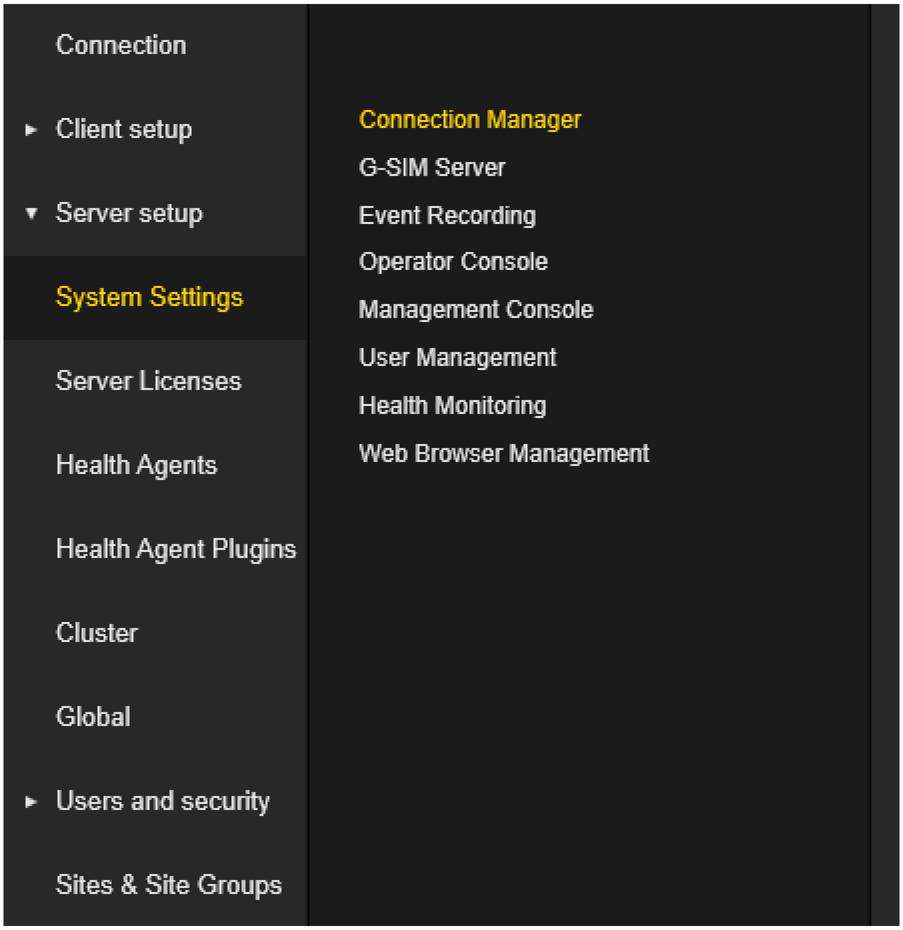


Server Setup

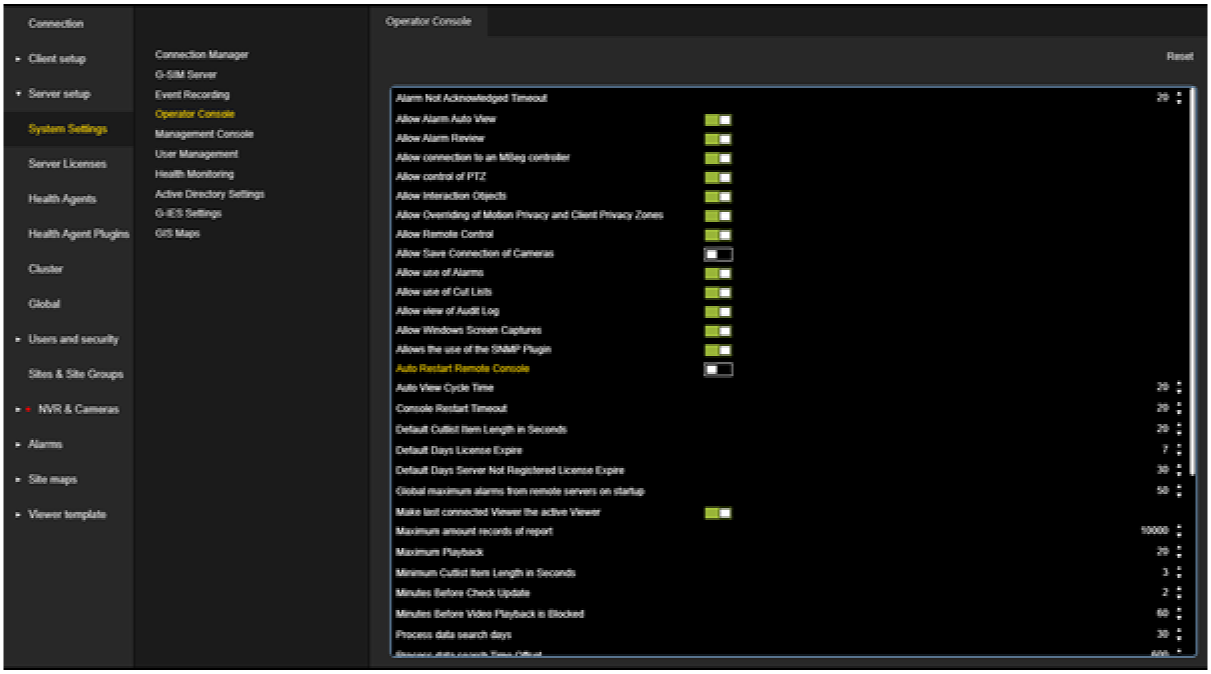
System Settings

The **System Settings** view contains the list of system settings categories.

Non-licensed categories are not displayed in the list.



The **System Settings** category view shows system settings that belong to a specific category. The administrator can hold the mouse cursor over the setting to see a detailed description. Click the **Reset** button to set all settings of the specific category to default values.



Alarm Not Acknowledged Timeout	20
Allow Alarm Auto View	☑
Allow Alarm Review	☑
Allow connection to an MBeg controller	☑
Allow control of PTZ	☑
Allow Interaction Objects	☑
Allow Overriding of Motion Privacy and Client Privacy Zones	☑
Allow Remote Control	☑
Allow Save Connection of Cameras	☐
Allow use of Alarms	☑
Allow use of Cut Lists	☑
Allow view of Audit Log	☑
Allow Windows Screen Captures	☑
Allows the use of the SNMP Plugin	☑
Auto Restart Remote Console	☐
Auto View Cycle Time	20
Console Restart Timeout	20
Default Cutlist Item Length in Seconds	20
Default Days License Expire	7
Default Days Server Not Registered License Expire	30
Global maximum alarms from remote servers on startup	50
Make last connected Viewer the active Viewer	☑
Maximum amount records of report	10000
Maximum Playback	20
Minimum Cutlist Item Length in Seconds	3
Minutes Before Check Update	2
Minutes Before Video Playback is Blocked	60
Process data search days	30
Process data search Time Offset	600

The following system settings are available for configuration:

Connection Manager

Setting	Description	Default
Allow Client Side Media Source Checking	Indicates whether LAN NVRs must be checked for availability with Device Browser. If Primary is not available then directly connect to Secondary.	Enabled
Allow Playback Over Slow Connections	Indicates whether to allow video playback over slow (ISDN/Dial-up) connections.	Disabled
Check Availability With PING	Indicates whether LAN sites availability should be checked with PING or not.	Disabled
Default Connection Retry Count	The default, connection-retry count, for network connections (e.g. LAN or Ping-dialler). Also see DefaultCon-	5

Setting	Description	Default
	nectRetryTimeout.	
Default Connection Retry Timeout	The default, connection-retry timeout in milliseconds, for network connections. This value should be small for fast networks. Also see DefaultConnectRetryCount.	500
Default Keep Alive Period	The default keep alive period in milliseconds.	5000
Default Keep Alive Timeout	The default, keep-alive timeout in milliseconds. This timeout indicates a failure for the keep-alive mechanism.	10000
Default Maximum Connections Over DSL	The default number of video connections allowed to a site connected with DSL. (0 for auto determined)	2
Default Maximum Connections Over ISDN Or Analog	The default number of connections allowed to a site connected via ISDN or analog dail-up. (0 for auto determined)	1
Default Maximum Connections To LAN	The default number of video connections allowed to a site connected on a LAN. (0 for auto determined)	0
Default Timeout ISDN	The default timeout in milliseconds for ISDN or analogue dial-up connections. This timeout indicates the time to wait for a connection to the NVR before it shows site unavailable.	30000
Default Timeout LAN	The default timeout in mil-	5000

Setting	Description	Default
	liseconds for LAN connections. This timeout indicates the time to wait for a connection to the NVR before it shows site unavailable.	
Guard Tour Minimum Switch Time	The minimum switch time in seconds between Cameras in a Guard Tour. This is the minimum time that is allowed for a Guard Tour to switch between 2 Cameras.	5
Guard Tour Time Before Connect ISDN	The time in milliseconds for ISDN connections before a connection is requested from the server. This is also the minimum switch-over time for a guard tour.	10000
Guard Tour Time Before Connect LAN	The time in milliseconds for LAN connections before a connection is requested from the server. This is also the minimum switch-over time for a guard tour.	1000
Guard Tour Time Show Unavailable Banner	The time in milliseconds to show the unavailable message before continuing with the Guard Tour.	3000
Guard Tour Time Wait Images ISDN	The time in milliseconds for Guard Tours to wait before showing WaitingForImages for ISDN connections. This timeout indicates the time to wait after a connection to the NVR has been made, before it shows that it is still waiting for images from the cameras. Most likely	5000

Setting	Description	Default
	cause is sync-loss or slow connection.	
Guard Tour Time Wait Images LAN	The time in milliseconds for Guard Tours to wait before showing WaitingForImages for LAN connections. This timeout indicates the time to wait after a connection to the NVR has been made, before it shows that it is still waiting for images from the cameras. Most likely cause is sync-loss or slow connection.	3000
Has Live Stream Timeout	The timeout in milliseconds to wait for Live streams.	3000
Maximum Outgoing ISDN Lines To Use	The maximum number of ISDN lines to use for outgoing video traffic.	17
Minimum Frame Difference ISDN	The time difference between frames (in milliseconds) before the failover Media Channel is tried during playback for ISDN connections.	360000
Minimum Frame Difference LAN	The time difference between frames (in milliseconds) before the failover Media Channel is tried during playback for LAN connections.	180000
Multicast Keep Alive Timeout	The timeout in milliseconds to keep multicast alive.	0
Recovery Wait Period Before Auto Logout	The time in seconds to wait for server recovery before an operator UI is automatically logged out after a server failure was	180

Setting	Description	Default
	detected.	
Time Wait Images ISDN	The time in milliseconds for Viewers to wait before showing WaitingForImages for ISDN connections. This timeout indicates the time to wait after a connection to the NVR has been made, before it shows that it is still waiting for images from the cameras. Most likely cause is sync-loss or slow connection.	30000
Time Wait Images LAN	The time in milliseconds for Viewers to wait before showing WaitingForImages for LAN connections. This timeout indicates the time to wait after a connection to the NVR has been made, before it shows that it is still waiting for images from the cameras. Most likely cause is sync-loss or slow connection.	10000
Unused NVR Disconnect Timeout Seconds	The amount of seconds before a NVR is disconnected after the last camera is closed. A value of 0 will disable this mechanism	0
Update Site Availablity On Checkin	Update the Site Availability when a Health Agent Checks-in.	Disabled

G-SIM Server

Setting	Description	Default
Alarm expiry check interval	Interval in minutes when the server checks if alarms are expired. ℹ **Prerequisite: The setting Allow Alarm Expire must be set to true.** ℹ **The first check is performed 10 minutes after the start of the G-SIM server.**	30
Alarm Purge Days	The number of days after the alarms are deleted.	30
Allow Alarm Expansion	Indicates that additional alarm functionality can be configured and used by the Operator Console.	Disabled
Allow Alarm Expiry	Indicates if alarms are allowed to expire.	Enabled
Allow Restrictions	Allow the configuring of Data Restrictions.	True
Allow Windows Authentication	Indicates that Windows Authentication can be configured and used by the Operator or Management Console. More information can be found under **Automatic Login via Windows Authentication**.	Disabled
Audit Purge Days	The number of days after the audit items are deleted.	60
Delete outdated Refer-	Interval in months to check if	3

Setting	Description	Default
ence Images interval	reference images on Client can be deleted when they are outdated.	
Global Server Client No Response Alarm Hours	The number of hours the Global Server will wait before creating a No Response from Client alarm.	48
Global Server Key	The Key that will allow the Global Enrollment.	
Global Server Sync Minutes	The number of minutes the Global Server will wait between synchronizations.	360
Health Agent Not Checkin Notify	The number of days after which a Health Agent's alarm will be raised again if it didn't check-in.	7
Local Server Identity	Configure G-SIM Server IP/HostName/FQDN. See **Local Server Identity**.	
Raise Alarms for Channels not configured in G-SIM	Indicates if Alarms coming from Cameras not configured in G-SIM must be raised.	Enabled
Raise Alarms For Fail Over Channels	Indicates if Alarms coming from FailOver Cameras must be raised.	Disabled
Switch additional alarm cameras into alarm state	This setting determines the permission for additional cameras to switch into alarm state.	Disabled

Event Recording

Setting	Description	Default
Database Reserve MB	Number of Megabytes the Server will keep open as a reserve	100
Delete Cycle Minutes	Number of minutes that the Server must delete the GSC Events that have expired	1
Delete Top Row Count	Number of row to be deleted per cycle. The more rows deleted the bigger the impact of the operation in regards to performance	1000
Local Cache Expire Seconds	Number of second to keep the local Event cache in memory.	300
Must Delete	Indicates if the Server must delete expired GscEvents proactively. If this setting is enabled, the G-SIM server regularly deletes expired events. When the process data database reaches its maximum size, the oldest events are removed. If you want to avoid deleting events, you must disable this setting and specify an unlimited size for the database files.	Enabled
Query Buffer Seconds	Number of seconds to select as a buffer from the SQL DB	30
Top Return Rows	SettingsDescGscEvent_ TopReturnRows	1000

Operator Console

Setting	Description	Default
Activate PTZ Control on Viewer Selection	Activate PTZ Control on Viewer Selection.	Disabled
Alarm Not Acknowledged Timeout	The amount of time in seconds before the Alarm sound volume is increased.	20
Allow Alarm Auto View	Indicates that a Operator Console can Auto View Alarms.	Enabled
Allow Alarm Review	Indicates that a user can Review Alarms.	Enabled
Allow connection to an MBeg controller	Indicates that an Operator Console can be connected to an MBeg controller.	Enabled
Allow control of PTZ	Indicates that a user can control PTZ.	Enabled
Allow Interaction Objects	Indicates that a user can configure interaction objects that indicates the state of components and allow for state changes by clicking on these objects.	Enabled
Allow Overriding of Motion Privacy and Client Privacy Zones	Indicates that user's privileges can override the rendering of Motion Privacy and Client Privacy Zones.	Disabled
Allow Remote Control	Indicates that a Operator Console can be Remotely Controlled.	Enabled
Allow Save Connection of Cameras	Indicates that a Operator Console can save Connection of Cameras for templates.	Disabled
Allow use of Alarms	Indicates if any alarms can be used in G-SIM.	Enabled

Setting	Description	Default
Allow use of Cut Lists	Indicates that a user can view and create Cut Lists.	Enabled
Allow view of Audit Log	Indicates that a user can view the Audit Log.	Enabled
Allow Windows Screen Captures	Indicates whether users are allowed to use PrintScreen.	Disabled
Allows the use of the SNMP Plugin	Indicates the Health Agents may use the SNMP Plugin.	Disabled
Auto View Cycle Time	The amount of time in seconds before the Auto Alarm view is swapped with another Auto Alarm view (if another is present). The minimum is 5 seconds, the maximum is 900 seconds. Set 0 to disable Auto Alarm swapping.	20
Default Cutlist Item Length in Seconds	The number of Seconds to be used when creating a new Cutlist Item.	20
Default Days License Expire	The number of days before the License Expire warning will be shown.	7
Default Days Server Not Registered License Expire	The number of days before the License Expire warning will be shown if a server is not Registered.	30
Global maximum alarms from remote servers on startup	For Global installations, the maximum number of unhandled alarms to be requested from every enterprise remote server on startup.	50
Make last connected Viewer the active Viewer	Indicates that a Operator Console can do active viewer from	True

Setting	Description	Default
	last connected viewer.	
Maximum amount records of report	This setting determines the maximum amount of records for alarm report.	10000
Maximum Playback	Maximum Playback is used to control maximum speed for synchronized viewers.	20
Minimum Cutlist Item Length in Seconds	The minimum number of Seconds to be used when creating a new Cutlist Item.	3
Minutes Before Check Update	The number of minutes before the Client checks for Updates.	2
Minutes Before Video Playback is Blocked	The number of minutes before a user is forced to enter a comment to enable video playback.	60
Press F2 to use PTZ on MBEG	Indicates if operator should press F2 to use PTZ on MBEG. If this setting is enabled, the user must press F2 in order to use PTZ on MBEG. If this setting is disabled, the joystick functionality for zoom in / zoom out / PTZ movement is directly usable.	Enabled
Process data search days	The maximum number of days that the process data search can query.	30
Process data search Time Offset	The amount in seconds to offset the EventData Time in the query. The Default is 600 seconds (10 minutes).	600

Setting	Description	Default
PTZ Control Auto Timeout	The amount of inactive time in minutes before the PTZ control is released.	3
PTZ Control Home Timeout	The amount of time in seconds after the PTZ control was released before it is moved to the 'Home Position'.	60
Reinitialize Viewer after Reconnect	Viewers are reinitialized after reconnect to GSimServer. If true viewers are cleared and reconnected, if false viewers are not cleared after Server has been reconnected but viewer statistic data could be incorrect.	Enabled
Request Data Changes	The console will re-request data when the 'ConfigSet' event has fired.	Enabled
Send CustomAction for User Login / Logout and Camera changes	This enables the OpCon to send out an CustomActionExtended to G-Core systems with the information that an G-SIM User has logged in to the OpCon. The action includes timestamp, G-SIM Username, Hostname and Login or Logout. For Login the Value is 1, for Logout the Value is 0. The action is also send whenever the camera list of the operator has been updated using parameter 2 = CamerasChanged.The action is only send when the console has a valid console global number.	Disabled

Setting	Description	Default
Show Event Description in OSD Text	Indicates that the Event Description is added to OSD Text if Event Text is enabled for this client.	Disabled
Show Event Parameter in OSD Text	Indicates that the Event Parameters are added to OSD Text if Event Text is enabled for this client.	Enabled
Show OSD Text while Zoomed	Indicates that the OSD Text should be rendered even if the Viewer is Zoomed.	Disabled
Unpause Suspended Live Viewers	Viewers that was in Live Stream mode before suspension.	Enabled
Viewer Action Mode	Sends a viewer connected action, viewer cleared action, viewer playmode changed action and viewer selection changed action according to the mode selected. If no populated template is used the viewer number inside the action will be the operator consoles global number if it differs from 0. If no console global number is set in that case the action will get dropped.	Send to None
Viewer Process Data Lookup Mode	The way in which the Process data is matched with the Video Images.	Event ID
Viewer Process Data Offset Correction	The number of miliseconds to correct the process data time. This will not work with EventID lookup mode and is limited to 0 to 750 miliseconds.	0

Management Console

Setting	Description	Default
Allow Custom System Component Categories	Indicates the Custom System Component Categories may be added and used by G-SIM.	Enabled
Allow Management Console Reporting	Indicates that Reporting can be used by the Management Console users.	Enabled
Maximum number of simultaneously connected ManCons	Sets the maximum number of simultaneously connected ManCons, "0" - means unlimited connections.	

User Management

Setting	Description	Default
Enforce Password History	Enforce password history for user.	Disabled
Idle Minutes Before Auto Log Out	The number of minutes before a user is automatically logged out if the system is idle. i **If this value is set to 0, the function is disabled.**	60
Idle Minutes Before ManCon Auto Log Out	The number of minutes before a user is automatically logged out of the ManCon if the system is idle (0 = disabled).	60
Invalid Login Attempts	The number of invalid login	6

Setting	Description	Default
	attempts before the account is Locked.	
Maximum Password Age	This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0.	0
Minimum length of login comment	Minimum length of comment that needs to be entered on second user login.	5
Minimum Password Length	The Minimum password length.	12
Minutes Before Forced Log Out	The number of minutes before a user is forced to log out. i **If this value is set to 0, the function is disabled.**	360
Remaining time before password expiry notification	This security setting determines the amount of time (in days) before the user is notified that the password will be expired in the amount of Day´s that was set. (is disabled if Maximum Password Age is 0)	0
Timeout for second user	The timeout (in minutes) after which the second user gets	10

Setting	Description	Default
	logged out automatically.	
Windows Authentication auto login timer	Timer (in seconds) to log in automatically into OpCon via Windows Authentication. More information can be found under **Automatic Login via Windows Authentication**.	0

Health Monitoring

Setting	Description	Default
Health Agent Checkin Critical Flag Period	The time period in hours after which a site will be flagged (This is due to no communication from the Health Agent). ℹ **Converted into seconds, this value must be more than twice the check-in period to allow the server to start.**	12
Health Agent Checkin Period	The time period in seconds a Health Agent periodically will have to check-in with the CM to report its health.	600

Active Directory Settings

Setting	Description	Default
Active Directory Domain Controller Hostname	The fully qualified domain name of the domain controller, e.g domain-name.toplevel-domain `companyname.com`.	Empty string
Active Directory Domain Controller Port	Indicates the current port number. It changes depending on whether LDAP-S is activated or not. The default port for LDAP is 389 and for LDAP-S 636. ⓘ **You can enter any port number in this field. If no port is selected, the default port is used.**	389 / 636
Active Directory Domain Controller User Name	Indicates the user name. ⓘ **It must be a user with login access to the domain to be able to retrieve the active directory information from the specific Active Directory Search Path.** This field can remain empty. In this case, the G-SIM agent should be started by a user who is included in the domain and has the appropriate user rights to retrieve the active directory information.	Empty string

Setting	Description	Default
Active Directory Domain Controller User Password	Indicates the user password. ℹ **It must be a user with login access to the domain to be able to retrieve the active directory information from the specific Active Directory Search Path.** This field can remain empty. In this case the G-SIM agent should be started by a user who is included in the domain and has the appropriate user rights to retrieve the active directory information.	Empty string
Active Directory Search Path	The distinguished name of the active directory components in which the user groups are located. Multiple distinguished names can be specified separated by a semicolon.	Empty string
Active Directory synchronization interval in minutes	The interval in minutes when the active directory user synchronization takes place.	10
Delete G-SIM users on Active Directory synchronization	If this option is enabled, all unassigned G-SIM users are deleted from the user database, either because they have been deleted from the active directory or because the group assignment has been removed.	Disabled

Setting	Description	Default
	If this option is disabled, the G-SIM users are only deactivated and remain in the G-SIM user database. **The audit logs of deleted users will be removed and displayed as 'unknown user'.**	
Use automatic G-SIM group assignment on synchronization	If this option is enabled, the automatic user group assignment is used for every synchronization. This means that the linked G-SIM user group will be automatically adjusted to the first group which is assigned to the active directory group with this user as a group member. If this option is disabled, the user remains in the G-SIM group which was manually assigned to them.	Disabled
Use LDAP-S as Active Directory Domain Controller Protocol	If this option is enabled, LDAP-S is activ. If this option is disabled, LDAP is activ.	Disabled

SAML Support

Setting	Description	Default
Active	Active/Deactivate SAML support.	Disabled
Service Provider URL	URL for Service Provider.	Empty string

G-IES Settings

Setting	Description	Default
G-Core G-IES Service Port	The Portnumber of the G-Core G-IES Export Service.	Empty string
GeViScope G-IES Service Port	The Portnumber of the GeViScope G-IES Export Service.	Empty string
G-IES Service Address	The IP-Address of the G-IES Export Service.	Empty string
G-IES Service Password	The Password used for access to the G-IES Export Service.	Empty string
G-IES Service Username	The Username used for access to the G-IES Export Service.	Empty string

Web Browser Management

Setting	Description	Default
Create audit entries	Set to true to log all Webbrowser navigation. Set to false to log Webbrowser navigation according to individual Browser Bookmark "Create audit entries" setting.	Disabled
Disable Webbrowser GPU acceleration	Set to true will disable the Webbrowser Framework to use GPU acceleration for rendering.	Disabled
Enable Auto Play for Webbrowser Content	Set to true will enable Auto Play for Webbrowser content without user gesture.	Disabled
Ignore Certificate Errors	Set to FALSE to handle Browser certificates per default. Set to TRUE to ignore	Disabled

Setting	Description	Default
	Certificate errors (not recommended).	
Use cookies in the Webbrowser	Set to true will enable saving and using cookies in the Webbrowser.	Disabled

GIS Maps

Setting	Description
GIS Maps MapTiles Service Adress	IP or hostname of the computer on which the MapTiles service is installed. The MapTiles Service acts as a proxy between the GIS map controller and the GIS map provider. When the address is specified, the GIS map control makes a request to the map tile service each time it needs a map tile image. The MapTiles Service uses the **GIS Maps provider**, **GIS Maps provider key**, **GIS Maps mode**, and **Path to MBTiles package** settings to obtain MapTiles images. i **The MapTiles package provider is only available if the address of the Map Tile service is specified.**
GIS Maps mode	Three modes are available: • **Server only**: In this mode, the GIS map control makes a request to the map provider each time it needs a map tile image. If the request is successful, the MapTile image is displayed in the GIS Map control. If the request is not successful, an error message is displayed in the GIS Map control. • **Server and cache**: In this mode, the GIS Map control makes a request to the cache database each time it needs a MapTile image. If the request is not successful, the GIS map control makes a request to the

Setting	Description
	map provider. If the request is successful, the MapTile image is added to the cache database and displayed in the GIS map control. If the request is not successful, an error message is displayed in the GIS Map control. - **Cache only**: This is the "Offline" mode. The GIS Map control attempts to retrieve the MapTile image from the cache database. If the MapTile image is retrieved, it is displayed in the GIS Map control, otherwise an error message is displayed in the GIS Map control. i **The Server and cache and Cache only options are not available for the Google Maps and Map Tiles Package provider.**
GIS Maps Provider	Select the provider to request map tiles images for GIS map control. Available providers are **Google maps**, **OpenStreetMap maps** and **Map tiles package**. The name of the provider is displayed at the bottom of the GIS map control.
GIS Maps Provider Key	Enter the license key for your maps provider. This setting is mandatory for the Google Maps provider. The key can be requested via https://developers.google.com/maps/documentation/maps-static/get-api-key.
Map Objects Cluster Alarm Color	Defines the color for the icon of a map object cluster when one of the associated map objects is in alarm.
Map Objects Cluster Color	Defines the color for the symbol of a map object group.

Setting	Description
Map Objects Icon Size	Defines the icon size of all GIS map objects and map object groups. ⓘ **Changing the icon size may affect the grouping of map objects.**
Path to MBTiles package	The path to the MBTiles DataSet file on the computer running the MapTiles Service. This package will be used as offline tile source. This setting is mandatory for the MapTiles package provider. The MBTiles package can be obtained from the website **https://openmaptiles.com/downloads/planet**/. The MapTiles package provider supports both raster and vector datasets for MapTiles.

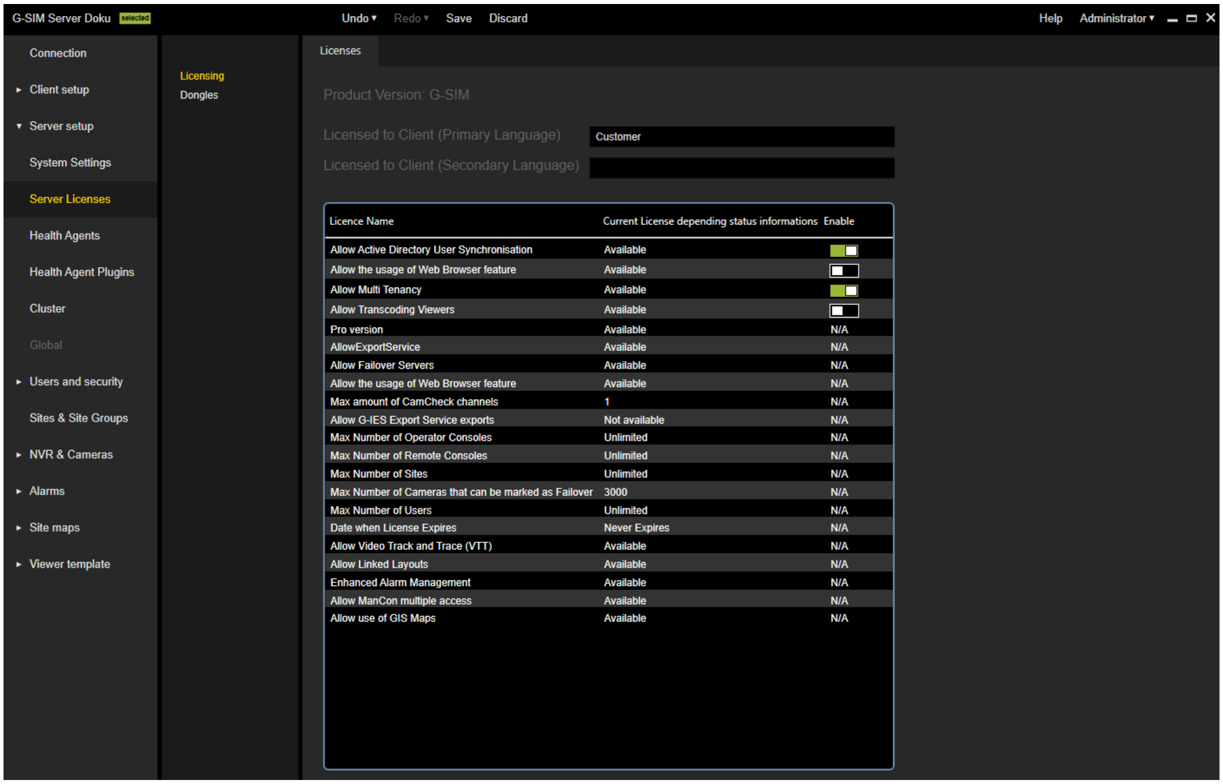
Server Licenses

The Server Licenses menu contains dialog windows: **Licensing** and **Dongles**.

Licensing

The Licensing dialog window provides a list of the dongle-related licenses and their status. You can activate or deactivate some of the available licenses. Move the mouse cursor over an entry to display a description of the license.

You can configure the Licensed to Client setting for both primary and secondary languages. This setting is displayed in the login screen of the Operator Console.



Product Version: G-SIM

Licensed to Client (Primary Language): Customer

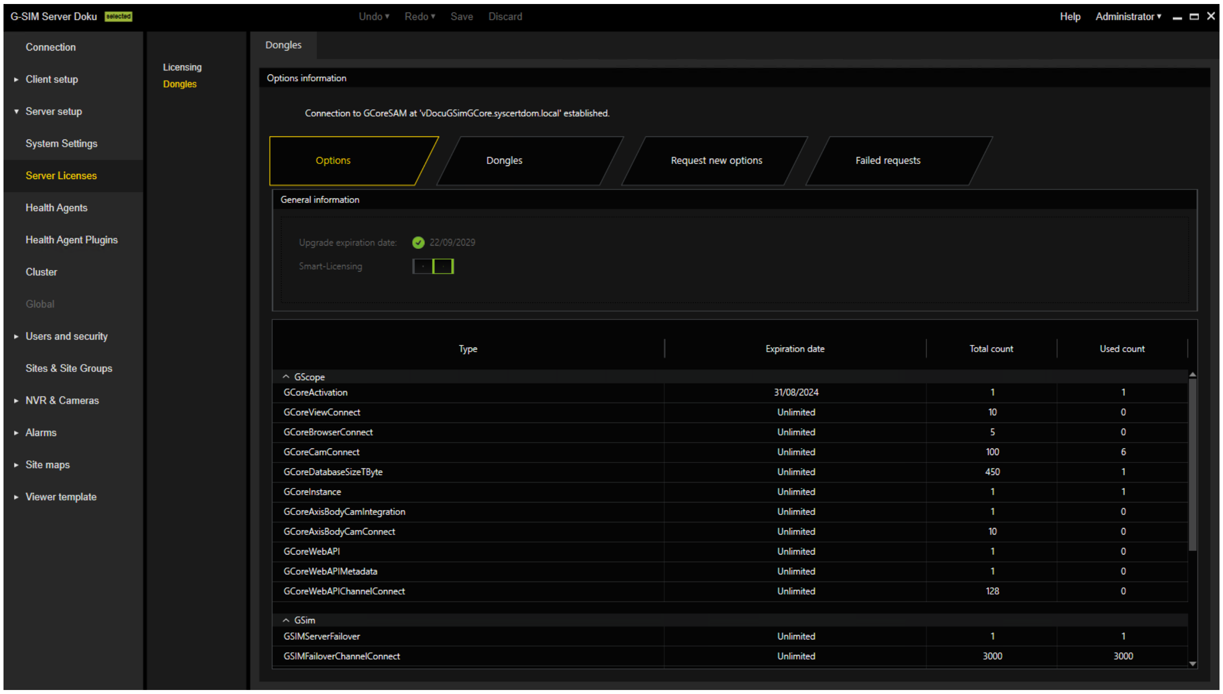
Licensed to Client (Secondary Language):

Licence Name	Current License depending status informations	Enable
Allow Active Directory User Synchronisation	Available	☑
Allow the usage of Web Browser feature	Available	☐
Allow Multi Tenancy	Available	☑
Allow Transcoding Viewers	Available	☐
Pro version	Available	N/A
AllowExportService	Available	N/A
Allow Failover Servers	Available	N/A
Allow the usage of Web Browser feature	Available	N/A
Max amount of CamCheck channels	1	N/A
Allow G-IES Export Service exports	Not available	N/A
Max Number of Operator Consoles	Unlimited	N/A
Max Number of Remote Consoles	Unlimited	N/A
Max Number of Sites	Unlimited	N/A
Max Number of Cameras that can be marked as Failover	3000	N/A
Max Number of Users	Unlimited	N/A
Date when License Expires	Never Expires	N/A
Allow Video Track and Trace (VTT)	Available	N/A
Allow Linked Layouts	Available	N/A
Enhanced Alarm Management	Available	N/A
Allow ManCon multiple access	Available	N/A
Allow use of GIS Maps	Available	N/A

Dongles

In the **Dongles** dialog window you can manage your licenses or options and import new licenses. It provides an overview of the available licenses and contains information about the options in the database.

For detailed information about the Dongle dialog window, see Server Licenses **and for information on Geutebrück Software Licensing, see** Software Licensing**.**



Connection to GCoreSAM at 'vDocuGSimGCore.syscertdom.local' established.

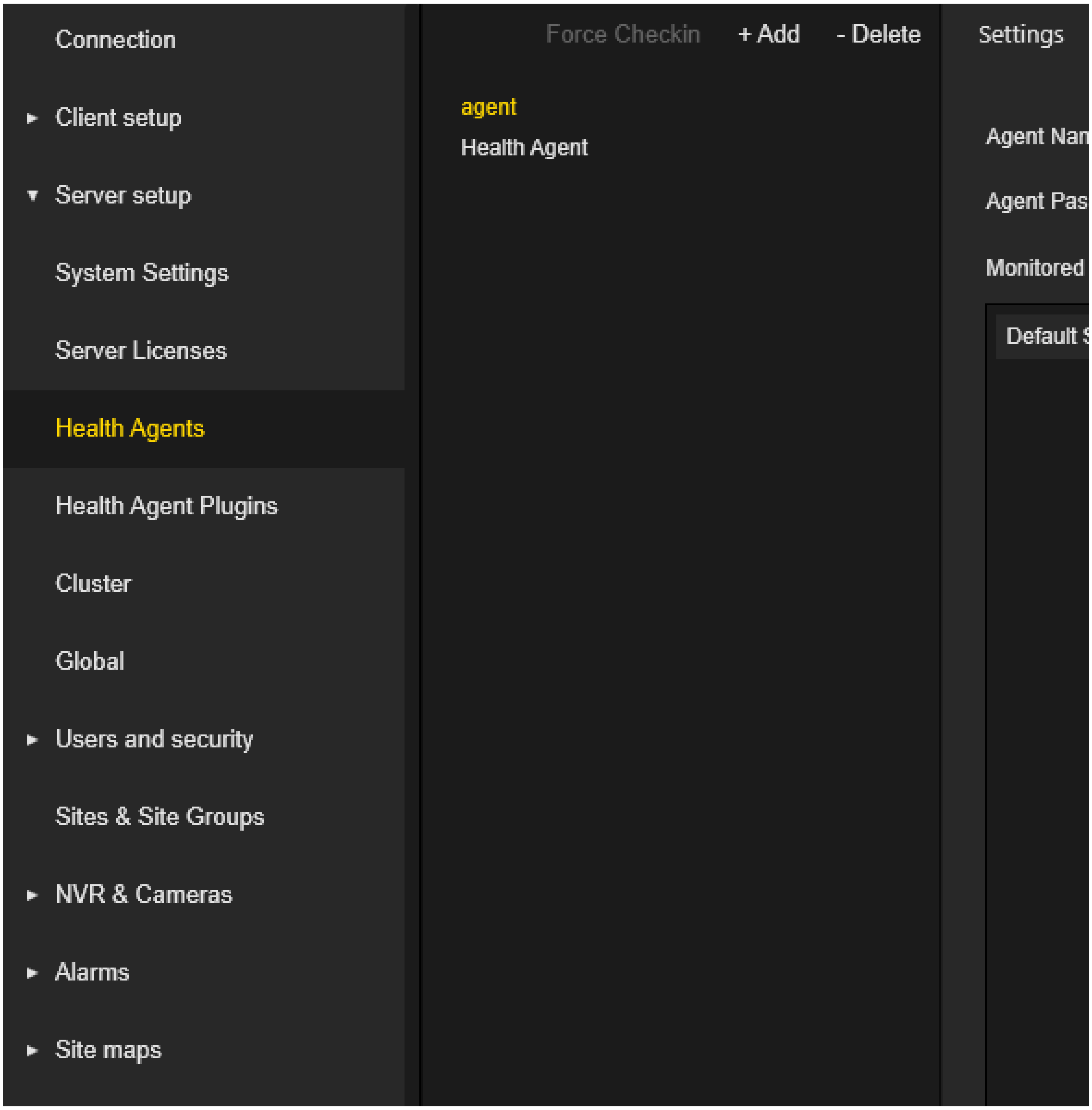
Upgrade expiration date: ✓ 22/09/2029

Smart-Licensing

Type	Expiration date	Total count	Used count
GScope			
GCoreActivation	31/08/2024	1	1
GCoreViewConnect	Unlimited	10	0
GCoreBrowserConnect	Unlimited	5	0
GCoreCamConnect	Unlimited	100	6
GCoreDatabaseSizeTByte	Unlimited	450	1
GCoreInstance	Unlimited	1	1
GCoreAxisBodyCamIntegration	Unlimited	1	0
GCoreAxisBodyCamConnect	Unlimited	10	0
GCoreWebAPI	Unlimited	1	0
GCoreWebAPIMetadata	Unlimited	1	0
GCoreWebAPIChannelConnect	Unlimited	128	0
GSim			
GSIMServerFailover	Unlimited	1	1
GSIMFailoverChannelConnect	Unlimited	3000	3000

Health Agents

The **Health Agents** view contains the list of Health Agents. The Health Agent is a software component that runs as a service on a designated computer. Health Agents perform health information monitoring, intercept events, and generate alarms.

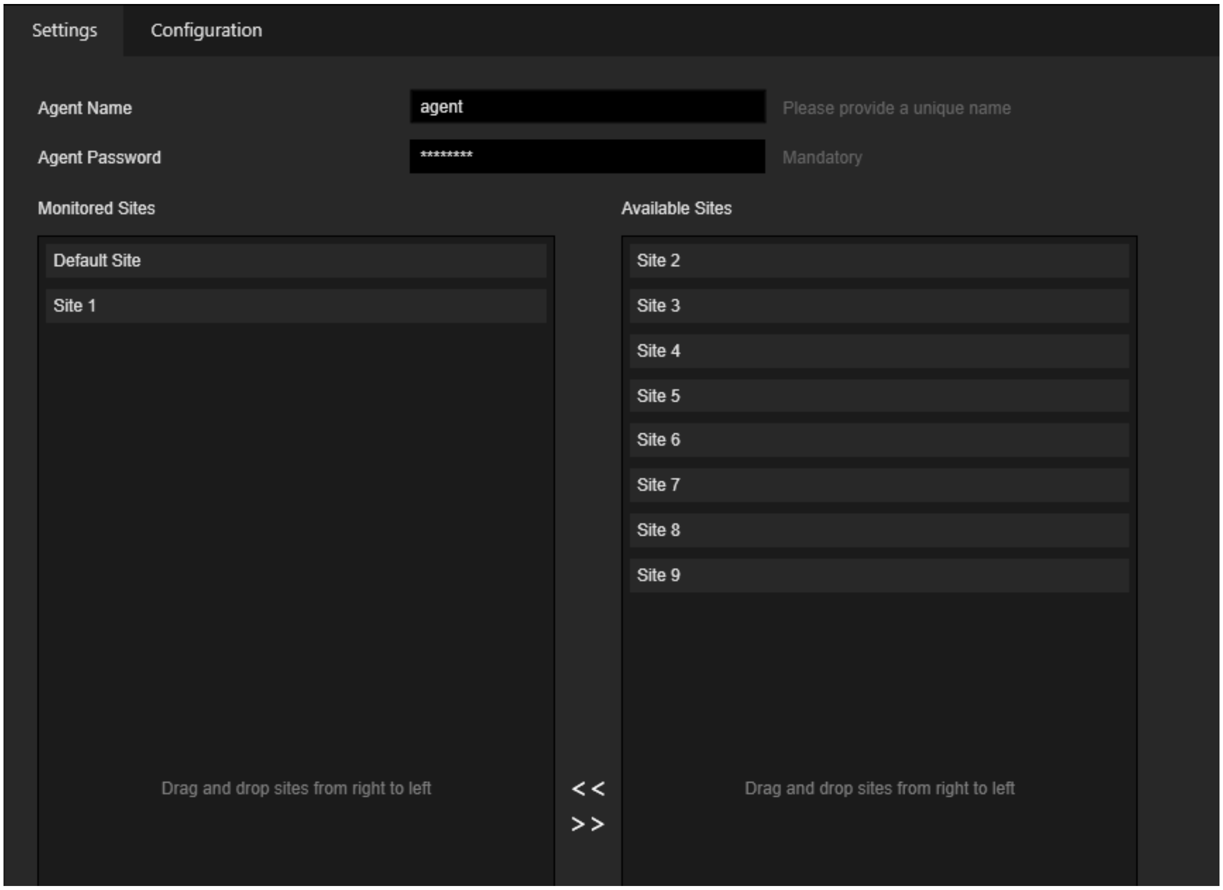


The Health Agents settings are grouped in tabs.

Settings

The administrator should configure the **Agent Name** and **Agent Password** settings. The same settings should be configured in the **GSIM.AgentConfig.exe** utility on the computer where the specific agent is installed.

The administrator can select sites that are to be monitored by the specific agent.



Agent Name: agent — Please provide a unique name

Agent Password: ******** — Mandatory

Monitored Sites:
- Default Site
- Site 1

Drag and drop sites from right to left

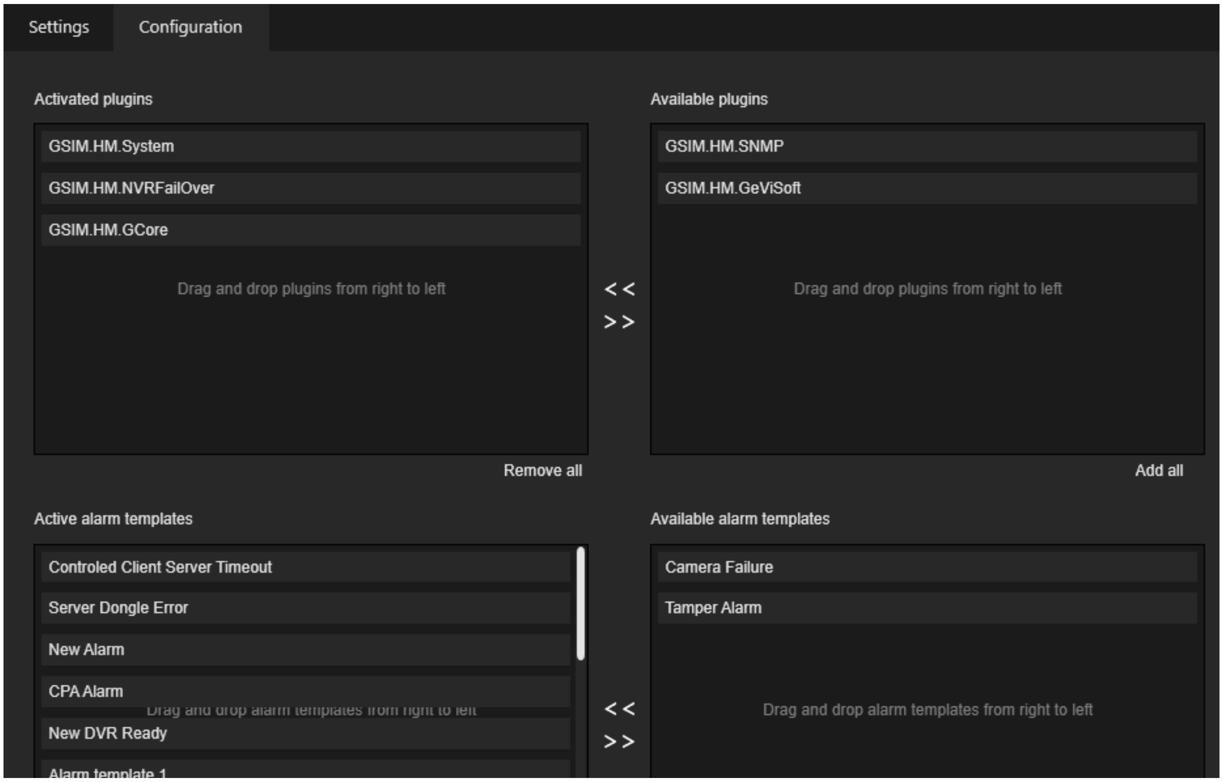
Available Sites:
- Site 2
- Site 3
- Site 4
- Site 5
- Site 6
- Site 7
- Site 8
- Site 9

Drag and drop sites from right to left

Configuration

The administrator can select Health Agent plugins that will be used by the specific Health Agent. Health Agent plugins are software components that can only be run inside the Health Agent process. Health Agent plugins collect health information that is sent to the G-SIM server by the specific Health Agent.

The administrator can also select alarm templates that can be used by specific Health Agents to generate alarms.


Settings
Configuration
<<
>>
Remove all
Add all
Drag and drop plugins from right to left
Drag and drop plugins from right to left
Drag and drop alarm templates from right to left
Drag and drop alarm templates from right to left
<<
>>

Activated plugins

- GSIM.HM.System
- GSIM.HM.NVRFailOver
- GSIM.HM.GCore

Available plugins

- GSIM.HM.SNMP
- GSIM.HM.GeViSoft

Active alarm templates

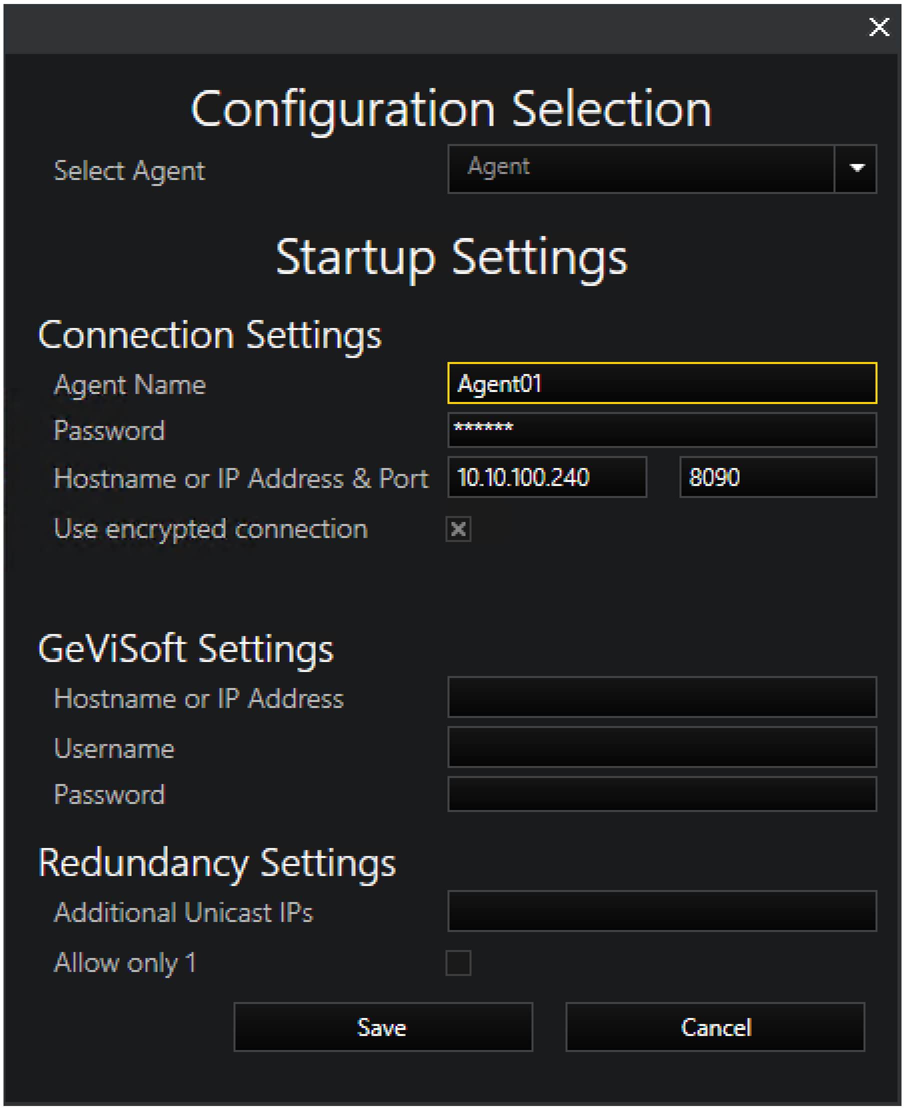
- Controled Client Server Timeout
- Server Dongle Error
- New Alarm
- CPA Alarm
- New DVR Ready
- Alarm template 1

Available alarm templates

- Camera Failure
- Tamper Alarm

Configuring Health Agents

The configuration of the deployed Agents must be performed on each machine by using the GSIM.AgentConfig program:



Configuration Selection

Select Agent: Agent

Startup Settings

Connection Settings

Agent Name: Agent01

Password: ******

Hostname or IP Address & Port: 10.10.100.240 8090

Use encrypted connection ☒

GeViSoft Settings

Hostname or IP Address:

Username:

Password:

Redundancy Settings

Additional Unicast IPs:

Allow only 1 □

The following parameters must be specified:

Parameters	Description
Select Agent	Defines the type of the running agent: Agent or Health Agent. Agents run locally on the system, Health Agents run on a remote system and are used for NVR-Failover.
Connection Settings	
Agent Name	The Agent name.

Parameters	Description
Password	Password used for the connection to the G-SIM server.
Hostname or IP Address & Port	Hostname or IP Address & Port of the G-SIM server to which the agent is connecting.
Use encrypted connection	Enable this checkbox when you use an encrypted connection for G-SIM.
GeViSoft Settings	
Hostname or IP Address	IP Address of the GeViSoft server.
Username	Username for the connection to the GeViSoft server.
Password	Password for the connection to the GeViSoft server.
Redundancy Settings*	
Additional Unicast IPs	IP addresses of all systems in this cluster separated with ; (the first IP is the local IP).
Allow only 1	Only one agent, when both are running, processes the alarms to prevent duplicate entries.

* These settings are required when you run a G-SIM cluster system.

Configuring the deployed Health Agents require adding a Health Agent entry for every Health Agent deployed.

i **You require the following rights to amend Health Agents (HAs): Administrator; Health and Alarms Access.**

New Health Agents are added via right-clicking on Health Agents in the top part of the configuration chooser pane. That is also where you can choose to force Health Agents to check in with the G-SIM server via a self-explanatory pop-up window.

Removing Health Agents s is done via the delete icon in the title bar.

If you are running a G-SIM cluster system and require NVR-Failover, it is necessary to add Agents and Health Agents to your system. These Health agents are only used for NVR-Failover in this scenario.

Parameters

Agent name: The agent name that is defined in the GSIM.AgentConfig software.

Agent Password: To specify an agent's password for authentication on the server.

Agent/Health Agent performs authentication procedure only in case of connecting to a server that supports this functionality. Otherwise it proceeds without authentication. In case of an upgrade, all agents must be configured to have passwords using both the Management Console and the AgentConfig application.

Monitor Sites: The sites to be monitored by this Health Agent.

Plug-in Management: Which plug-ins this Health Agent must load.

Alarm Management: Choose which alarms the Health Agent is responsible for generating when the desired conditions are met. The individual Health Agent local parameters of the alarm are also configured here.

Configuring Health Agents

The procedure for configuring a Health Agent is outlined below:

1. Add the desired Health Agent entry.

2. Set the agent name.

3. Go to the Monitor Sites tab.
Add the sites the Health Agent is responsible for monitoring to the Monitor Sites list. Sites can be removed by right clicking the Monitor Sites list and selecting the Remove Selected or Remove All action.

4. Go to the Plug-in Management tab.
Select the health monitor plug-ins that the Health Agent should load at start-up. See the Health Agent Start-up Procedure section for more details. This can be accomplished by simply checking the plug-ins to include.

5. Go to the Alarm Management tab.
Select the alarms the Health Agent is responsible for generating when the desired conditions are met. This can be accomplished by simply checking the alarms to enable.

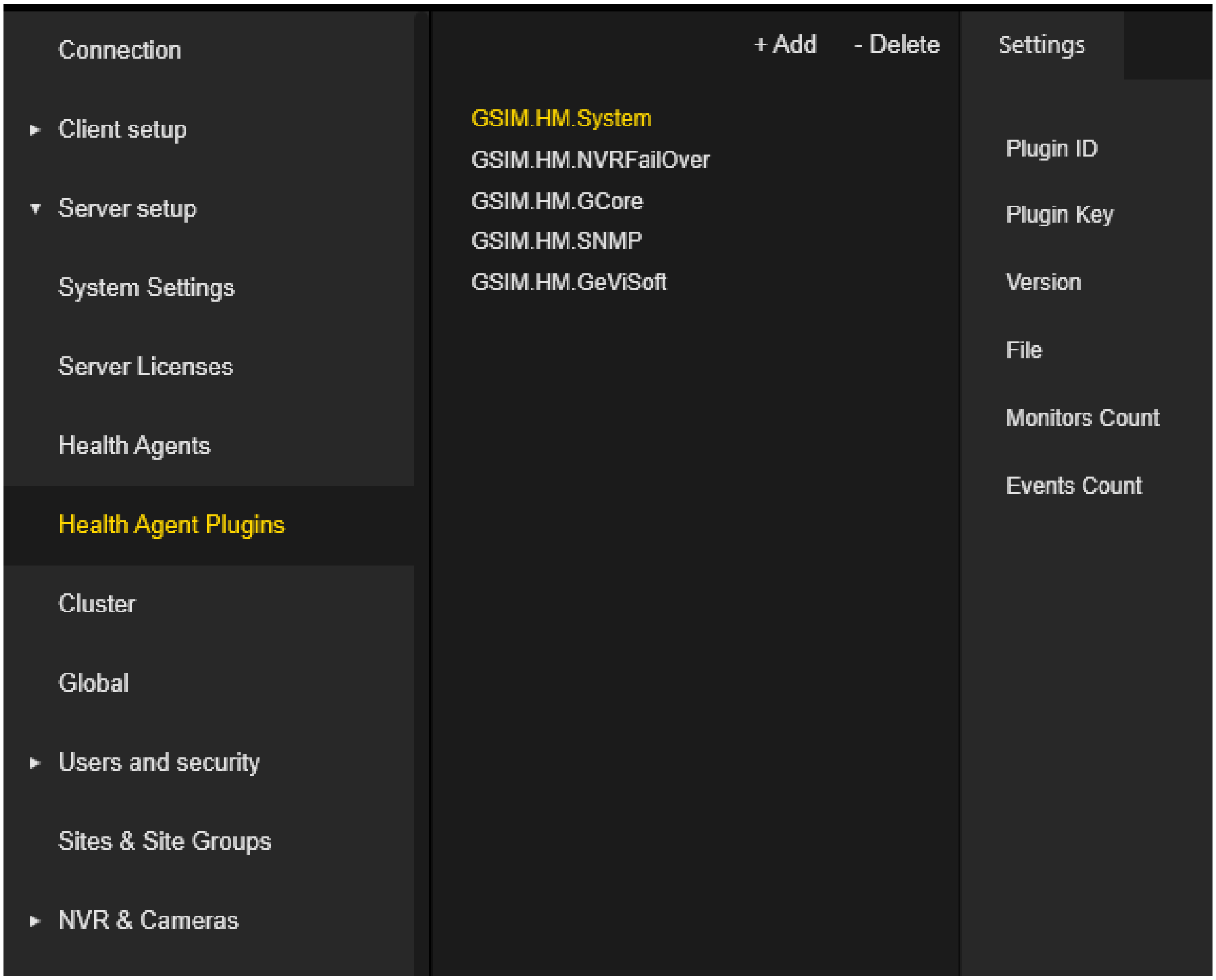
6. Configure the alarm local parameters.
Parameters that customise or define the behaviour of the alarm managed by the Health Agent in question can now be added or changed. Please refer to the Health Monitor Plug-in documentation or the G-SIM Configuration and Implementation Manual for more information on parameters and their meaning.

To do so, select the required alarm and use the parameter editor to add, edit or delete parameters. The save and cancel buttons will be available in add and edit mode.

There are three additional buttons available: Add Alarm Logic, Add Input Contacts and Alarm Logic Range Wizard.

Health Agent Plugins

The **Health Agent Plugins** view contains a list of plugins that can be used in the Health Agents. The administrator can click the **+ Add** button and select a file with a valid plugin implementation to add a new Health Agent Plugin.



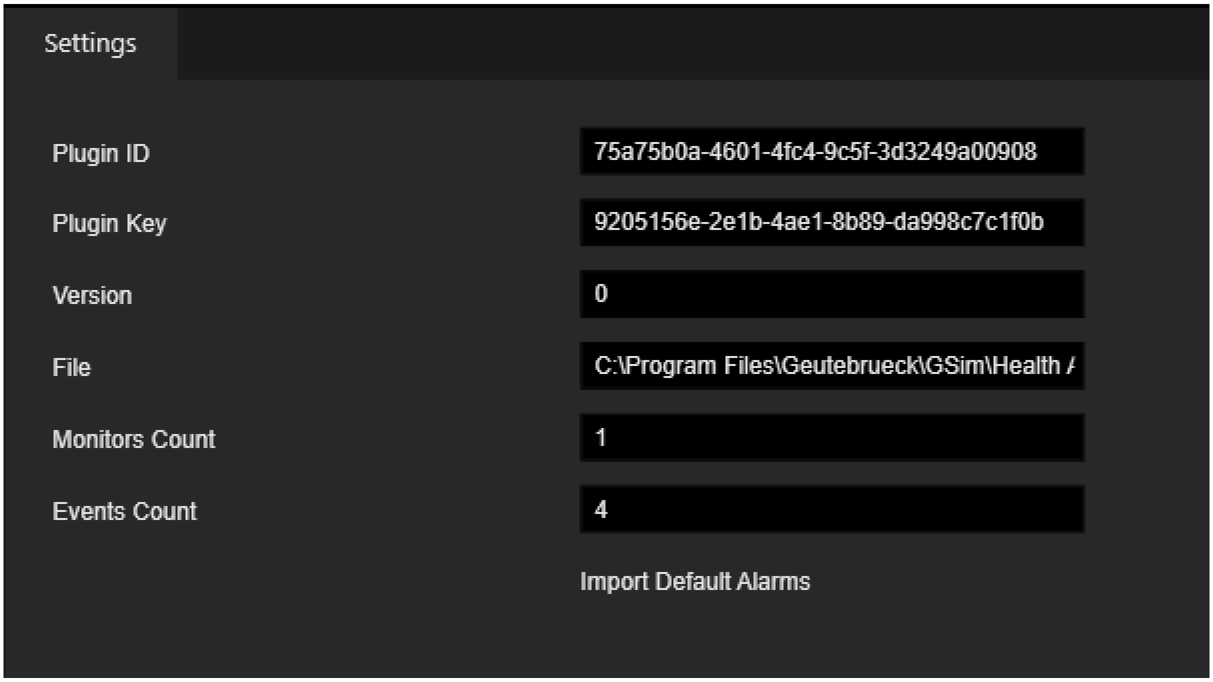
GSIM.HM.System
GSIM.HM.NVRFailOver
GSIM.HM.GCore
GSIM.HM.SNMP
GSIM.HM.GeViSoft

Plugin ID
Plugin Key
Version
File
Monitors Count
Events Count

Settings

The **Health Agent Plugins** settings view contains plugin specific information.

The administrator can click the **Import Default Alarms** button to automatically create alarm templates that are supported by specific plugins.



Plugin ID 75a75b0a-4601-4fc4-9c5f-3d3249a00908

Plugin Key 9205156e-2e1b-4ae1-8b89-da998c7c1f0b

Version 0

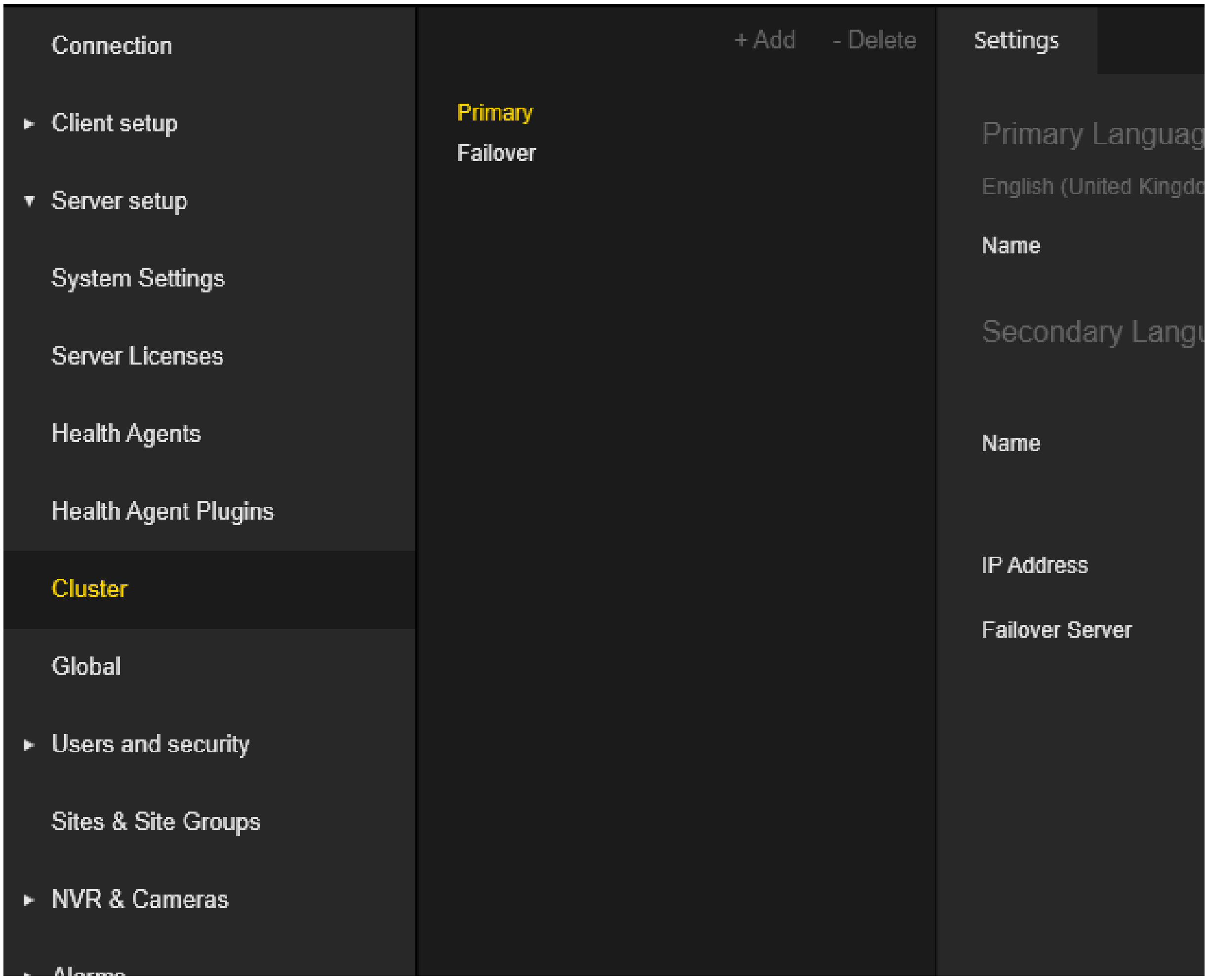
File C:\Program Files\Geutebrueck\GSim\Health /

Monitors Count 1

Events Count 4

Cluster

The **Cluster** view contains up to two servers. **Primary** server (first record in the list) and **Failover** server (if configured). The cluster menu is enabled if the **Allow Failover Servers** license is available. The Primary server record cannot be deleted. The Failover server stores the same setup as the Primary server. If the Primary server is down, the Operator Console will connect to the Failover server.



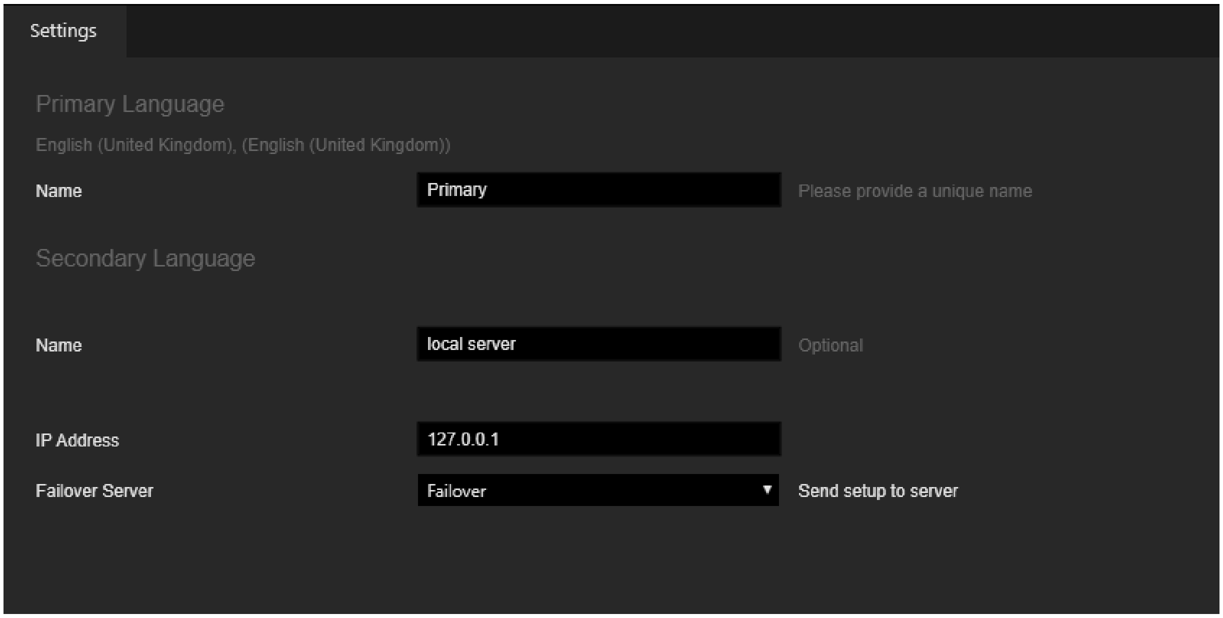
Settings

The administrator can configure the name and IP Address of the specific server.

If a Failover sever record is created, it can be selected in the **Failover Server** combo box of the Primary server.

When Failover Server is selected, the **Send setup to server** button will be enabled. The administrator can click this button to send the setup of the Primary server to the Failover server.

The **Failover Server** combo box and **Send setup to server** button are disabled when a specific server is a Failover server.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Primary — Please provide a unique name

Secondary Language

Name: local server — Optional

IP Address: 127.0.0.1

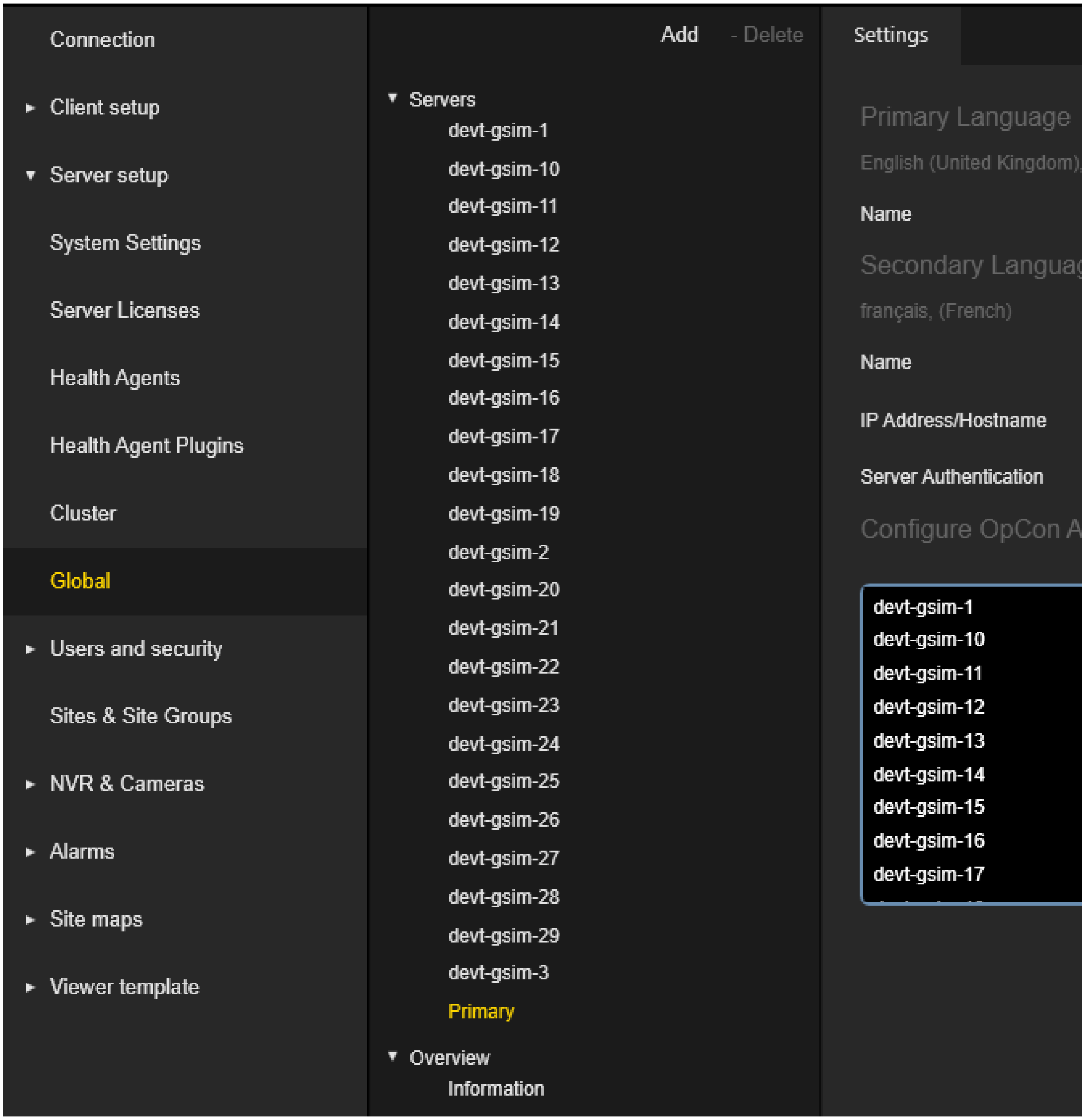
Failover Server: Failover ▾ — Send setup to server

Global

The **Global** view contains two items:

- **Servers**: Contains a list of the G-SIM servers that are added to the global environment.
- **Overview**: Contains an information view for the global environment.

The global menu is enabled if the **Allow Global Servers Connections** license is available and enabled.



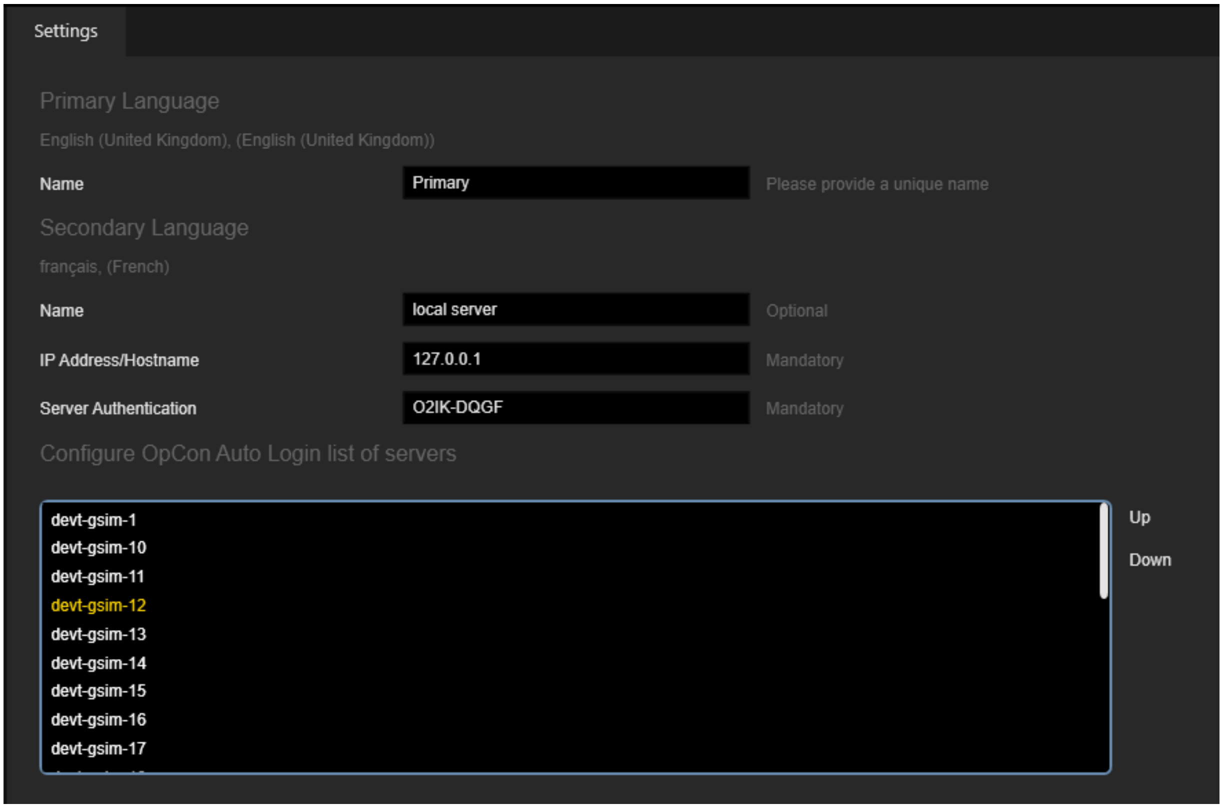
Primary Language
English (United Kingdom),
Name
Secondary Languag
français, (French)
Name
IP Address/Hostname
Server Authentication
Configure OpCon A

Global Server Settings

The **Global** server settings view is different for server that represent the currently connected G-SIM server and other servers in a global environment. For both types of servers, the administrator should configure **Name**, **IP Address/Hostname** and **Server Authentication** key.

Currently connected G-SIM Server

The administrator can configure the order of the global servers using the **Up** and **Down** buttons. The Operator Console will take the first available G-SIM server from this list in case the local server is down.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name	Primary	Please provide a unique name

Secondary Language

français, (French)

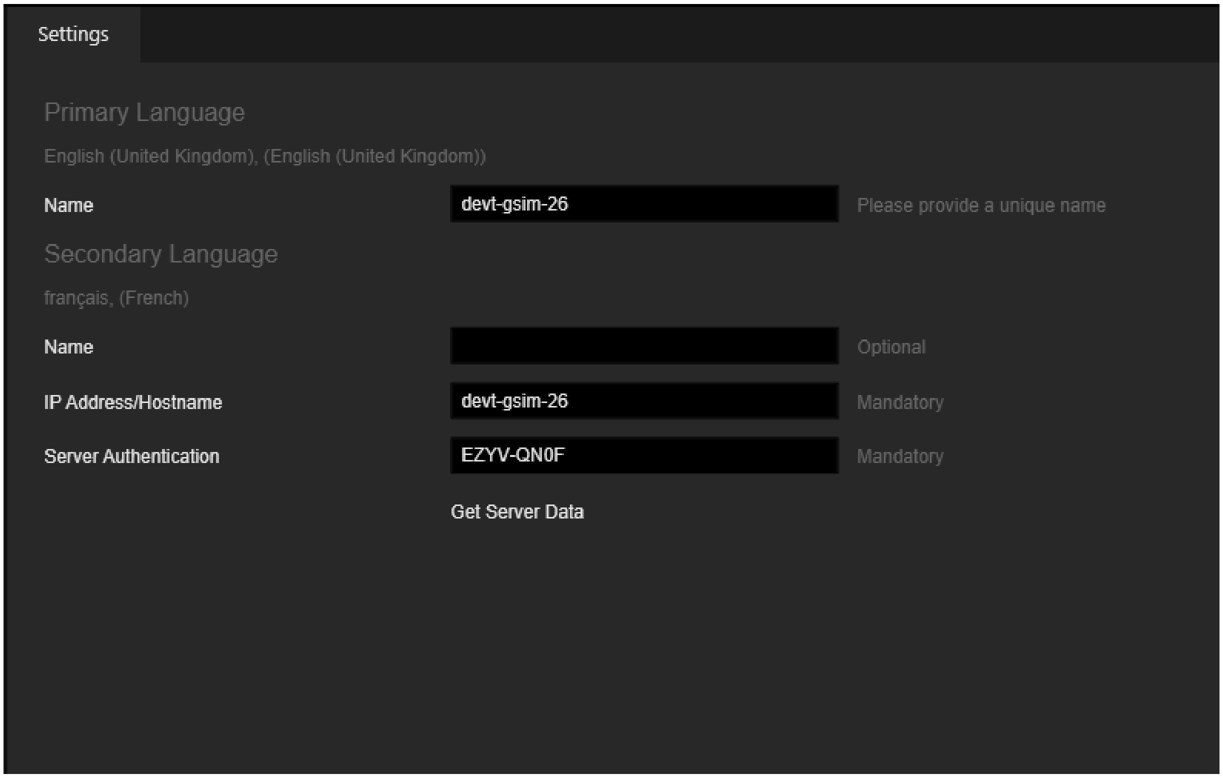
Name	local server	Optional
IP Address/Hostname	127.0.0.1	Mandatory
Server Authentication	O2IK-DQGF	Mandatory

Configure OpCon Auto Login list of servers

devt-gsim-1
devt-gsim-10
devt-gsim-11
devt-gsim-12
devt-gsim-13
devt-gsim-14
devt-gsim-15
devt-gsim-16
devt-gsim-17

Other G-SIM Servers

The administrator can click the **Get Server Data** button to retrieve setup form specific server and merge them with the setup of the currently connected G-SIM server.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: devt-gsim-26 — Please provide a unique name

Secondary Language

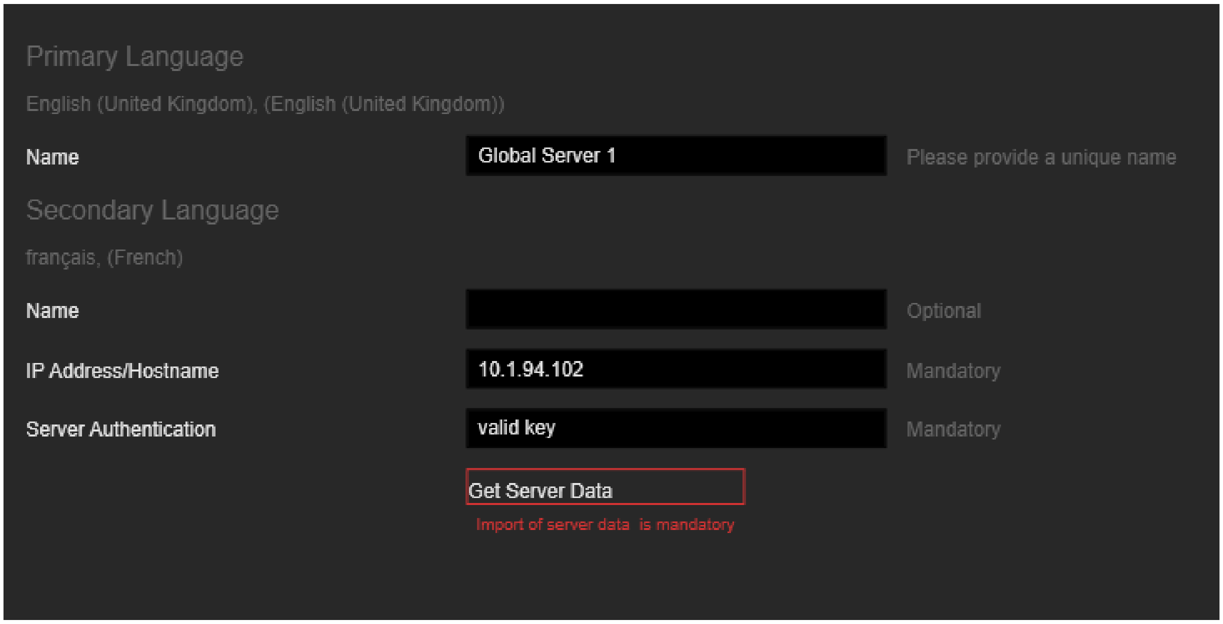
français, (French)

Name: — Optional

IP Address/Hostname: devt-gsim-26 — Mandatory

Server Authentication: EZYV-QN0F — Mandatory

If a new G-SIM server is added, the administrator is obligated to click the **Get Server Data** button to complete adding the server to the global environment.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Global Server 1 — Please provide a unique name

Secondary Language

français, (French)

Name: — Optional

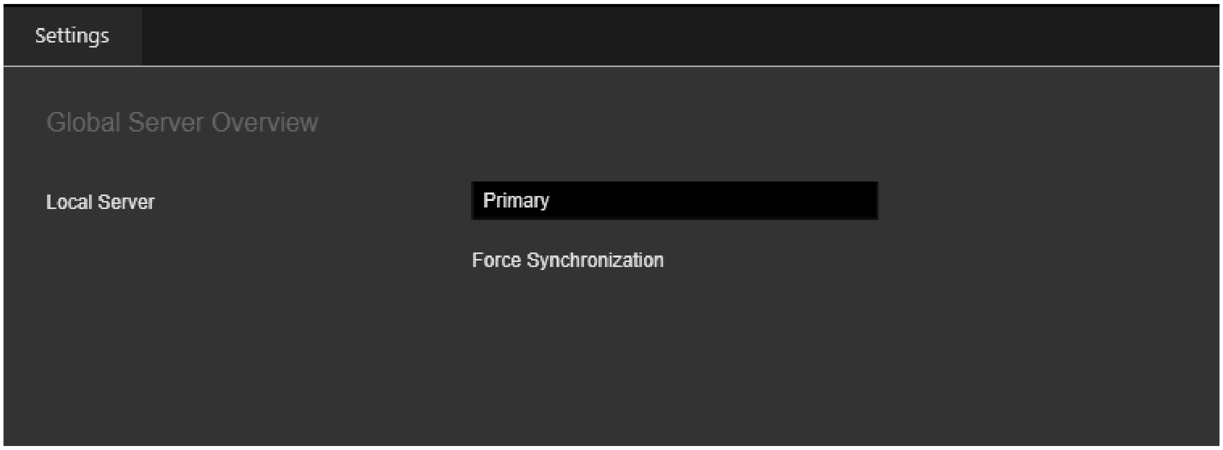
IP Address/Hostname: 10.1.94.102 — Mandatory

Server Authentication: valid key — Mandatory

Import of server data is mandatory

Overview Settings

The administrator can click the Force Synchronization button to immediately start the setup synchronization process between global servers.



Settings

Global Server Overview

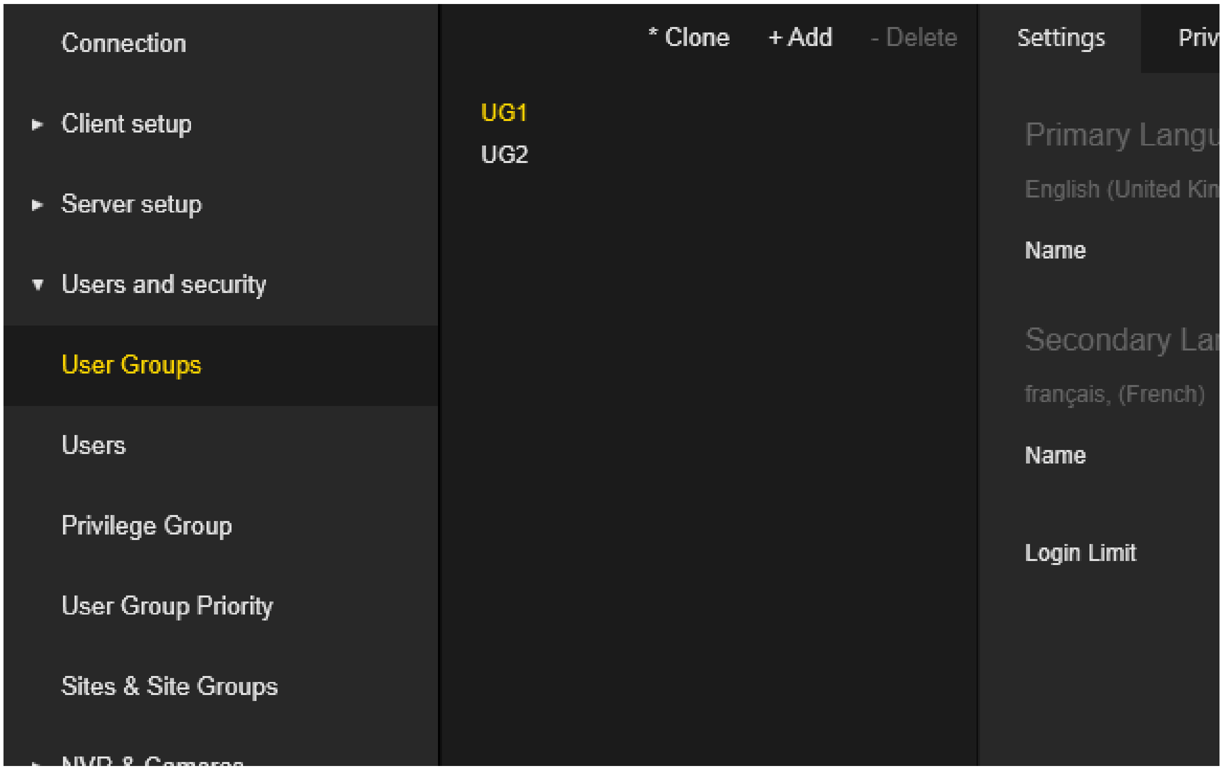
Local Server: Primary

Users and Security

User Groups

The User Groups view contains a list of user groups. There are three uses for user groups:

- Several users are grouped together in one user group. This allows you to send a message to all users of this group at the same time, e.g. in the Operator Console.
- A user group has a set of default privileges.
- A User Group can be part of a privilege group.

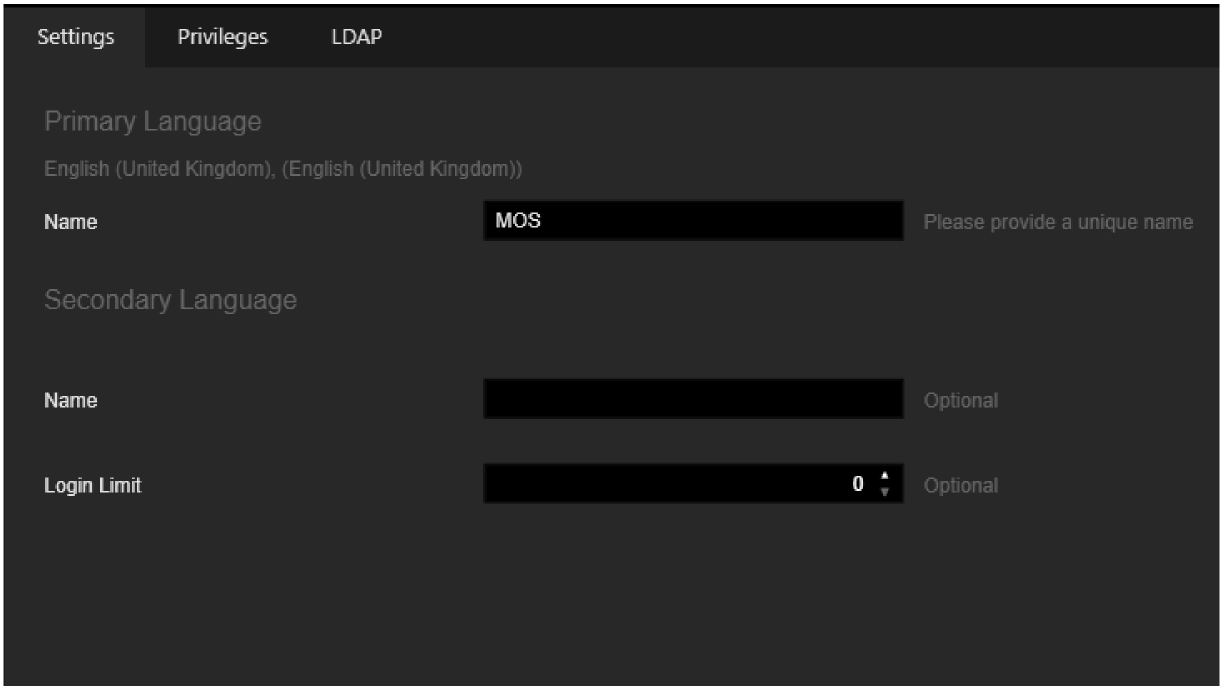


The **User Group** settings are grouped in tabs.

Settings

In the **Settings** tab the administrator can configure the name of the user group for the primary and secondary language.

The administrator can configure the **Login Limit** for the users of the user group. The login limit is the number of allowed logins for the Operator Console user. If the number of allowed logins is exceeded, the login will fail and the user will receive a message indicating that the number of allowed logins has been reached. A login limit with the value 0 means an unlimited number of available logins.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: MOS — Please provide a unique name

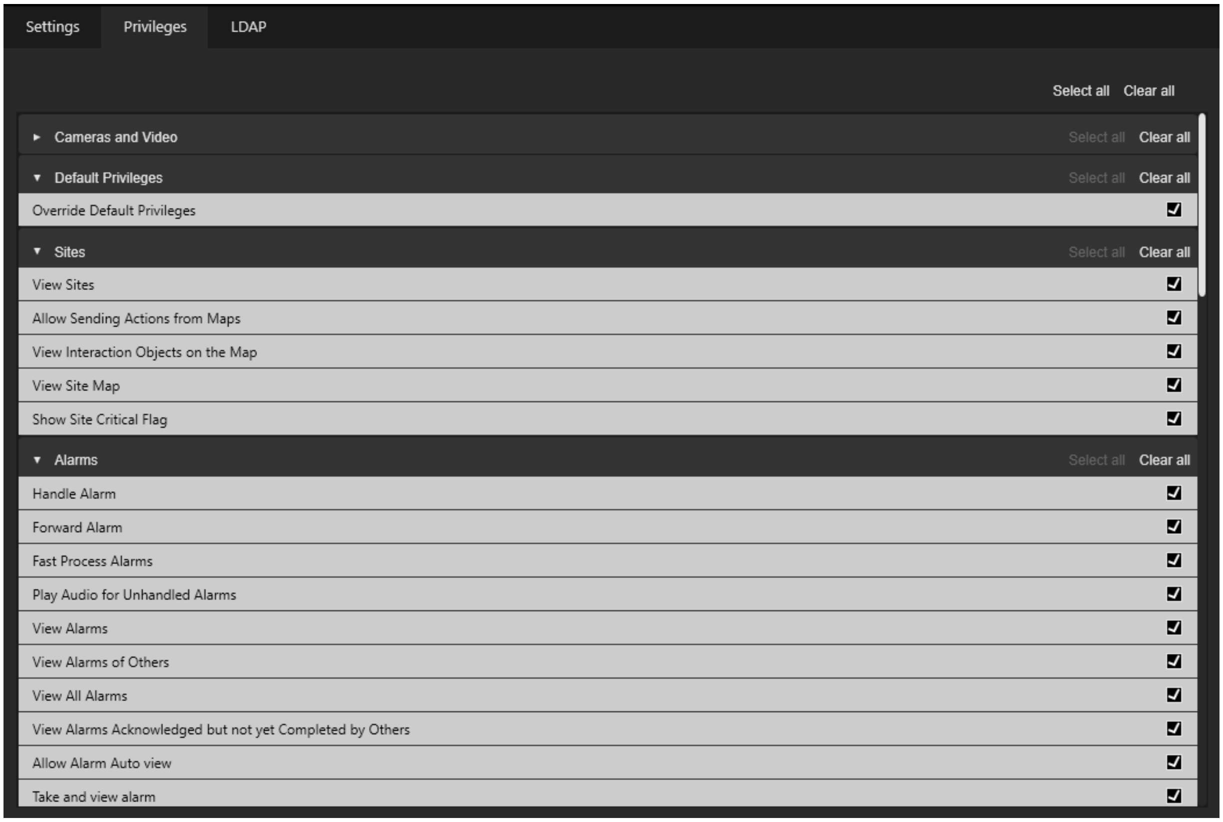
Secondary Language

Name: — Optional

Login Limit: 0 — Optional

Privileges

In the **Privileges** tab, the administrator can configure the privileges of the specific user group. The privileges are organized in groups. The administrator can use the **Select all** and **Clear all** buttons to select or deselect all privileges with one click. To display a detailed description, the administrator can hold the mouse cursor over the specific privilege.

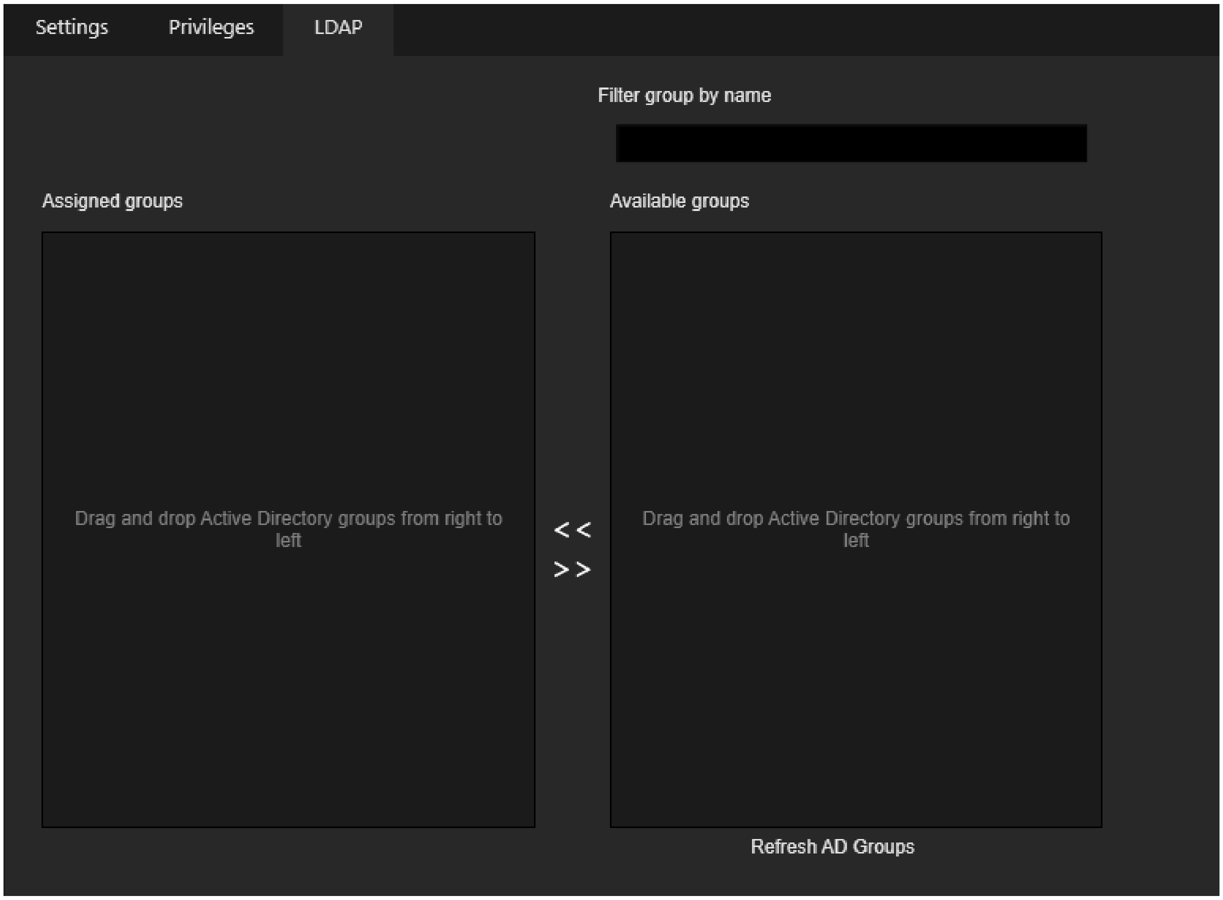


▸ Cameras and Video	Select all Clear all
▾ Default Privileges	Select all Clear all
Override Default Privileges	☑
▾ Sites	Select all Clear all
View Sites	☑
Allow Sending Actions from Maps	☑
View Interaction Objects on the Map	☑
View Site Map	☑
Show Site Critical Flag	☑
▾ Alarms	Select all Clear all
Handle Alarm	☑
Forward Alarm	☑
Fast Process Alarms	☑
Play Audio for Unhandled Alarms	☑
View Alarms	☑
View Alarms of Others	☑
View All Alarms	☑
View Alarms Acknowledged but not yet Completed by Others	☑
Allow Alarm Auto view	☑
Take and view alarm	☑

LDAP

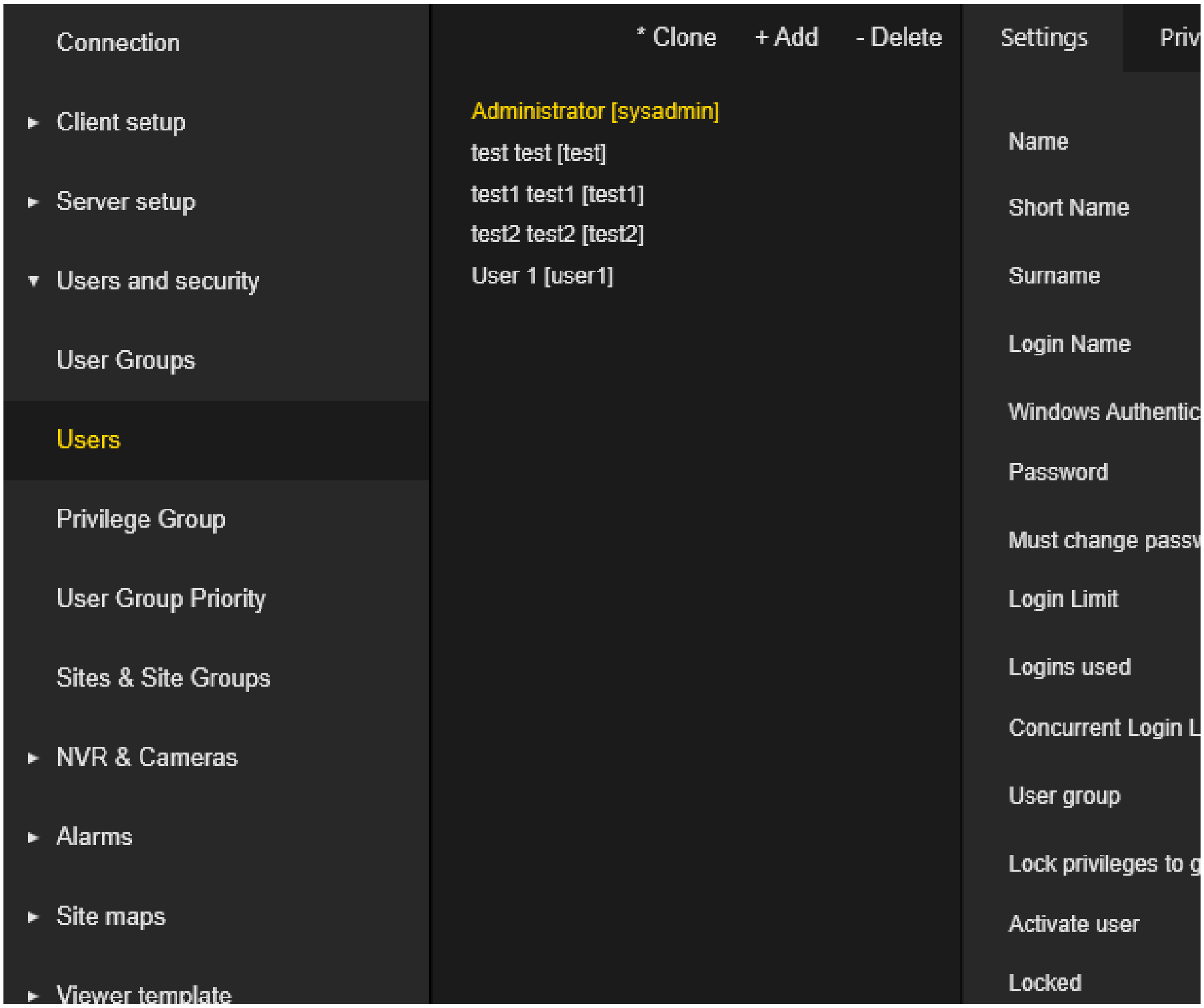
The LDAP tab is visible if the Allow Active Directory User Synchronization license is available and enabled (refer to **Server Licenses**).

If the Active Directory settings are configured correctly (refer to **System Settings**), the administrator can assign one or more Active Directory groups to a specific user group.


Settings
Privileges
LDAP
Filter group by name
Assigned groups
Available groups
Drag and drop Active Directory groups from right to left
<<
>>
Drag and drop Active Directory groups from right to left
Refresh AD Groups

Users

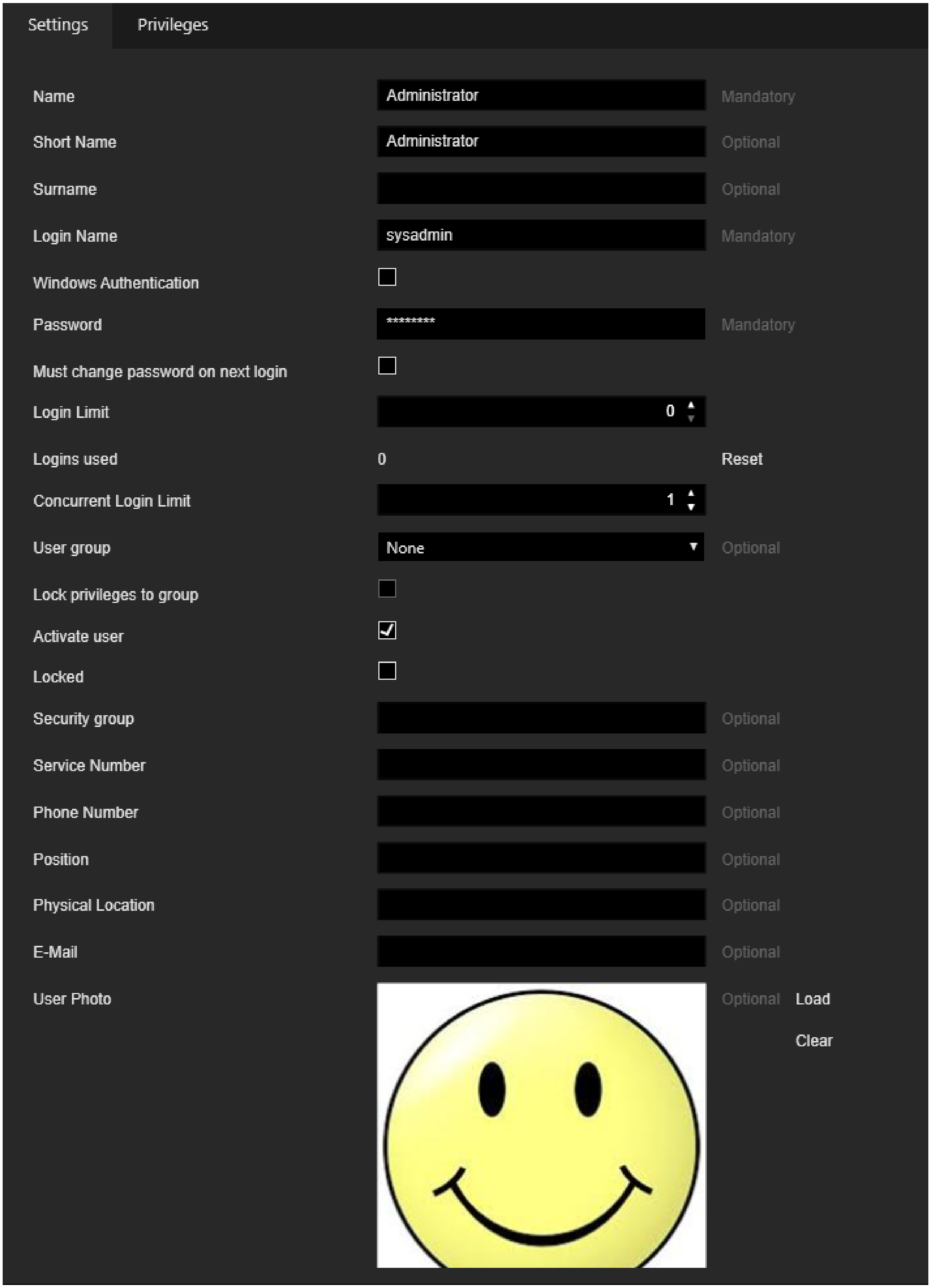
The **Users** view contains a list of G-SIM users.



The settings of the Users are grouped in tabs.

Settings

The administrator can configure the following user settings:



Name	Administrator	Mandatory	
Short Name	Administrator	Optional	
Surname		Optional	
Login Name	sysadmin	Mandatory	
Windows Authentication	□		
Password	********	Mandatory	
Must change password on next login	□		
Login Limit	0		
Logins used	0	Reset	
Concurrent Login Limit	1		
User group	None ▼	Optional	
Lock privileges to group	□		
Activate user	☑		
Locked	□		
Security group		Optional	
Service Number		Optional	
Phone Number		Optional	
Position		Optional	
Physical Location		Optional	
E-Mail		Optional	
User Photo		Optional	Load Clear

Settings	Description
Name / Short Name / Surname	These settings are used to display the user in the list, cards, etc.
Login Name	Used to perform login to the Operator Console / Management Console.
Windows Authentication	Select this checkbox to use Windows Authentication. In this case, the login name should be in the format of domain / username. This setting is enabled only when **Allow Windows Authentication** setting (see **System Settings**) is selected.
Password	The user password. The setting is empty and disabled when **Windows Authentication** is selected. Otherwise, the password is mandatory. The length of the password should not be shorter than the value **Minimum Password Length** (see **System Settings**).
Must change password on next login	Select to obligate the user to change the password the next time the user logs in to the Operator Console.
Login Limit	The Login Limit is the number of login times allowed for users of the Operator Console. If the number of allowed logins is exceeded, the login will fail, and the user will receive a message indicating that the number of allowed logins has been reached. A zero value means an unlimited number of available logins. If the user is assigned to a user group, the login limit will be overridden by the login limit value of the user group.
Logins used	The number of used logins. The administrator can reset the number to 0 by using the **Reset** button.
Concurrent Login Limit	This setting specifies the number of allowed concurrent logins to the operator console for a user. It specifies how many OpCons with the same user can concurrently login to the same G-SIM server. If the allowed number of concurrent logins is exceeded, the login fails and the user receives a corresponding message.

Settings	Description
	The value 0 means an unlimited number of concurrent logins. ⓘ **This setting works only if the license Allow Global Server Connections is available and activated (global environment).** ⓘ **In case of a non-global environment, it is not possible to connect more then one user with the same login name concurrently to the same G-SIM server.** Example The user Test has ”Concurrent Login Limit” = 2. You start the OpCon on computer A and login with user Test. The login will be successful. You start the OpCon on computer B and login with user Test. The login will be successful. You start the OpCon on computer C and login with user Test. The login will not be successful. You will get the message “For current user allow only 2 concurrent login.”
User group	Select a user group to assign the user to it. **None** means that the user is not assigned to any of the user group.
Lock privileges to group	Select this checkbox to use the privileges of the user group as set privileges for the user.

Settings	Description
Activate user	The administrator can activate or deactivate the users. Only active users can log in to the Operator Console or Management Console.
Locked	The administrator can lock or unlock a user. The user is automatically locked if he exceeds the number of **Invalid Login Attempts** (see **System Settings**). Only unlocked users can log in to the Operator Console or Management Console.
Security group / Service Number / Phone Number / Position / Physical Location / E-Mail	These fields are optional and intended for your own organizational use.
User Photo	Click the **Load** button to select the image file to be used as the user photo. The image will automatically be resized to be not larger than 250 px in each dimension, the aspect ratio of the original image will be maintained. Click the **Clear** button to remove the user photo.

Privileges

The Privileges tab is available only if the Lock privileges to group checkbox is unchecked. Otherwise, the privileges of the selected user group are applied to the user.

In this tab, the administrator can configure the privileges of the specific user. The privileges are organized in groups. With the Select all and Clear all buttons, the administrator can select or deselect all privileges with one click. To display a detailed description, he can hold the mouse pointer over the individual privileges.

The administrator can select a user group from Default for User group to reset the privileges of the specific user to those of the selected user group.

The following privileges are available:

Alarms

Name	Description	ID
Handle Alarm	The user may take responsibility for a selected alarm.	41
Forward Alarm	The user may transfer the responsibility of an acknowledged alarm to a specific user.	42
Fast Process Alarms	The user may Fast Process an alarm which means he may acknowledge and complete an alarm in a single click. Default action settings will be used where actions are required.	43
Play Audio for Unhandled Alarms	The system will play audio beeps while there are unhandled alarms.	45
View Alarms	The user may view a list of all alarms.	40
View Alarms of Others	The user may view alarms that are being handled by other users.	44
View All Alarms	The user may see all the alarms on the system.	46
View Alarms Acknowledged but not yet Completed by Others	The user may view alarms that were Acknowledged (but are not yet completed) by other users.	48
Allow Alarm Auto view	The user will receive alarms automatically in the specified screen.	47
Take and view alarm	The user, user group or privilege group may use a combined button for taking and viewing an alarm in one step.	52
Allow the use of alarm report manager	The operator is allowed to use the Alarm report manager.	53

Audit Log

Name	Description	ID
View Own Audit Log	The user may view his own audit log.	80
View Audit Logs of other Users	The user may view the audit logs of all system users.	81
Generate Audit Log Report	The user may print or email an audit log report.	82

Cameras and Video

Name	Description	ID
View Cameras	The user may view a list of all the available cameras.	10
View Live Video	The user may view the live video stream from a selected camera.	11
Playback Control	The user may play back the video footage of a selected camera.	17
View Archived Video Footage	The user may view archived video footage / images.	27
Show Camera On Map	The user may view the position of a selected camera on the map.	12
Block Camera	The user may block a camera so that it cannot be viewed by specific users or user groups.	14
PTZ Control	The user may control Pan, Tilt & Zoom cameras. If this box is not checked, the user will not have any PTZ control functionality and another user will not be able to grant him any such functionality. If this box and the next one is checked, the user will have to ask permission to use PTZ control.	16

Name	Description	ID
	Examples: 1. To give a user full PTZ control to all cameras, check this box and uncheck the next one. 2. To give a user no default PTZ control, but with the option to request control, check this box and check the next one. 3. To give a user control to only some PTZ cameras, with the option to request control of the others, check this box, check the next one, and define PTZ Control Restrictions for specific cameras or groups. 4. To give a user only control to some PTZ cameras, do the same as in (3), but do not check the next box - no additional control may be granted.	
PTZ restricted Cameras may be unlocked	Another user (with the PTZ Unlock privilege) may unlock PTZ cameras with restricted control for this user. If no restrictions were applied to any PTZ camera, checking this box will force this user to ask for permission for any PTZ control.	54
May unlock PTZ control for other users	The user may temporary grant PTZ control to users who normally do not have control BUT who do have the previous privilege.	55
Allow PTZ Presets Recall	The user may recall Pre-set positions for PTZ cameras.	18
Allow PTZ Presets Save	The user may save Pre-set positions for PTZ Cameras.	19
Manage reference frame	The user may modify the reference frame of a camera used for Camera Position Authentication.	20

Name	Description	ID
Export Video to preconfigured locations	The user may export video to one of multiple preconfigured export locations.	24
Export Video to any location	The user may export video to any location.	26
Export Frame to pre-configured locations	The user may export a frame to one of multiple preconfigured export locations.	21
Export Frame to any location	The user may export a frame to any location.	25
The user may create a new export directory	The user may create a new export directory.	29
Override Console Restrictions	The user can override the console restrictions.	22
Video Audio Playback	The user may enable Video Audio Playback.	28
Show AD on Video	The user can see AD rectangles on Video.	250
Show VMD on Video	The user can see VMD rectangles on Video.	251
Show GTECT on Video	The user can see GTECT rectangles on Video.	252
Show Action Text on Video	The user can see Action Text rectangles on Video.	253
Override Motion Privacy and Client Pri-	The user may override the default rendering of Motion Privacy and Client Privacy Zone.	254

Name	Description	ID
vacy		
View the Failover Overview screen	The user may view the Failover Overview screen. This will only makes sense if failover is configured for this setup.	255
May disable privacy protection for another user	This privilege allows the user to export a video with removable privacy masking. If the user does not have this privilege, he can only export videos with irremovable privacy masking. In this case, the option is hidden in the export menu.	256
Camera check allowed	The user is allowed to use the camera check service.	257
Process SetClientVCA action	Privilege to process SetClientVCA Action.	258
Enable bookmark functionality	Enable bookmark functionality to set bookmarks for video.	259
Allow Face Recognition Enrollment	Allow Face Recognition Enrollment.	260
Process Viewer Actions	Enables the OpCon to process the Viewer Actions send from an external device to open cameras or scenes, change playmodes and clear viewer from remote even if the operator does not have the privilege to view cameras.	261
Show the "Viewed by" table	The user is allowed to see the "Viewed by" table to see which other operators are viewing the camera.	262
Show the template selector	User can access the template selector and change templates.	263
Override console location	This privilege enables the user-/group/privilege group/console to override	270

Name	Description	ID
configuration	the location setup made on sites (Local/Remote connection setup).	
Allow High Resolution Channel Export	The user can export high resolution video on remote locations where only low resolution footage can be viewed.	271
Allow Forensic Search	The operator is allowed to start a forensic search for the specific camera. Please note that the forensic search is an external application. The forensic search is only start when the console has a valid console global number.	272

Cut Lists

Name	Description	ID
Create Cut Lists	The user may create and edit his own Cut Lists.	90
Export Cut Lists	The user may export his own Cut Lists.	91
Delete Cut Lists of other users	The user may delete the Cut Lists created by other users.	92

Default Privileges

Name	Description	ID
Override Default Privileges	The user's privileges will be used if this option is selected. If this option is NOT selected and the console has NO privileges set, then the user's privileges will be used. If this option is NOT selected and the console has	23

Name	Description	ID
	privileges set, then only the privileges where both the console and user privileges are selected, will be used.	

General / Control

Name	Description	ID
Allow the use of Custom Buttons	The user may view and use Custom Events / Camera controls.	300
Allow change password	The user may change password.	301
Show the Customize menu	Shows or Hides the customize menu for the operator.	264
May connect to Global Servers	The user is allowed to connect to Global Servers and view cameras etc. from these remote servers.	701
Show Global Servers status page	Enables Status page to be seen in OpCon.	702

Guard Tours

Name	Description	ID
View Public Guard Tours	The user may view public guard tours.	70
Edit Public Guard Tours	The user may create, edit and delete public guard tours.	71
Edit/View Private Guard Tours	The user may create, edit, delete and view his own guard tours.	72

Investigation

Name	Description	ID
Generate Process Data Report	The user may print or email a Process Data search results report.	103
Motion Search (MOS)	The user may perform a Motion Search.	101
Process Data	Process Data.	102
Video Footage restricted to Process Data	If this privilege is enabled: • Only videos from Process Data search results can be dropped into the viewers. • Video footage is limited to the event time range of the Process Data. • Live Video mode is disabled. • All other Video modes works inside Process Data event time range. • Drag and Drop of cameras, cut list, alarms, guard tours into the viewers is disabled. • Alarms, populated and linked layouts are displayed without cameras. ⓘ **In addition to the new privilege the user/user group also needs the privileges View Cameras and Playback Control for full functionality.** ⓘ **In order for restricted users to view the process data, you must enable this option for the user as well as the Override Default Privileges option for the console.** ⓘ **As this privilege does not work if the**	104

Name	Description	ID
	ℹ **View further than Event Runtime for Process Data privilege is enabled as well, there is a function which prevents both privileges from being activated at the same time.**	
View further than Event Runtime for Process Data	If this privilege is enabled the process data of the video material is displayed in the viewer. When the event is over, the video material continues to run after the event. ℹ **As this privilege does not work if the Video Footage restricted to Process Data privilege is enabled as well, there is a function which prevents both privileges from being activated at the same time.** ℹ **With this privilege the freeflow mode is activated which only works with process data and not with items from the cutlist.**	105

Management Console

Name	Description	ID
Administrator	The user may run the Management console in order to administer the system.	200
Connection Manager Settings Access	The user may change the Connection Manager configuration. ⚠ **IMPORTANT:** Changing these parameters could result in a system malfunction.	201

Name	Description	ID
Users and Security Settings Access	The user may add and remove users and change user permissions.	202
Sites and Maps Access	The user may change Site settings as well as add and setup maps.	203
Mediasources and Cameras Access	The user may change the Mediasource settings and configure cameras.	204
Health and Alarms Access	The user may change how system health is monitored and also configure alarms.	205
Viewer Templates Access	The user may change which viewer templates are available for the Operator user interface.	206
Tools Access	The user has access to system tools. ⚠ **IMPORTANT:** Invalid test data could be distributed.	207
Alarm Simulator	The user may simulate alarms.	208
Add/Manage Plugins	The user may change health monitor plugins.	209
Manage Alarm Actions	The user may change alarm handling actions.	210
Client Data Settings Access	The user may change client settings.	211
Restrictions and Allowances Access	The user may change client restrictions and allowances.	213
Limited Administrator	The following behaviour is expected if this privilege only is set: • Every other administrator privilige	214

Name	Description	ID
	should be unchecked to ensure a senseful privilege structure. • The limited administrator can add & edit users without administrator or limited administrator rights. • The limited administrator can add & edit users groups without administrator or limited administrator rights. • The limited administrator can add & edit privilige groups without administrator or limited administrator rights. • The limited administrator can add & edit priviliges of users without administrator or limited administrator rights. • Edit in this case includes the adaption of passwords. Limitations of this privilege: • The limited administrator can NOT add & edit users with administrator or limited administrator rights. • The limited administrator can NOT add administrator or limited administrator rights to users. • The limited administrator can NOT edit the privileges of users with administrator or limited administrator rights. • The limited administrator can NOT add administrator or limited administrator rights to privilige groups. • The limited administrator can NOT add administrator or limited administrator rights to user groups. • The limited administrator can NOT delete users, user groups or privilige groups.	

Messages

Name	Description	ID
View Messages	The user may view received messages.	50
Send Message	The user may reply to messages and send new messages.	51

Sites

Name	Description	ID
View Sites	The user may view a list of all Sites.	30
Allow Sending Actions from Maps	The user may send custom defined Actions from Maps by clicking on interaction objects.	33
View Interaction Objects on the Map	The user may see any Interaction Objects on Maps.	34
View Site Map	The user may view the map(s) of a selected Site.	31
Show Site Critical Flag	The user will see when a Site is in critical state (i.e. when the HealthAgentCheckinCriticalFlagPeriod has been exceeded).	32

Tasks

Name	Description	ID
Show Task Tab	The user have access to Tasks through a Task Tab.	60

Name	Description	ID
Create Tasks	The user may create new default tasks. Any task created indirectly (camera related etc.) or transferred, can still be handled without this permission.	61
View Tasks of all Users	The user may view the tasks assigned by and to all users.	63
Transfer Camera	The user may transfer a camera to another user.	13

Users

Name	Description	ID
Show User Tab	The user have access to Users through a User Tab.	67

Video Wall & Remote Control

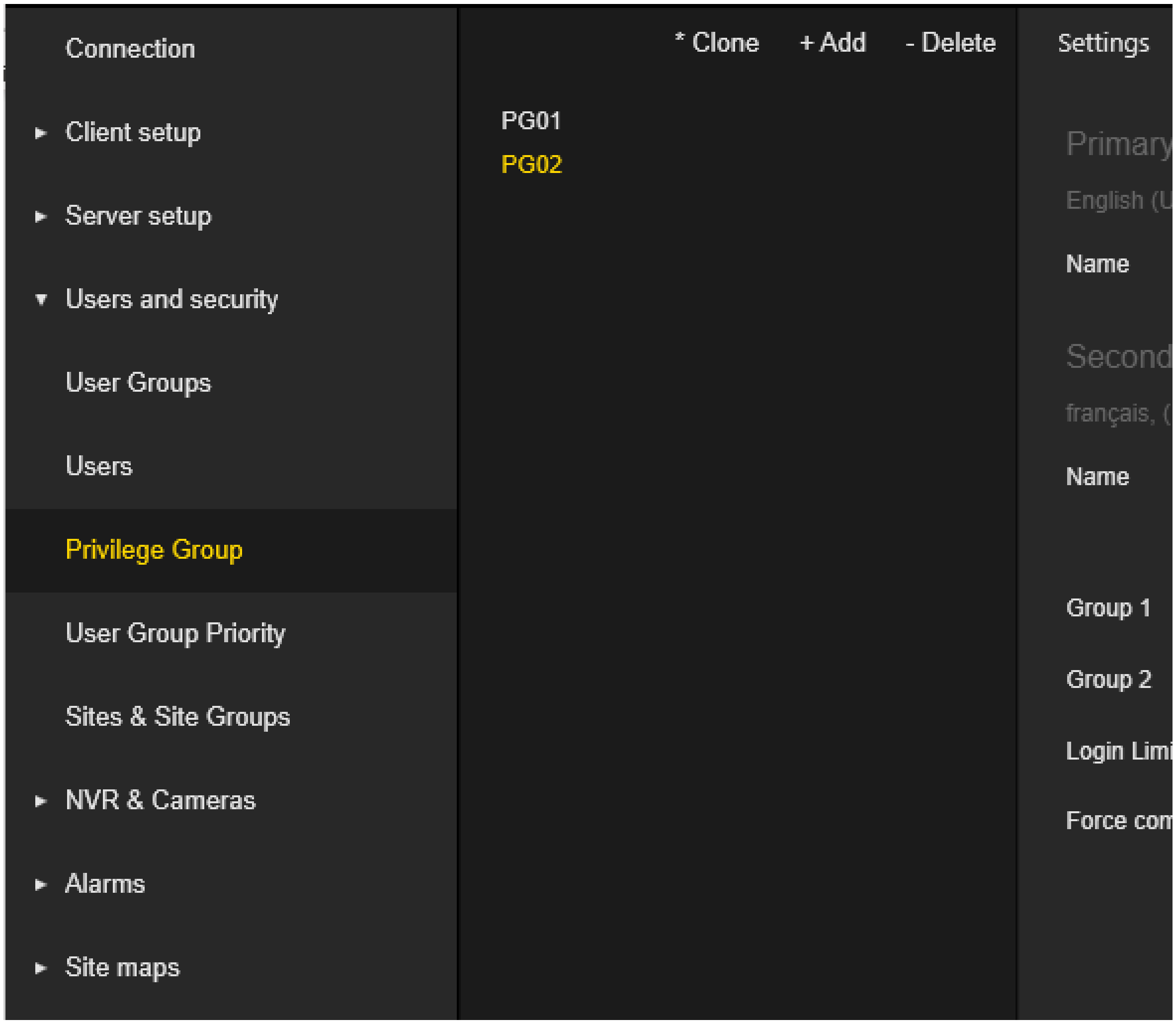
Name	Description	ID
Set Video Wall Layout	The user may set and change the layout of video wall consoles.	110
Clear Video Wall	The user may clear all the viewers on a video wall screen.	111
Set Video Wall Content	The user may send content to Video Wall viewers.	112
Set Viewer content on remote Operator Consoles.	The user may send content to viewers on remote Operator Consoles, including manned consoles with remoting enabled.	115
Can restart Remote Operator Console	The user can restart Remote Operator Console.	116

Web Browser

Name	Description	ID
Show Browser Tab	The user have access to Bookmarks through a Browser Tab.	120

Privilege Group

The **Privilege Group** view contains a list of privilege groups. Privilege groups are used in the login procedure for the second user of the Operator Console (two-man rule).



The settings of the **Privilege Group** are grouped in tabs.

Settings

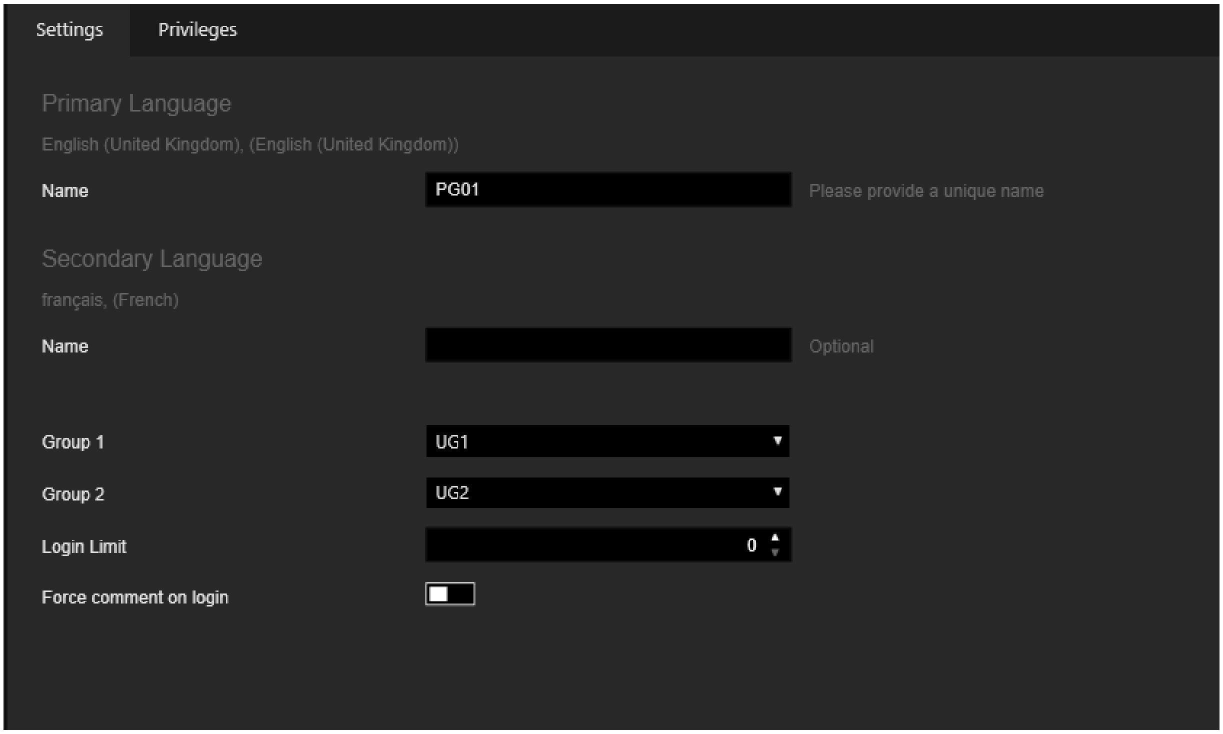
The administrator can configure the names of the privilege group for both the primary and secondary languages.

The administrator should set Group 1 and Group 2 by selecting existing user groups. The settings for Group 1 and Group 2 are used to determine the privilege group in case of login as a secondary user.

The administrator can configure the Login Limit for the specific privilege group. The login limit is the number of login times allowed on the Operator Console. If the number of allowed logins is exceeded, the login will fail, and the user will receive a message indicating that the number of allowed logins has been reached.

A zero value means an unlimited number of available logins.

The administrator can select Force comment on login to obligate user to enter the login reason for the second user.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name PG01 Please provide a unique name

Secondary Language

français, (French)

Name Optional

Group 1 UG1 ▾

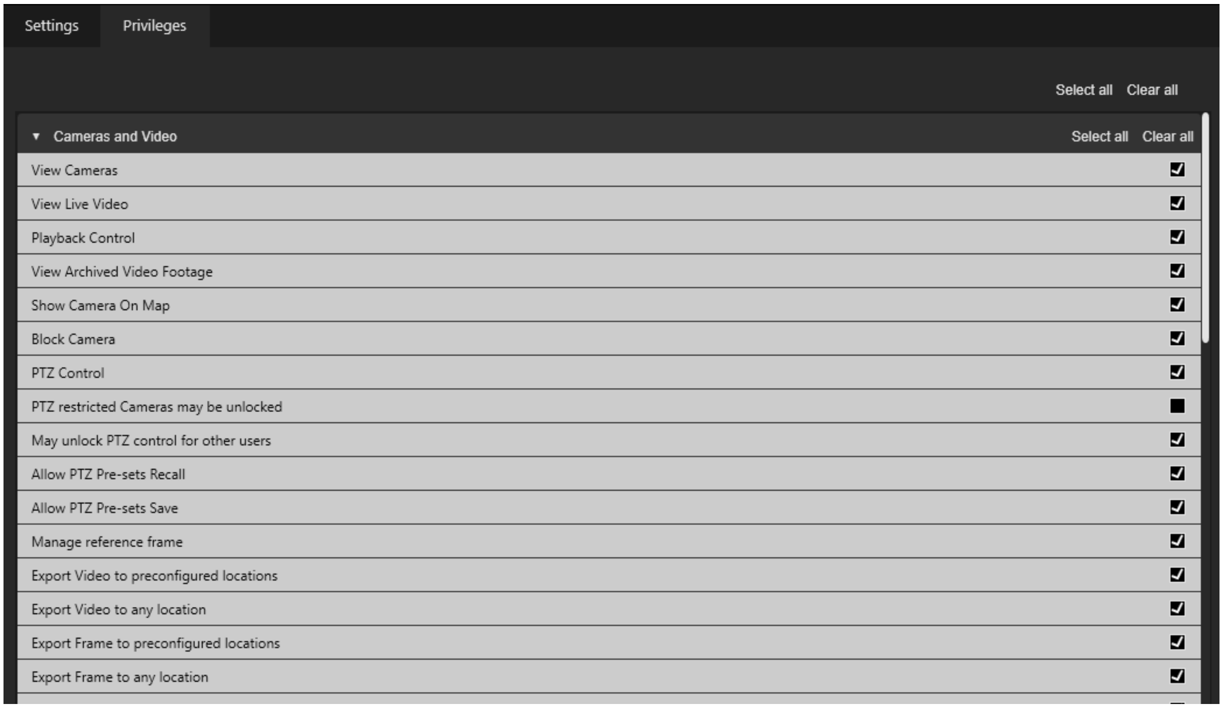
Group 2 UG2 ▾

Login Limit 0

Force comment on login ☐

Privileges

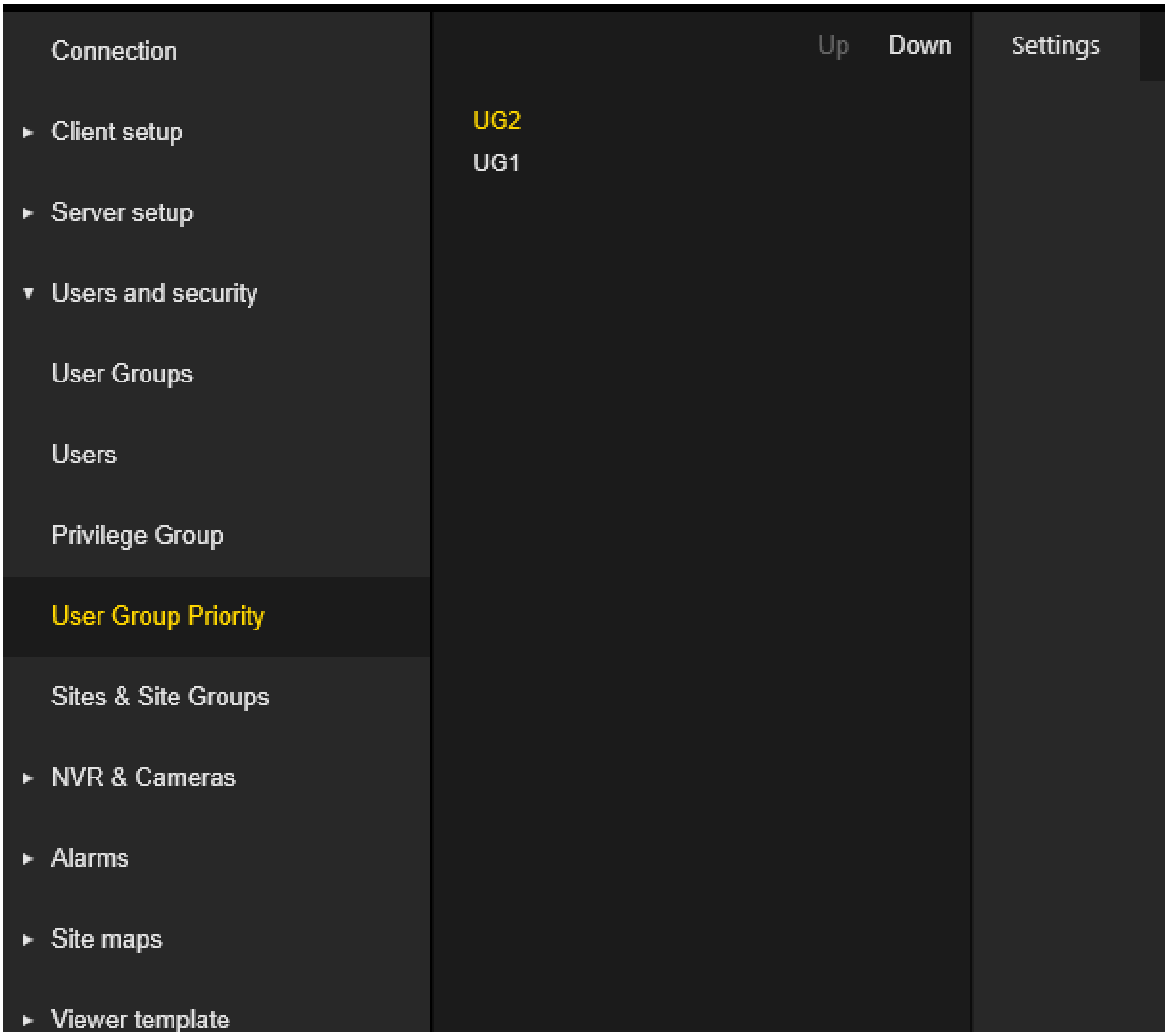
The administrator can configure the privileges of the specific privilege group. The privileges are organized in groups. The administrator can use Select all and Clear all buttons to set or revoke all privileges in the group with one click. The administrator can hold the mouse cursor over the privilege to see a detailed description.



View Cameras	☑
View Live Video	☑
Playback Control	☑
View Archived Video Footage	☑
Show Camera On Map	☑
Block Camera	☑
PTZ Control	☑
PTZ restricted Cameras may be unlocked	■
May unlock PTZ control for other users	☑
Allow PTZ Pre-sets Recall	☑
Allow PTZ Pre-sets Save	☑
Manage reference frame	☑
Export Video to preconfigured locations	☑
Export Video to any location	☑
Export Frame to preconfigured locations	☑
Export Frame to any location	☑

User Group Priority

User Group Priority contains an order list of the existing user groups. User Group Priority is used in the Operator Console to determine who has priority when controlling a PTZ camera. The administrator can change the user group priority by using Drag & Drop or the Up and Down buttons.

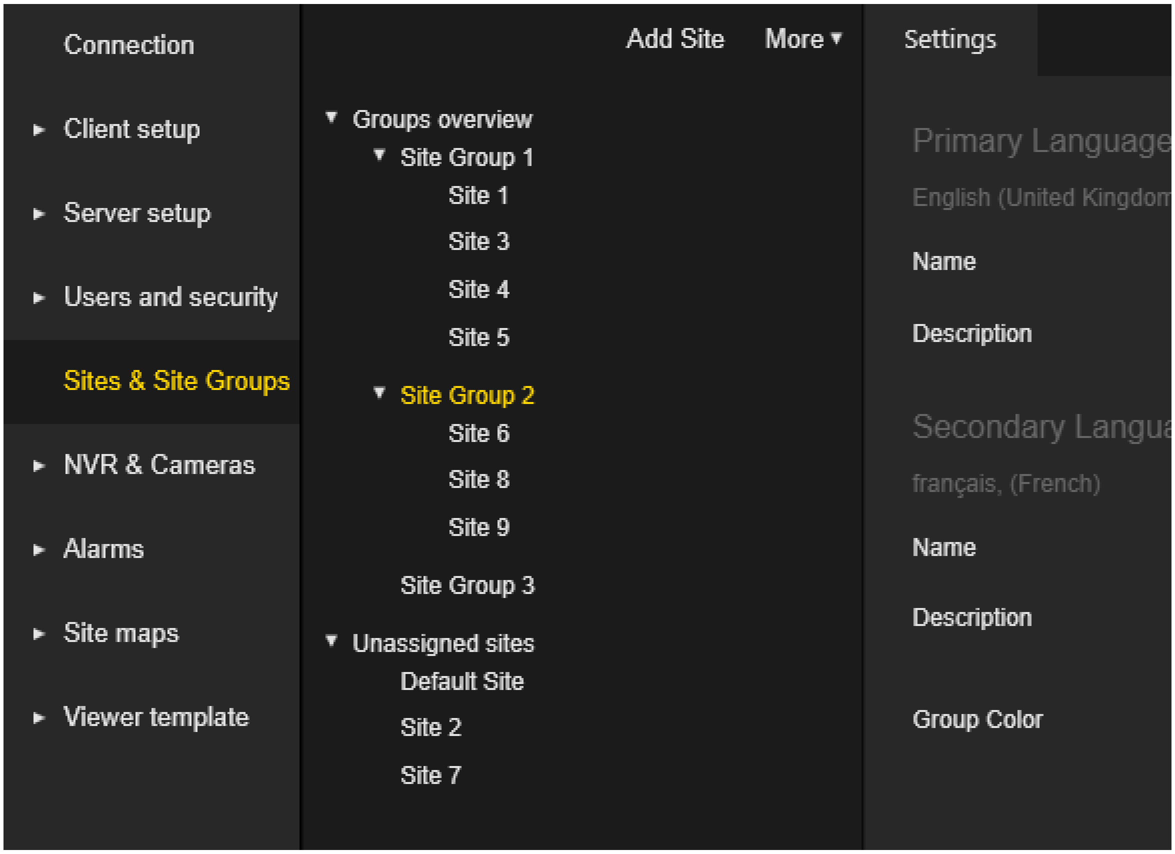


Sites & Site Groups

G-SIM uses the concept of sites to organize NVRs and their respective cameras into logical groups. A site is helpful for grouping related NVRs and for monitoring their collective health as a unit. See **Health Agents** for more details.

In turn, a site can belong to a site group to help manage large video network enterprises. You are free to adapt the definitions of sites and site groups to fit the requirements of your installation.

The Sites & Site Groups view contains a tree view of the site groups with their sites. Sites can be moved between site groups by using Drag & Drop.



Primary Language

English (United Kingdom

Name

Description

Secondary Langua

français, (French)

Name

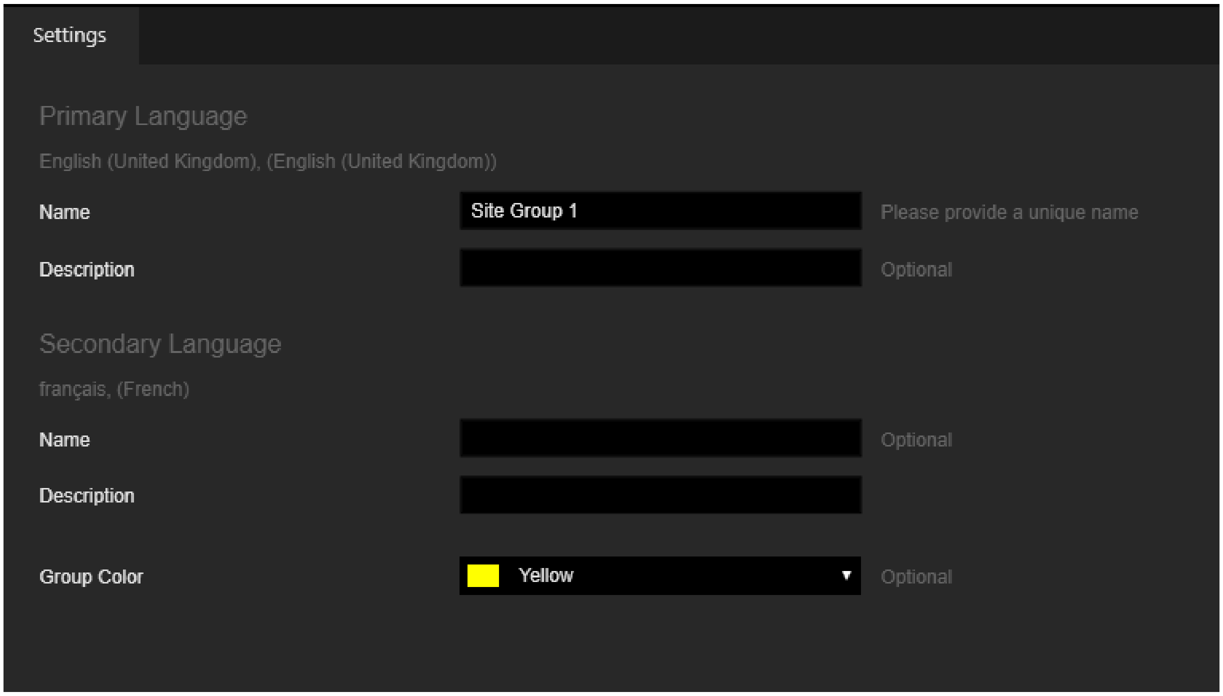
Description

Group Color

Site Group Settings

The administrator can configure the names and descriptions of the site group for both primary and secondary languages.

The administrator can configure the color of the site group. Sites that belong to this site group will be displayed in the Operator Console with the color specified here.



Settings

Primary Language

English (United Kingdom), (English (United Kingdom))

Name	Site Group 1	Please provide a unique name
Description		Optional

Secondary Language

français, (French)

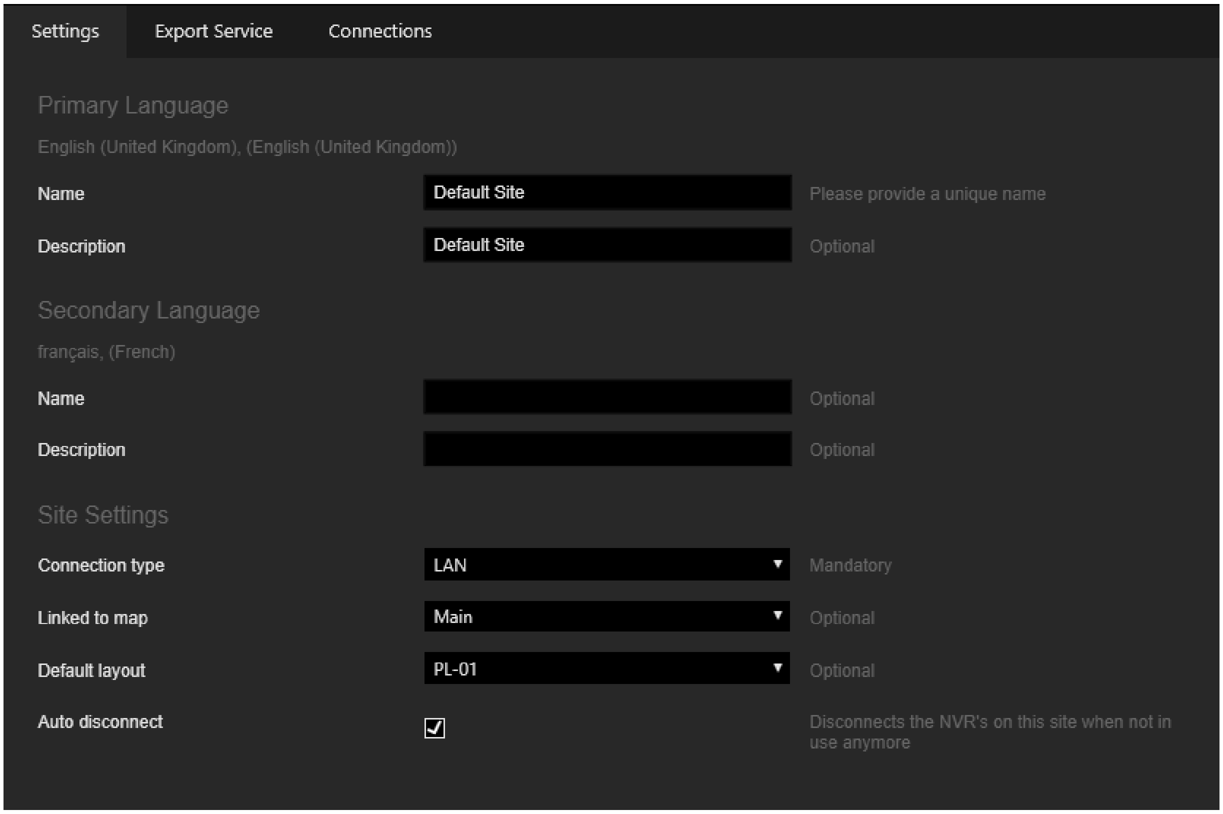
Name		Optional
Description		
Group Color	🟨 Yellow ▼	Optional

Site Settings

The settings of the Site are grouped in tabs.

Settings

The administrator can configure the following settings:



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Default Site — Please provide a unique name

Description: Default Site — Optional

Secondary Language

français, (French)

Name: — Optional

Description: — Optional

Site Settings

Connection type: LAN — Mandatory

Linked to map: Main — Optional

Default layout: PL-01 — Optional

Auto disconnect: ☑ — Disconnects the NVR's on this site when not in use anymore

Settings	Description
Name	Name of the site for both primary and secondary languages.
Description	Description of the site for both primary and secondary languages.
Connection type	For installations that have different connection speeds to different sites, it may be important to specify the connection type as, for example accessing video could have a significant cost implication.
Linked to map	Select the default map to be displayed in the Operator Console when using this site.
Default layout	Select a populated or linked layout to be displayed in the Operator Console when the **View Cameras** button is clicked.
Auto disconnect	Select this checkbox to close the connection to the NVR when the last camera connection has been closed. The connection will be closed after the Unused NVR Disconnect Timeout

Settings	Description
	Seconds (see **System Settings**) (value 0 means the NVRs will not be disconnect).

Export Service

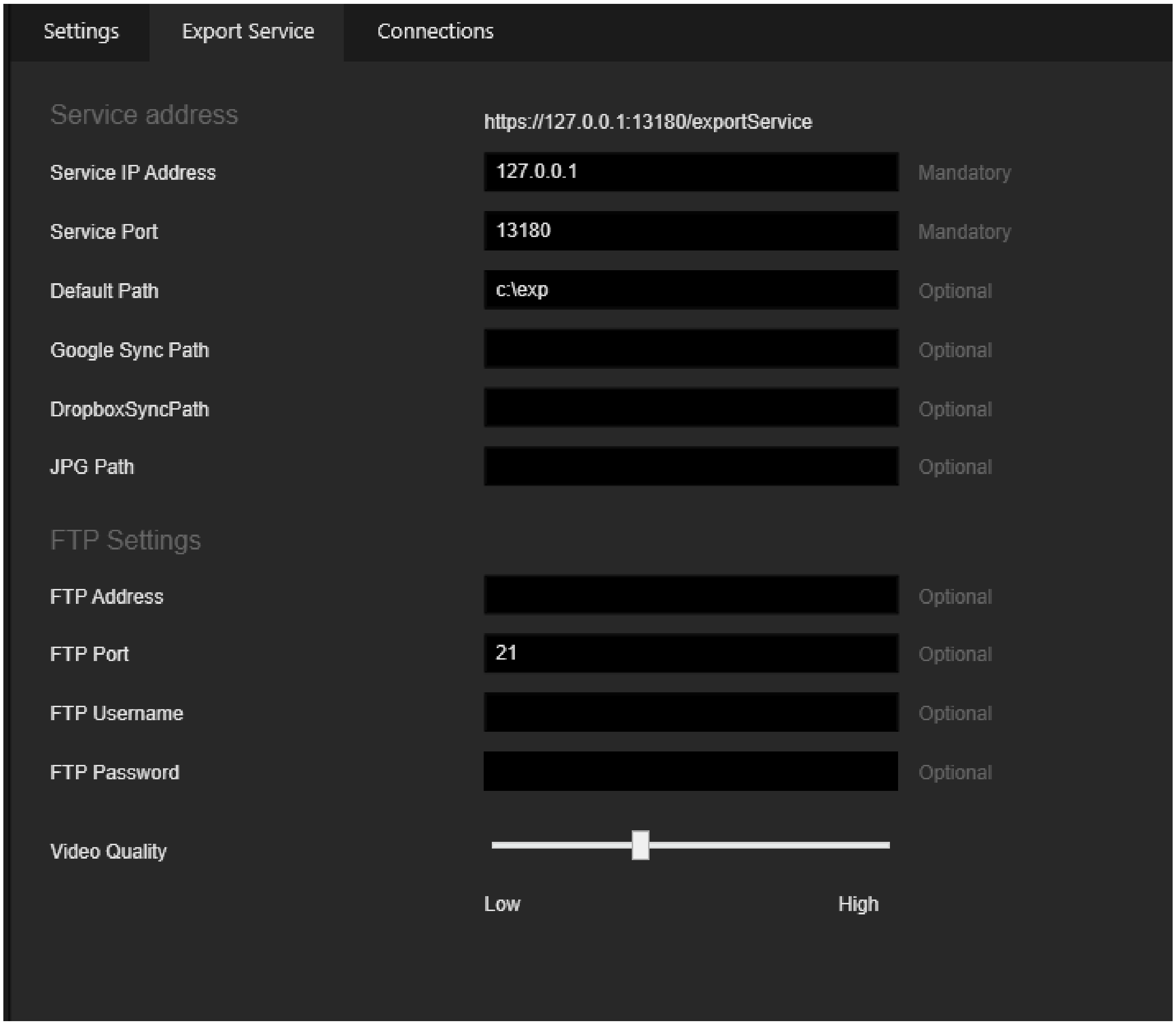
The **Export Service** tab is visible when a "Pro version" license is available (refer to **Server Licenses**).

The administrator can configure the export service address, video quality, and network folders to be used for export.

Using the export service, video data (GBF or MPEG) as well as single frames can be saved to a preconfigured location on the network as part of a quick export, single frame transport or cut list export.

The directory for synchronization with Google Drive and Dropbox can be configured (the synchronization of the created directories must be configured with Google Drive or Dropbox. The export service only saves the data for synchronization, it does not perform the actual synchronization with Google Drive or Dropbox).

The administrator can configure FTP server settings that will be used by the export service.



Service address https://127.0.0.1:13180/exportService

Service IP Address	127.0.0.1	Mandatory
Service Port	13180	Mandatory
Default Path	c:\exp	Optional
Google Sync Path		Optional
DropboxSyncPath		Optional
JPG Path		Optional

FTP Settings

FTP Address		Optional
FTP Port	21	Optional
FTP Username		Optional
FTP Password		Optional

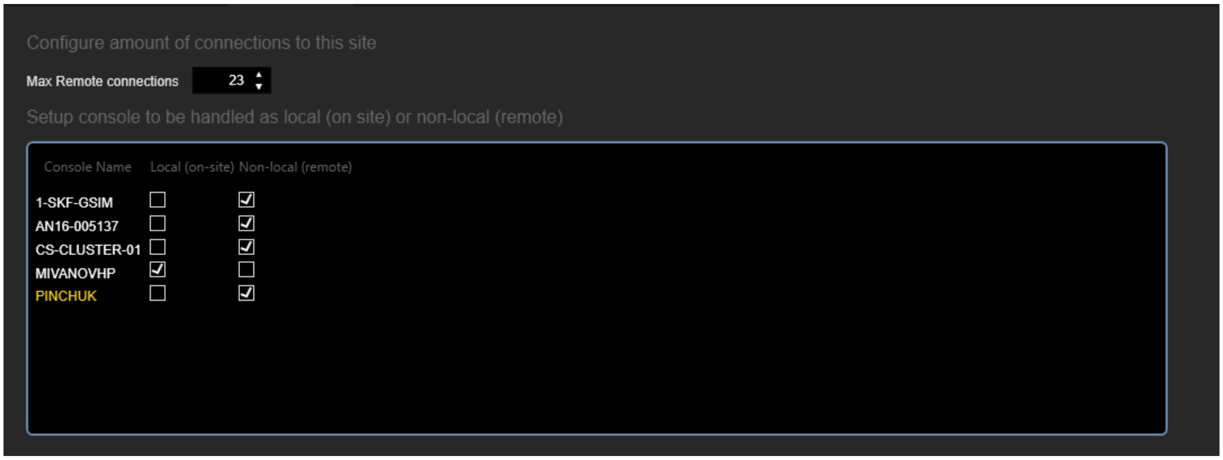
Video Quality

Connections

The administrator can configure the **Max Remote connections** setting.

Related to the **Connection type** setting, the communication technology used to connect to certain sites may impose a limit on the number of connections to the site at any given time. This parameter allows you to enforce such limits as Default Maximum Connections Over DSL, Default Maximum Connections Over ISDN Or Analog, Default Maximum Connections To LAN settings for default values (see **System Settings**).

The administrator can configure which Operator Console should be treated as remote.



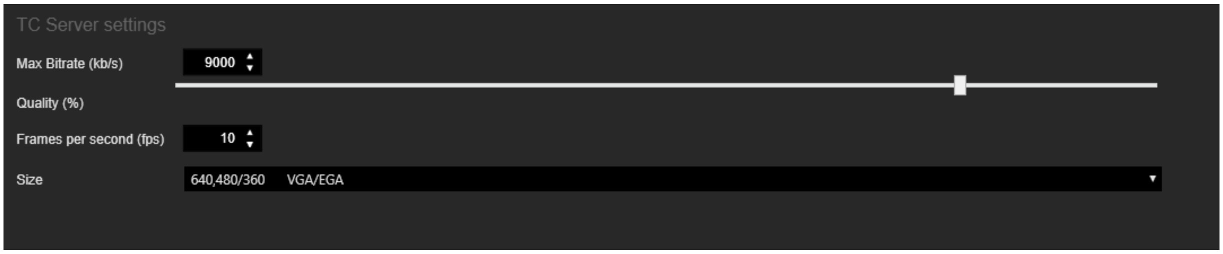
Configure amount of connections to this site

Max Remote connections 23

Setup console to be handled as local (on site) or non-local (remote)

Console Name	Local (on-site)	Non-local (remote)
1-SKF-GSIM	☐	☑
AN16-005137	☐	☑
CS-CLUSTER-01	☐	☑
MIVANOVHP	☑	☐
PINCHUK	☐	☑

The administrator can configure settings for the Transcoding Viewer. These settings are visible if the **Allow Transcoding Viewers** license is available and enabled (refer to **Server Licenses**).



TC Server settings

Max Bitrate (kb/s) 9000

Quality (%)

Frames per second (fps) 10

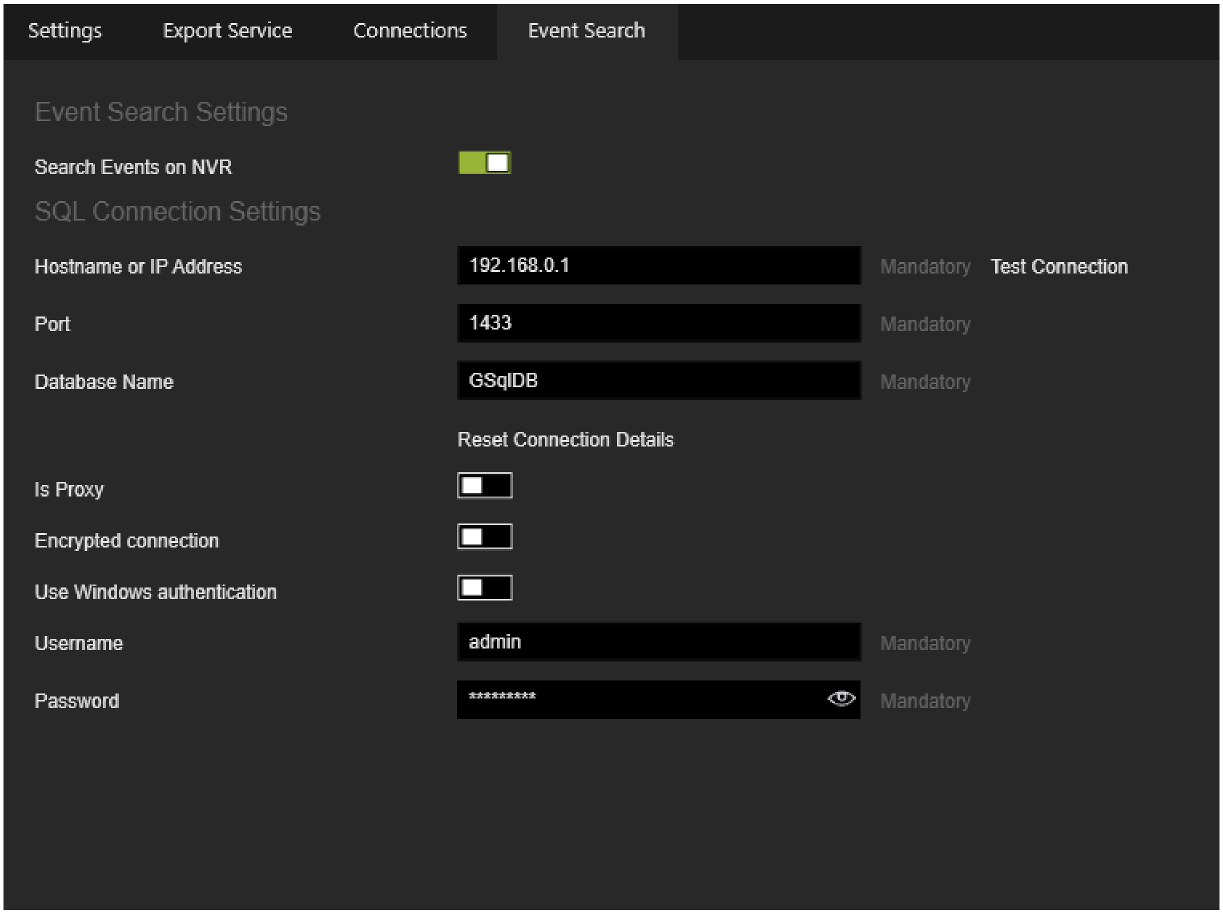
Size 640,480/360 VGA/EGA

Event Search

In the **Site** view, there is an **Event Search** tab to set up the newly added event data search options.

If you want to search G-SIM search event data directly in the G-Core event database instead of the standard G-SIM event database, you must specify the connection settings to this device here. The settings apply to all media sources assigned to this site. G-SIM cannot distinguish between these assigned media sources, so it is highly recommended that only **one** mediasource be assigned to **one** site to avoid unwanted behavior during OSD display and process data search.

The administrator can configure the following settings that relate to the event search:



Event Search Settings

Search Events on NVR

SQL Connection Settings

Hostname or IP Address: 192.168.0.1 Mandatory Test Connection

Port: 1433 Mandatory

Database Name: GSqlDB Mandatory

Reset Connection Details

Is Proxy

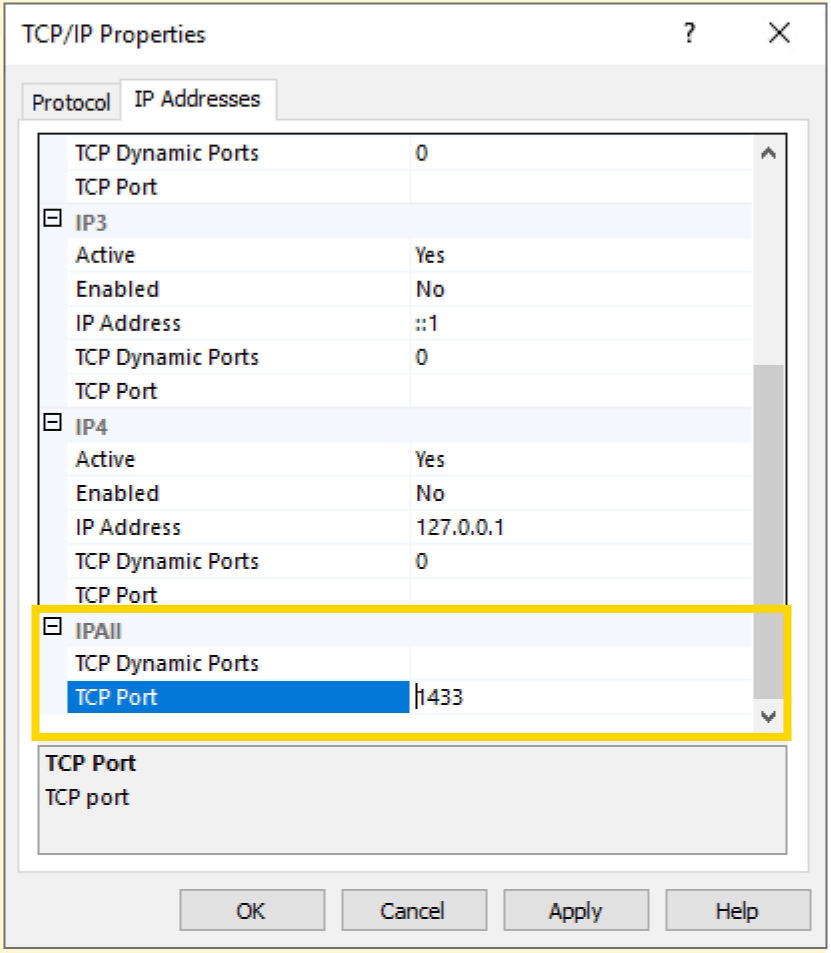
Encrypted connection

Use Windows authentication

Username: admin Mandatory

Password: ********* Mandatory

Settings	Description
Search Events on NVR	If active, all event data related to the selected mediasource will be searched using the provided MSSQL database connection (new mode). When inactive, all event data related to the selected site's mediasource will be searched in the standard G-SIM MSSQL event database (standard mode).
Hostname or IP	Hostname or IP of the MSSQL database. Default value is the Hostname / IP.
Test Connection	When clicked, the Management Console will attempt to connect to the given MSSQL database and perform a simple query on it (“SELECT 1”) to verify that the entered connection settings are correct. The result of the test connection will be displayed in a toast notification to provide basic feedback on the success or failure of the connection attempt. For more

Settings	Description
	detailed error messages, check the trace output of the G-SIM server service.
Port	The access port of the MSSQL database. **The SQL instance uses a dynamic port by default. To use the event search function, you must change the port in the SQL Server Configuration Manager and set it to port 1433.**  TCP/IP Properties ? ✕ Protocol IP Addresses OK Cancel Apply Help TCP Dynamic Ports 0 TCP Port ⊟ IP3 Active Yes Enabled No IP Address ::1 TCP Dynamic Ports 0 TCP Port ⊟ IP4 Active Yes Enabled No IP Address 127.0.0.1 TCP Dynamic Ports 0 TCP Port ⊟ IPAll TCP Dynamic Ports TCP Port 1433 **TCP Port** TCP port
Database Name	The name of the MSSQL database. Default value is the standard name of the G-Core event database **GSqlDB**.
Reset Connection Details	This button resets the **Hostname or IP**, **Port**, **Database Name** and **Encrypt Connection** fields to their default values. All pre-

Settings	Description
	viously entered data will be overwritten.
Is Proxy	This must be selected if the G-Core mediasource is used as a proxy for other G-Core mediasources (see also: Remote server settings in G-Set). If you have a replication server set up in G-Core and want to receive live events, make sure that the **Event Forwarding** setting in G-Set is active.
Encrypted connection	If active, the communication between G-SIM and the event database will be encrypted. You must have valid certificates installed to encrypt the communication between G-SIM and MSSQL. The default setting is inactive.
Use Windows authentication	If active, G-SIM will authenticate at the database with Integrated Security (Windows authentication). The **Username** and **Password** textboxes are then disabled. If inactive, the user must specify the local MSSQL user with access rights to the event database.
Username	The local MSSQL username with access rights to the event database data (read access). The user must be available in the MSSQL server.
Password	The password for authenticating the local user to the MSSQL server.

NVR & Cameras

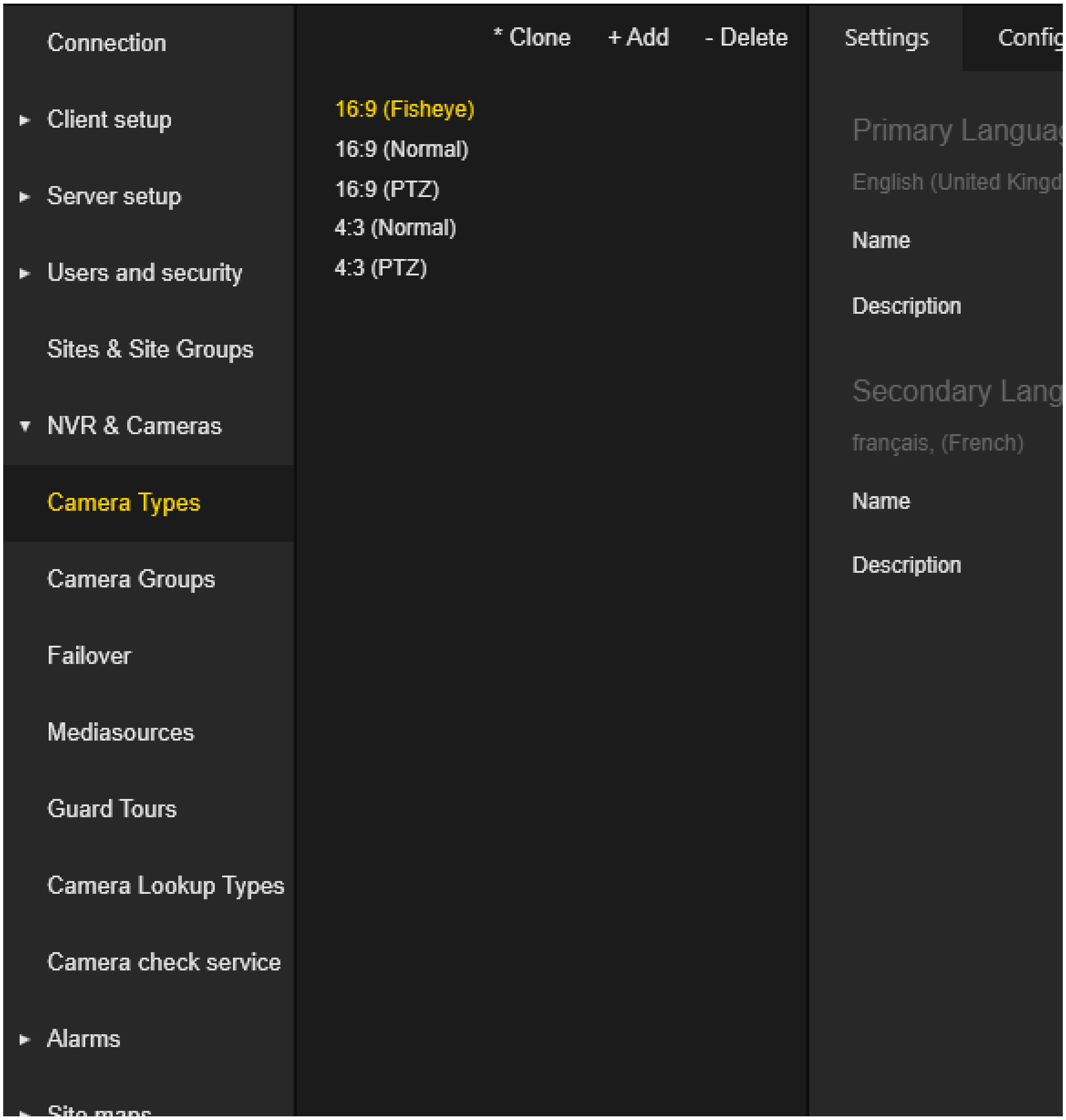
A digital video recorder (DVR) is a device that records video in a digital format to a disc drive or other memory medium in a device. The Geutebrück NVRs are the backbone of the G-SIM system, which derives much of its power from their capabilities.

All different types of video cameras are simply referred to as cameras and are connected to an NVR. Usually a camera is connected to a single NVR, but this is not necessary for fail-over installations. From the user's perspective, however, a camera provides a good enough entry point into a video network, where the video data is stored (NVR or other storage system) is irrelevant to use of G-SIM. For this reason, G-SIM is designed to be NVR-insensitive from the user's perspective. The Operator Console does not even refer to a NVR in any way. However, from a management perspective, configuring NVRs is critical, which is explained in this chapter, but first a very important note.

IMPORTANT: It is absolutely critical that all components of a G-SIM installation are properly time synchronized. If this is not the case, you will have many and varied issues.

Camera Types

The **Camera Types** view contains a list of camera types. The default set of camera types is created when G-SIM server is installed.



16:9 (Fisheye)
16:9 (Normal)
16:9 (PTZ)
4:3 (Normal)
4:3 (PTZ)

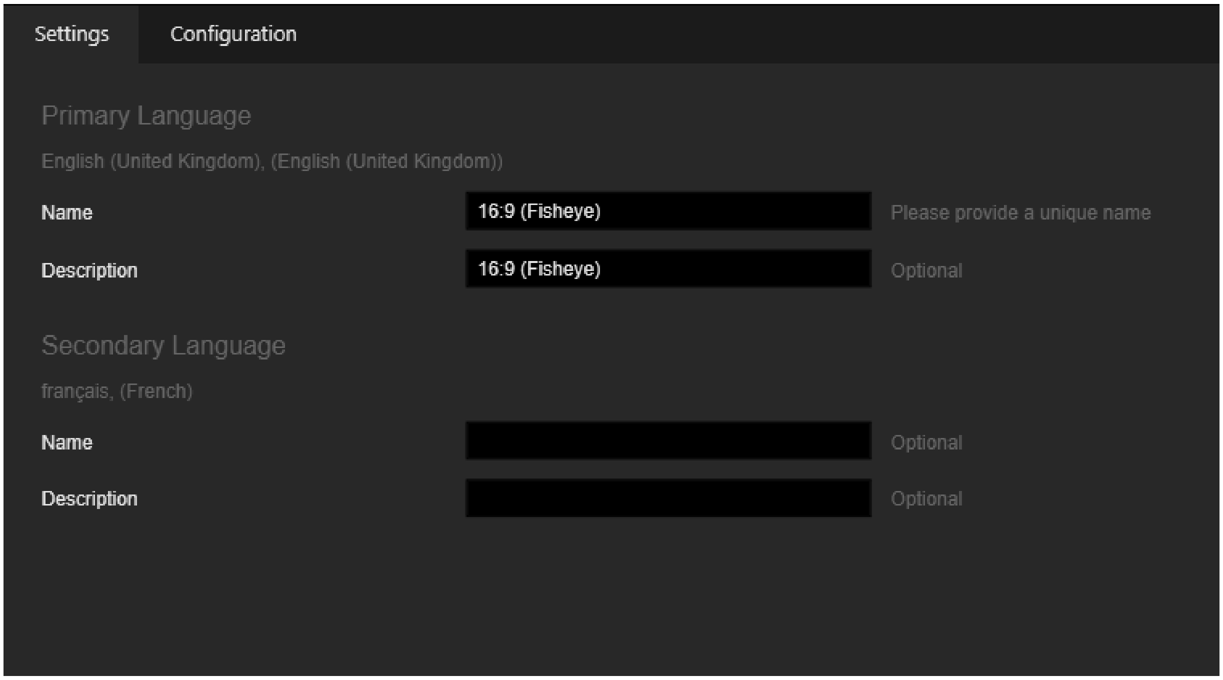
Primary Languag
English (United Kingd
Name
Description

Secondary Lang
français, (French)
Name
Description

The **Camera Type** settings are grouped in tabs.

Settings

The administrator can configure the name and description of the camera type for both the primary and secondary languages.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: 16:9 (Fisheye) — Please provide a unique name

Description: 16:9 (Fisheye) — Optional

Secondary Language

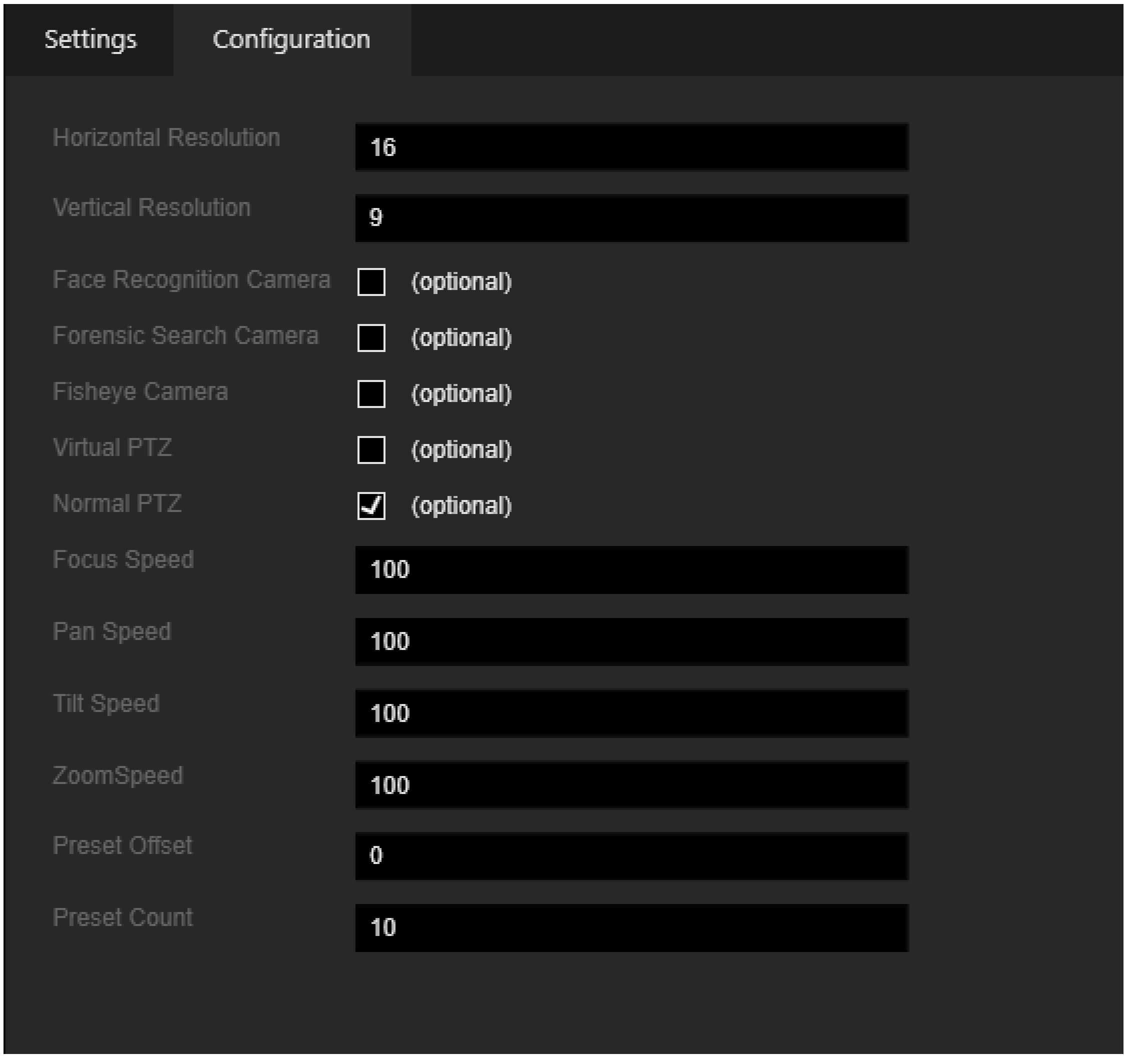
français, (French)

Name: — Optional

Description: — Optional

Configuration

The administrator can configure the following camera type settings:



Horizontal Resolution 16

Vertical Resolution 9

Face Recognition Camera □ (optional)

Forensic Search Camera □ (optional)

Fisheye Camera □ (optional)

Virtual PTZ □ (optional)

Normal PTZ ☑ (optional)

Focus Speed 100

Pan Speed 100

Tilt Speed 100

ZoomSpeed 100

Preset Offset 0

Preset Count 10

Settings	Description
Horizontal Resolution / Vertical Resolution	Horizontal and Vertical Resolution of the Camera Type.
Face Recognition Camera	Select this checkbox to display the corresponding button in the Viewer of the Operator Console. The **Face Recognition Camera** function is used for the integration of face recognition in G-SIM, in particular for enabling the **enrollment** function. If the user sees a face in the viewer that he wants to register for face recognition, he can trigger this from

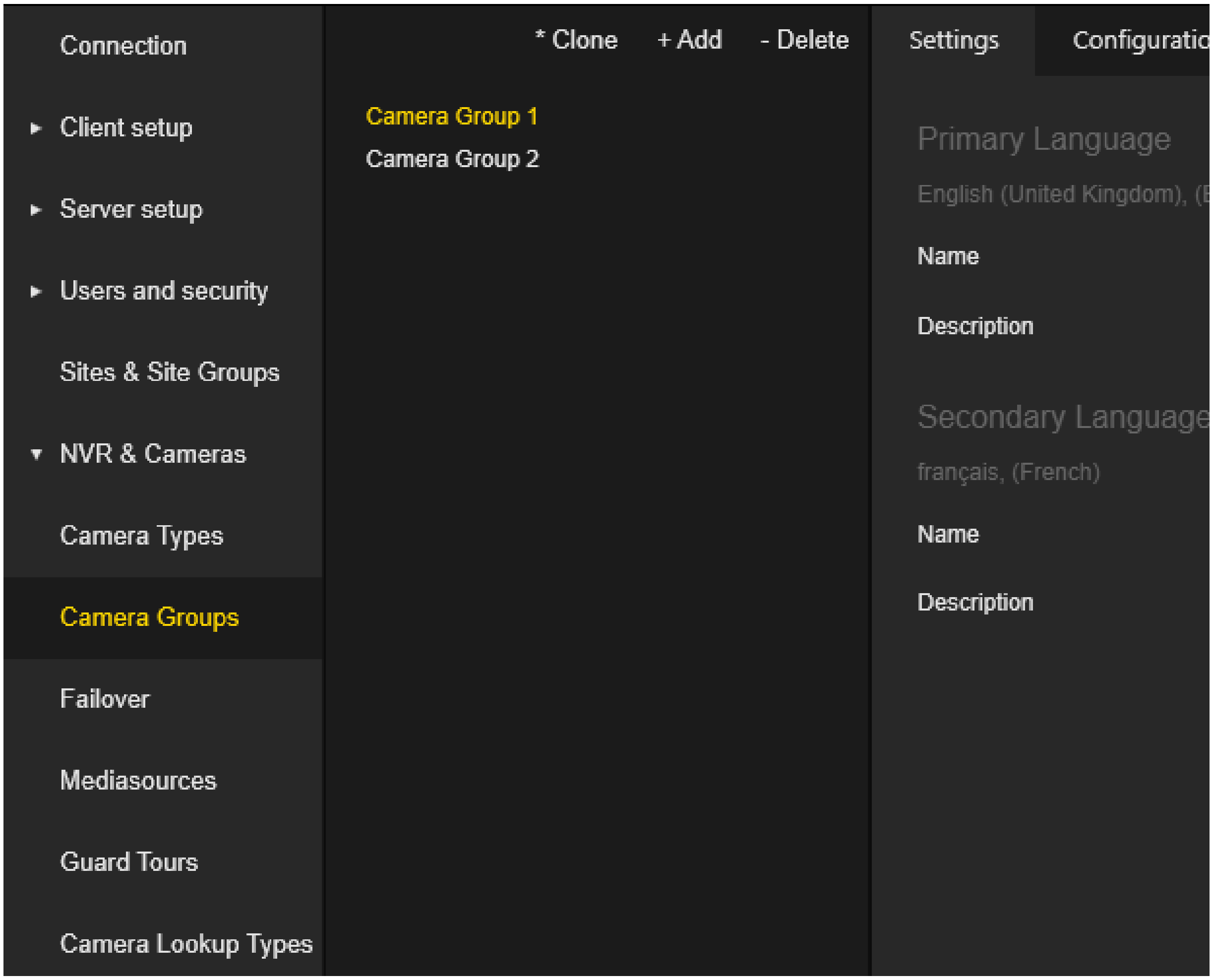
Settings	Description
	G-SIM with this button, because this button sends the image from the camera to the face recognition process.
Forensic Search Camera	Select this checkbox to display the corresponding button in the Viewer of the Operator Console. This button sends actions from the camera to the Forensic Search process. The use of this function is restricted because it is a project-specific integration.
Fisheye Camera	Select this checkbox to enable the Fisheye Camera option.
Virtual PTZ	Select this checkbox to enable the Virtual PTZ option.
Normal PTZ	Select this checkbox to enable the Normal PTZ option.

When **Normal PTZ** is selected, the following PTZ options are enabled:

- Focus Speed
- Pan Speed
- Tilt Speed
- Zoom Speed
- Preset Offset
- Preset Count

Camera Groups

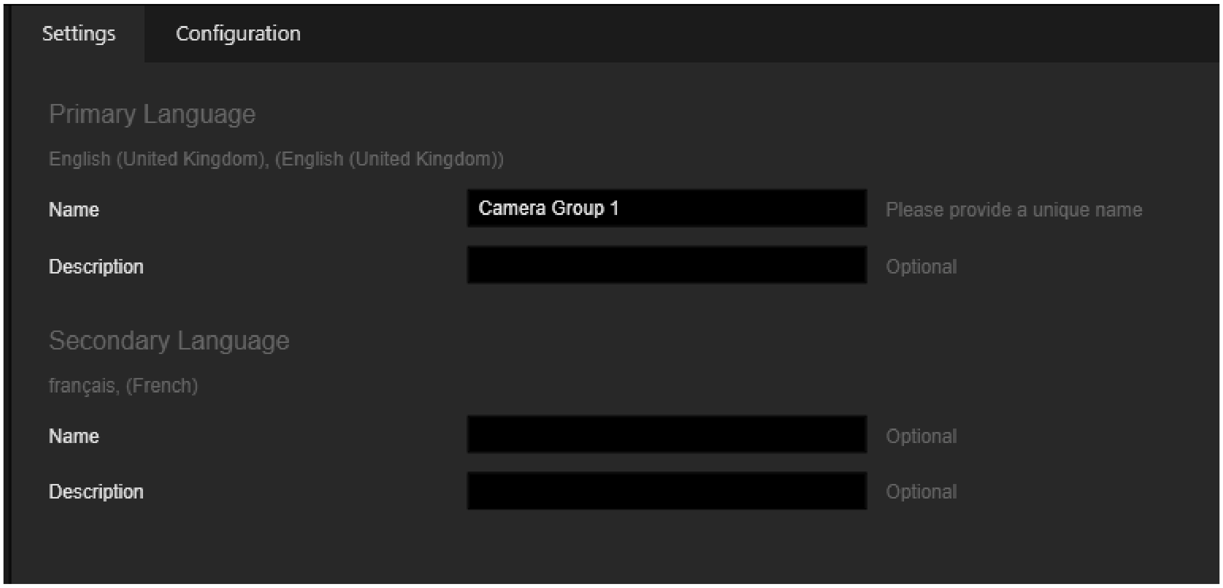
The **Camera Groups** view contains a list of camera groups.



The **Camera Group** settings are grouped in tabs.

Settings

The administrator can configure the name and description of the camera group for both primary and secondary languages.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Camera Group 1 — Please provide a unique name

Description: — Optional

Secondary Language

français, (French)

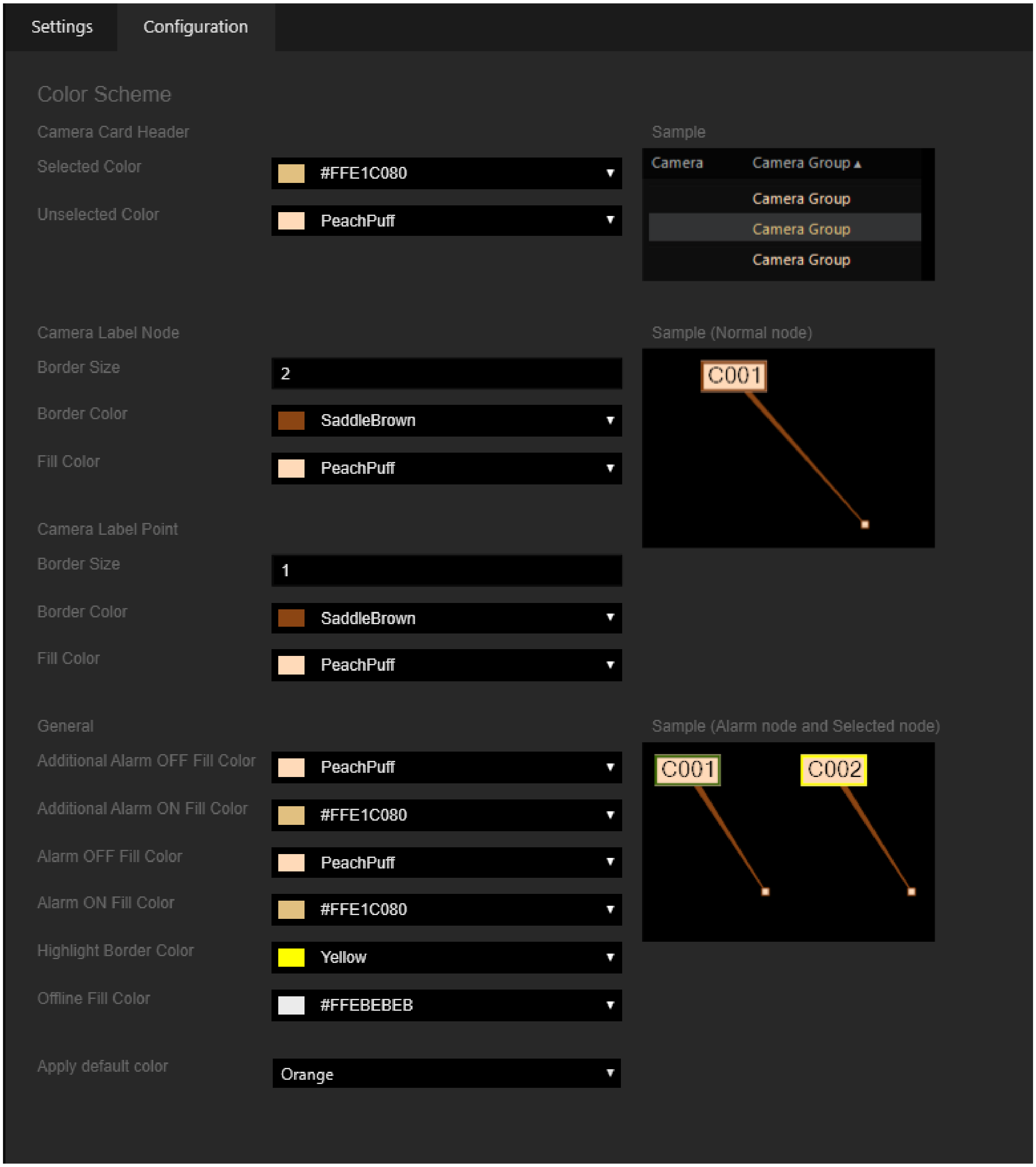
Name: — Optional

Description: — Optional

Configuration

The administrator can configure the colors for visualization cameras of specific camera groups in the cameras tab of the Operator Console.

The administrator can configure the settings for visualization camera labels of specific camera groups on the map.



Color Scheme

Camera Card Header

Selected Color: #FFE1C080 ▾

Unselected Color: PeachPuff ▾

Camera Label Node

Border Size: 2

Border Color: SaddleBrown ▾

Fill Color: PeachPuff ▾

Camera Label Point

Border Size: 1

Border Color: SaddleBrown ▾

Fill Color: PeachPuff ▾

General

Additional Alarm OFF Fill Color: PeachPuff ▾

Additional Alarm ON Fill Color: #FFE1C080 ▾

Alarm OFF Fill Color: PeachPuff ▾

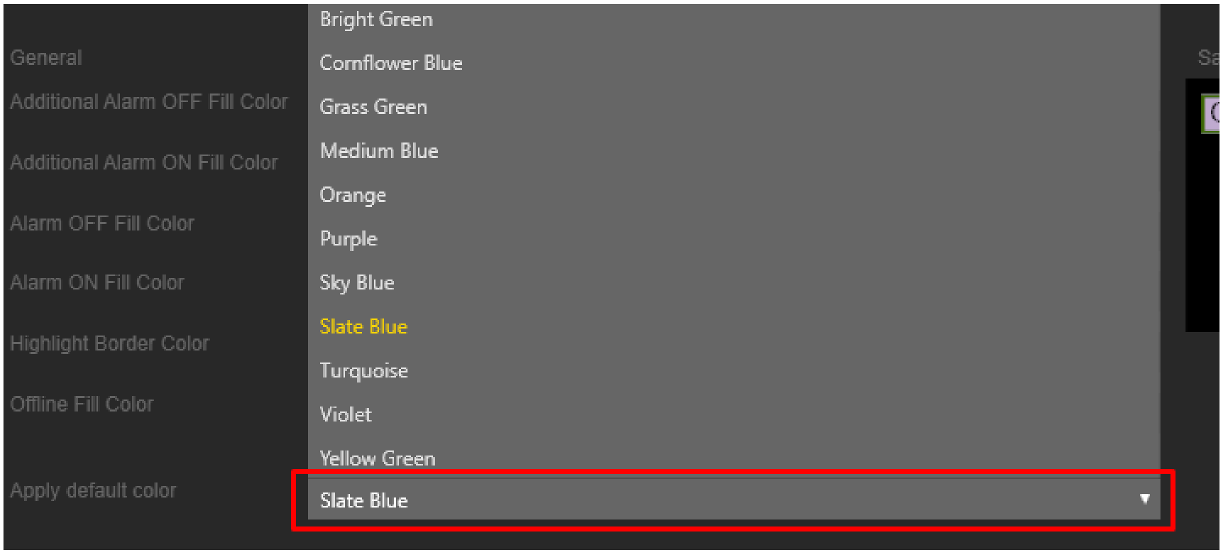
Alarm ON Fill Color: #FFE1C080 ▾

Highlight Border Color: Yellow ▾

Offline Fill Color: #FFEBEBEB ▾

Apply default color: Orange ▾

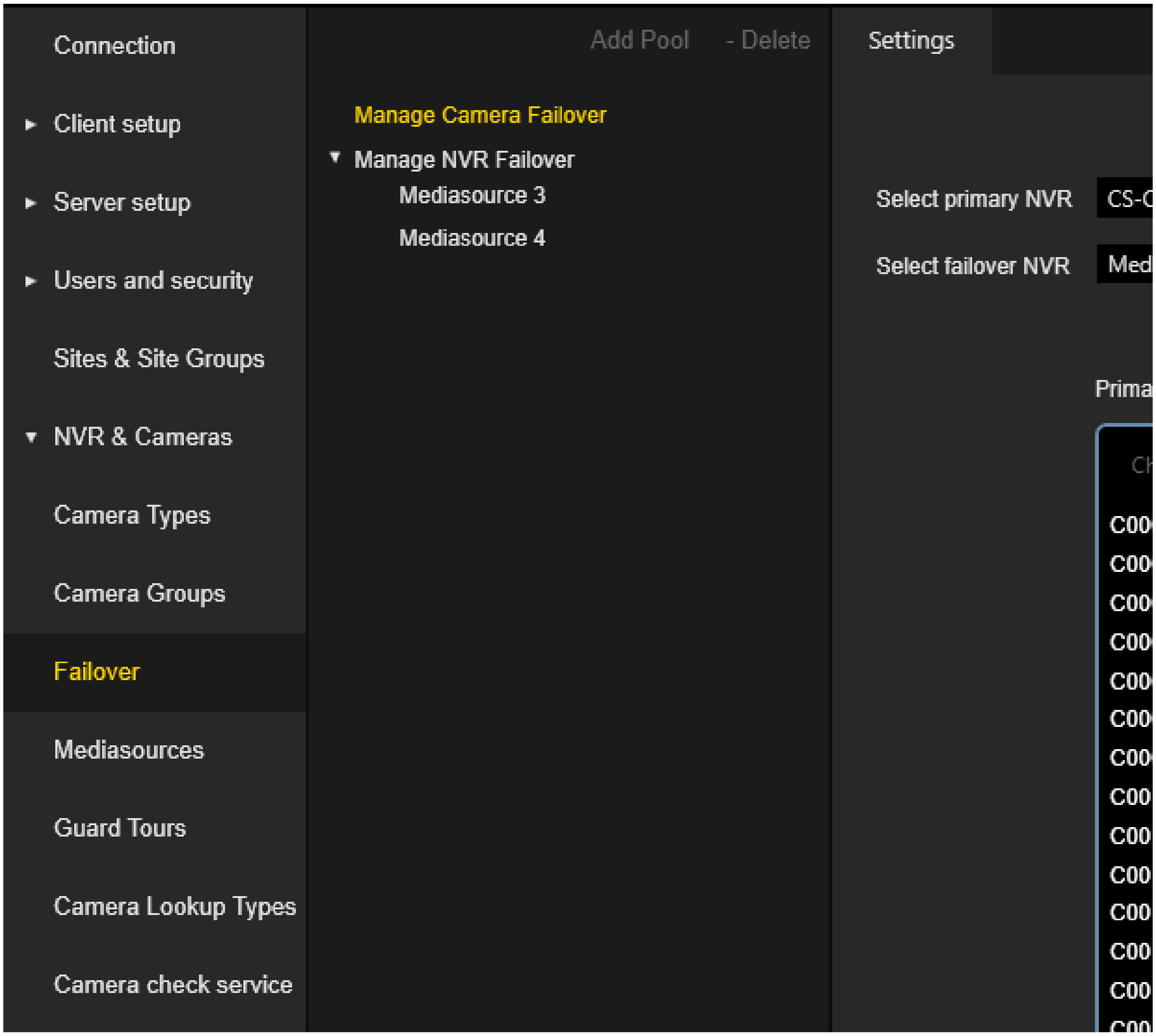
The administrator can select a color scheme to set all visualization settings with one click.



Failover

The **Failover** view contains two items in the tree view: **Manage Camera Failover** and **Manage NVR Failover**.

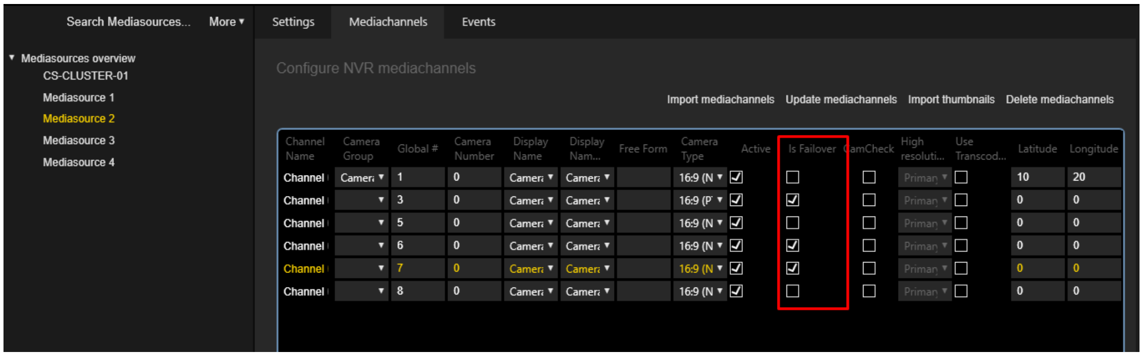
The **Manage NVR Failover** item contains a list of the configured NVR Failover Pools. Click the **Add Pool** button to create a new NVR Failover Pool. Click the **- Delete** button to remove the selected NVR Failover Pool.



Camera Failover Settings

To configure the camera matching, do the following:

1. Select the camera from the primary NVR.
2. Select the corresponding camera from the failover NVR. A failover NVR is a NVR that contains cameras with the **Is Failover** option (refer to **Mediachannels**).



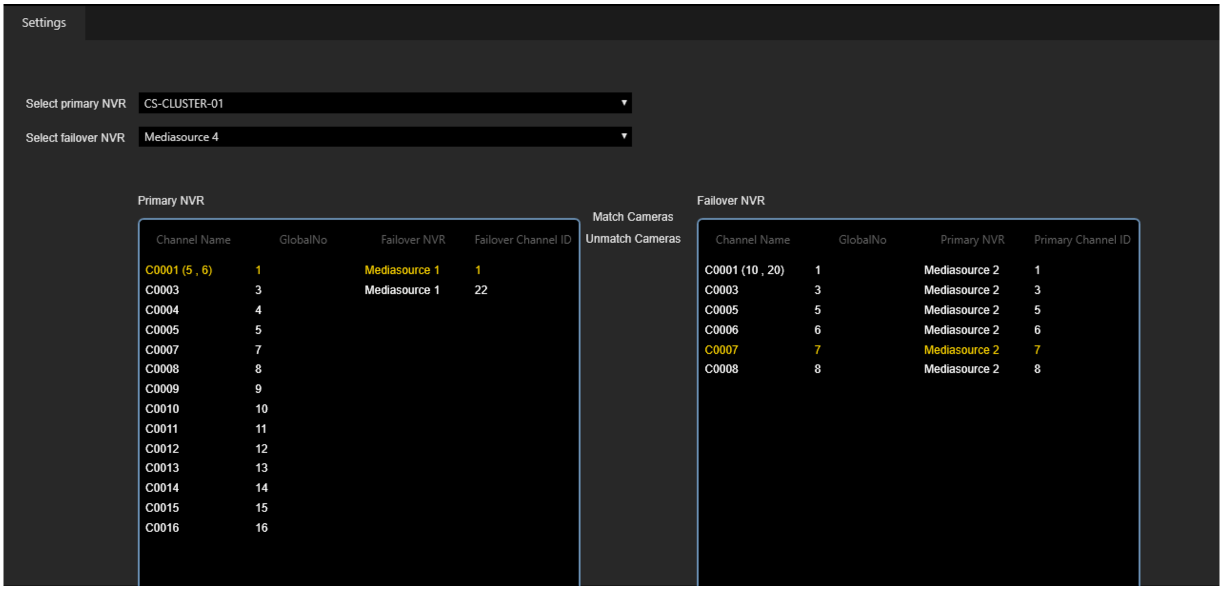
Configure NVR mediachannels

Channel Name	Camera Group	Global #	Camera Number	Display Name	Display Nam...	Free Form	Camera Type	Active	Is Failover	CamCheck	High resoluti...	Use Transcod...	Latitude	Longitude
Channel	Camera ▾	1	0	Camera ▾	Camera ▾		16:9 (N ▾	☑	□	□	Priman ▾	□	10	20
Channel	▾	3	0	Camera ▾	Camera ▾		16:9 (P ▾	☑	☑	□	Priman ▾	□	0	0
Channel	▾	5	0	Camera ▾	Camera ▾		16:9 (N ▾	☑	□	□	Priman ▾	□	0	0
Channel	▾	6	0	Camera ▾	Camera ▾		16:9 (N ▾	☑	☑	□	Priman ▾	□	0	0
Channel	▾	7	0	Camera ▾	Camera ▾		16:9 (N ▾	☑	☑	□	Priman ▾	□	0	0
Channel	▾	8	0	Camera ▾	Camera ▾		16:9 (N ▾	☑	□	□	Priman ▾	□	0	0

3. Click the **Match Cameras** button.

4. Select a camera from the list of **Primary NVR** and click the **Unmatch cameras** button to display unmatched cameras.

The **Failover Channel ID** column in the Primary NVR list and the **Primary Channel ID** column in the Failover NVR list will display the matching cameras.



Select primary NVR: CS-CLUSTER-01

Select failover NVR: Mediasource 4

Primary NVR

Channel Name	GlobalNo	Failover NVR	Failover Channel ID
C0001 (5 , 6)	1	Mediasource 1	1
C0003	3	Mediasource 1	22
C0004	4		
C0005	5		
C0007	7		
C0008	8		
C0009	9		
C0010	10		
C0011	11		
C0012	12		
C0013	13		
C0014	14		
C0015	15		
C0016	16		

Failover NVR

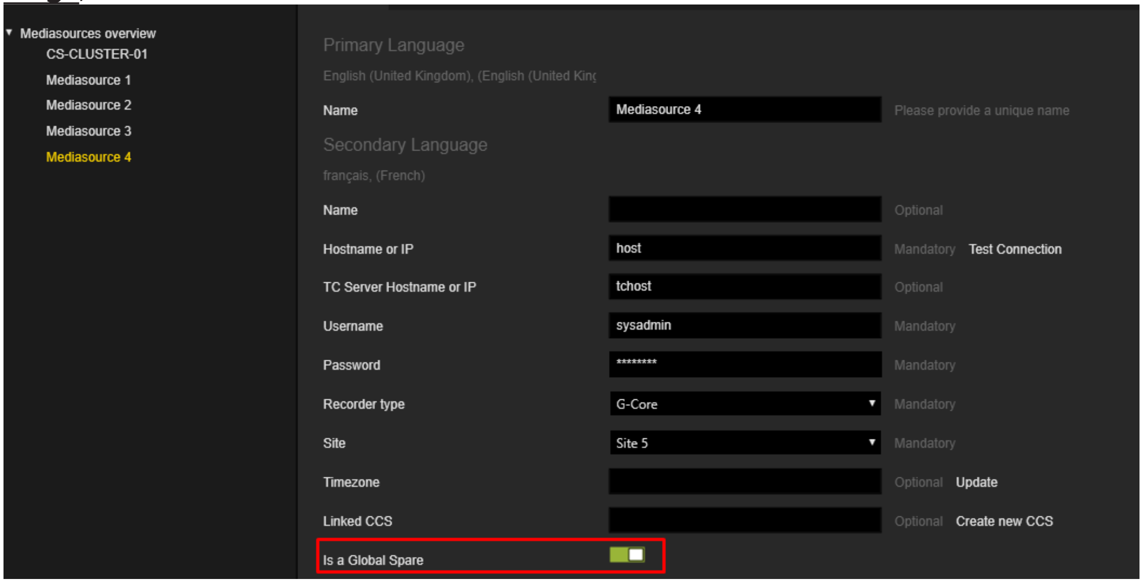
Channel Name	GlobalNo	Primary NVR	Primary Channel ID
C0001 (10 , 20)	1	Mediasource 2	1
C0003	3	Mediasource 2	3
C0005	5	Mediasource 2	5
C0006	6	Mediasource 2	6
C0007	7	Mediasource 2	7
C0008	8	Mediasource 2	8

NVR Failover Pool Settings

There are three steps to configure a specific NVR Failover Pool:

1. **Create Pool:**

Select failover recorders to be added to the Pool. Failover recorder is a mediasource with the **Is a Global Spare** option selected (refer to **Media source Settings**).



Primary Language

English (United Kingdom), (English (United King

Name	Mediasource 4	Please provide a unique name

Secondary Language

français, (French)

Name		Optional
Hostname or IP	host	Mandatory Test Connection
TC Server Hostname or IP	tchost	Optional
Username	sysadmin	Mandatory
Password	********	Mandatory
Recorder type	G-Core	Mandatory
Site	Site 5	Mandatory
Timezone		Optional Update
Linked CCS		Optional Create new CCS
Is a Global Spare	●	

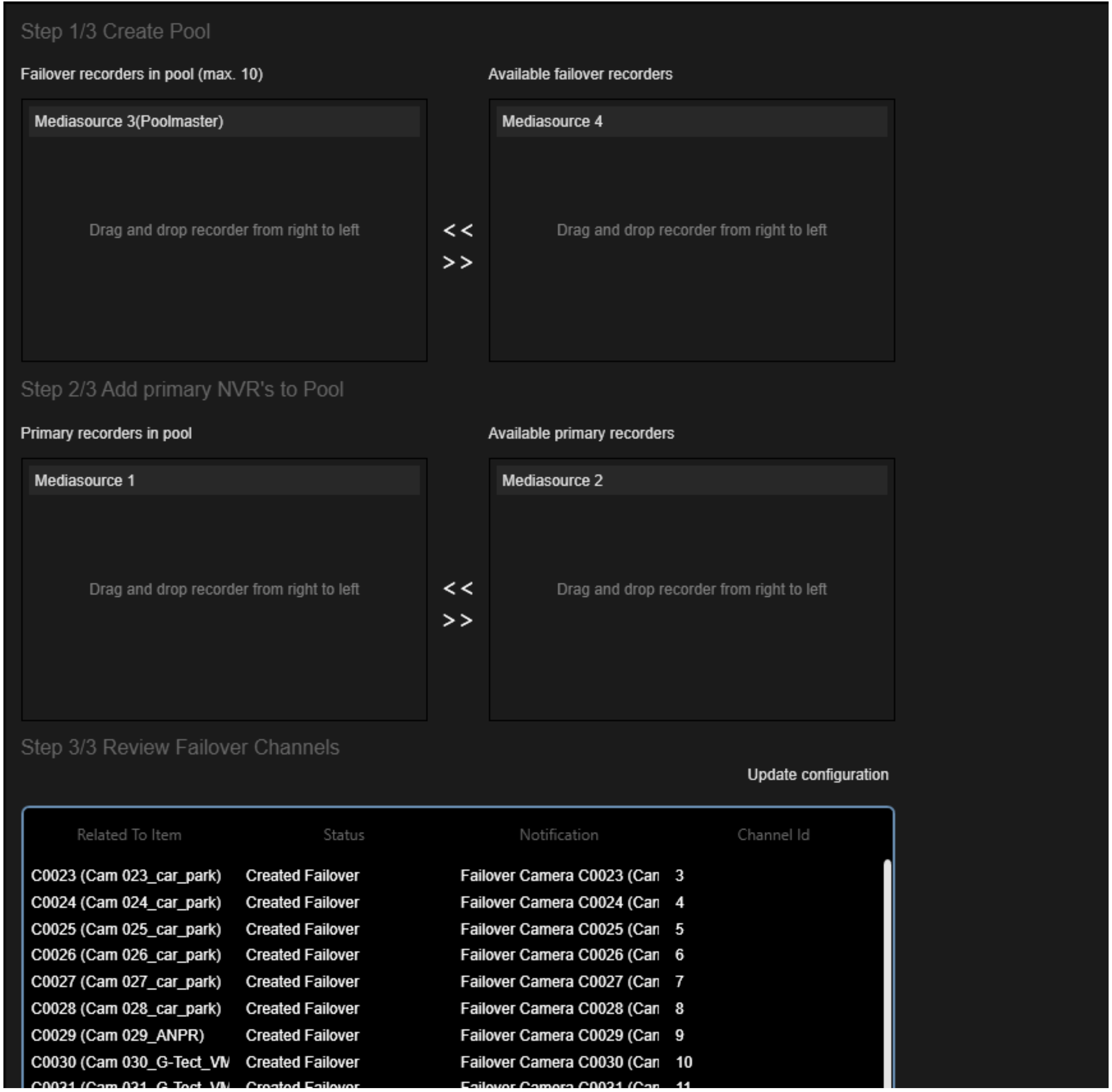
→ The first selected failover recorder in the pool will be marked as **Pool-master**.

2. **Add primary NVR's to pool:**

   Select the primary recorders to be added to the pool.

3. **Review Failover Channels:**

The failover channels table contains the cameras of the selected primary recorders. Click **Update configuration** if there were changes in the media-source cameras after the NVR failover pool was created.



Step 1/3 Create Pool

Failover recorders in pool (max. 10)

Mediasource 3(Poolmaster)

Available failover recorders

Mediasource 4

Drag and drop recorder from right to left
<<
>>
Drag and drop recorder from right to left

Step 2/3 Add primary NVR's to Pool

Primary recorders in pool

Mediasource 1

Available primary recorders

Mediasource 2

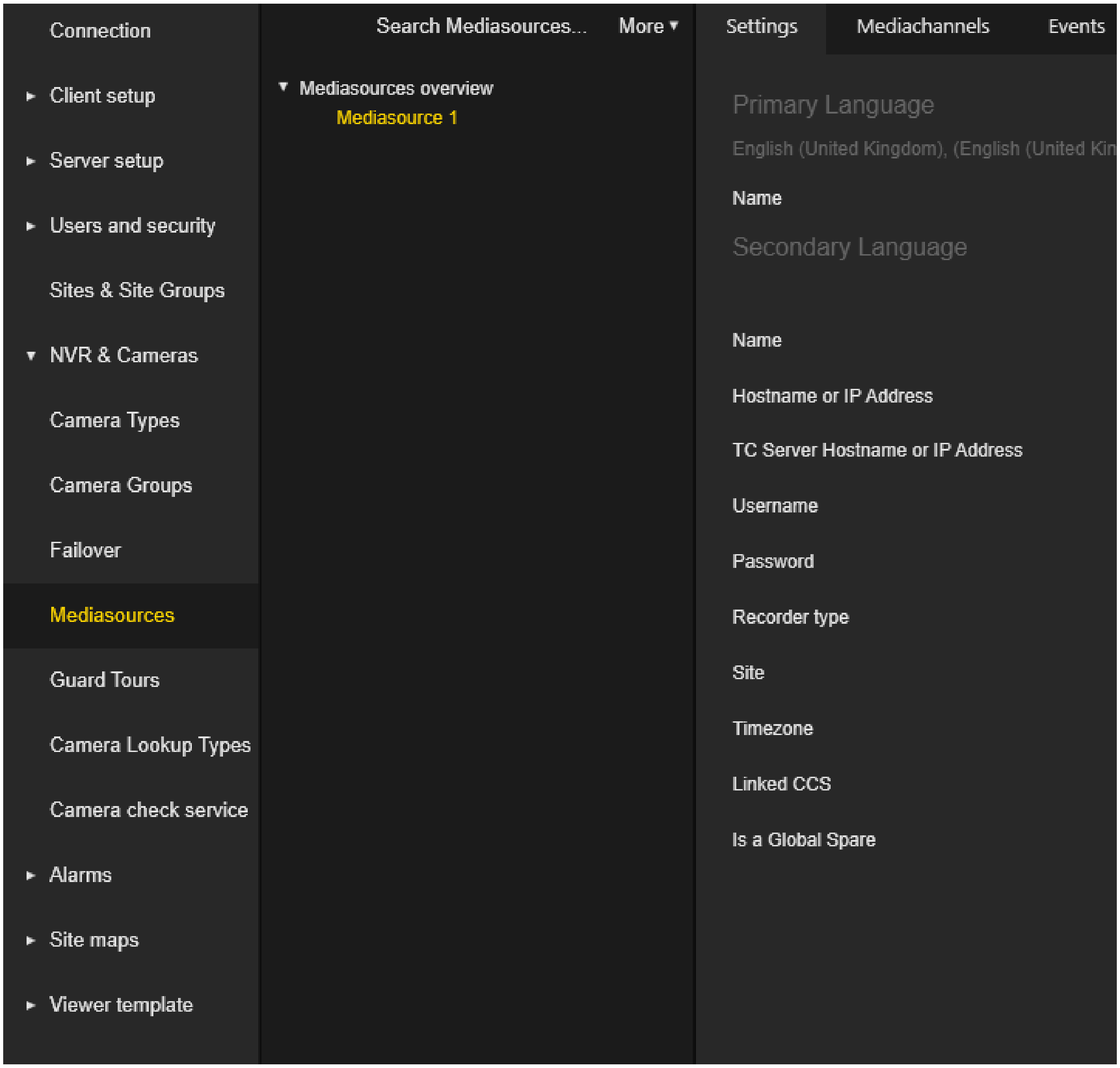
Drag and drop recorder from right to left
<<
>>
Drag and drop recorder from right to left

Step 3/3 Review Failover Channels

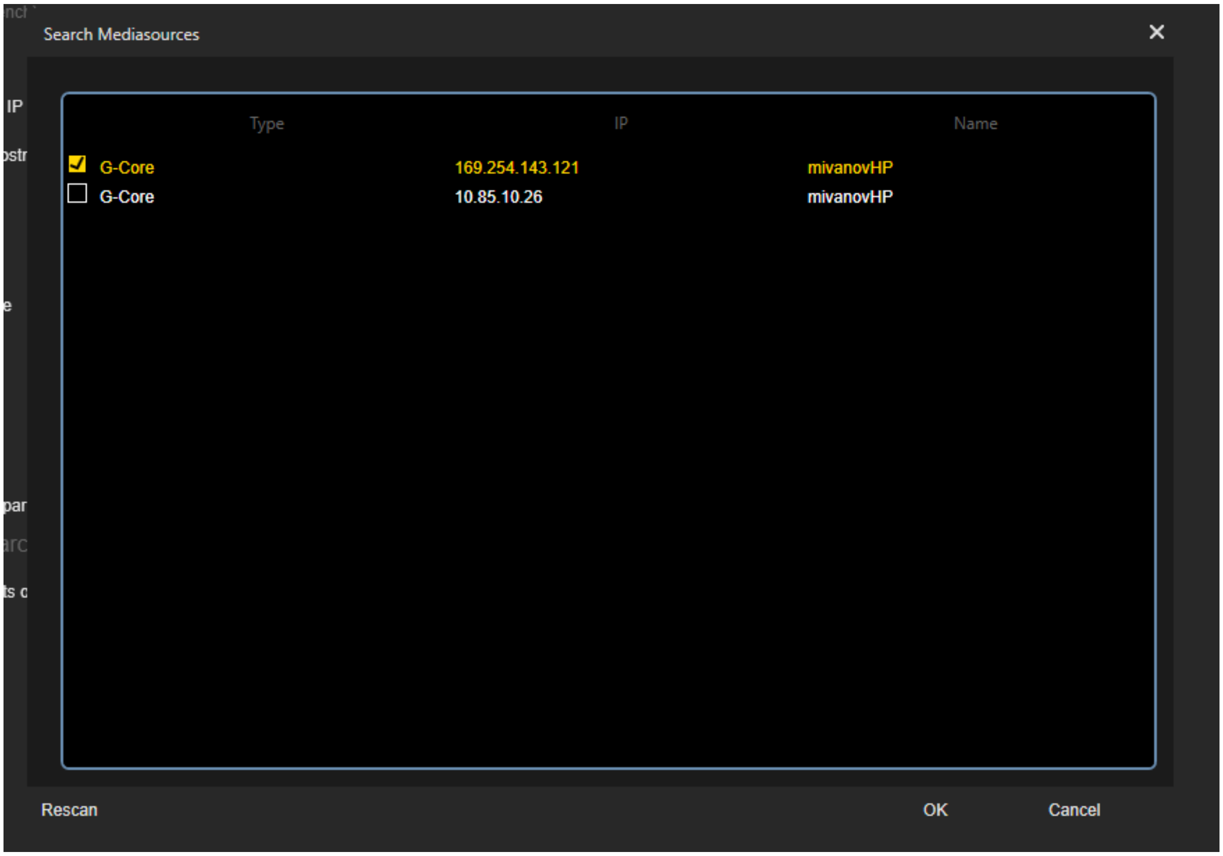
Related To Item	Status	Notification	Channel Id
C0023 (Cam 023_car_park)	Created Failover	Failover Camera C0023 (Can	3
C0024 (Cam 024_car_park)	Created Failover	Failover Camera C0024 (Can	4
C0025 (Cam 025_car_park)	Created Failover	Failover Camera C0025 (Can	5
C0026 (Cam 026_car_park)	Created Failover	Failover Camera C0026 (Can	6
C0027 (Cam 027_car_park)	Created Failover	Failover Camera C0027 (Can	7
C0028 (Cam 028_car_park)	Created Failover	Failover Camera C0028 (Can	8
C0029 (Cam 029_ANPR)	Created Failover	Failover Camera C0029 (Can	9
C0030 (Cam 030_G-Tect_VM	Created Failover	Failover Camera C0030 (Can	10
C0031 (Cam 031_G-Tect_VM	Created Failover	Failover Camera C0031 (Can	11

Mediasources

The **Mediasources** view contains a list of the mediasources (NVRs).



In addition to the general **+ Add**, **- Delete** and *** Clone** buttons, there is a **Search Mediasources...** button. Click this button to search G-Core mediasources on the local network. The administrator can select mediasources to be automatically added to the mediasouces list.

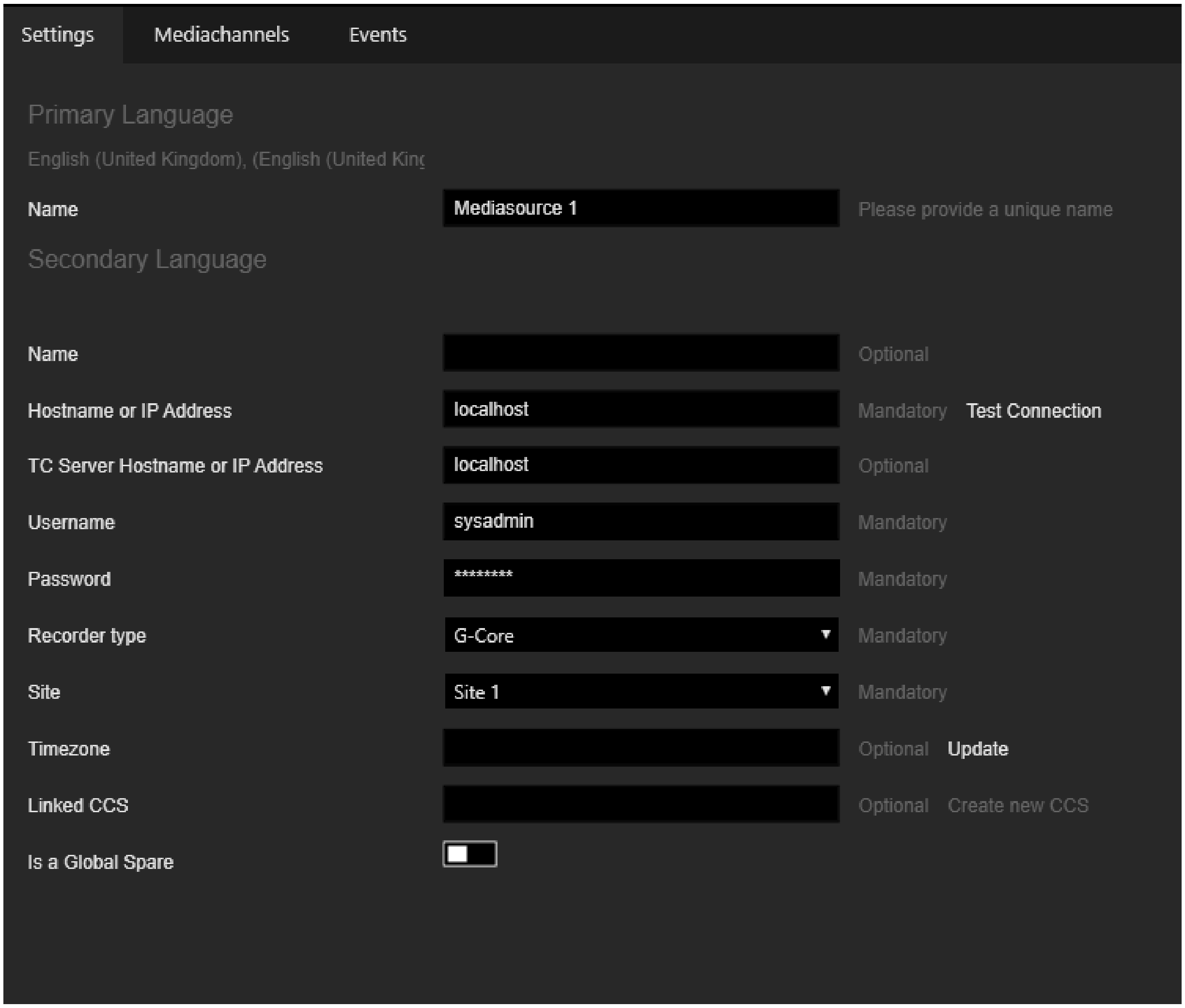


	Type	IP	Name
☑	G-Core	169.254.143.121	mivanovHP
□	G-Core	10.85.10.26	mivanovHP

The **Mediasource** settings are grouped in tabs.

Settings

The administrator can configure the following settings of the mediasource:



Primary Language

English (United Kingdom), (English (United Kinc

Name	Mediasource 1	Please provide a unique name

Secondary Language

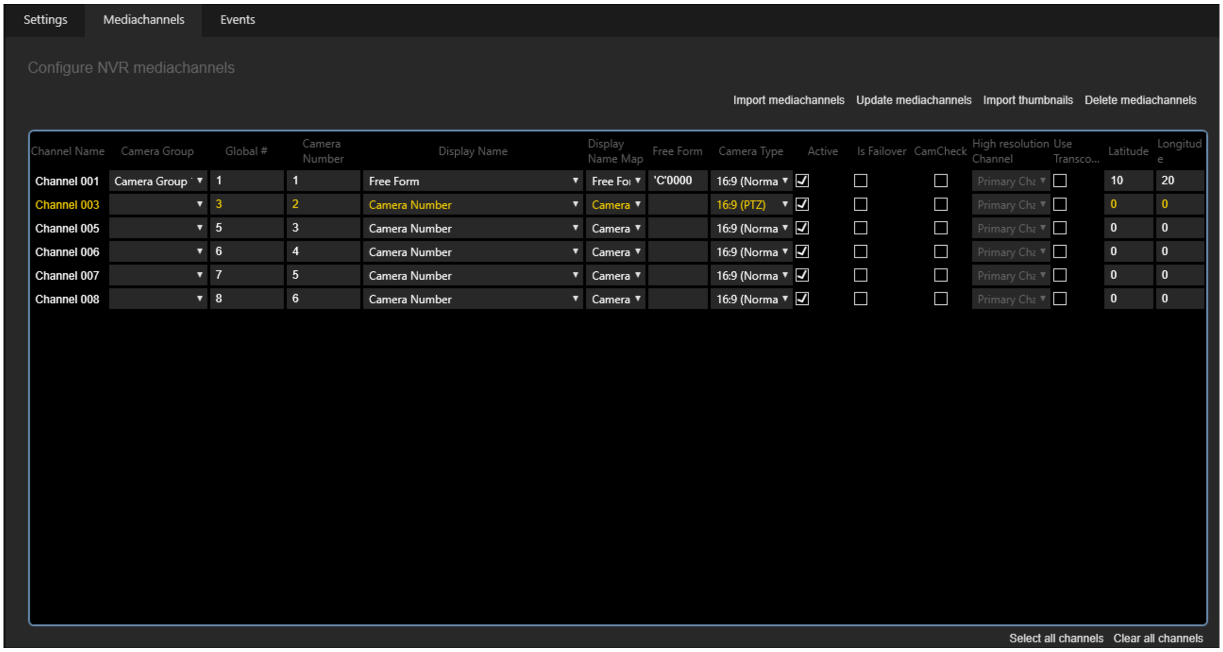
Name		Optional
Hostname or IP Address	localhost	Mandatory
TC Server Hostname or IP Address	localhost	Optional
Username	sysadmin	Mandatory
Password	********	Mandatory
Recorder type	G-Core	Mandatory
Site	Site 1	Mandatory
Timezone		Optional
Linked CCS		Optional
Is a Global Spare	□	

Settings	Description
Name	Name of the mediasource for both primary and secondary languages.
Hostname or IP	Address of the computer running the NVR service (G-Core/GeViScope).
Test Connection	Click this button to check if the connection settings (Hostname, Username, Password) to the NVR are valid.
TC Server Hostname or IP Adress	Address of the computer on which the Transcoding Server runs. This setting is visible if the **Allow Transcoding Viewers** license is available and enabled (refer to

Settings	Description
	Server Licenses).
Username	Name of the NVR user.
Password	Password of the NVR user.
Recorder type	Type of the NVR. The administrator can select between the types G-Core and GeViScope.
Site	The administrator must select the site to which a specific mediasource is to be linked.
Timezone	Time zone of the specific mediasource. Click the **Update** button to retrieve the time zone of the NVR.
Linked CCS	Name of the camera check service that monitors the site of the specific mediasource (refer to **Camera check service**).
Update	This button is visible when there is a camera check service that monitors the site of the specific mediasource. This button is enabled if a **Pro version** license is available and enabled (refer to **Server Licenses**) and mediachannels (cameras) are existing on the specific Mediasource. Click this button to update the linked camera check service.
Create new CSS	This button is visible when there is no camera check service that monitors the site of the specific mediasource. This button is enabled if a **Pro version** license is available and enabled (refer to **Server Licenses**) and mediachannels (cameras) are existing on specific mediasource. Click this button to create a new camera check service based on the settings of the specific mediasource.
Is a Global Spare	This checkbox is visible if the license **Max Number of Cameras that can be marked as Failover** is greater than 0 (refer to **Server Licenses**). Select this checkbox to mark a specific Mediasource as a Failover Mediasource (see **NVR Failover Pool Settings**).

Mediachannels

The **Mediachannels** tab contains a list of mediachannels (cameras) of the specific mediasource:



Channel Name	Camera Group	Global #	Camera Number	Display Name	Display Name Map	Free Form	Camera Type	Active	Is Failover	CamCheck	High resolution Channel	Use Transco...	Latitude	Longitude
Channel 001	Camera Group	1	1	Free Form	Free Fo	'C'0000	16:9 (Norma	☑	□	□	Primary Cha	□	10	20
Channel 003		3	2	Camera Number	Camera		16:9 (PTZ)	☑	□	□	Primary Cha	□	0	0
Channel 005		5	3	Camera Number	Camera		16:9 (Norma	☑	□	□	Primary Cha	□	0	0
Channel 006		6	4	Camera Number	Camera		16:9 (Norma	☑	□	□	Primary Cha	□	0	0
Channel 007		7	5	Camera Number	Camera		16:9 (Norma	☑	□	□	Primary Cha	□	0	0
Channel 008		8	6	Camera Number	Camera		16:9 (Norma	☑	□	□	Primary Cha	□	0	0

The administrator can configure the following settings per mediachannel (camera) (some of the settings can be edited for multiselected mediachannels):

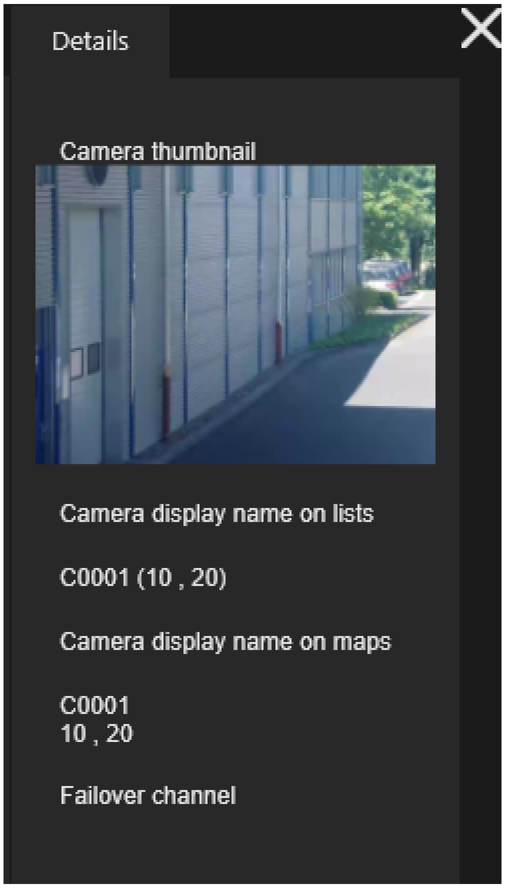
Settings	Description
Camera Group	Assign the camera to the specific Camera Group (**see Camera Groups**). Can be edited with multiselect.
Global #	By default, this value is retrieved from the NVR. Is used to correspond a specific mediachannel with the mediachannel of the NVR.
Camera number	By default, this value is retrieved from the NVR. Can be used to display the camera name when using Free Form.
Display Name	Configure how the camera is to be visualised in the lists, card etc. Can be edited with multiselect. Possible values are: • **Camera Name**

Settings	Description
	- **Camera Number**: Display the camera Global # according to the **Camera Display Format** (see Language & Format Settings). - **Camera Number and Name**: Display the camera Global # according to the **Camera Display Format** plus Camera Name. - **Camera Number and Coordinates**: Display the camera Global # according to the **Camera Display Format** plus Camera Coordinates (Latitude and Longitude settings). - **Free Form**: Display the camera number according to the free form template.
Display Name Map	Configure how the camera label should be visualised on the maps. The same values as for **Display Name** are available. Can be edited with multiselect.
Free Form	Configure template of the camera name for the free form display type. Can be edited with multiselect.
Camera Type	By default, this value is retrieved from the NVR. Assign a camera to a Specific Camera Type (see Camera Types). Can be edited with multiselect.
Active	Activate or deactivate the camera. Can be edited with multiselect.
Is Failover	Select the camera to be used as a failover for another camera (see Failover). Can be edited with multiselect.
CamCheck	Read only. Shows that the camera is monitored by the camera check service.
High resolution Channel	This field is enabled when the mediachannel of the NVR has a secondary channel. The administrator can select which channel is playing the high resolution video.
Use Transcoding	Select if the camera has a transcoding channel. Can be edited with multiselect.
Latitude / Longitude	Configure the geographical coordinates of the camera. Can be edited with multiselect.

- Click the Import mediachannels button to retrieve existing mediachannels from specific NVRs from Mediasource. Any previous data in G-SIM will be overwritten with the imported data. Even if the NVR configuration has not changed, this function regenerates the configuration in G-SIM. Existing tours and video events would therefore need to be reconnected. The same applies to map placement and other links. Before using this function, you should be aware of the consequences.
- Click the Update medichannels button to update existing mediachannels with mediachannels from specific mediasource NVR. In the pop-up dialog, the administrator can choose to add new mediachannels of the NVR to the specific mediasource or not. Mediachannels that are no longer existing on the NVR will be deactivated but not removed.
- Click the Import thumbnails button to retrieve thumbnails for the selected mediachannels from the NVR of specific mediasource.
- Click the Delete mediachannels button to remove selected mediachannels from a specific mediasource.
- Click Select all channels or Clear all channels to select or unselect all mediachannels with one click.

Camera Details

The administrator can select a mediachannel to see camera details:



Camera display name on lists

C0001 (10 , 20)

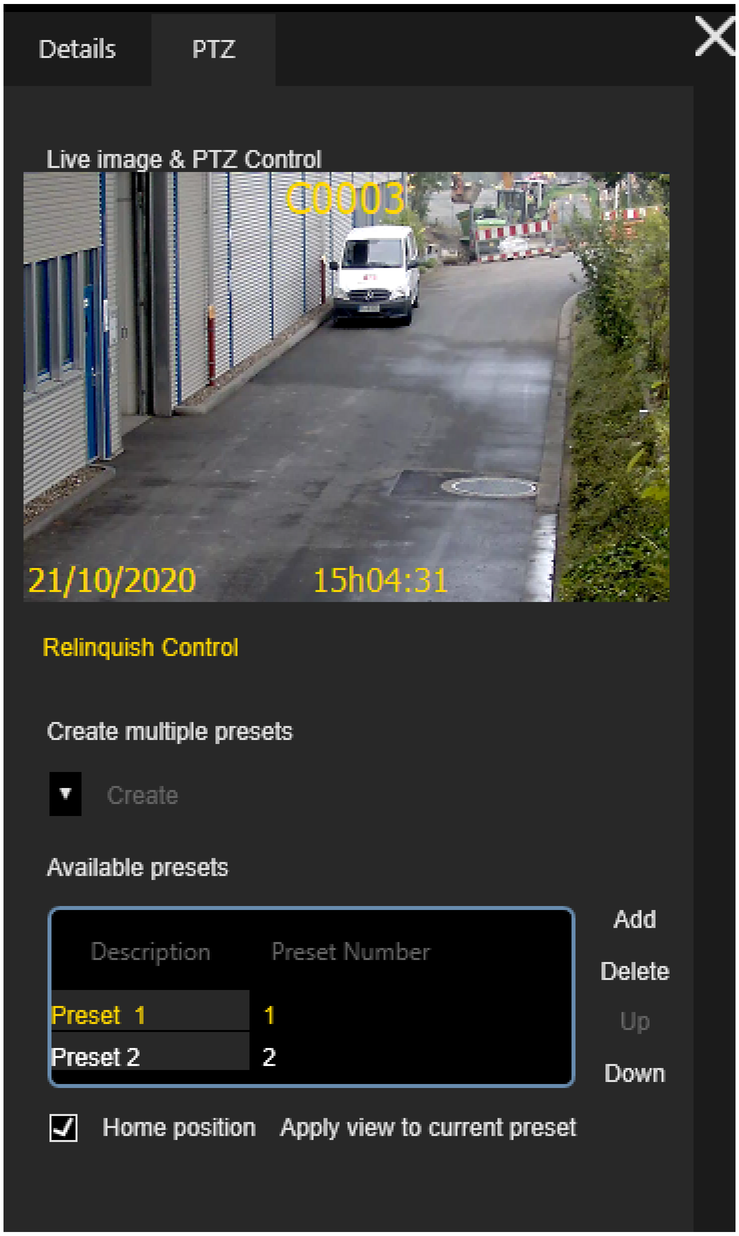
Camera display name on maps

C0001
10 , 20

Failover channel

PTZ Presets

If the **Normal PTZ** option is selected for the camera type of the selected media channel, the PTZ tab is visible.



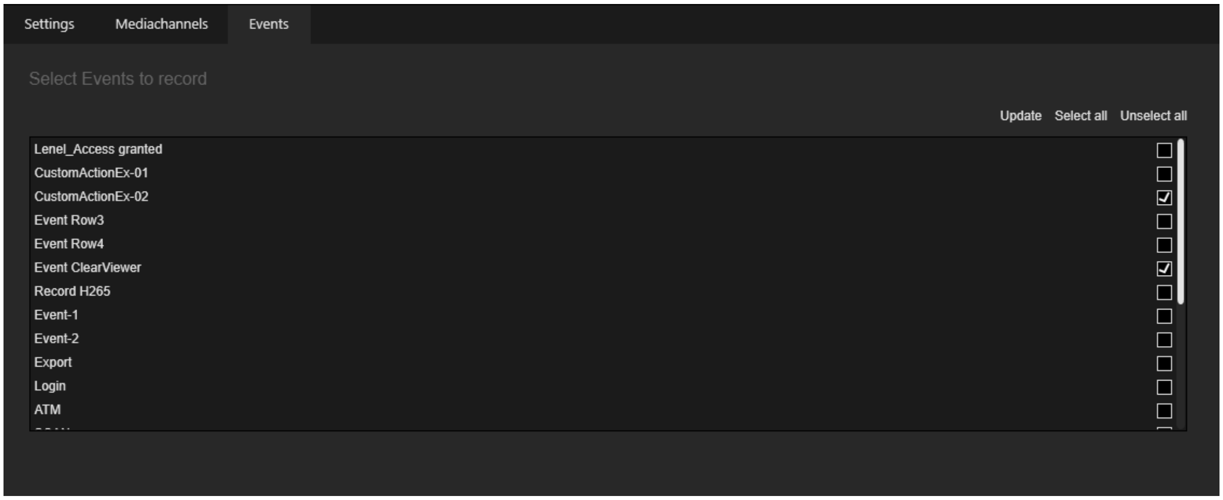
Description	Preset Number
Preset 1	1
Preset 2	2

- Click the **Live image & PTZ Control** button to edit PTZ presets for the selected camera.
- Click the **Relinquish Control** button to stop editing the PTZ presets of the selected camera.
- After taking control of the PTZ camera, the administrator can edit the presets.

- The administrator can create multiple presets by selecting the number of the presets and clicking the **Create** button. The maximum number of presets is defined in the camera type of the mediachannel.
- The administrator can create or delete single preset by clicking the **Add** or **Delete** button.
- The administrator can order existing presets by using the **Up** and **Down** buttons.
- The administrator can configure the description of the selected preset, mark it as the **Home position** and correspond to the current camera position and zoom level with the **Apply view to current preset** button.

Events

The **Events** tab contains a list of the events from the specific mediasource NVR.



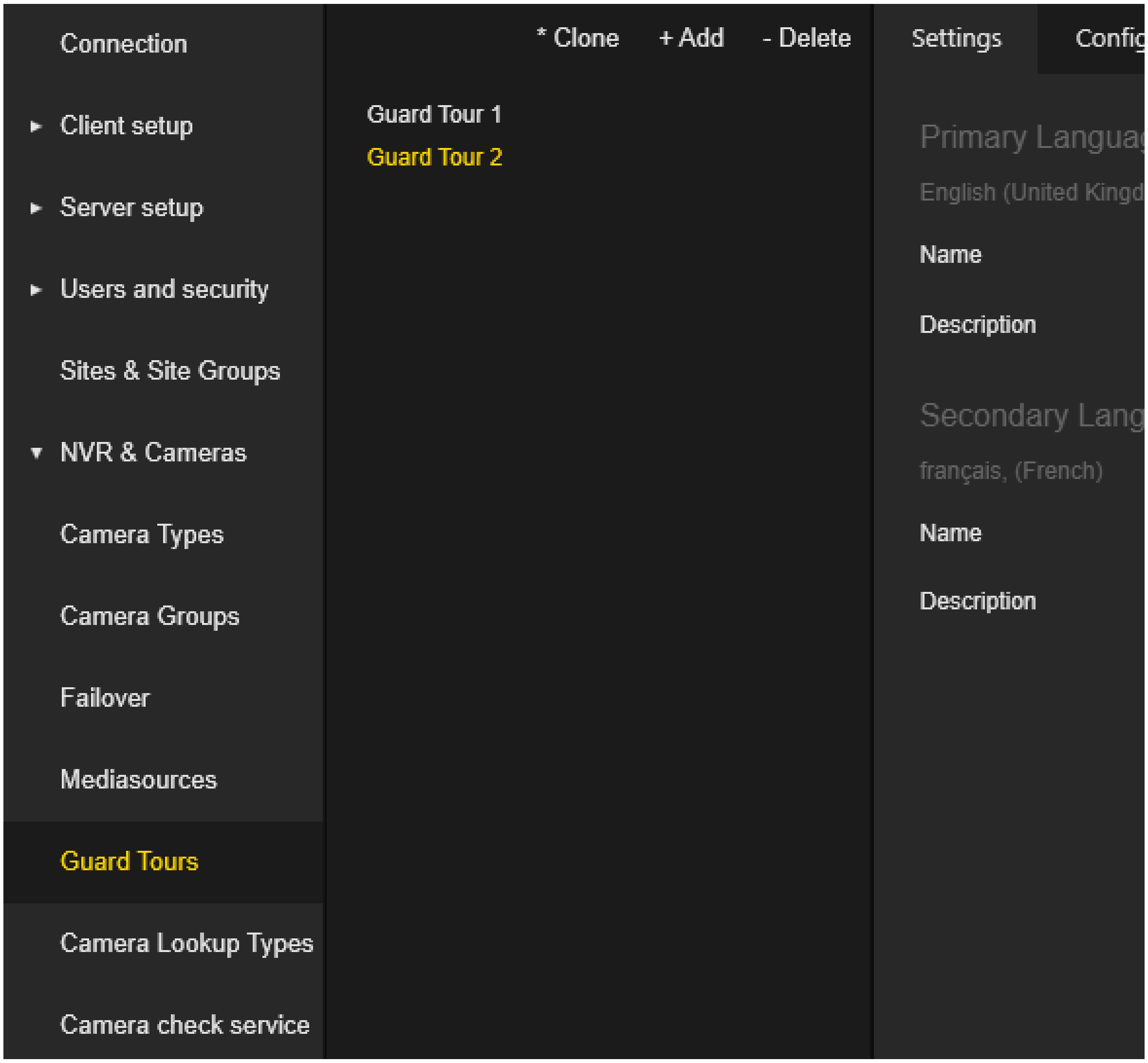
Lenel_Access granted □
CustomActionEx-01 □
CustomActionEx-02 ☑
Event Row3 □
Event Row4 □
Event ClearViewer ☑
Record H265 □
Event-1 □
Event-2 □
Export □
Login □
ATM □

- The administrator can click the **Update** button to retrieve events form the specific mediasource NVR.
- The administrator can check the events to be saved in the database. Saved events are used in the Process Data Search and to display the viewer OSD in the Operator Console.
- Click the **Select all** or **Unselect all** button to check or uncheck all events with one click.

Guard Tours

The **Guard Tour** view contains a list of public guard tours.

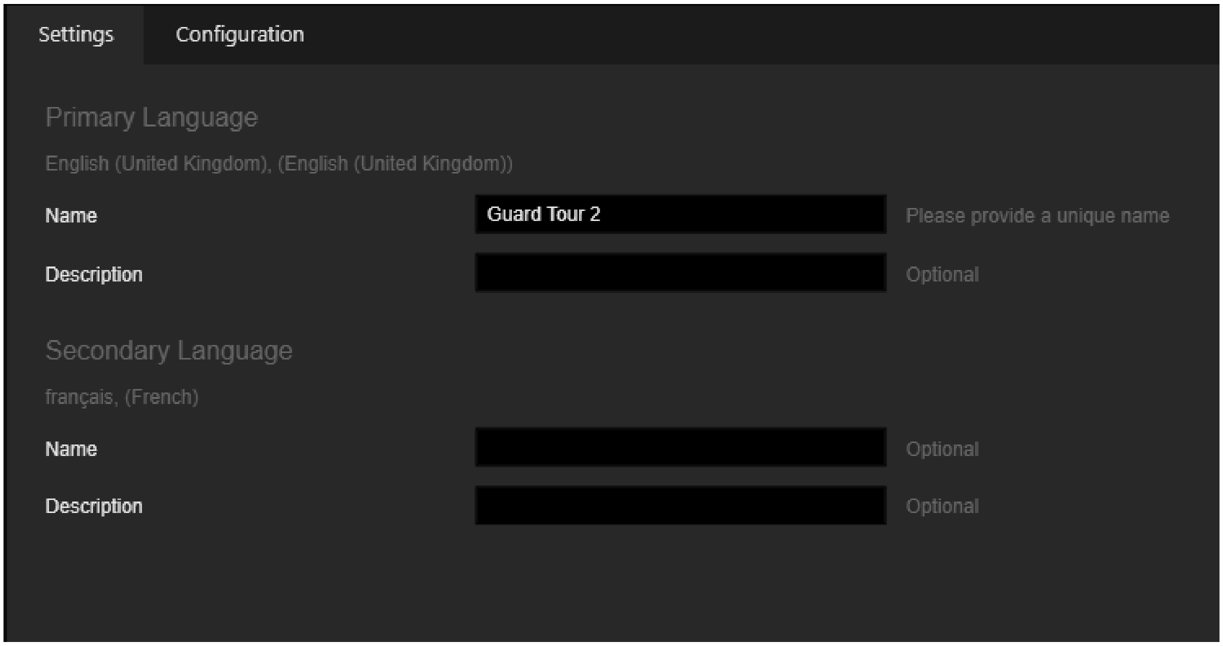
A guard tour is a predefined sequence of cameras, each of which is viewed in the same viewer for a specified time. Think of it as a guard walking from point to point. Guard tours assist a user in general surveillance, because a relatively large number of cameras can be easily monitored.



The **Guard Tour** settings are grouped in tabs.

Settings

The administrator can configure the name and description of the guard tour for both primary and secondary languages.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Guard Tour 2 — Please provide a unique name

Description: — Optional

Secondary Language

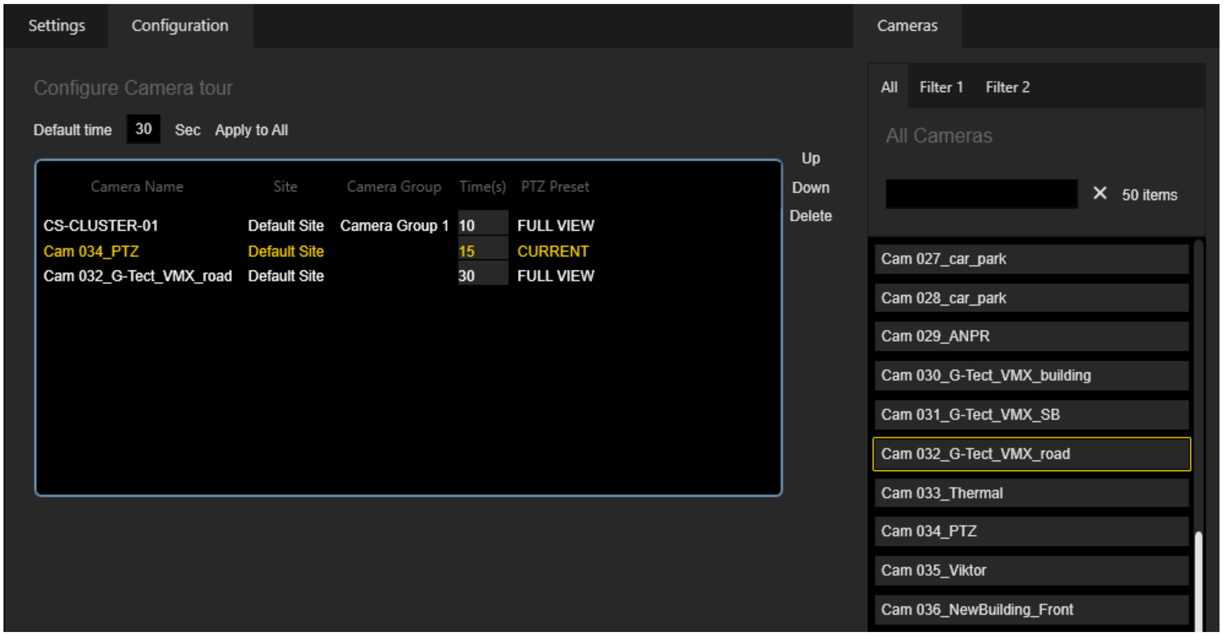
français, (French)

Name: — Optional

Description: — Optional

Configuration

The administrator can add cameras to the guard tour by using Drag & Drop from the **Cameras** tab.



Configure Camera tour

Default time 30 Sec

Camera Name	Site	Camera Group	Time(s)	PTZ Preset
CS-CLUSTER-01	Default Site	Camera Group 1	10	FULL VIEW
Cam 034_PTZ	Default Site		15	CURRENT
Cam 032_G-Tect_VMX_road	Default Site		30	FULL VIEW

All Cameras

50 items

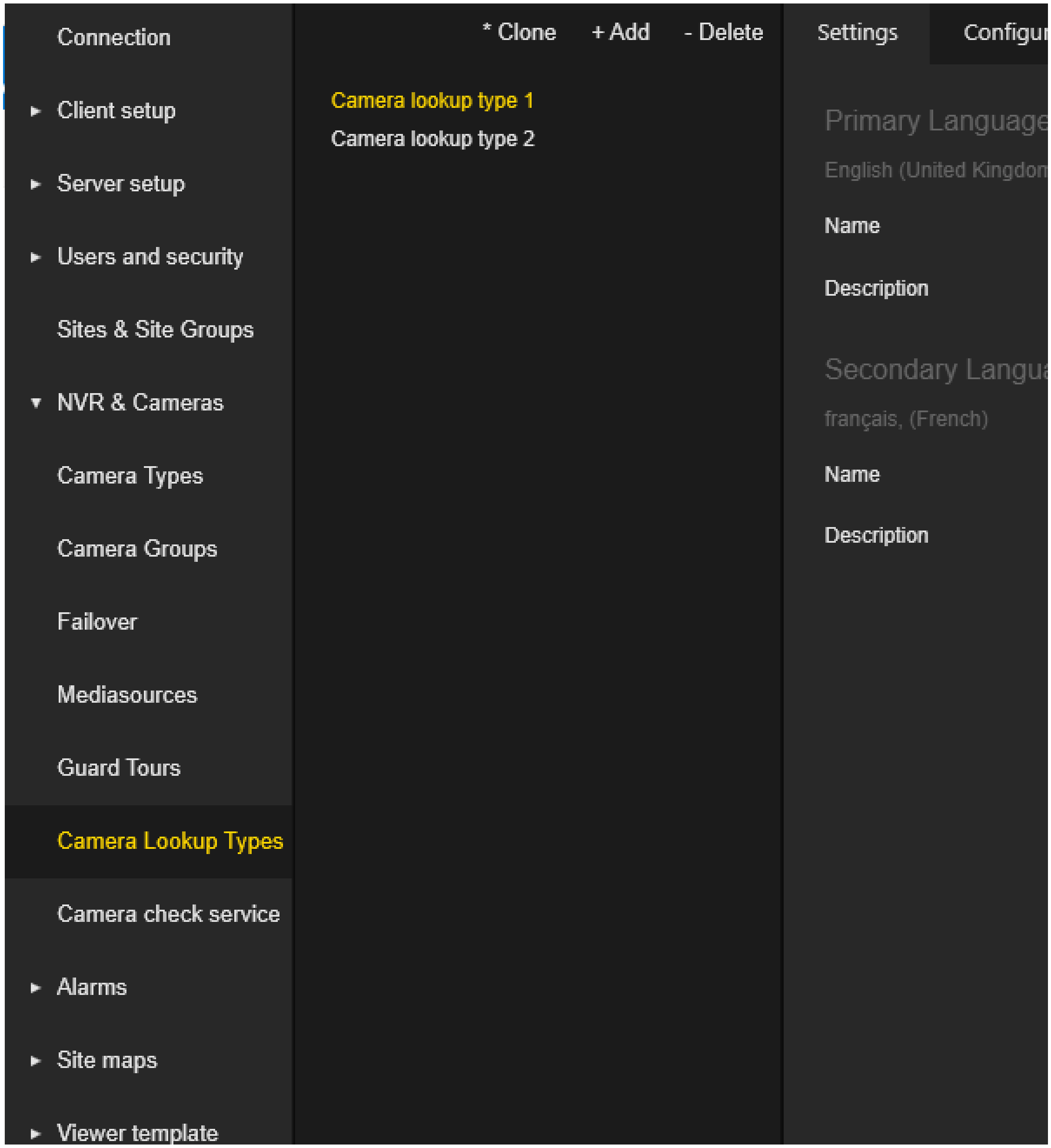
- Cam 027_car_park
- Cam 028_car_park
- Cam 029_ANPR
- Cam 030_G-Tect_VMX_building
- Cam 031_G-Tect_VMX_SB
- Cam 032_G-Tect_VMX_road
- Cam 033_Thermal
- Cam 034_PTZ
- Cam 035_Viktor
- Cam 036_NewBuilding_Front

- The administrator can arrange cameras in the guard tour by using the **Up** and **Down** buttons.

- The administrator can click the Delete button to remove the selected camera from the guard tour.
- The administrator can set the Default time (in seconds) for displaying the camera stream per camera in the guard tour. Click the Apply to All button to set the default time for all cameras in the guard tour.
- The administrator can select predefined PTZ Preset for PTZ cameras in the guard tour.

Camera Lookup Types

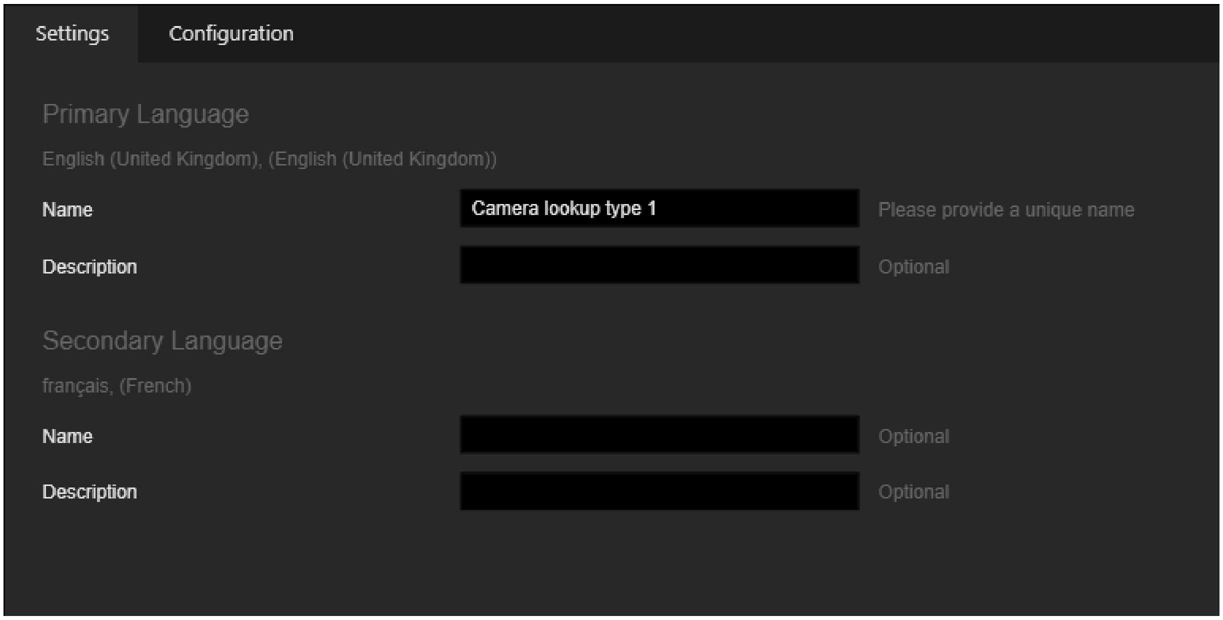
The Camera Lookup Types view contains a list of the camera lookup types.



The settings of the **Camera Lookup Type** are grouped in tabs.

Settings

The administrator can configure the name and description of the camera lookup type for both primary and secondary languages.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name	Camera lookup type 1	Please provide a unique name
Description		Optional

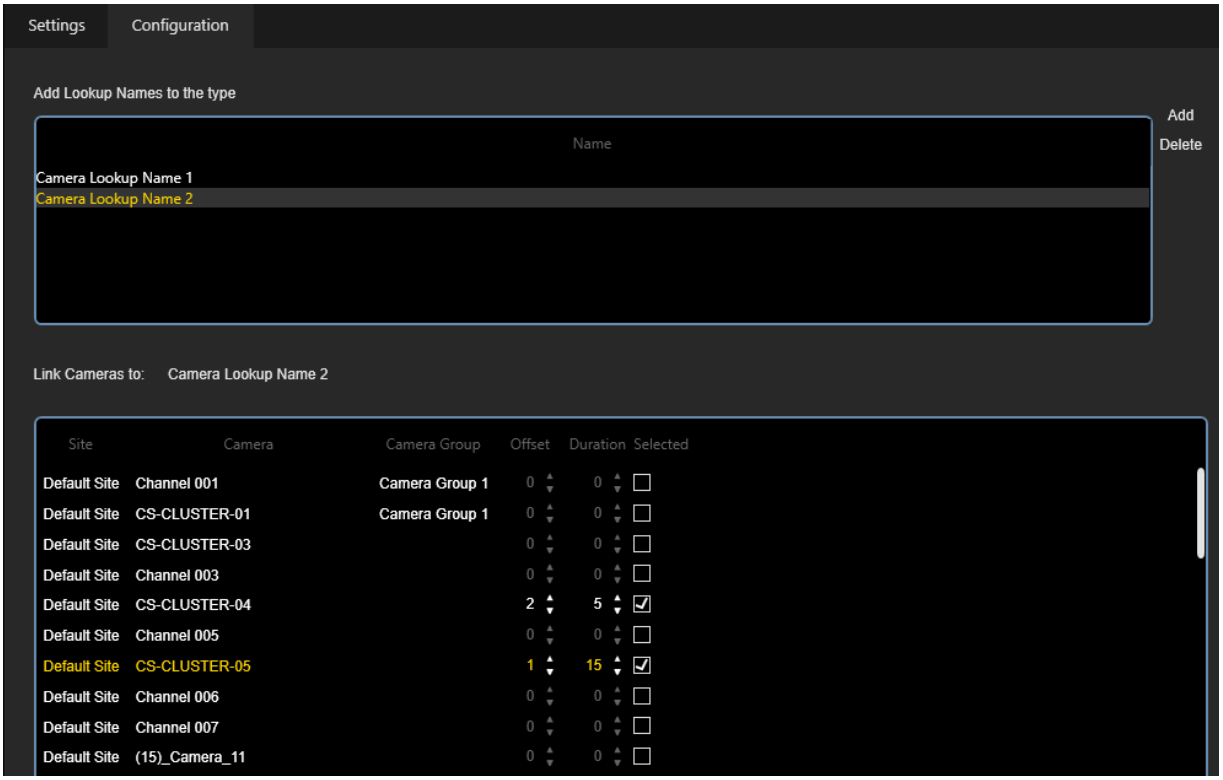
Secondary Language

français, (French)

Name		Optional
Description		Optional

Configuration

The administrator can configure the following camera lookup type settings:



Add Lookup Names to the type

Name
Camera Lookup Name 1
Camera Lookup Name 2

Link Cameras to: Camera Lookup Name 2

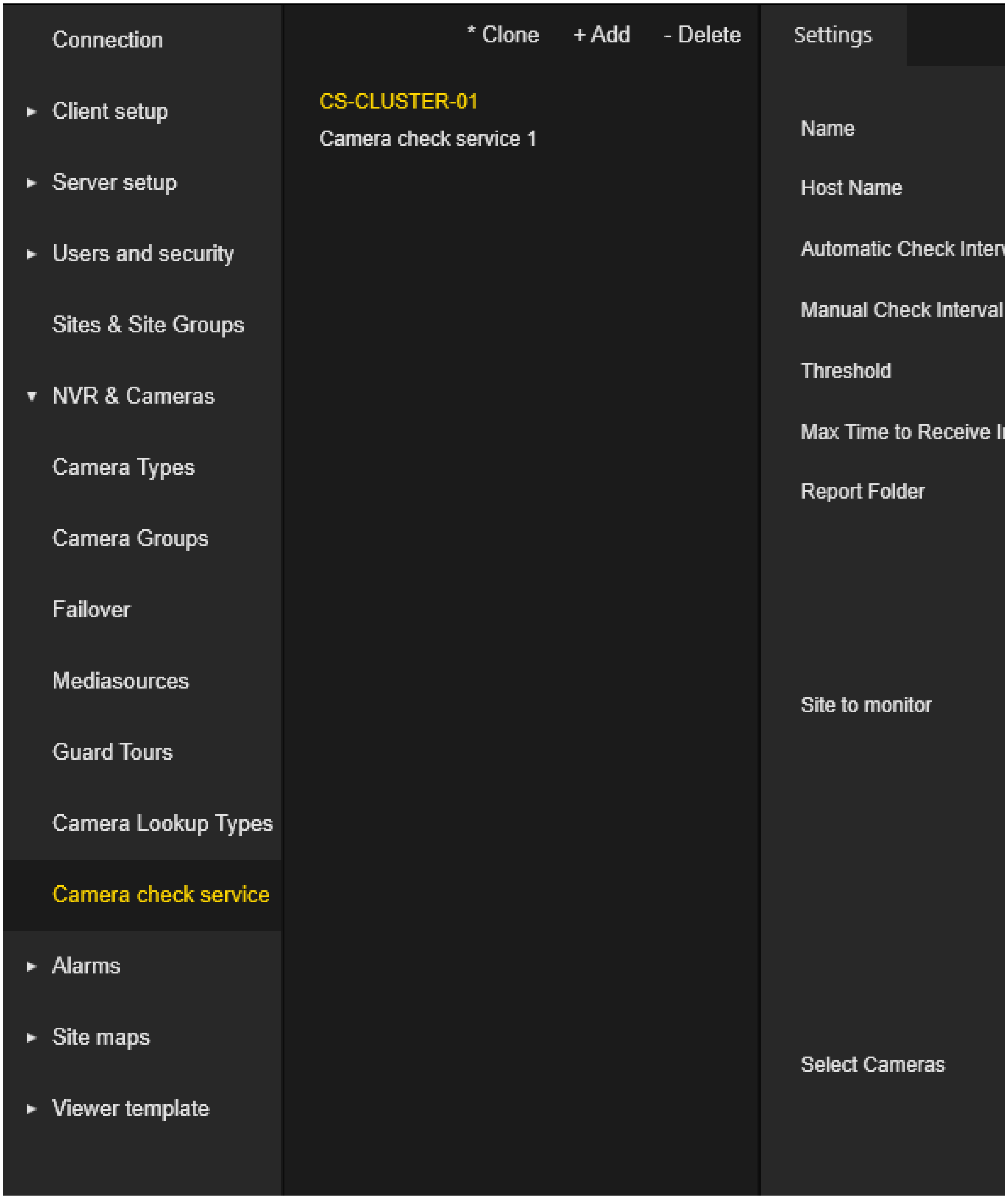
Site	Camera	Camera Group	Offset	Duration	Selected
Default Site	Channel 001	Camera Group 1	0	0	□
Default Site	CS-CLUSTER-01	Camera Group 1	0	0	□
Default Site	CS-CLUSTER-03		0	0	□
Default Site	Channel 003		0	0	□
Default Site	CS-CLUSTER-04		2	5	☑
Default Site	Channel 005		0	0	□
Default Site	CS-CLUSTER-05		1	15	☑
Default Site	Channel 006		0	0	□
Default Site	Channel 007		0	0	□
Default Site	(15)_Camera_11		0	0	□

- The administrator can click the Add button to add a new Camera Lookup Name to the camera lookup type.
- The administrator can click the Delete button to remove the selected lookup name from the camera lookup type.
- The administrator can click the selected Camera Lookup Name entry to rename it.
- The administrator can select which cameras are to be included in the selected lookup name. For selected cameras, Offset and Duration can be configured.

Camera Check Service

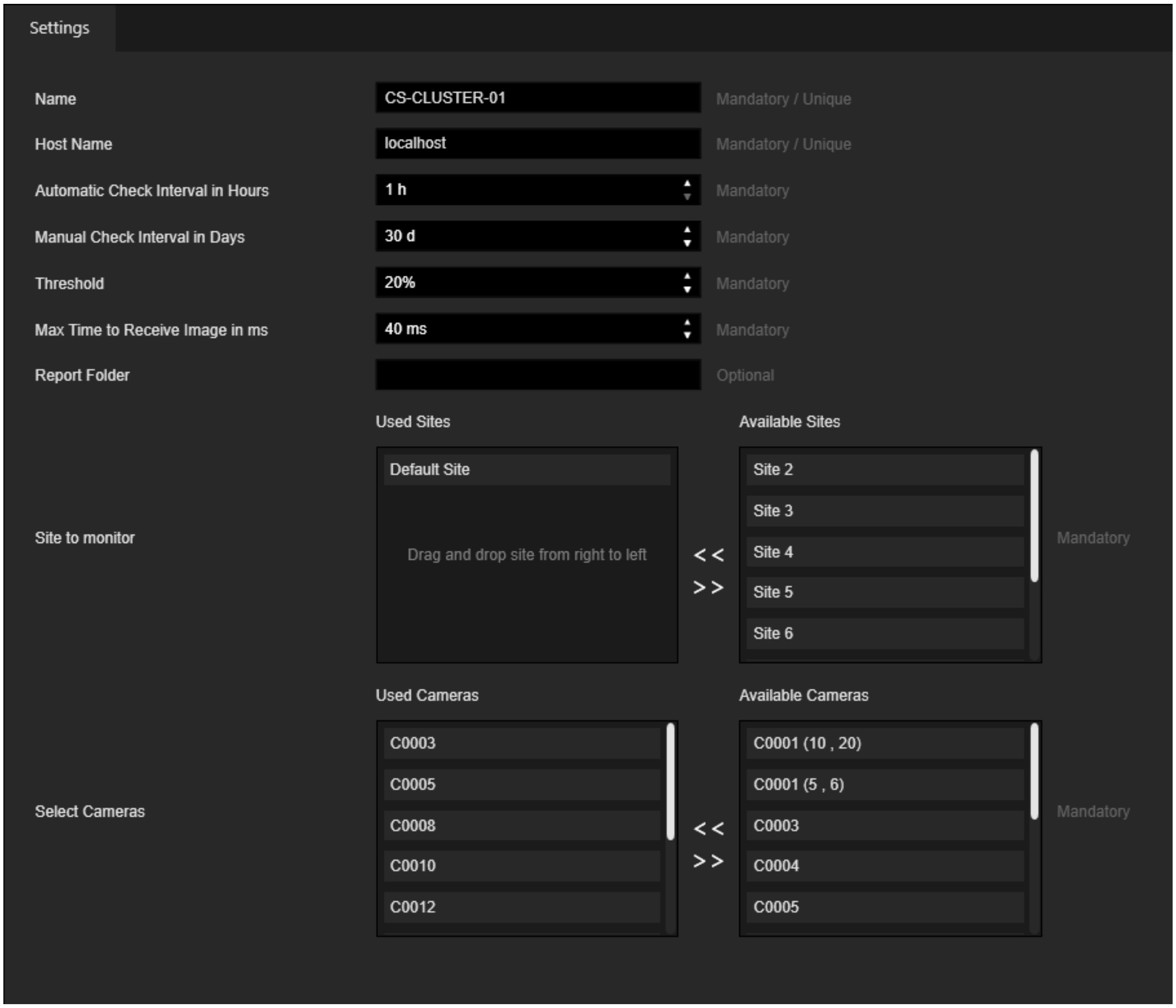
The Camera check service view contains a list of the camera check service configurations.

The Camera check service menu is enabled if a Pro version license is available.



Settings

The administrator can configure the following settings of the camera check service:



Settings

Name	CS-CLUSTER-01	Mandatory / Unique
Host Name	localhost	Mandatory / Unique
Automatic Check Interval in Hours	1 h	Mandatory
Manual Check Interval in Days	30 d	Mandatory
Threshold	20%	Mandatory
Max Time to Receive Image in ms	40 ms	Mandatory
Report Folder		Optional

Site to monitor — Mandatory

Used Sites: Default Site
Drag and drop site from right to left

Available Sites: Site 2, Site 3, Site 4, Site 5, Site 6

Select Cameras — Mandatory

Used Cameras: C0003, C0005, C0008, C0010, C0012

Available Cameras: C0001 (10 , 20), C0001 (5 , 6), C0003, C0004, C0005

Settings	Description
Name	Service name to differentiate between several service instances (only G-SIM-side, no service connection itself).
Host Name	Host name of the server where the camera check service is running.
Automatic Check Interval in Hours	Time span after which the service automatically compares the reference image with the live image.
Manual Check Interval in Days	Time span after which the camera must be manually checked by an operator (open the CCS window in the Operator Console, compare the reference image and

Settings	Description
	the live video from the camera, and then click the green or red button accordingly).
Threshold	Threshold for the CPA algorithm (between zero and one hundred percent).
Max Time to Receive Image in ms	Maximum time span for receive an image from the camera.
Report Folder	Local path of the Camera check service to the a.csv file in which the service logs events.
Site to monitor	The administrator should select sites to be monitored by the camera check service. Camera check services can be configured to allow one service per site or multiple sites to be used for one service.
Select Cameras	The administrator should select the cameras at the monitored sites to be checked by the camera check service.

Alarms

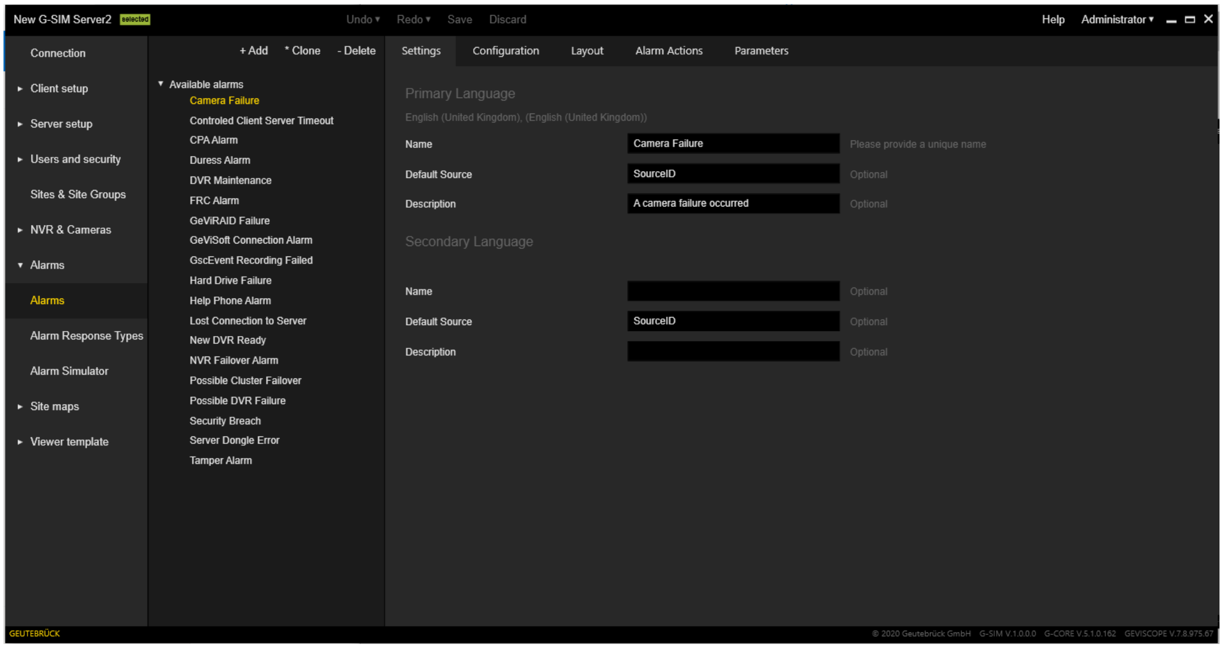
Alarms

Alarms or health event definitions are imported from the plug-ins and can be added by the user.

The settings of **Alarms** are grouped in tabs.

Settings

The administrator can specify the name, default source and description of the alarm for the primary and secondary language in the **Settings** tab.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Camera Failure — Please provide a unique name

Default Source: SourceID — Optional

Description: A camera failure occurred — Optional

Secondary Language

Name: — Optional

Default Source: SourceID — Optional

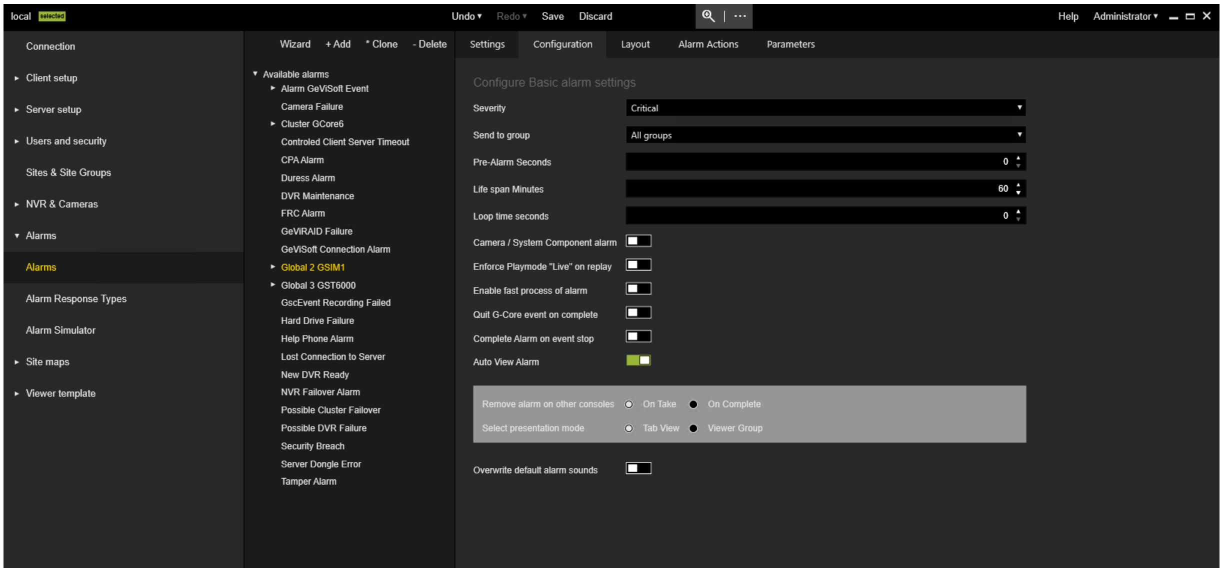
Description: — Optional

If no source data (e.g. camera etc.) is received from health agents, the default source text will be used instead. Within the source, tags can be used which are replaced by the actual data on the server side once data is received, according to the following definitions:

- {SITE} the site name
- {SITE_DESC} the site description
- {SOURCE} the media source name
- {CAMERA} the camera (media channel) name
- {CAMERA_DESC} the camera description
- {DEVICE} the device (system component) name

Configuration

The **Configuration** tab contains the following settings:



Configure Basic alarm settings

Severity: Critical ▾

Send to group: All groups ▾

Pre-Alarm Seconds: 0

Life span Minutes: 60

Loop time seconds: 0

Camera / System Component alarm □

Enforce Playmode "Live" on replay □

Enable fast process of alarm □

Quit G-Core event on complete □

Complete Alarm on event stop □

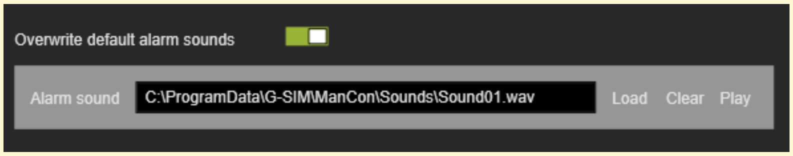
Auto View Alarm ☑

Remove alarm on other consoles ○ On Take ● On Complete

Select presentation mode ○ Tab View ● Viewer Group

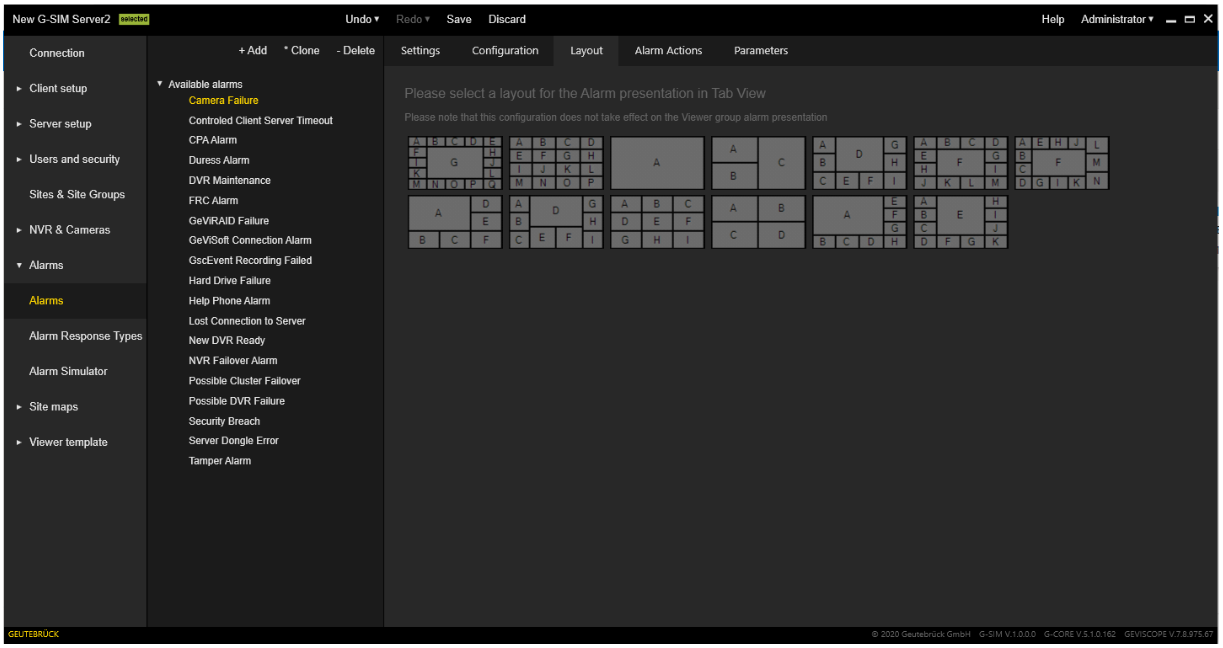
Overwrite default alarm sounds □

Settings	Description
Severity	The following levels are currently defined: **Critical**, **Non-Critical**, **Information**.
Send to Group	The user group to which alarms of this type are sent.
Pre-Alarm Seconds	The number of seconds that the video starts before the event time. This is to give operators an idea of the context in which the alarm occurred.
Life span Minutes	Time span, how long the alarm exists before it is treated as an expired event. If an alarm event is received by the server that is older than its lifespan, it is not triggered as an alarm, but is archived in the audit log. This way, auditors can still see how often the same alarm event has occurred, but the information does not clutter the operators' displays.
Loop time seconds	Duration of the alarm loop time.
Camera / System Component alarm	Select this checkbox if the primary camera that has been linked to this alarm is the cause of the alarm, such as camera failure or sync-loss.
Enforce Playmode “Live” on replay	Configure an alarm type to force the play mode to be "live" when reviewing an alarm that occurred in the past.

Settings	Description
Enable fast process of alarm	Allows to complete alarms with configured actions. The action will automatically be set to the default value.
Quit G-Core alarm on complete	Select this checkbox to quit the G-core alarm on completion.
Complete Alarm on event stop	Select this checkbox to automatically complete the G-SIM alarm when the G-Core or GeViScope event is stopped. **This setting is only available if the "Pro Version" license is available and activated (see Server Licenses).**
Auto View Alarm	Select this if this alarm is to be automatically displayed on the Operator Console when it is triggered, such as intruder alarms. You can specify the settings **Remove alarm on other consoles** and **Select presentation mode**.
Overwrite default alarm sounds	Select this to override the default sound for each alarm type independently.  Overwrite default alarm sounds ● Alarm sound C:\ProgramData\G-SIM\ManCon\Sounds\Sound01.wav

Layout

The **Layout** tab allows the user to select a default screen layout to be used for the alarm presentation in Tab view.



Please select a layout for the Alarm presentation in Tab View

Please note that this configuration does not take effect on the Viewer group alarm presentation

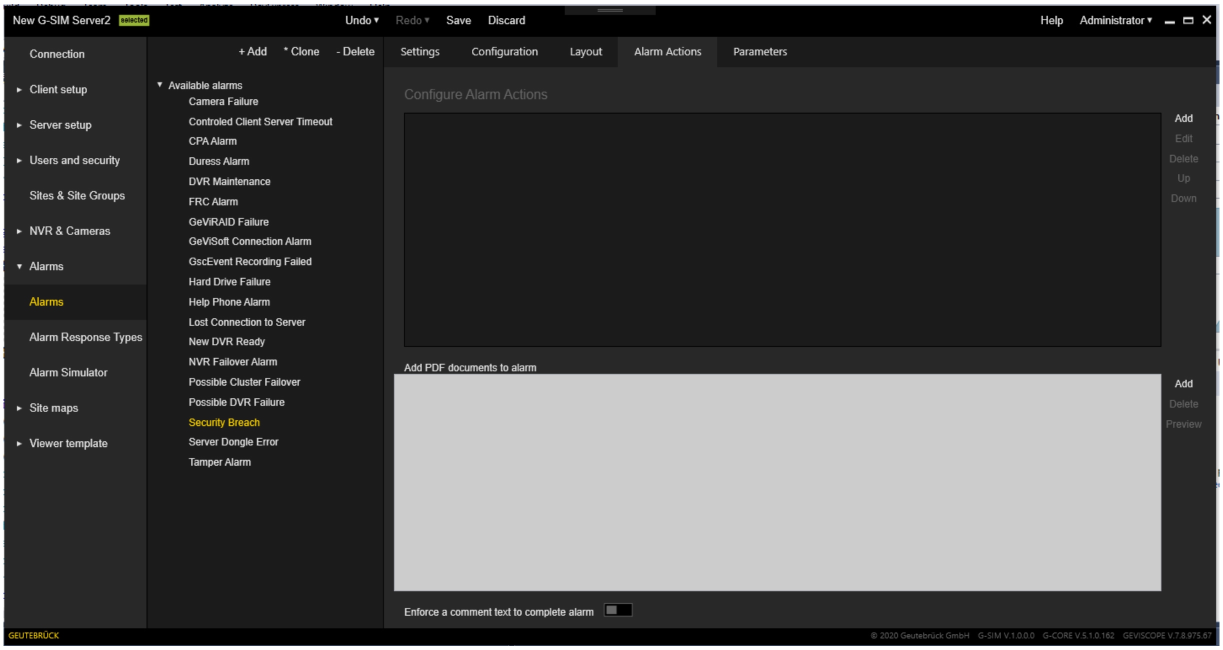
Alarm Actions

The **Alarm Actions** tab contains the actions that a user must take for taking responsibility for this alarm. G-SIM enforces these actions and allows you to define standard alarm handling procedures.

Each action has one of the following response types:

- Text
- Check box
- Choice between Yes and No
- Drop-down menu with configured Alarm Response Type
- Link to a PDF file that contains more detailed instructions

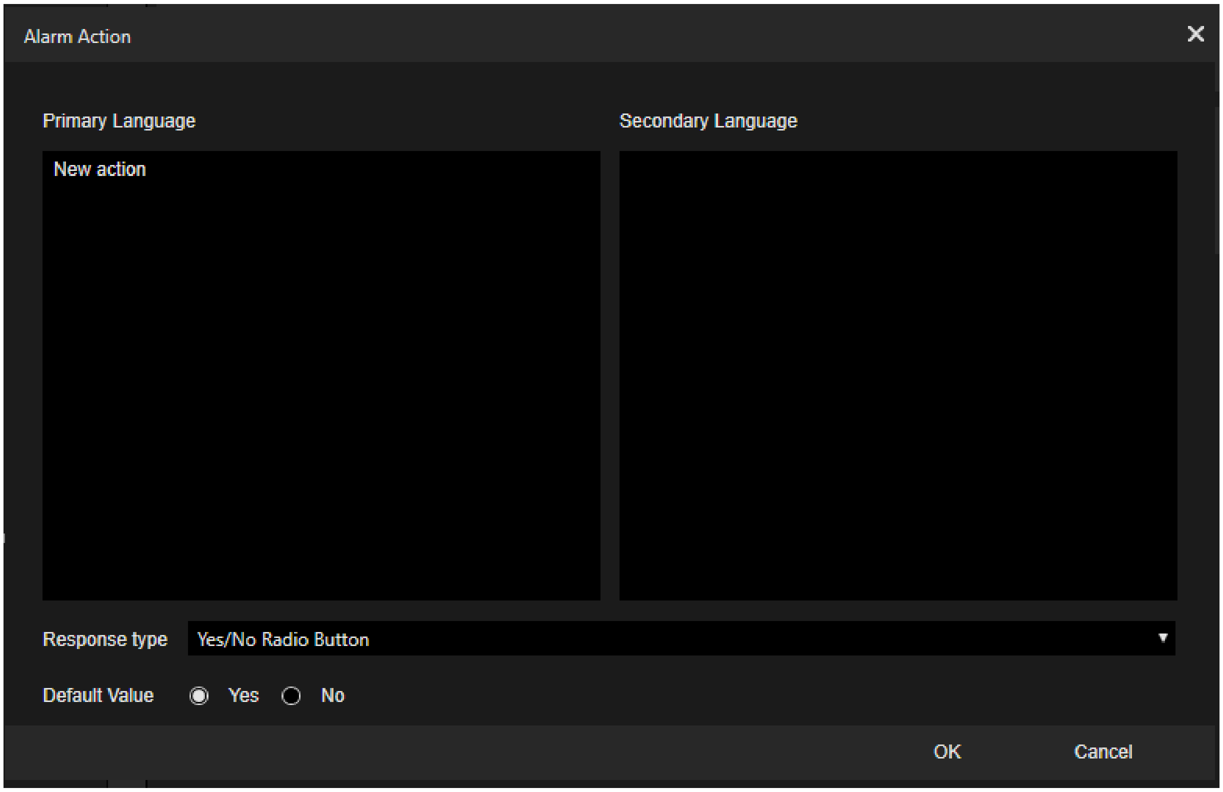
This option is available when Allow alarm expansion is activated (see System Settings).



- Use the **Add** and **Delete** buttons to add or remove actions from the list.
- The **Up** and **Down** buttons are responsible for changing the order of the actions.
- Press the **Edit** button to edit an existing action.
- **Enforce a comment text to complete alarm**: This check box is available if at least one action is added. Switch it on to restrict the alarm completion without commenting.

The pop-up window for editing the alarm action contains:

- Description of the action (for both languages)
- **Response type** selector
- **Default value** selector (depends on the selected response type)



Alarm Action

Primary Language: New action

Secondary Language:

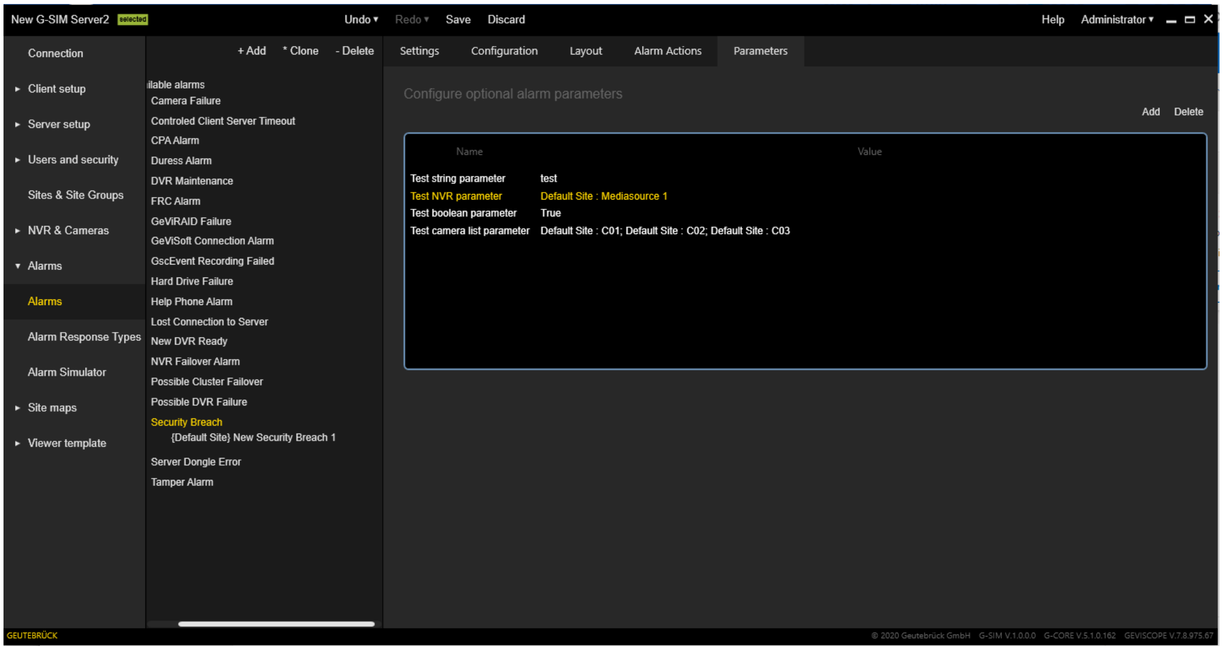
Response type: Yes/No Radio Button

Default Value: ● Yes ○ No

Parameters

The **Parameters** tab allows the user to specify additional parameters for alarms. Some predefined alarms contain parameters that should be configured.

Use the **Add** and **Delete** buttons to add and remove parameters from the list. Use a double click on a row with parameters to open the menu with the parameter editor.



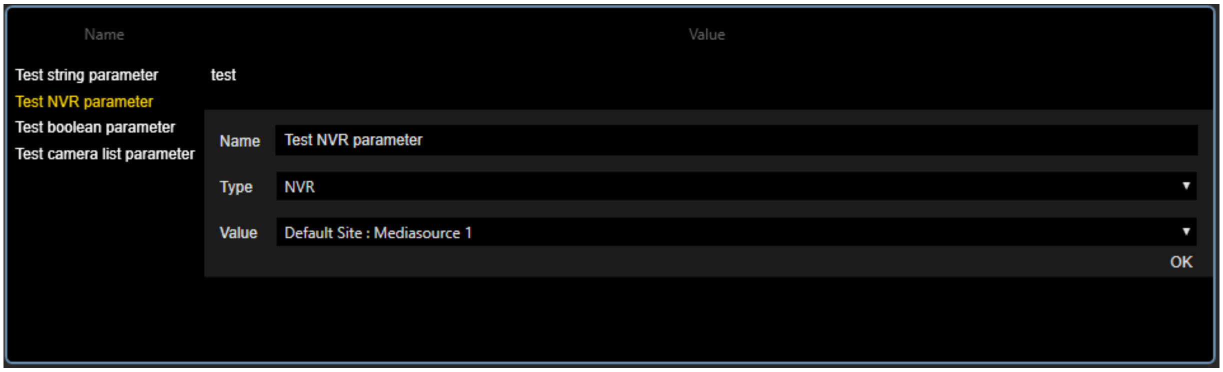
ilable alarms
Camera Failure
Controled Client Server Timeout
CPA Alarm
Duress Alarm
DVR Maintenance
FRC Alarm
GeViRAID Failure
GeViSoft Connection Alarm
GscEvent Recording Failed
Hard Drive Failure
Help Phone Alarm
Lost Connection to Server
New DVR Ready
NVR Failover Alarm
Possible Cluster Failover
Possible DVR Failure
Security Breach
{Default Site} New Security Breach 1
Server Dongle Error
Tamper Alarm

Configure optional alarm parameters

Name	Value
Test string parameter	test
Test NVR parameter	Default Site : Mediasource 1
Test boolean parameter	True
Test camera list parameter	Default Site : C01; Default Site : C02; Default Site : C03

The following parameter fields can be configured;

- Name
- Type: Specifies the data type of the parameter value. These can be basic data types (string, integer, etc.) and more complex (list of cameras, mediasource).
- Value: Parameter value that depends on its type.



Name	Value
Test string parameter	test
Test NVR parameter	
Test boolean parameter	
Test camera list parameter	

Name: Test NVR parameter

Type: NVR ▾

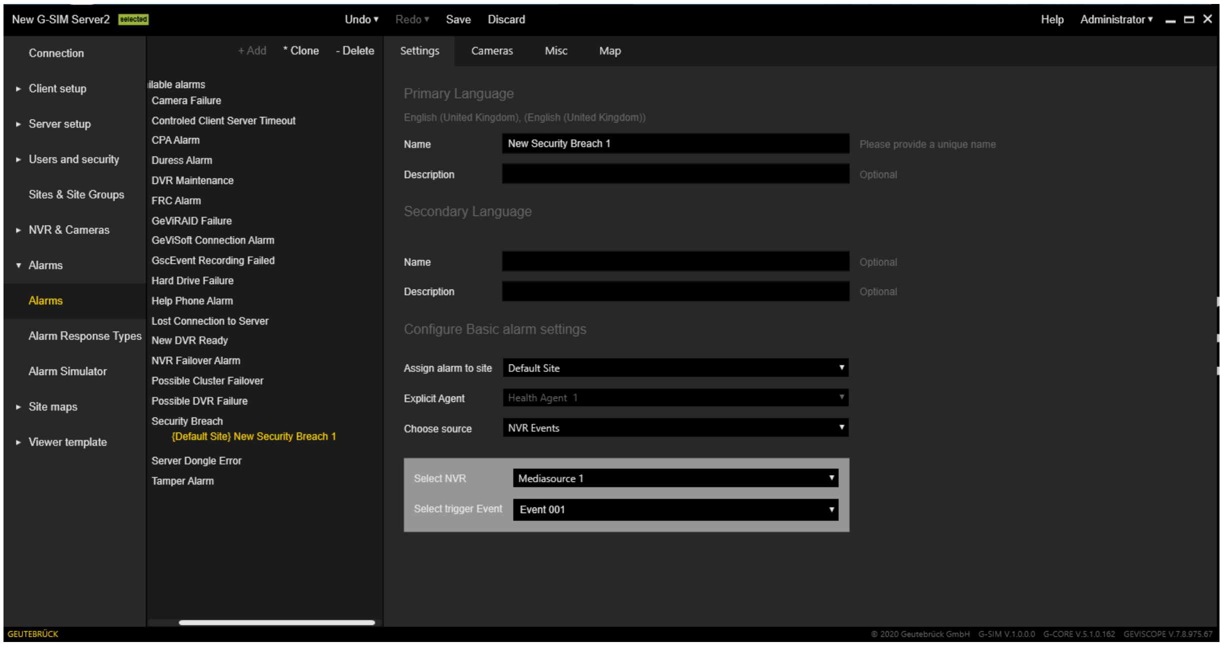
Value: Default Site : Mediasource 1 ▾

Alarm Instances

Alarm instances are added as child nodes of alarm nodes. This allows you to create various instances of the alarm type with different configurations.

Settings

The **Settings** tab contains the following settings:



Primary Language
English (United Kingdom), (English (United Kingdom))
Name: New Security Breach 1 — Please provide a unique name
Description: — Optional

Secondary Language
Name: — Optional
Description: — Optional

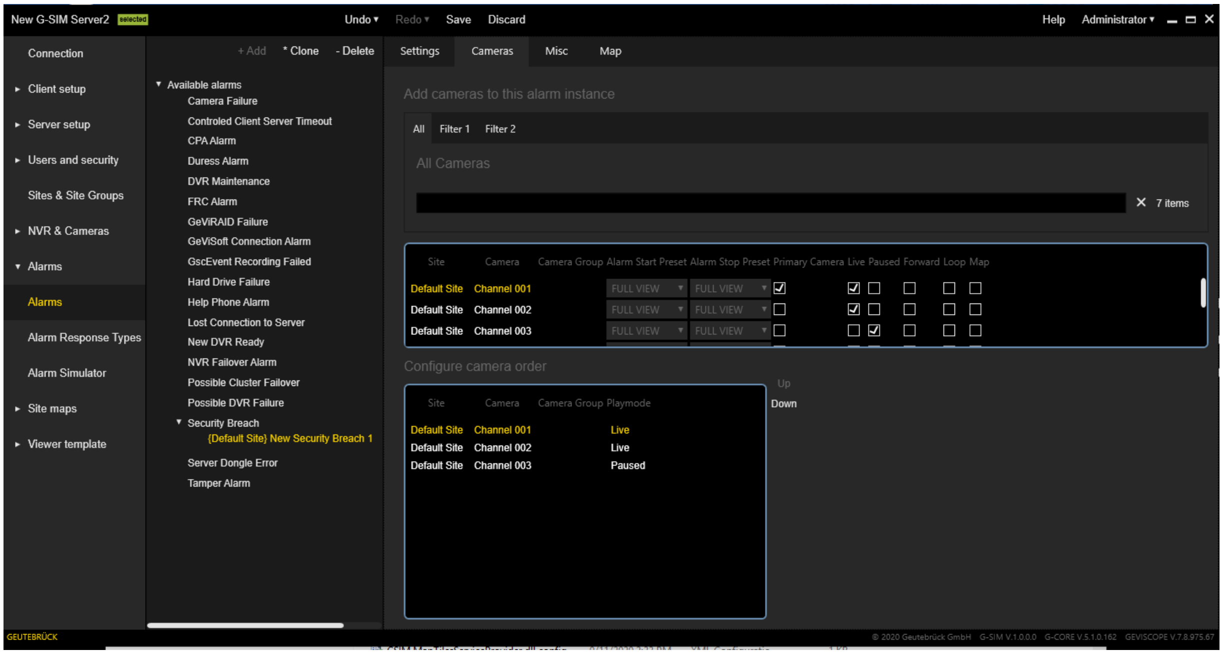
Configure Basic alarm settings
Assign alarm to site: Default Site
Explicit Agent: Health Agent 1
Choose source: NVR Events
Select NVR: Mediasource 1
Select trigger Event: Event 001

Settings	Description
Name	Name of the alarm instance for both primary and secondary languages.
Description	Description of the alarm instance for both primary and secondary languages.
Assign alarm to site	This is a drop-down menu that allows you to specify the site from which the alarm is originated. **Only sites that are configured to be monitored by an agent are available.**
Explicit Agent	Allows the user to specify which agent will be responsible for alarm handling if the site is monitored by more than one agent.
Choose source	Configures a source for an alarm. **If NVR Events is selected, available events will be retrieved from the selected mediasource.**

Cameras

The **Camera** tab allows you to configure which cameras are assigned to the current alarm instance. Specify a convenient playback mode to add cameras to the alarm instance. It is possible to select multiple playback modes of a camera.

Selected cameras with playback modes are added to the **Configure camera order** list, where the order of the cameras can be configured using the **Up** and **Down** buttons for the selected camera row.



Add cameras to this alarm instance

All · Filter 1 · Filter 2

All Cameras

✕ 7 items

Site	Camera	Camera Group	Alarm Start Preset	Alarm Stop Preset	Primary Camera	Live	Paused	Forward	Loop	Map
Default Site	Channel 001		FULL VIEW ▾	FULL VIEW ▾	☑	☑	□	□	□	□
Default Site	Channel 002		FULL VIEW ▾	FULL VIEW ▾	□	☑	□	□	□	□
Default Site	Channel 003		FULL VIEW ▾	FULL VIEW ▾	□	□	☑	□	□	□

Configure camera order

Site	Camera	Camera Group	Playmode
Default Site	Channel 001		Live
Default Site	Channel 002		Live
Default Site	Channel 003		Paused

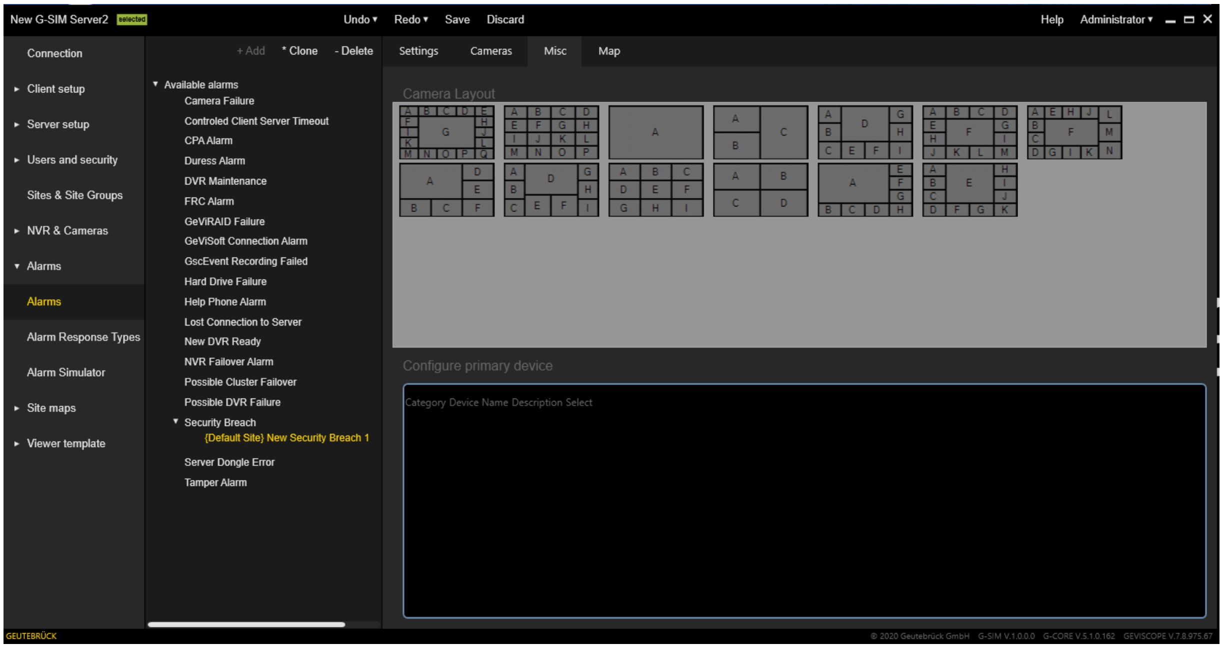
Up

Down

Misc

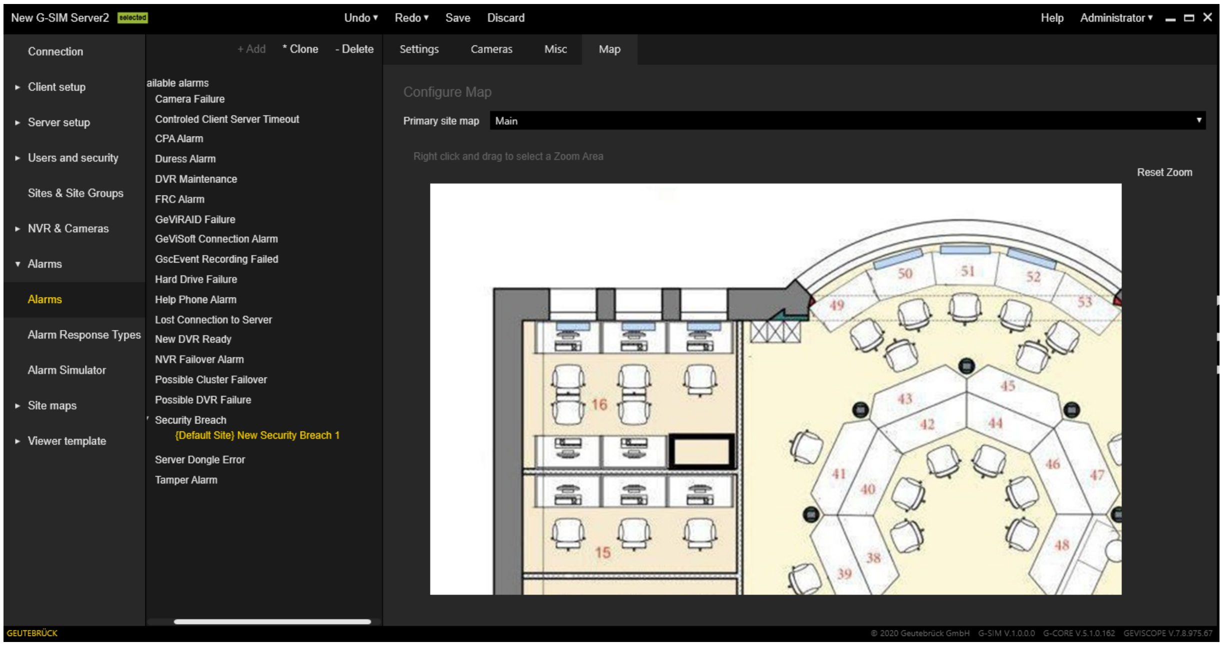
The **Misc** tab allows you to configure the following:

- **Camera Layout**: Specify the layout to overwrite the layout from the base alarm.
- **Configure primary device**: Allows to associate a selected alarm instance with a certain system component.



Map

Use the **Map** tab to specify the associated map with the zoomed area. When specified, all alarm cameras with the playback mode **Map** will display this map area.



Primary site map: Main

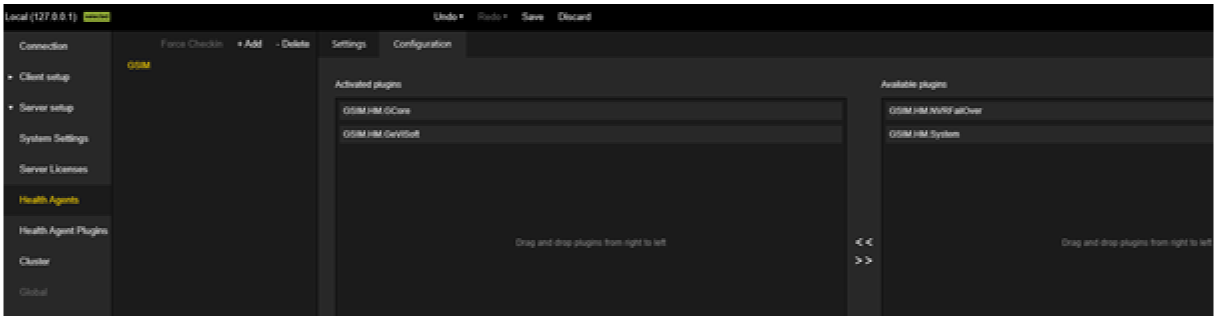
Alarm Setup Wizard

The Alarm Setup Wizard helps you to create and set up alarm templates as well as NVR and GeViSoft event-based alarm instances.

If no health agent exists in G-SIM yet, the Alarm Setup Wizard creates a new health agent, adds the default plug-ins to it, and adds all the sites to be monitored by this agent.

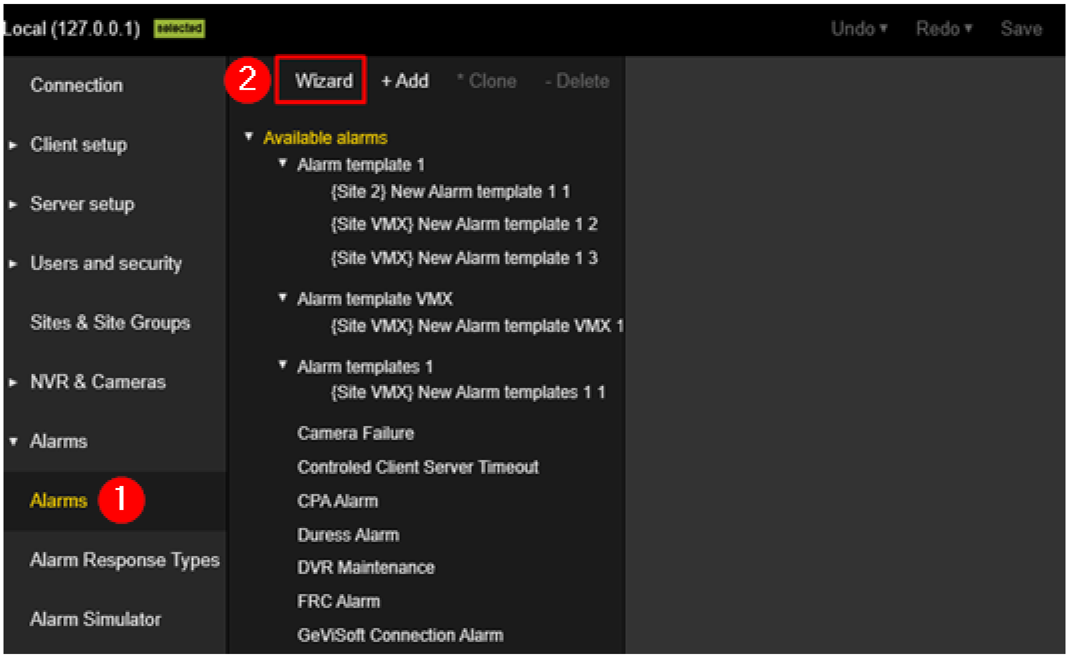
If at least one health agent already exists in G-SIM, the Alarm Setup Wizard activates the G-Core and GeViSoft default plugins for this health agent.

During its work, the Alarm Setup Wizard uses the first health agent of the "Health Agents" list as the default agent for the NVR and GeViSoft event-based alarm instances.

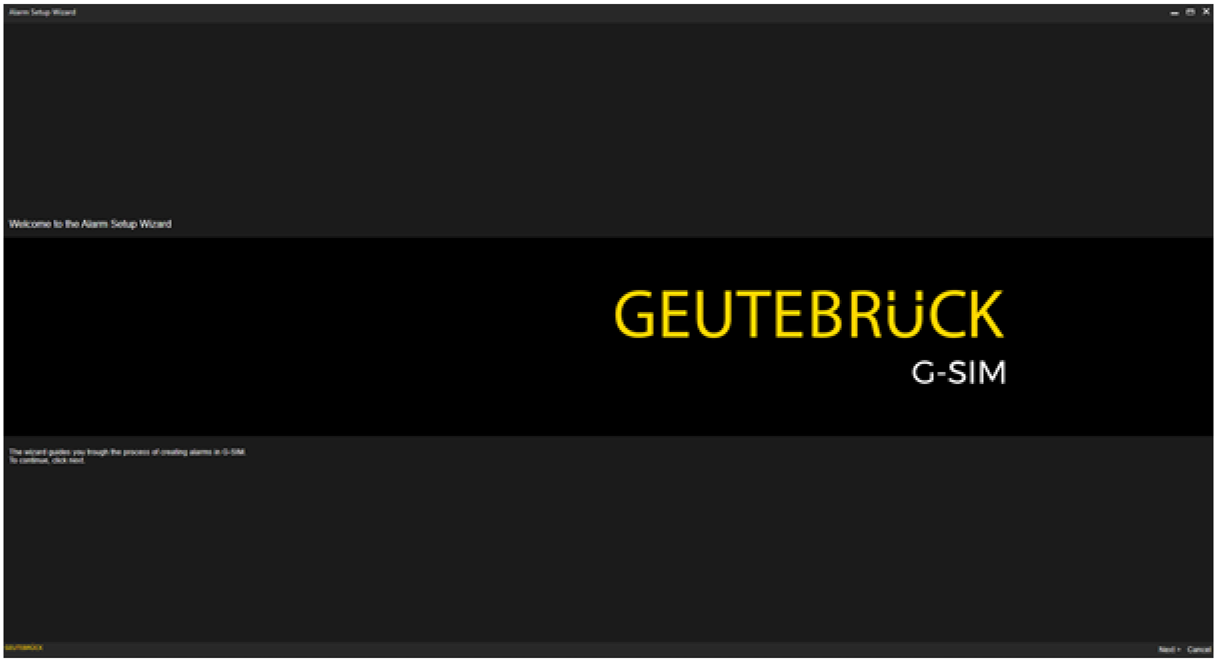


Starting the Wizard

In the **Alarms** view (1), click the **Wizard** button (2)to start the Alarm Setup Wizard.



The start page of the Alarm setup wizard opens. It contains brief information about the Alarm Setup Wizard.



Welcome to the Alarm Setup Wizard

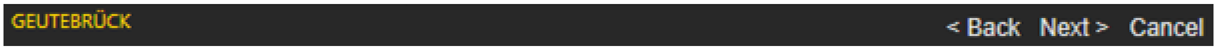
The wizard guides you trough the process of creating alarms in G-SIM.
To continue, click Next.

Click the **Next** button to continue.

Navigation in the Wizard

The Alarm Setup Wizard divides the entire process of creating and setting up alarms into simple steps. It consists of several consecutive dialog windows.

For navigation between pages, each dialog window contains the following buttons in the bottom right corner:



Name	Description
<Back	Click this button to go to the previous page.
Next >	Click this button to go to the next page.
Cancel	Click this button to close the wizard and discard the changes.

Create and Edit Alarm Templates

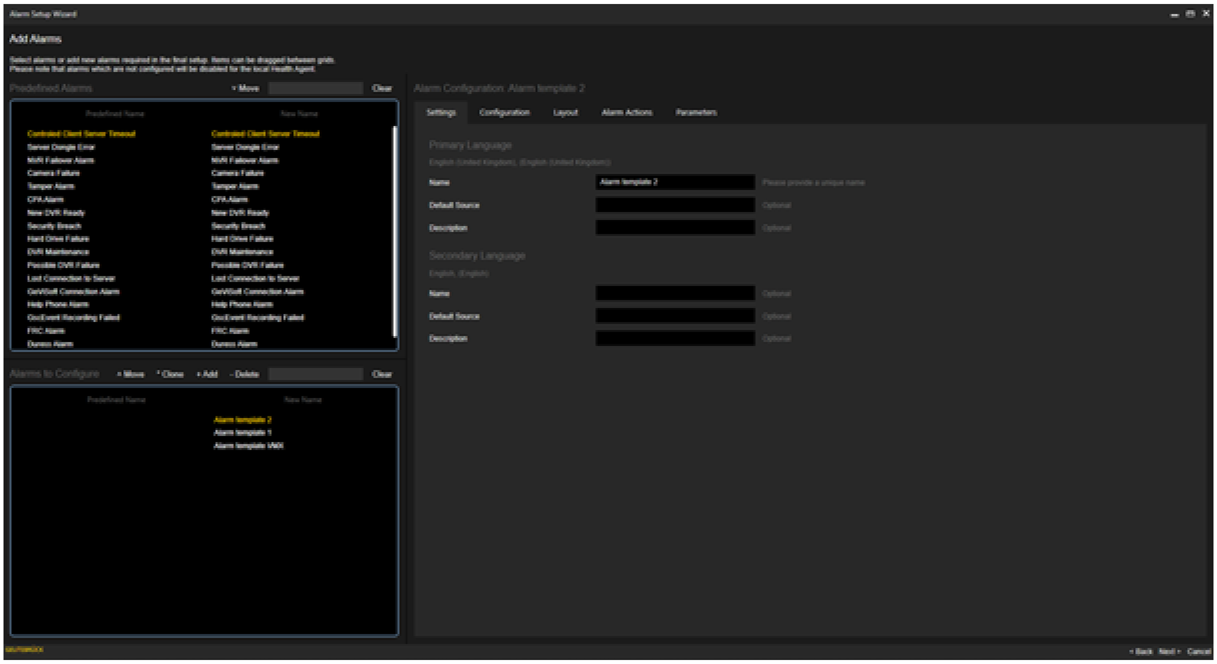
In **the Add Alarms** dialog window you can create new alarm templates or edit existing alarm templates.

Select Alarm Templates

By default, all alarm templates generated by the plugin are in the **Predefined Alarms** list. These predefined alarms are not displayed in the following dialog windows.

To be able to configure alarm templates in the following dialog windows, you have to select them. To do this, move the corresponding alarm templates to the **Alarms to Configure** list.

You can move the alarm templates between the **Alarms to Configure** and **Predefined Alarms** lists using drag and drop or the ^ **Move** and v **Move** buttons.



Select alarms or add new alarms required in the final setup. Items can be dragged between grids.
Please note that alarms which are not configured will be disabled for the local Health Agent.

Predefined Name	New Name
Controlled Client Server Timeout	Controlled Client Server Timeout
Server Dongle Error	Server Dongle Error
NVR Failover Alarm	NVR Failover Alarm
Camera Failure	Camera Failure
Tamper Alarm	Tamper Alarm
CFA Alarm	CFA Alarm
New DVR Ready	New DVR Ready
Security Breach	Security Breach
Hard Drive Failure	Hard Drive Failure
DVR Maintenance	DVR Maintenance
Possible DVR Failure	Possible DVR Failure
Lost Connection to Server	Lost Connection to Server
GeViSoft Connection Alarm	GeViSoft Connection Alarm
Help Phone Alarm	Help Phone Alarm
GscEvent Recording Failed	GscEvent Recording Failed
FRC Alarm	FRC Alarm
Duress Alarm	Duress Alarm

Predefined Name	New Name
	Alarm template 2
	Alarm template 1
	Alarm template VAX

Primary Language
English (United Kingdom), (English (United Kingdom))

Name: Alarm template 2 — Please provide a unique name
Default Source: — Optional
Description: — Optional

Secondary Language
English, (English)

Name: — Optional
Default Source: — Optional
Description: — Optional

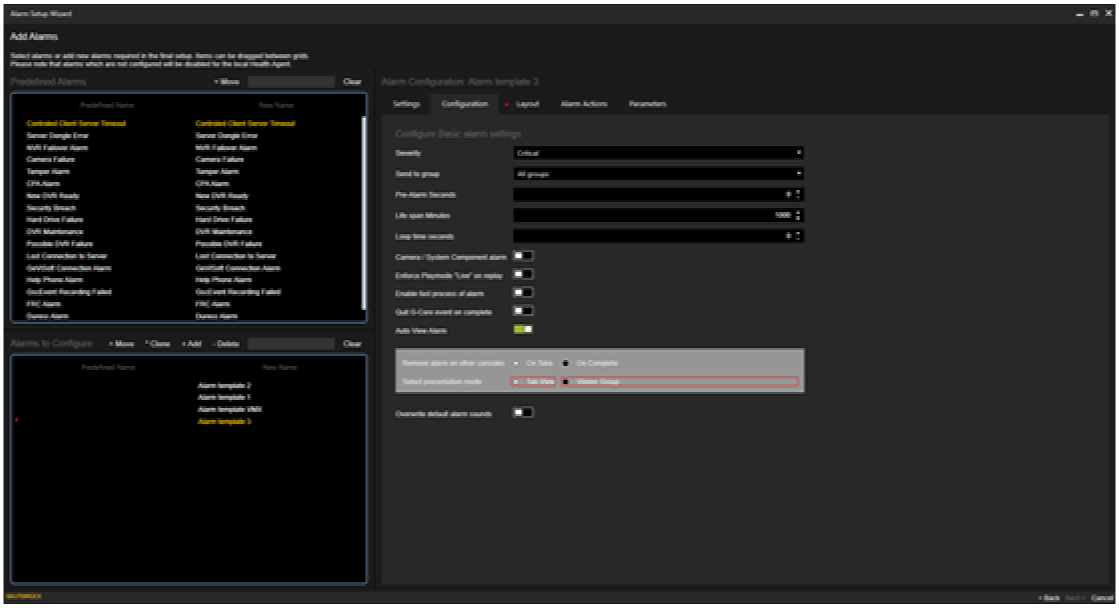
To activate the **Next >** button, at least one alarm template must be included in the **Alarms to Configure** list.

The alarm templates must not have any validation errors. If there are any validation errors, they will be displayed with a red dot at the corresponding position.

Configuring the Basic Settings

Click the **Configuration** tab and select an alarm template from the **Alarms to Configure** list.

Configure the basic settings. For the **Select presentation mode** setting, select the **Tab View** option.



Alarm Setup Wizard

Add Alarms

Select alarms or add new alarms required in the final setup. Items can be dragged between grids.
Please note that alarms which are not configured will be disabled for the local Health Agent.

Predefined Alarms

Predefined Name	New Name
Controlled Client Server Timeout	Controlled Client Server Timeout
Server Dongle Error	Server Dongle Error
NVR Failover Alarm	NVR Failover Alarm
Camera Failure	Camera Failure
Tamper Alarm	Tamper Alarm
CPA Alarm	CPA Alarm
New DVR Ready	New DVR Ready
Security Breach	Security Breach
Hard Drive Failure	Hard Drive Failure
DVR Maintenance	DVR Maintenance
Possible DVR Failure	Possible DVR Failure
Lost Connection to Server	Lost Connection to Server
GeViSoft Connection Alarm	GeViSoft Connection Alarm
Help Phone Alarm	Help Phone Alarm
GscEvent Recording Failed	GscEvent Recording Failed
FRC Alarm	FRC Alarm
Duress Alarm	Duress Alarm

Alarms to Configure

Predefined Name	New Name
	Alarm template 2
	Alarm template 1
	Alarm template VMX
	Alarm template 3

Alarm Configuration: Alarm template 3

Configure Basic alarm settings

- Severity: Critical
- Send to group: All groups
- Pre-Alarm Seconds: 0
- Life span Minutes: 1000
- Loop time seconds: 0
- Camera / System Component alarm
- Enforce Playmode "Live" on replay
- Enable fast process of alarm
- Quit G-Core event on complete
- Auto View Alarm
- Remove alarm on other consoles: ○ On Take ● On Complete
- Select presentation mode: ○ Tab View ● Viewer Group
- Overwrite default alarm sounds

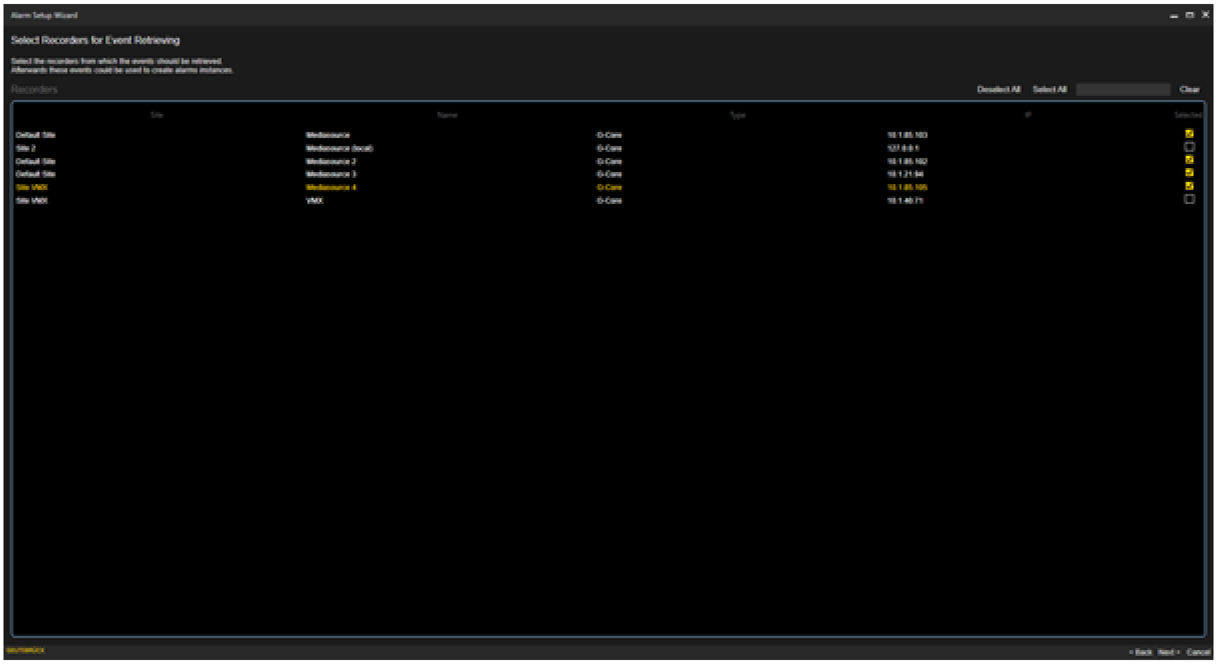
Select Layout

Click the **Layout** tab and select a layout for the alarm display in the tab view.

Select Recorders for Event Retrieving

In the **Select Recorders for Event Retrieving** dialog window, select the G-Core or GeViScope media sources (recorders) from which to retrieve events.

You can then use these events to create alarm instances.



Alarm Setup Wizard

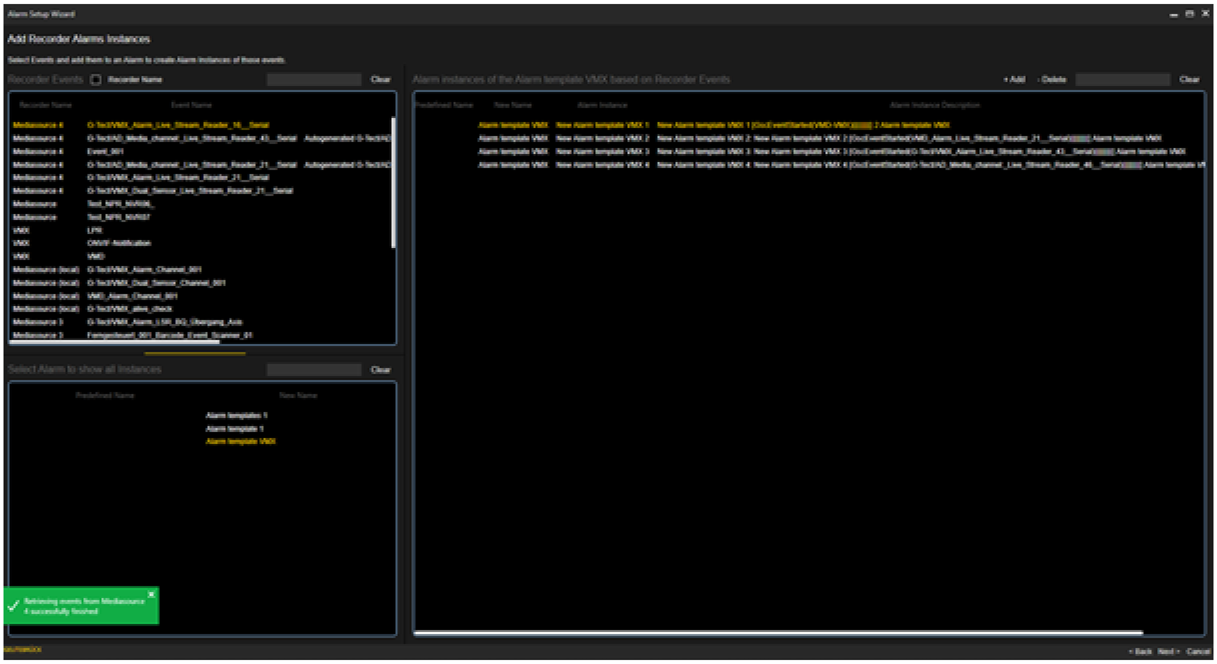
Select Recorders for Event Retrieving

Select the recorders from which the events should be retrieved.
Afterwards these events could be used to create alarms instances.

Site	Name	Type	IP	Selected
Default Site	Mediasource	G-Core	10.1.85.103	☑
Site 2	Mediasource (local)	G-Core	127.0.0.1	□
Default Site	Mediasource 2	G-Core	10.1.85.102	☑
Default Site	Mediasource 3	G-Core	10.1.21.94	☑
Site VMX	Mediasource 4	G-Core	10.1.85.105	☑
Site VMX	VMX	G-Core	10.1.40.71	□

Add Recorder Alarm Instances

In the **Add Recorder Alarms Instances** dialog window, you can create alarm instances based on recorder events.



Alarm Setup Wizard

Add Recorder Alarms Instances

Select Events and add them to an Alarm to create Alarm Instances of those events.

Recorder Name	Event Name
Mediasource 4	G-Tect/VMX_Alarm_Live_Stream_Reader_16__Serial
Mediasource 4	G-Tect/AD_Media_channel_Live_Stream_Reader_43__Serial Autogenerated G-Tect/AD
Mediasource 4	Event_001
Mediasource 4	G-Tect/AD_Media_channel_Live_Stream_Reader_21__Serial Autogenerated G-Tect/AD
Mediasource 4	G-Tect/VMX_Alarm_Live_Stream_Reader_21__Serial
Mediasource 4	G-Tect/VMX_Dual_Sensor_Live_Stream_Reader_21__Serial
Mediasource	Test_NPR_NVR06_
Mediasource	Test_NPR_NVR07
VMX	LPR
VMX	ONVIF-Notification
VMX	VMD
Mediasource (local)	G-Tect/VMX_Alarm_Channel_001
Mediasource (local)	G-Tect/VMX_Dual_Sensor_Channel_001
Mediasource (local)	VMD_Alarm_Channel_001
Mediasource (local)	G-Tect/VMX_alive_check
Mediasource 3	G-Tect/VMX_Alarm_LSR_BG_Übergang_Axis
Mediasource 3	Fernglasfeuer_001_Barcode_Event_Scanner_01

Predefined Name	New Name
	Alarm templates 1
	Alarm template 1
	Alarm template VMX

Alarm instances of the Alarm template VMX based on Recorder Events
+ Add
- Delete
Clear

Predefined Name	New Name	Alarm Instance	Alarm Instance Description
	Alarm template VMX	New Alarm template VMX 1	New Alarm template VMX 1 [GscEventStarted(VMD-VMX[illegible]] 2 Alarm template VMX
	Alarm template VMX	New Alarm template VMX 2	New Alarm template VMX 2: New Alarm template VMX 2 [GscEventStarted(VMD_Alarm_Live_Stream_Reader_21__Serial[illegible] Alarm template VMX
	Alarm template VMX	New Alarm template VMX 3	New Alarm template VMX 3: New Alarm template VMX 3 [GscEventStarted(G-Tect/VMX_Alarm_Live_Stream_Reader_43__Serial[illegible] Alarm template VMX
	Alarm template VMX	New Alarm template VMX 4	New Alarm template VMX 4: New Alarm template VMX 4 [GscEventStarted(G-Tect/AD_Media_channel_Live_Stream_Reader_46__Serial[illegible] Alarm template VI

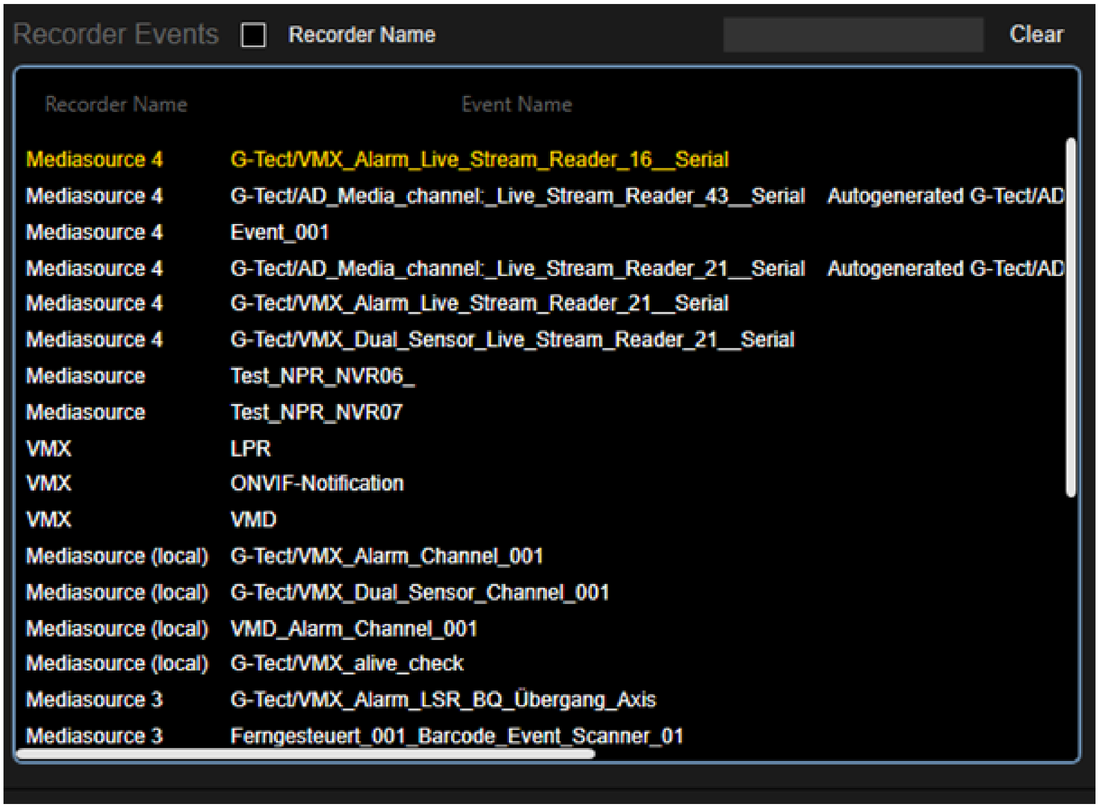
Retrieving events from Mediasource 4 successfully finished

The dialog window consists of the following three lists:

Recorder Events

The **Recorder Events** list contains the events retrieved from the selected G-Core or GeViScope media sources (recorders).

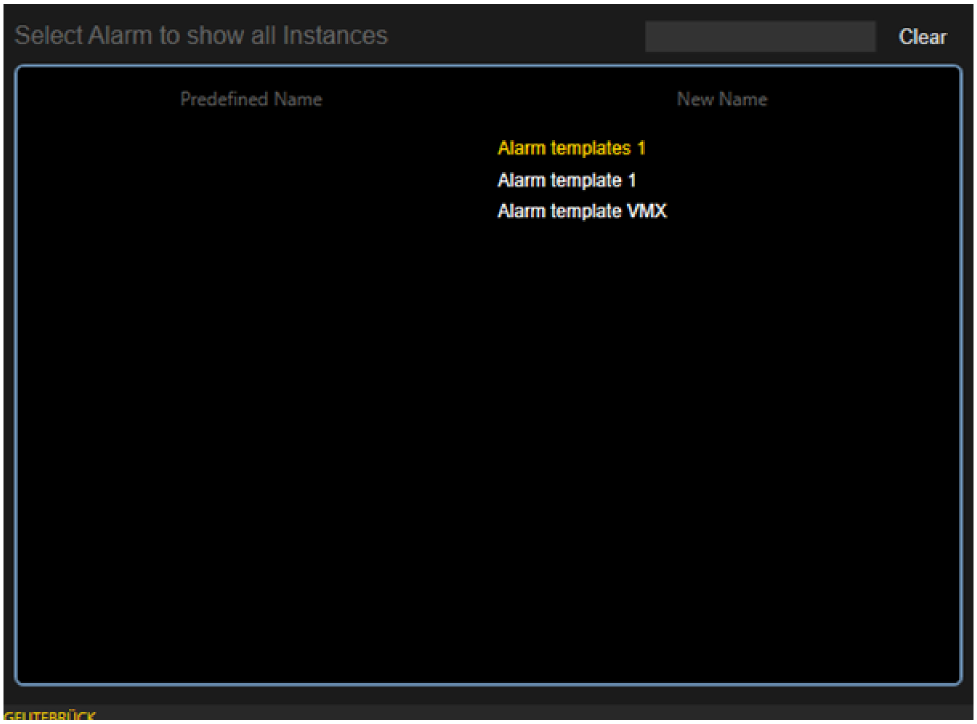
You can group the events by recorder name or filter by events using the search bar.



Recorder Name	Event Name	
Mediasource 4	G-Tect/VMX_Alarm_Live_Stream_Reader_16__Serial	
Mediasource 4	G-Tect/AD_Media_channel:_Live_Stream_Reader_43__Serial	Autogenerated G-Tect/AD
Mediasource 4	Event_001	
Mediasource 4	G-Tect/AD_Media_channel:_Live_Stream_Reader_21__Serial	Autogenerated G-Tect/AD
Mediasource 4	G-Tect/VMX_Alarm_Live_Stream_Reader_21__Serial	
Mediasource 4	G-Tect/VMX_Dual_Sensor_Live_Stream_Reader_21__Serial	
Mediasource	Test_NPR_NVR06_	
Mediasource	Test_NPR_NVR07	
VMX	LPR	
VMX	ONVIF-Notification	
VMX	VMD	
Mediasource (local)	G-Tect/VMX_Alarm_Channel_001	
Mediasource (local)	G-Tect/VMX_Dual_Sensor_Channel_001	
Mediasource (local)	VMD_Alarm_Channel_001	
Mediasource (local)	G-Tect/VMX_alive_check	
Mediasource 3	G-Tect/VMX_Alarm_LSR_BQ_Übergang_Axis	
Mediasource 3	Ferngesteuert_001_Barcode_Event_Scanner_01	

Select Alarm to show all Instances

The list **Select Alarm to show all Instances** contains all configurable alarm templates.



Select Alarm to show all Instances

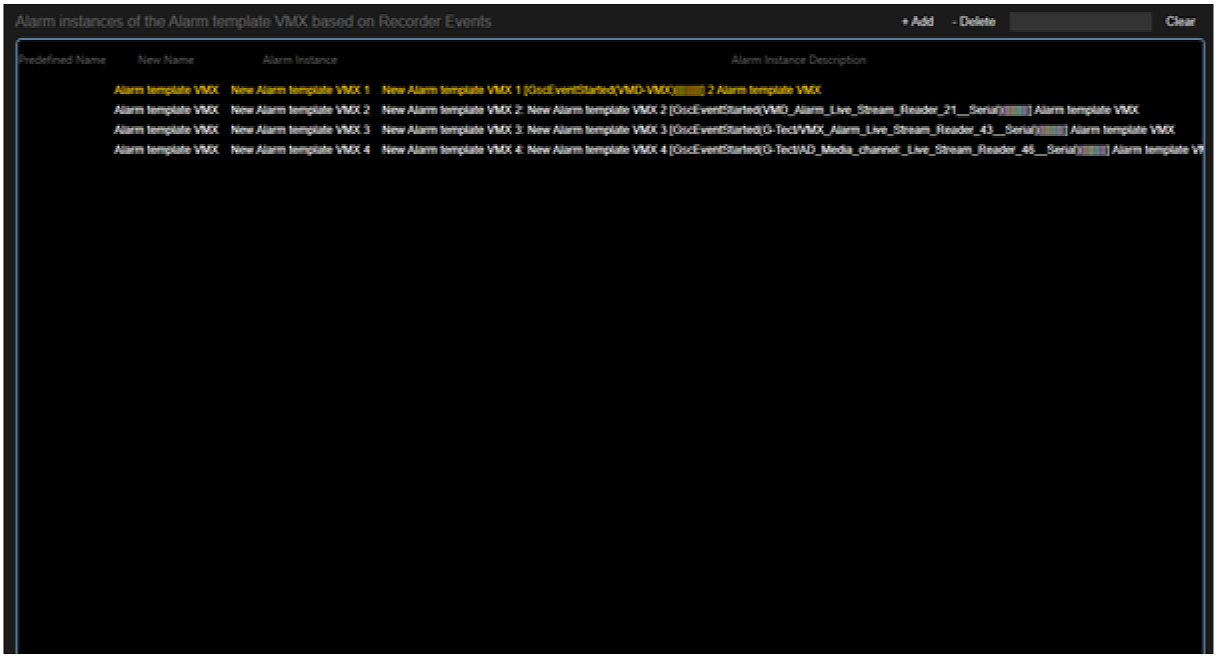
Clear

Predefined Name	New Name
	Alarm templates 1
	Alarm template 1
	Alarm template VMX

Alarm instances of the Alarm template based on Recorder Events

The list **Alarm instances of the Alarm template based on Recorder Events** contains the alarm instances of the selected alarm template based on recorder events.

Events used in the alarm instances of the selected alarm template are not displayed in the list of recorder events.



Alarm instances of the Alarm template VMX based on Recorder Events

Predefined Name	New Name	Alarm Instance	Alarm Instance Description
Alarm template VMX	New Alarm template VMX 1	New Alarm template VMX 1 [GscEventStarted(VMD-VMX)[redacted] 2 Alarm template VMX	
Alarm template VMX	New Alarm template VMX 2	New Alarm template VMX 2: New Alarm template VMX 2 [GscEventStarted(VMD_Alarm_Live_Stream_Reader_21__Serial()[redacted]] Alarm template VMX	
Alarm template VMX	New Alarm template VMX 3	New Alarm template VMX 3: New Alarm template VMX 3 [GscEventStarted(G-Tect/VMX_Alarm_Live_Stream_Reader_43__Serial()[redacted]] Alarm template VMX	
Alarm template VMX	New Alarm template VMX 4	New Alarm template VMX 4: New Alarm template VMX 4 [GscEventStarted(G-Tect/AD_Media_channel:_Live_Stream_Reader_46__Serial()[redacted]] Alarm template V	

Create Alarm Instances

To create new alarm instances for a selected alarm template, you must select an alarm template and add events:

1. Select an alarm template from the **Select Alarm to show all Instances** list.

2. Filter the **Recorder Events** list for the events you want to add to the list of alarm instances.

3. Add the selected events to the **Alarm instances of the Alarm template based on Recorder Events** list by clicking the **+ Add** button or by drag and drop.

> **To delete alarm instances for the selected alarm template, drag and drop the selected alarm instances to the Recorder Events list or click the - Delete button.**

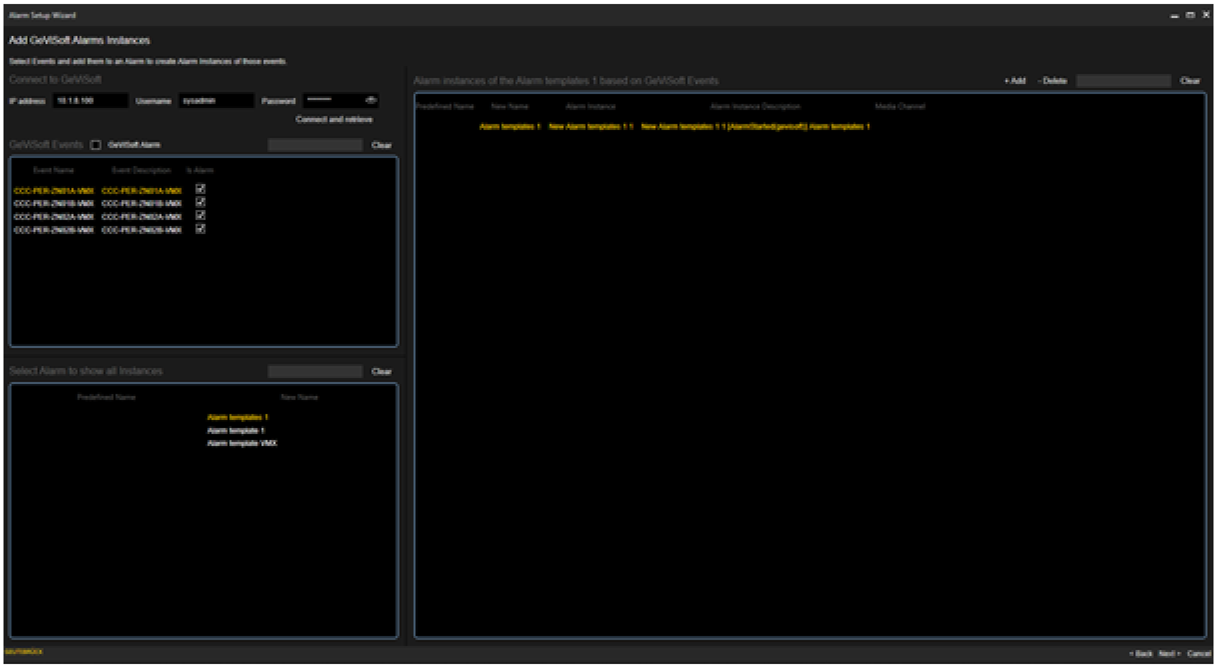
The cameras associated with the particular event are added to the alarm instance. The primary camera of the event is added to the alarm instance as the primary camera. Also, the live playback mode for this camera is set. Additional cameras are added with Live and Pause playback modes.

If more than one agent is monitoring the location of the selected event media source, alarm instances are created for each agent. If no agent is monitoring the location of the selected event media source, the first agent's list of monitored locations is expanded to include the location of the selected event media source, and an alarm instance is created for that agent.

The G-Core default plugin is added to each agent for which an alarm instance is created.

Add GeViSoft Alarm Instances

In the **Add GeViSoft Alarm Instances** dialog window, you can create GeViSoft event-based or alarm-based alarm instances.



Add GeViSoft Alarms Instances

Select Events and add them to an Alarm to create Alarm instances of those events.

Connect to GeViSoft

IP address: 10.1.6.100 Username: sysadmin Password: ••••••

Connect and retrieve

GeViSoft Events ☐ GeViSoft Alarm

Event Name	Event Description	Is Alarm
CCC-PER-ZN01A-VMX	CCC-PER-ZN01A-VMX	☑
CCC-PER-ZN01B-VMX	CCC-PER-ZN01B-VMX	☑
CCC-PER-ZN02A-VMX	CCC-PER-ZN02A-VMX	☑
CCC-PER-ZN02B-VMX	CCC-PER-ZN02B-VMX	☑

Select Alarm to show all Instances

Predefined Name	New Name
	Alarm templates 1
	Alarm template 1
	Alarm template VMX

Alarm instances of the Alarm templates 1 based on GeViSoft Events

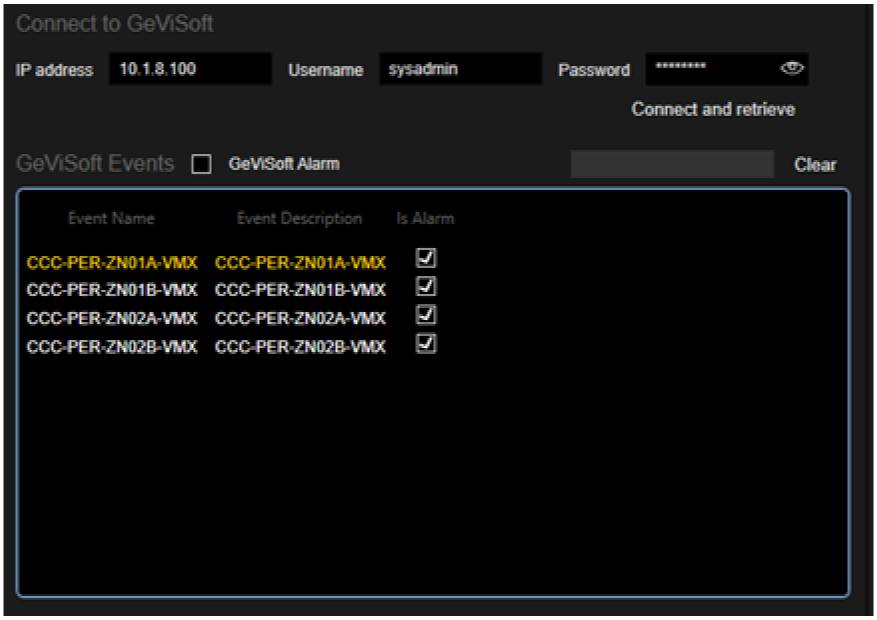
Predefined Name	New Name	Alarm Instance	Alarm Instance Description	Media Channel
Alarm templates 1	New Alarm templates 1 1	New Alarm templates 1 1 [AlarmStarted(gevisoft)] Alarm templates 1		

The dialog window consists of the following three lists:

GeViSoft Events

The **GeViSoft Events** list contains all events and alarms retrieved from the connected GeViSoft server.

You can group the list by alarms or events as well as filter by alarms or events using the search bar.



Connect to GeViSoft

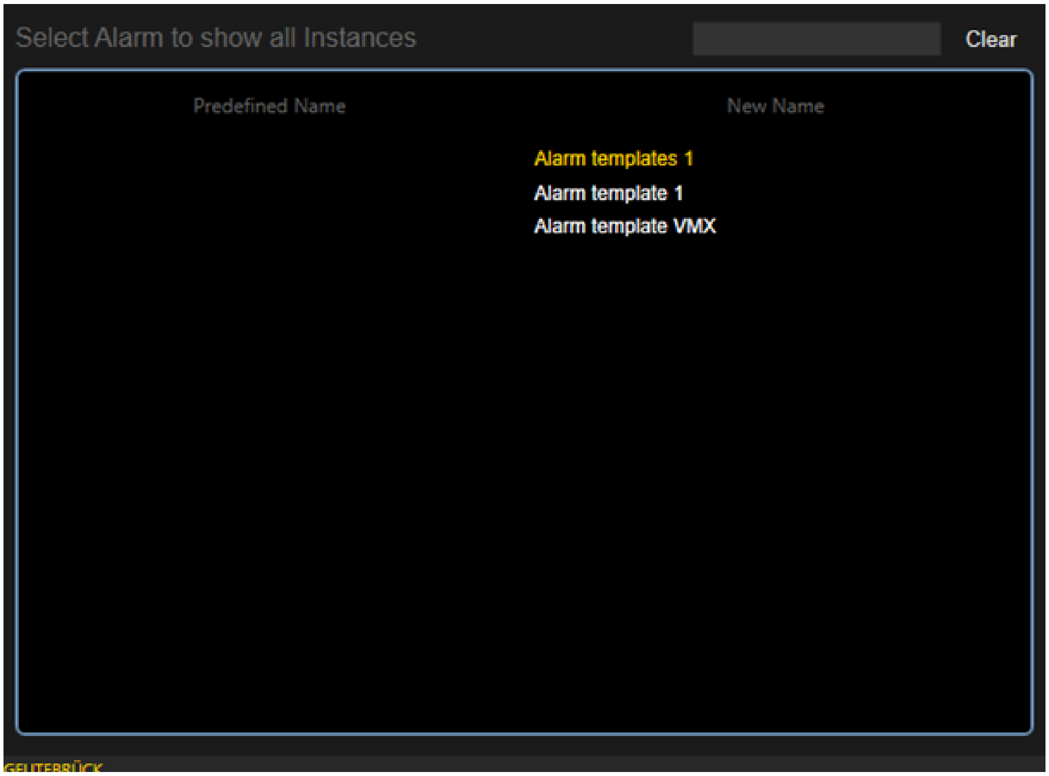
IP address 10.1.8.100 Username sysadmin Password *********

GeViSoft Events ☐ GeViSoft Alarm

Event Name	Event Description	Is Alarm
CCC-PER-ZN01A-VMX	CCC-PER-ZN01A-VMX	☑
CCC-PER-ZN01B-VMX	CCC-PER-ZN01B-VMX	☑
CCC-PER-ZN02A-VMX	CCC-PER-ZN02A-VMX	☑
CCC-PER-ZN02B-VMX	CCC-PER-ZN02B-VMX	☑

Select Alarm to show all instances

The **Select Alarm to show all instances** list contains all configurable alarm templates.



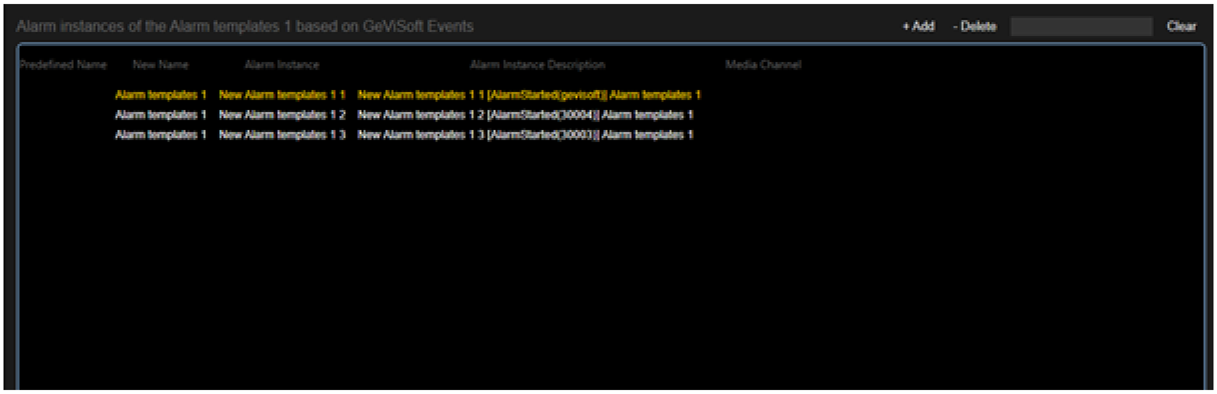
Select Alarm to show all Instances

Predefined Name New Name

Alarm templates 1
Alarm template 1
Alarm template VMX

Alarm instances of the Alarm template based on GeViSoft Events

The **Alarm instances of the Alarm template based on GeViSoft Events** list contains the GeViSoft event-based or alarm-based alarm instances of the selected alarm template. Events or alarms that are used in the alarm instances of the selected alarm template are not displayed in this list.



Alarm instances of the Alarm templates 1 based on GeViSoft Events

Predefined Name	New Name	Alarm Instance	Alarm Instance Description	Media Channel
	Alarm templates 1	New Alarm templates 1 1	New Alarm templates 1 1 [AlarmStarted(gevisoft)] Alarm templates 1	
	Alarm templates 1	New Alarm templates 1 2	New Alarm templates 1 2 [AlarmStarted(30004)] Alarm templates 1	
	Alarm templates 1	New Alarm templates 1 3	New Alarm templates 1 3 [AlarmStarted(30003)] Alarm templates 1	

Create Alarm Instances

To create new alarm instances for a selected alarm template, you must select an alarm template and add events or alarms:

1. Select an alarm template from the **Select Alarm to show all Instances** list.

2. Filter the **GeViSoft Events** list for the events or alarms you want to add to the list of alarm instances.

3. Add the selected events to the **Alarm instances of the Alarm template based on GeViSoft Events** list by clicking the **+ Add** button or by drag and drop.

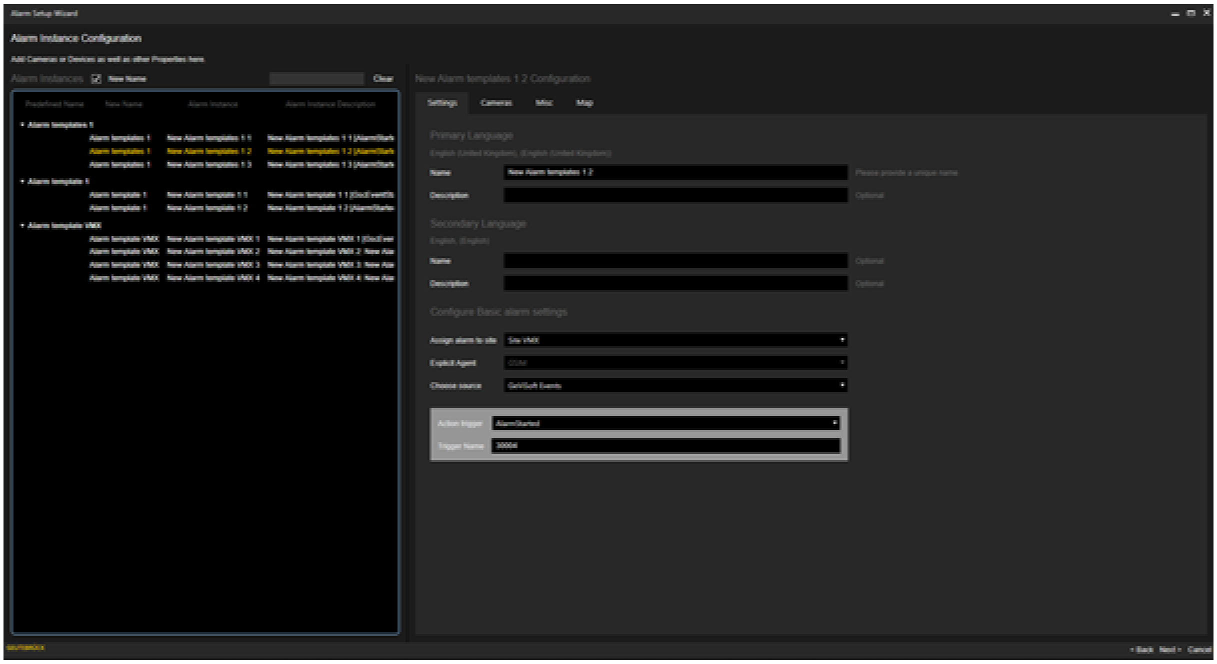
To delete alarm instances for the selected alarm template, drag and drop the selected alarm instances to the GeViSoft Events list or click the - Delete button.

The created alarm instance is associated with the first agent and the first monitored location of this agent.

Configuration of the Alarm Instances

In the **Alarm Instance Configuration** dialog window you can configure the created alarm instances.

To do this, select an alarm instance from the **Alarm Instances** list. You can group the list by the alarm template names as well as filter it using the search bar.



Alarm Setup Wizard

Alarm Instance Configuration

Add Cameras or Devices as well as other Properties here.

Alarm Instances ☑ New Name Clear

Predefined Name	New Name	Alarm Instance	Alarm Instance Description
▾ Alarm templates 1			
	Alarm templates 1	New Alarm templates 1 1	New Alarm templates 1 1 [AlarmStart
	Alarm templates 1	New Alarm templates 1 2	New Alarm templates 1 2 [AlarmStart
	Alarm templates 1	New Alarm templates 1 3	New Alarm templates 1 3 [AlarmStart
▾ Alarm template 1			
	Alarm template 1	New Alarm template 1 1	New Alarm template 1 1 [GscEventS
	Alarm template 1	New Alarm template 1 2	New Alarm template 1 2 [AlarmStarte
▾ Alarm template VMX			
	Alarm template VMX	New Alarm template VMX 1	New Alarm template VMX 1 [GscEver
	Alarm template VMX	New Alarm template VMX 2	New Alarm template VMX 2 : New Ala
	Alarm template VMX	New Alarm template VMX 3	New Alarm template VMX 3 : New Ala
	Alarm template VMX	New Alarm template VMX 4	New Alarm template VMX 4 : New Ala

New Alarm templates 1 2 Configuration

Primary Language

English (United Kingdom), (English (United Kingdom))

Name: New Alarm templates 1 2 — Please provide a unique name

Description: — Optional

Secondary Language

English, (English)

Name: — Optional

Description: — Optional

Configure Basic alarm settings

Assign alarm to site: Site VMX

Explicit Agent: GSIM

Choose source: GeViSoft Events

Action trigger: AlarmStarted

Trigger Name: 3000#

The Next > button is disabled if an alarm instance has validation errors.

Finishing the wizard

When you have finished the configuration, the last page of the wizard opens. Click the **Finish** button to close the wizard and apply the changes made to the current G-SIM setup.

Alarm Setup Completed ✓

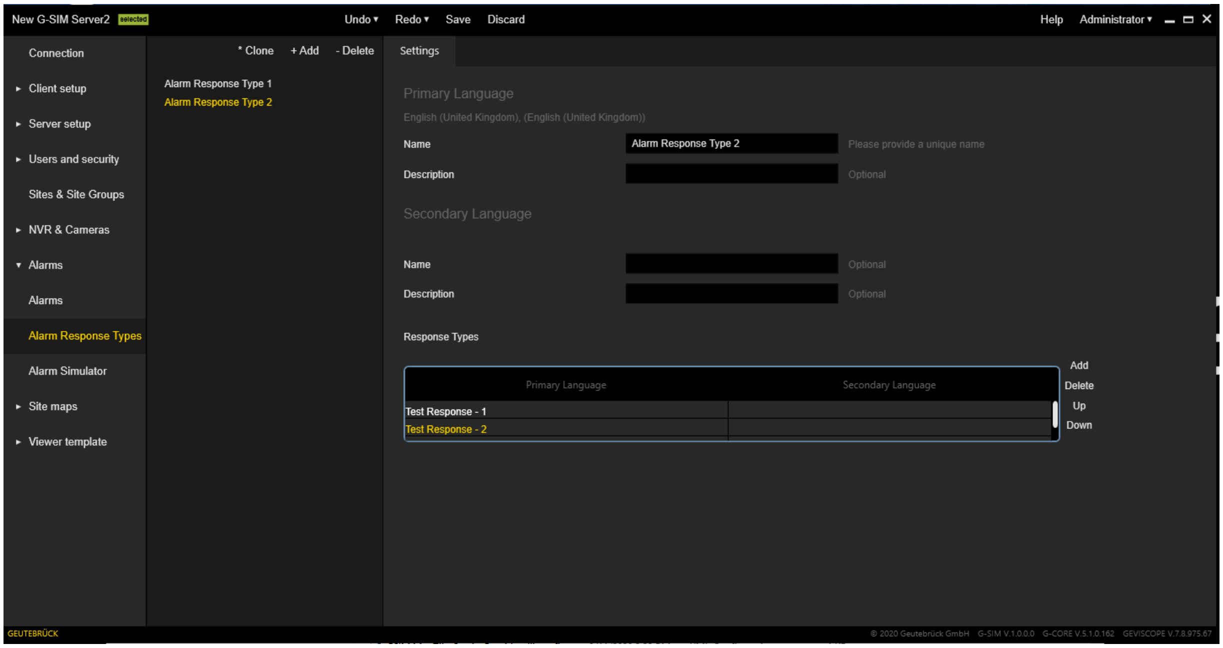
You have successfully completed the wizard.
To close this wizard, click finish.

Alarm Response Type

The Alarm Response Types are useful to make the processing of alarms more transparent and comprehensible.

Settings

The **Settings** tab allows you to configure the following:



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Alarm Response Type 2 — Please provide a unique name

Description: — Optional

Secondary Language

Name: — Optional

Description: — Optional

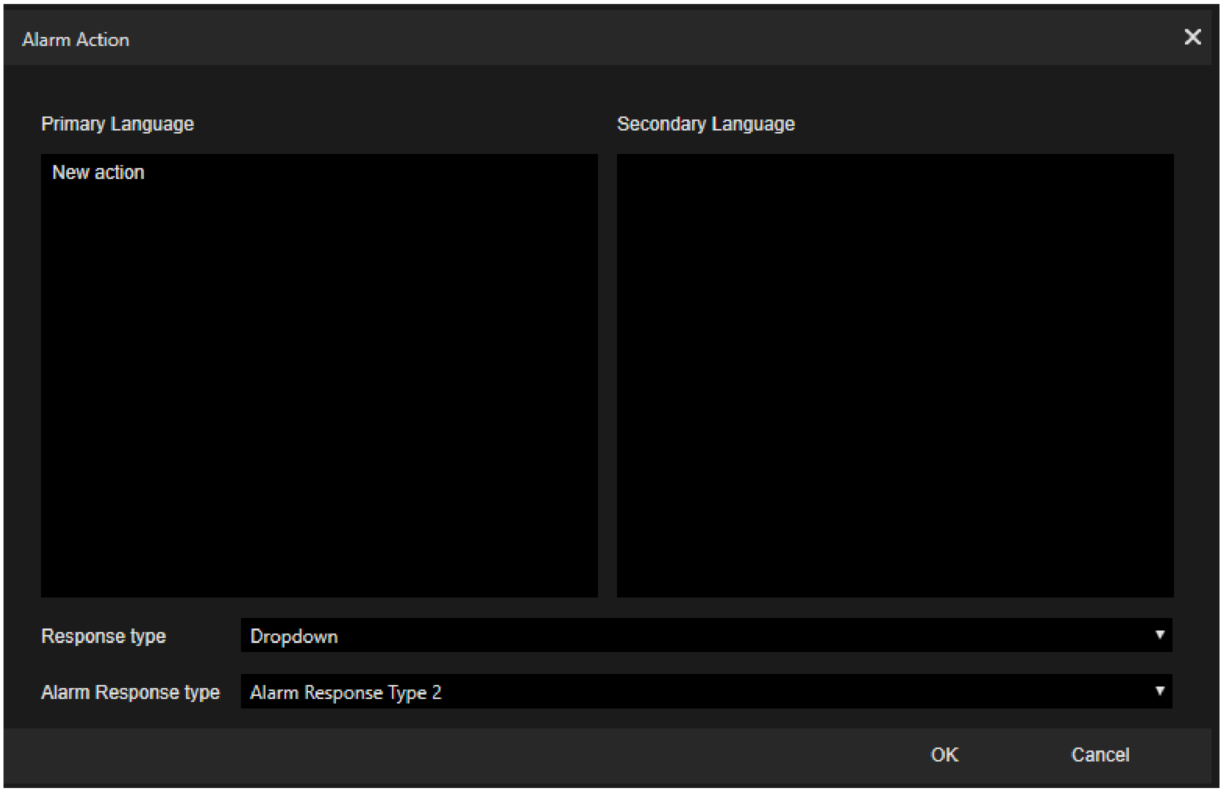
Response Types

Primary Language	Secondary Language
Test Response - 1	
Test Response - 2	

© 2020 Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67

Settings	Description
Name	Name of the alarm instance for both primary and secondary languages.
Description	Description of the alarm instance for both primary and secondary languages.
Response Types	This is a list of responses that are assigned to the selected Alarm response type. Use the **Add** or **Delete** buttons to add or remove responses from the list, and the **Up** or **Down** buttons to change the order of responses in the list. Once the response row is added, it can be edited in the appropriate cell (primary and secondary language columns).

The configured alarm response type is used as a list of response values for the alarm action if its type is Dropdown:



Alarm Action

Primary Language: New action

Secondary Language:

Response type: Dropdown

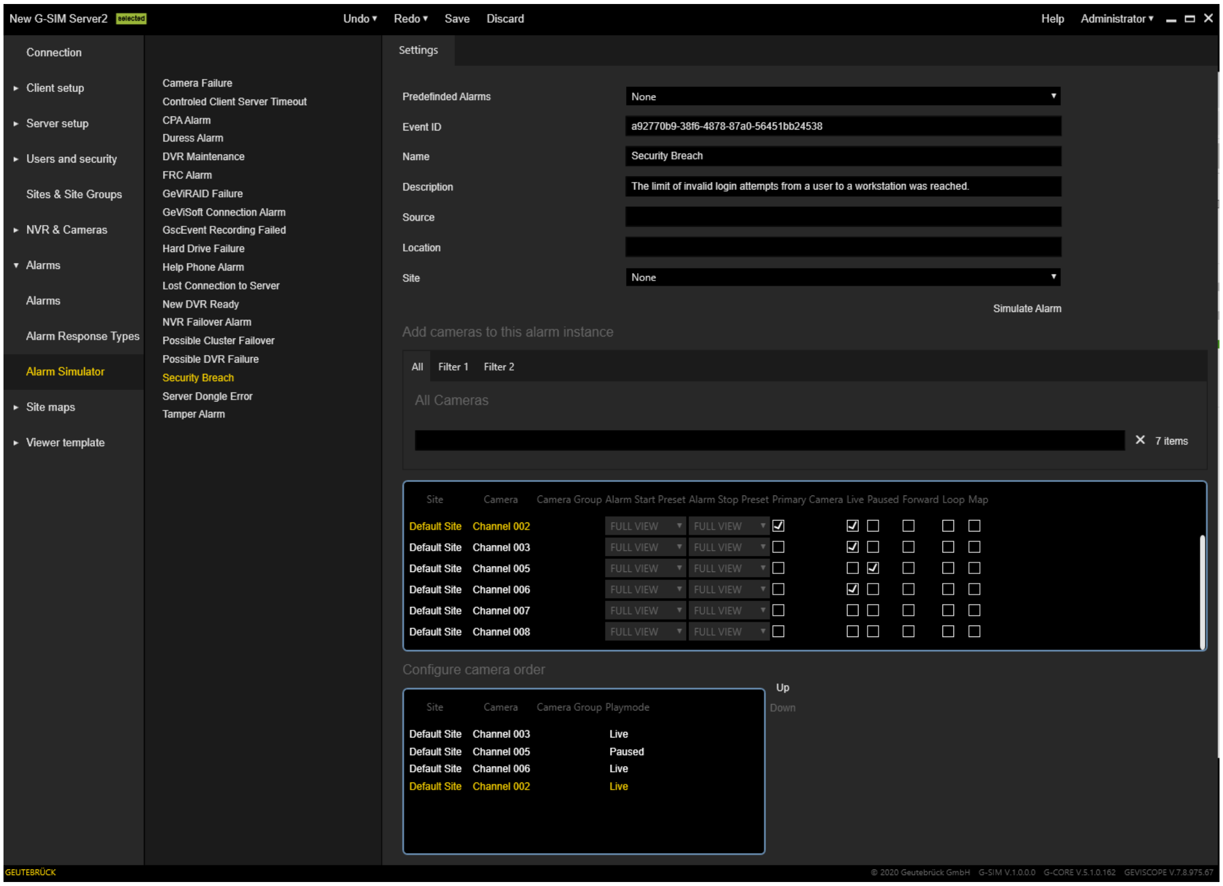
Alarm Response type: Alarm Response Type 2

Alarm Simulator

The **Alarm Simulator** simulates a Health Agent and generates a desired alarm with user-defined properties. The alarm is then sent to the connected G-SIM server. The list of available alarms is the same as the alarms in the alarms list.

It is possible to configure cameras with play modes and camera order for the generated alarm. Use filter tabs to find required cameras from the list.

Once the alarm is configured, press the **Simulate Alarm** button to send the alarm to the server.



Predefinded Alarms	None ▾
Event ID	a92770b9-38f6-4878-87a0-56451bb24538
Name	Security Breach
Description	The limit of invalid login attempts from a user to a workstation was reached.
Source	
Location	
Site	None ▾

Site	Camera	Camera Group	Alarm Start Preset	Alarm Stop Preset	Primary Camera	Live	Paused	Forward	Loop	Map
Default Site	Channel 002		FULL VIEW ▾	FULL VIEW ▾	☑	☑	□	□	□	□
Default Site	Channel 003		FULL VIEW ▾	FULL VIEW ▾	□	☑	□	□	□	□
Default Site	Channel 005		FULL VIEW ▾	FULL VIEW ▾	□	□	☑	□	□	□
Default Site	Channel 006		FULL VIEW ▾	FULL VIEW ▾	□	☑	□	□	□	□
Default Site	Channel 007		FULL VIEW ▾	FULL VIEW ▾	□	□	□	□	□	□
Default Site	Channel 008		FULL VIEW ▾	FULL VIEW ▾	□	□	□	□	□	□

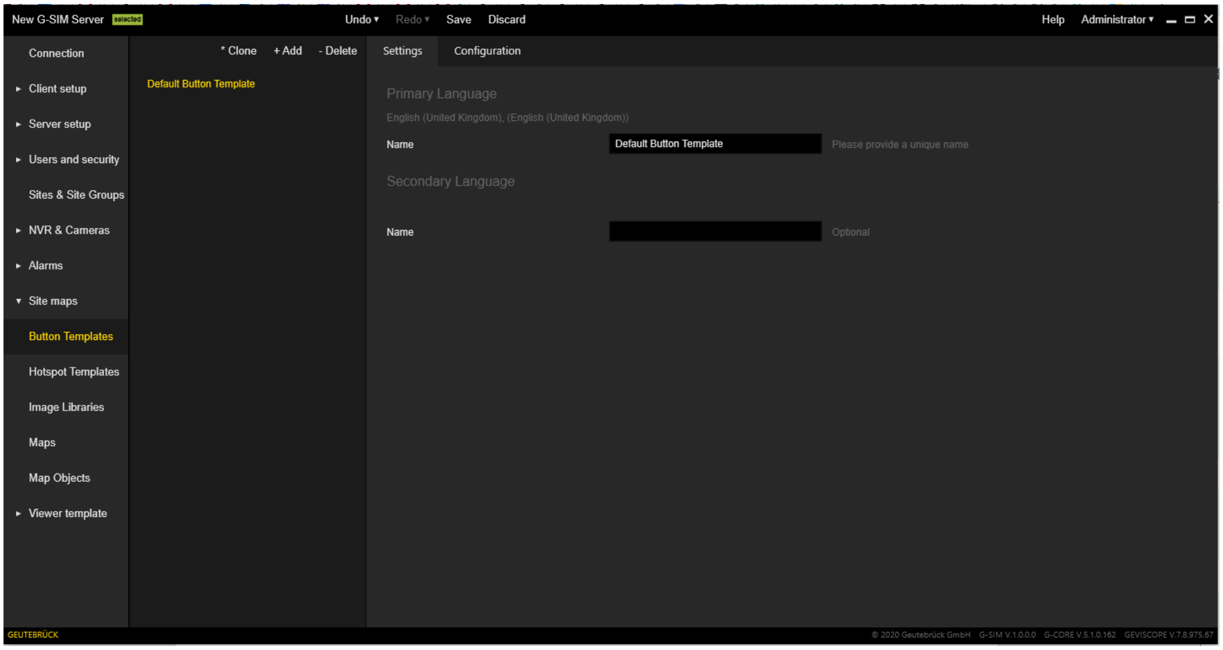
Site	Camera	Camera Group	Playmode
Default Site	Channel 003		Live
Default Site	Channel 005		Paused
Default Site	Channel 006		Live
Default Site	Channel 002		Live

Site Maps

Button Templates

Settings

The **Settings** tab contains the setting of the name for the primary and secondary language. This allows you to specify a name for the selected button template.



Primary Language

English (United Kingdom), (English (United Kingdom))

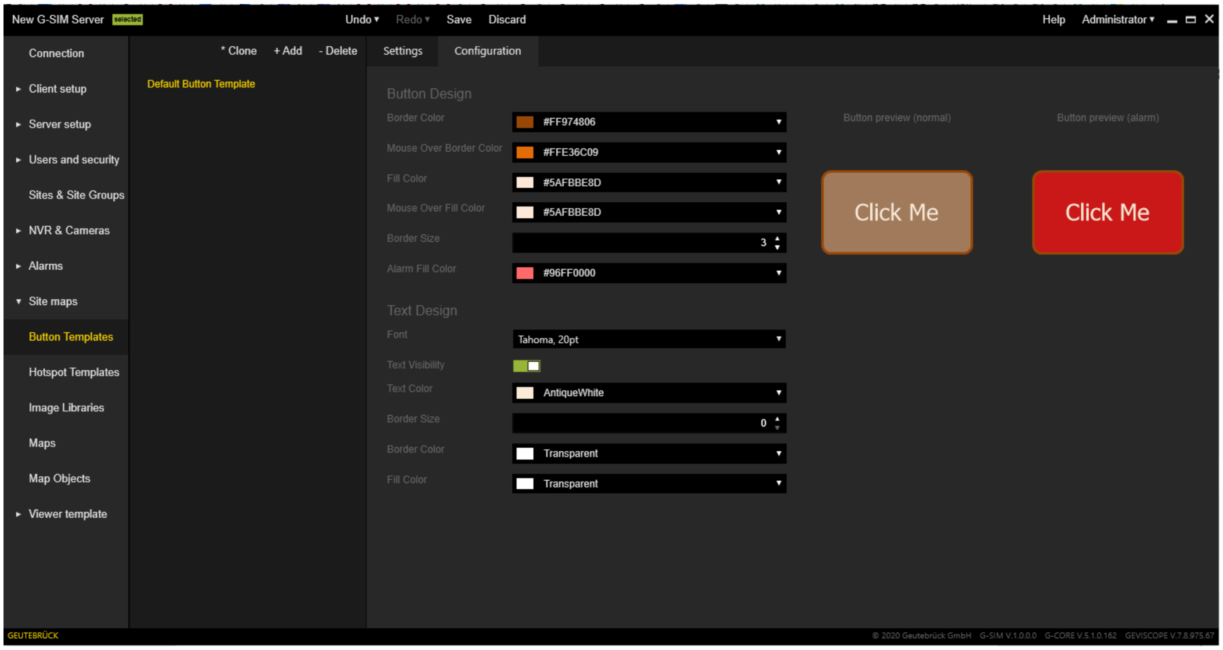
Name: Default Button Template — Please provide a unique name

Secondary Language

Name: — Optional

Configuration

The **Configuration** tab contains the following setting sections:



Button Design

Border Color: #FF974806

Mouse Over Border Color: #FFE36C09

Fill Color: #5AFBBE8D

Mouse Over Fill Color: #5AFBBE8D

Border Size: 3

Alarm Fill Color: #96FF0000

Text Design

Font: Tahoma, 20pt

Text Visibility

Text Color: AntiqueWhite

Border Size: 0

Border Color: Transparent

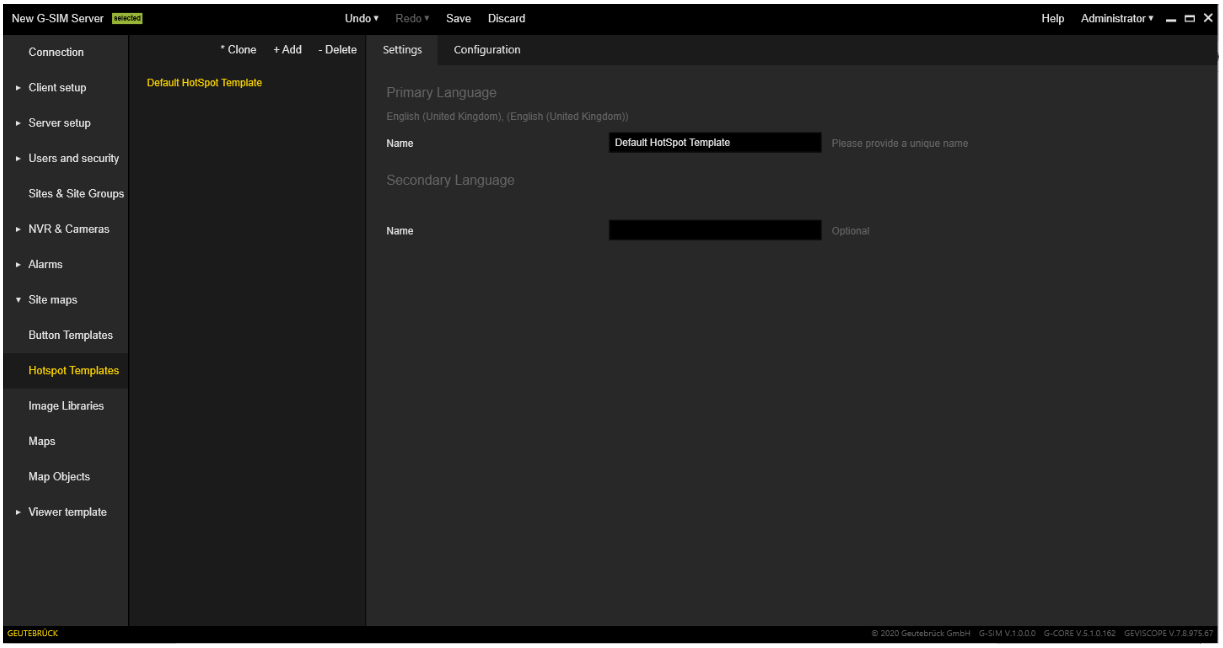
Fill Color: Transparent

Settings	Description
Button Design	Contains a list of fields that configure the appearance of the button body in normal and alarm conditions.
Text Design	Contains a list of fields that configure the text display of the button.
Button preview (normal) / Button preview (alarm)	Shows the button for the normal and alarm state and the respective mouse state (the user should place the mouse cursor over the preview to activate it).

Hotspot Templates

Settings

The **Settings** tab contains the setting of the name for the primary and secondary language. This allows you to specify a name for the selected hotspot template.



Default HotSpot Template

Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Default HotSpot Template — Please provide a unique name

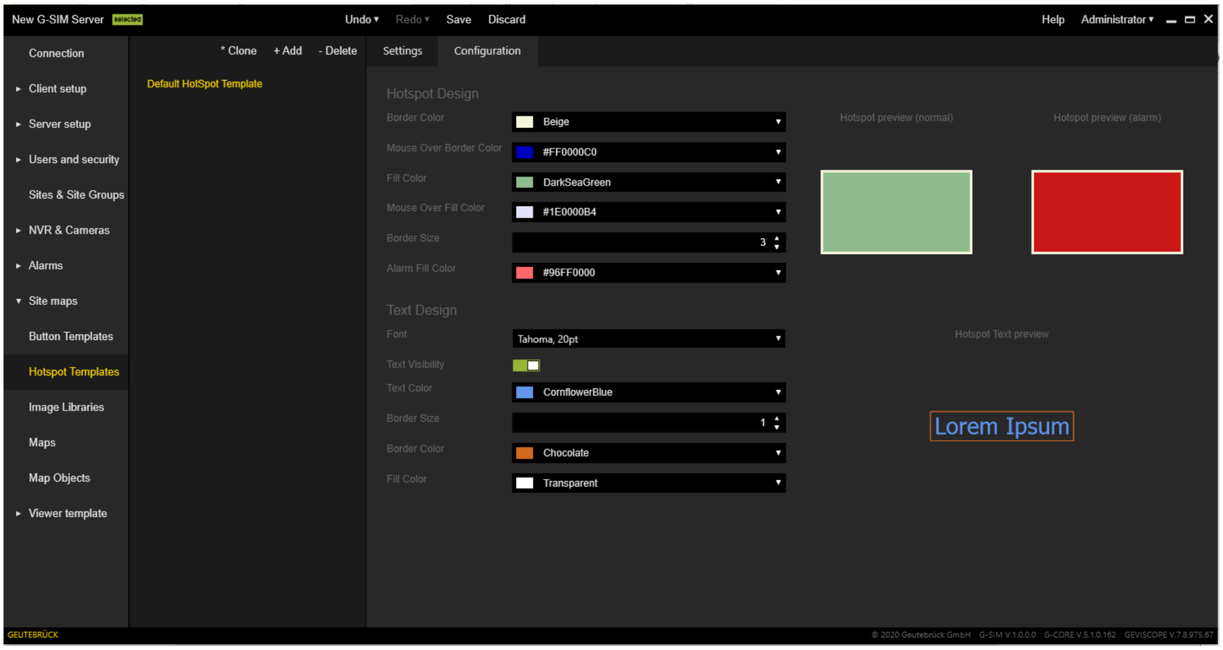
Secondary Language

Name: — Optional

© 2020 Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67

Configuration

The **Configuration** tab contains the following setting sections:



Default HotSpot Template

Hotspot Design

Border Color	Beige
Mouse Over Border Color	#FF0000C0
Fill Color	DarkSeaGreen
Mouse Over Fill Color	#1E0000B4
Border Size	3
Alarm Fill Color	#96FF0000

Text Design

Font	Tahoma, 20pt
Text Visibility	
Text Color	CornflowerBlue
Border Size	1
Border Color	Chocolate
Fill Color	Transparent

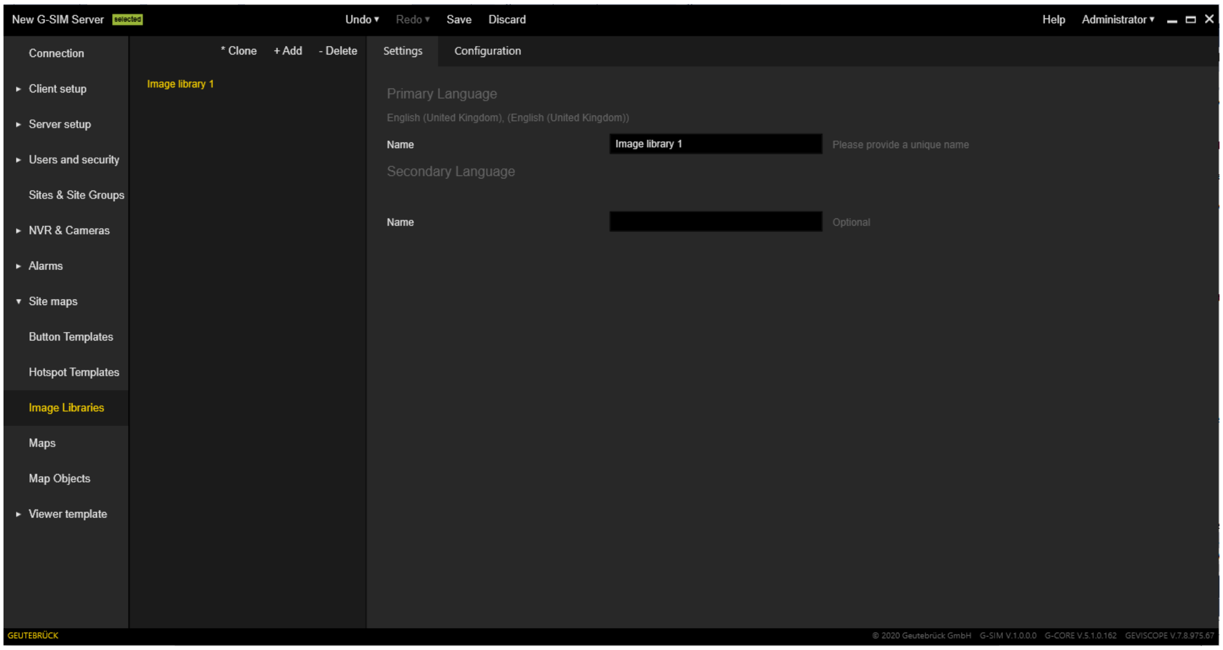
© 2020 Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67

Settings	Description
Hotspot design	Contains a list of fields that configure the appearance of the hotspot body in normal and alarm conditions.
Text design	Contains a list of fields that configure the appearance of hotspot text.
Hotspot preview (normal) / Hotspot preview (alarm)	Shows the button for the normal and alarm state and the respective mouse state (the user should place the mouse cursor over the preview to activate it).

Image Libraries

Settings

The **Settings** tab contains the setting of the name for the primary and secondary language. This allows you to specify a name for the selected image library.



Primary Language

English (United Kingdom), (English (United Kingdom))

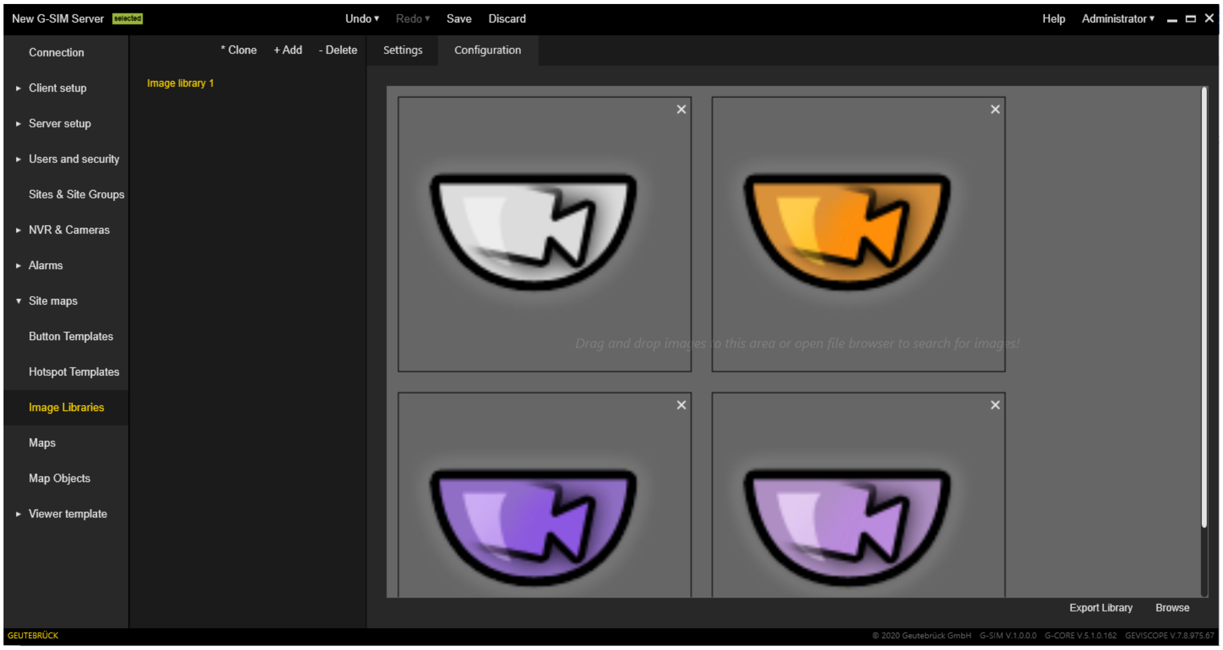
Name: Image library 1 — Please provide a unique name

Secondary Language

Name: — Optional

Configuration

The **Configuration** tab contains the following items:



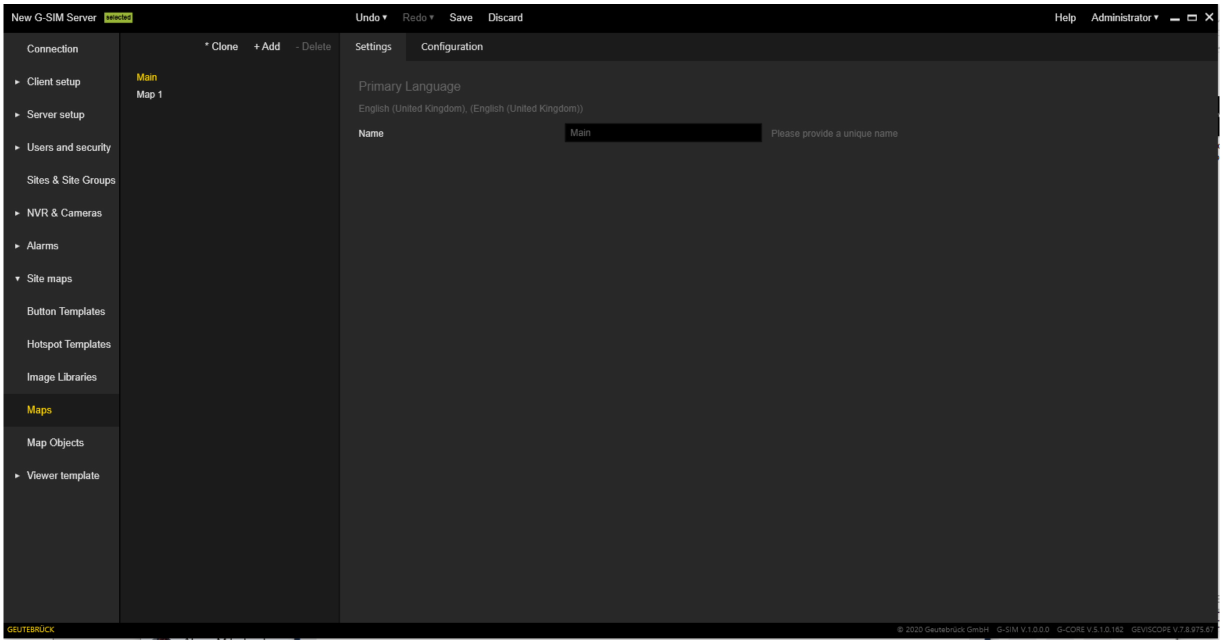
Drag and drop images to this area or open file browser to search for images!

Settings	Description
Images list	Displays added images. Each image can be deleted.
Export Library	Saves a .zip archive with images from the selected image library at the specified location.
Browse	Opens a system dialog to browse images to be added.

Maps

Settings

The **Settings** tab specifies the name of the selected map. It is not editable for the default **Main** map.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Main — Please provide a unique name

Configuration

The **Configuration** tab consists of two areas: The map editor area and the control area with tabs.

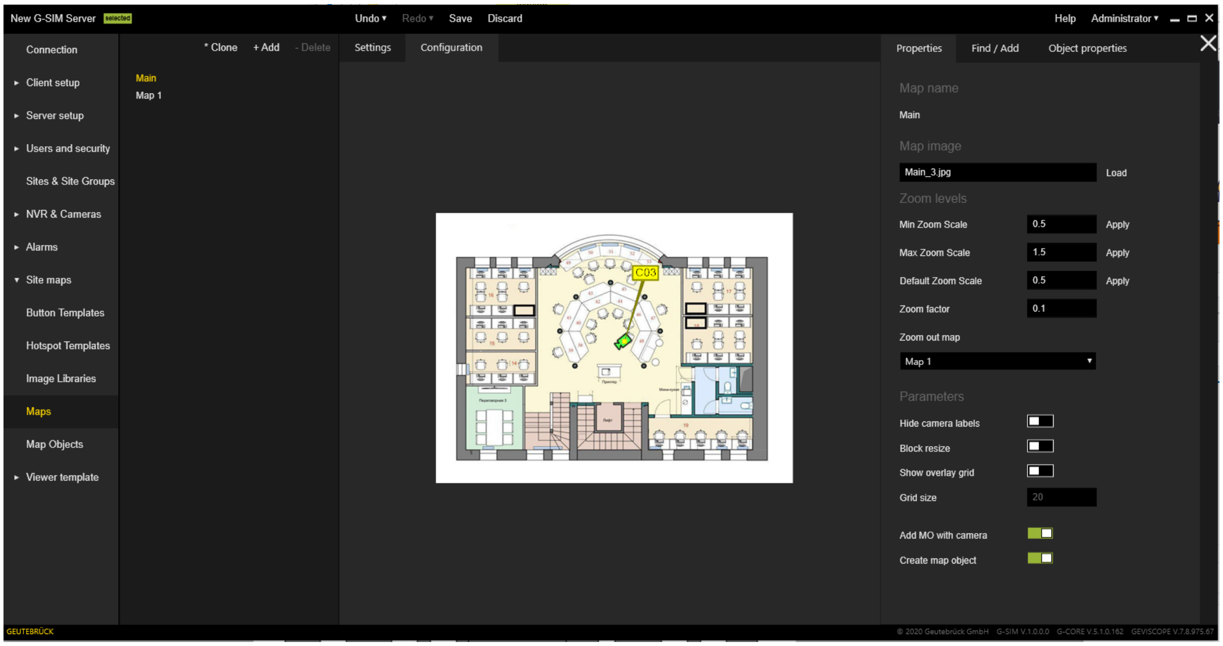
The map editor area allows the user to select and move or rotate map objects.

The settings in the control area are grouped in the following tabs:

- **Properties**
- **Find / Add**
- **Object Properties**

Properties

The **Properties** tab contains the following setting sections:



Map name

Main

Map image

Main_3.jpg Load

Zoom levels

Min Zoom Scale 0.5 Apply

Max Zoom Scale 1.5 Apply

Default Zoom Scale 0.5 Apply

Zoom factor 0.1

Zoom out map

Map 1 ▾

Parameters

Hide camera labels □

Block resize □

Show overlay grid □

Grid size 20

Add MO with camera ☑

Create map object ☑

Settings	Description
Map name	Displays the name of the selected map.
Map image	Allows the user to load the map image using the **Load** button.
Zoom levels	Contains a set of zoom settings.
Parameters	Contains settings for the map editor.

Zoom levels

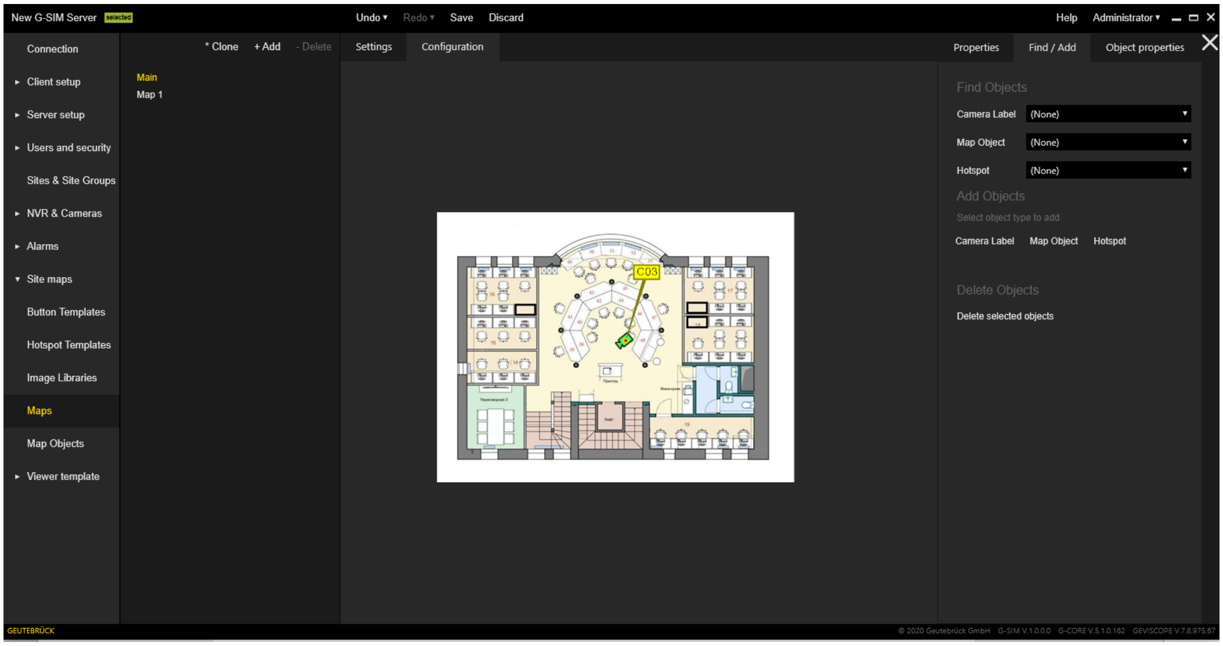
Settings	Description
Min Zoom Scale / Max Zoom Scale	Use these settings to configure the allowable zoom range.
Default Zoom Scale	Sets the zoom level that is applied by default (on the map placed on the viewer).
Zoom factor	Step of increasing\decreasing the zoom level by a single action.
Zoom out map	Specify the map that is displayed after exceeding the minimum zoom value (zoom out).

Parameters

Settings	Description
Hide camera labels	Enables or disables the camera labels on a map.
Block resize	Disables the map zoom for the “zoom to object” action.
Show overlay grid	Displays a grid over the map, which helps to place map objects more precisely.
Grid size	Defines the size of the grid.
Add MO with camera	Enables adding MO with the camera.
Create map object	Enables the creation of the map object.

Find / Add

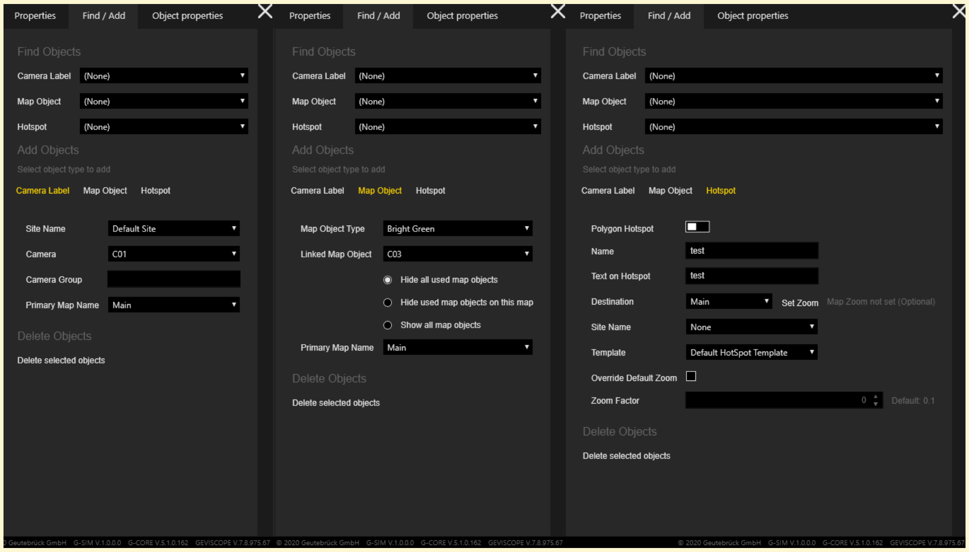
The **Find / Add** tab contains the following setting sections:



Camera Label (None)

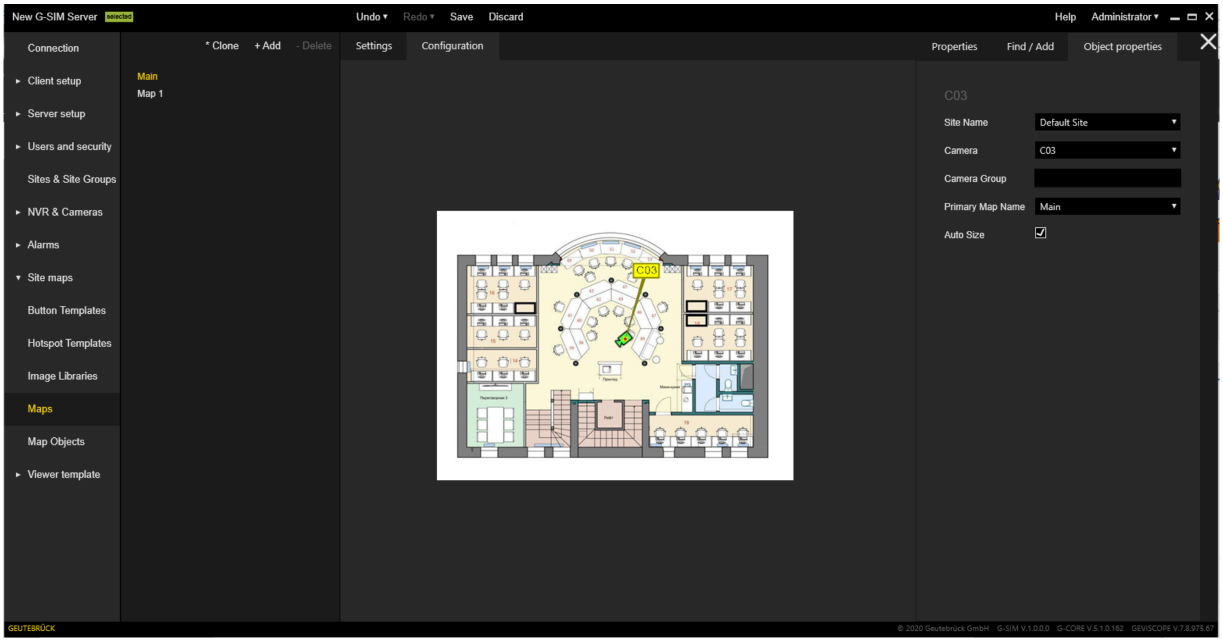
Map Object (None)

Hotspot (None)

Settings	Description
Find Objects	Contains drop-down lists of the assigned map objects. When the user selects an item from the list, the corresponding map object on the map will be selected.
Add Objects	Three types are available: **Camera Label**, **Map Object**, **Hotspot**. When on of them is selected, the corresponding settings are displayed. If the settings of the objects are specified and valid, it is possible to add the appropriate map object by using the mouse cursor on the map.  Properties · Find / Add · Object properties Find Objects Camera Label: (None) Map Object: (None) Hotspot: (None) Add Objects Select object type to add Camera Label · Map Object · Hotspot Site Name: Default Site Camera: C01 Camera Group: Primary Map Name: Main Delete Objects Delete selected objects © Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67 Properties · Find / Add · Object properties Find Objects Camera Label: (None) Map Object: (None) Hotspot: (None) Add Objects Select object type to add Camera Label · Map Object · Hotspot Map Object Type: Bright Green Linked Map Object: C03 ● Hide all used map objects ○ Hide used map objects on this map ○ Show all map objects Primary Map Name: Main Delete Objects Delete selected objects © 2020 Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67 Properties · Find / Add · Object properties Find Objects Camera Label: (None) Map Object: (None) Hotspot: (None) Add Objects Select object type to add Camera Label · Map Object · Hotspot Polygon Hotspot Name: test Text on Hotspot: test Destination: Main · Set Zoom · Map Zoom not set (Optional) Site Name: None Template: Default HotSpot Template Override Default Zoom: □ Zoom Factor: 0 · Default: 0.1 Delete Objects Delete selected objects © 2020 Geutebrück GmbH G-SIM V.1.0.0.0 G-CORE V.5.1.0.162 GEVISCOPE V.7.8.975.67
Delete Objects	Use **Delete selected objects** to remove selected objects from a map.

Object Properties

The **Object properties** tab contains a list of the properties of the selected map object. The set of properties depends on the object type (camera, hotspot, etc.).



C03

Site Name: Default Site

Camera: C03

Camera Group:

Primary Map Name: Main

Auto Size ☑

GIS Maps

Subject to license

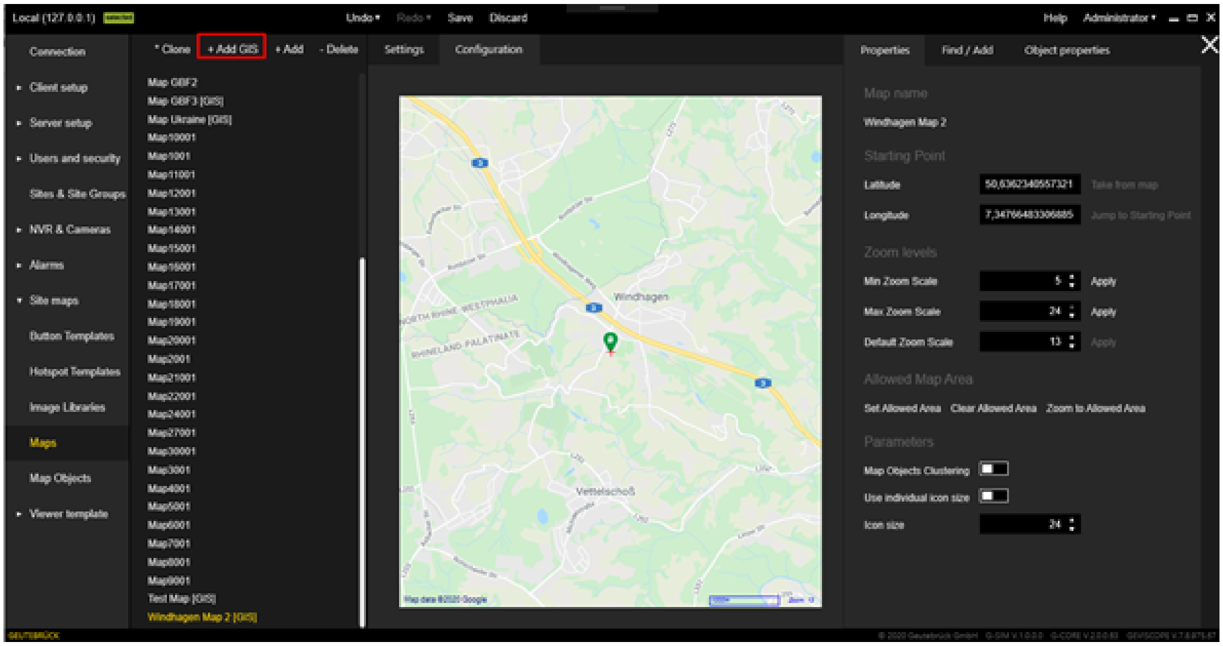
GIS maps enable the use of georeferenced map material from Open Street Maps and Google Street Maps and the display of the cameras or other objects on this map material. This saves time when placing the cameras on a map: If coordinates are already stored on a camera, it (or all selected objects) can simply be switched to the correct position.

The alignment of the cameras or map objects can be set manually, just as with a normal map.

To get access to the functionality of GIS Maps, check if the license Allow use of GIS Maps is available (see Server Licenses**). If this license is not available, the + Add GIS button (see** List of GIS Maps**) and the Location tab (see** Map Object Settings**) will be hidden.**

List of GIS Maps

The GIS maps are marked with the suffix [GIS] in the map list of the Maps view to distinguish them from the normal maps. Also, the additional + Add GIS button is available in the toolbar.



Map name

Windhagen Map 2

Starting Point

Latitude 50,6362340557321

Longitude 7,34766483306885

Zoom levels

Min Zoom Scale 5

Max Zoom Scale 24

Default Zoom Scale 13

Allowed Map Area

Parameters

Map Objects Clustering

Use individual icon size

Icon size 24

Add a GIS Map

To add a new GIS map, click the **+ Add GIS** button. The suffix **[GIS]** is automatically added to the name of the GIS map.

Clone a GIS Map

To clone the currently selected GIS map, click the *** Clone** button. The following settings of the original GIS map are applied to the cloned GIS map:

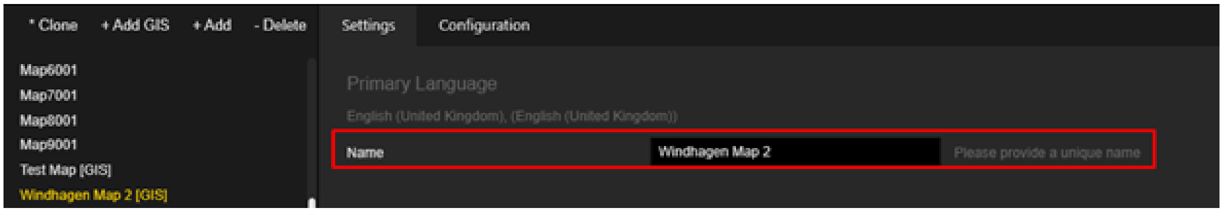
- Starting point
- Zoom levels
- Allowed map area
- Map objects

The name of the cloned GIS map is restricted to the name of the original GIS map including suffix to ensure a unique name.

Settings

In the **Settings** tab you can set the name of the selected GIS map.

The name must be unique, as it will be used in all views where the map can be selected.



Map6001
Map7001
Map8001
Map9001
Test Map [GIS]
Windhagen Map 2 [GIS]

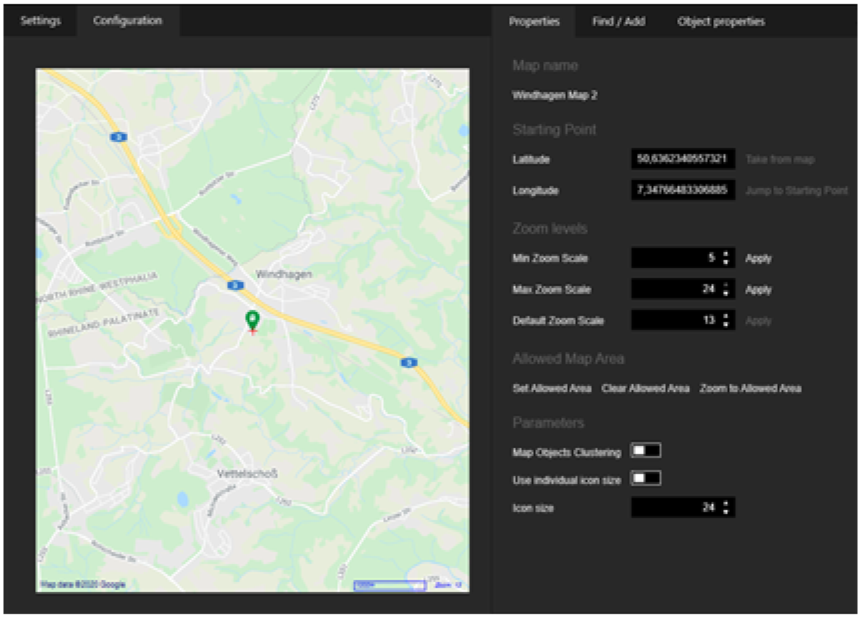
Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Windhagen Map 2 — Please provide a unique name

Configuration

The **Configuration** tab consists of two areas: The GIS Map control area of the selected GIS Map and the configuration area.



Map name

Windhagen Map 2

Starting Point

Latitude: 50,6362340557321 — Take from map

Longitude: 7,34766483306885 — Jump to Starting Point

Zoom levels

Min Zoom Scale: 5 — Apply

Max Zoom Scale: 24 — Apply

Default Zoom Scale: 13 — Apply

Allowed Map Area

Set Allowed Area — Clear Allowed Area — Zoom to Allowed Area

Parameters

Map Objects Clustering: □

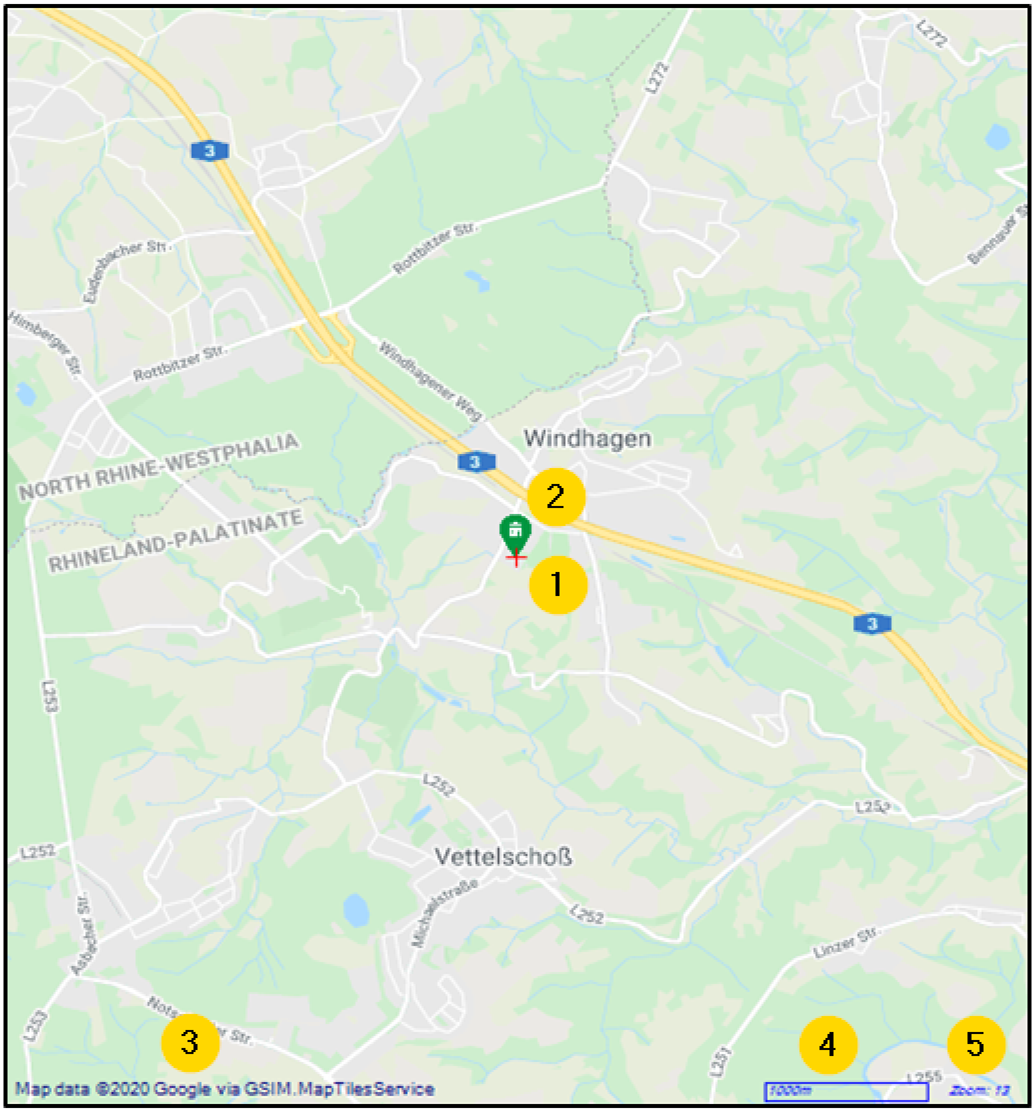
Use individual icon size: □

Icon size: 24

In the **GIS Map control** area the following information of the selected GIS Map can be seen, which can be set in the configuration area:

- 1 Current center of the map view (small red cross mark)
- 2 Starting point of the map view (green marker)
- 3 Name of the map provider
- 4 Scale

- 5 Set zoom level



To move the map view, hold down the left mouse button and move the mouse cursor. Use the mouse wheel to zoom in and out of the map view.

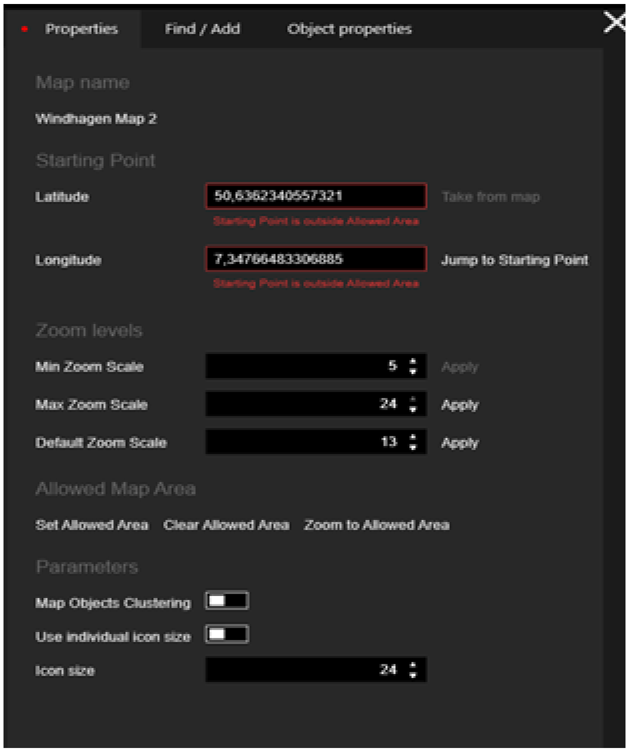
The settings in the configuration area are grouped into the following tabs:

- **Properties**
- **Find / Add**
- **Object Properties**

Properties

The **Properties** tab contains the following settings sections:

- **Map Name**
- **Starting Point**
- **Zoom Levels**
- **Allowed Map Area**
- **Parameters**



Map name

Windhagen Map 2

Starting Point

Latitude 50,6362340557321 Take from map

Starting Point is outside Allowed Area

Longitude 7,34766483306885 Jump to Starting Point

Starting Point is outside Allowed Area

Zoom levels

Min Zoom Scale 5 Apply

Max Zoom Scale 24 Apply

Default Zoom Scale 13 Apply

Allowed Map Area

Set Allowed Area Clear Allowed Area Zoom to Allowed Area

Parameters

Map Objects Clustering

Use individual icon size

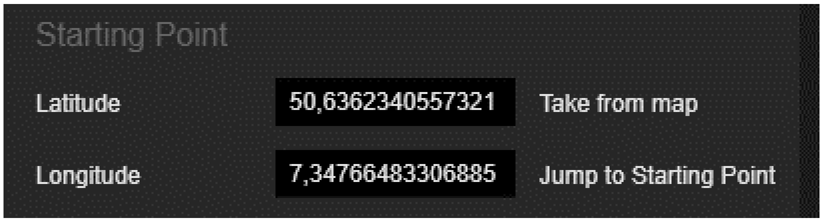
Icon size 24

Map Name

Displays the name of the selected GIS map.

Starting Point

This setting area contains the geographic coordinates (latitude and longitude) of the map's starting point. When the map is opened, it is centered at this starting point.



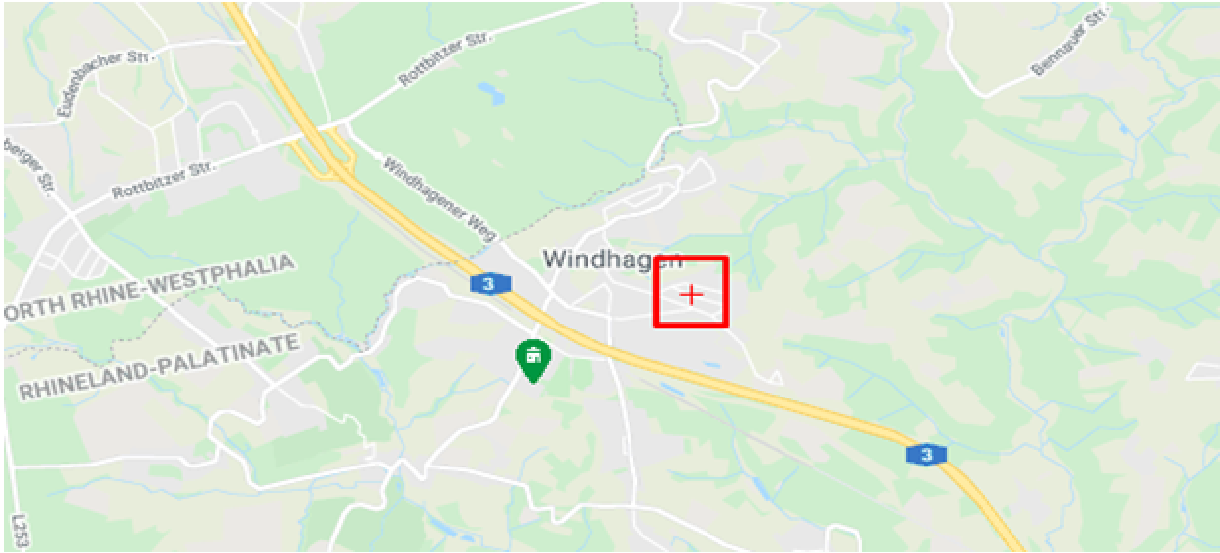
Starting Point

Latitude 50,6362340557321 Take from map

Longitude 7,34766483306885 Jump to Starting Point

Options	Description
Latitude	The specification of the latitude is mandatory. The value should be in the range [-90, 90].
Longitude	The specification of the longitude is mandatory. The value should be in the range [-180, 180].
Take from map	Click this button to set the current map center point as the starting point.
Jump to Starting Point	Click this button to center the map at the starting point.

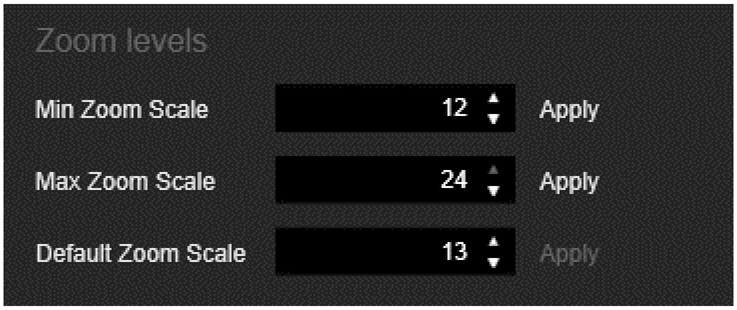
In the map, the starting point is marked with a green icon and the current center point is marked with a red cross:



Zoom Levels

In this setting area you can define the values of the zoom levels.

When opening the map, the Default Zoom Scale setting is always applied.



Zoom levels

Min Zoom Scale 12 Apply

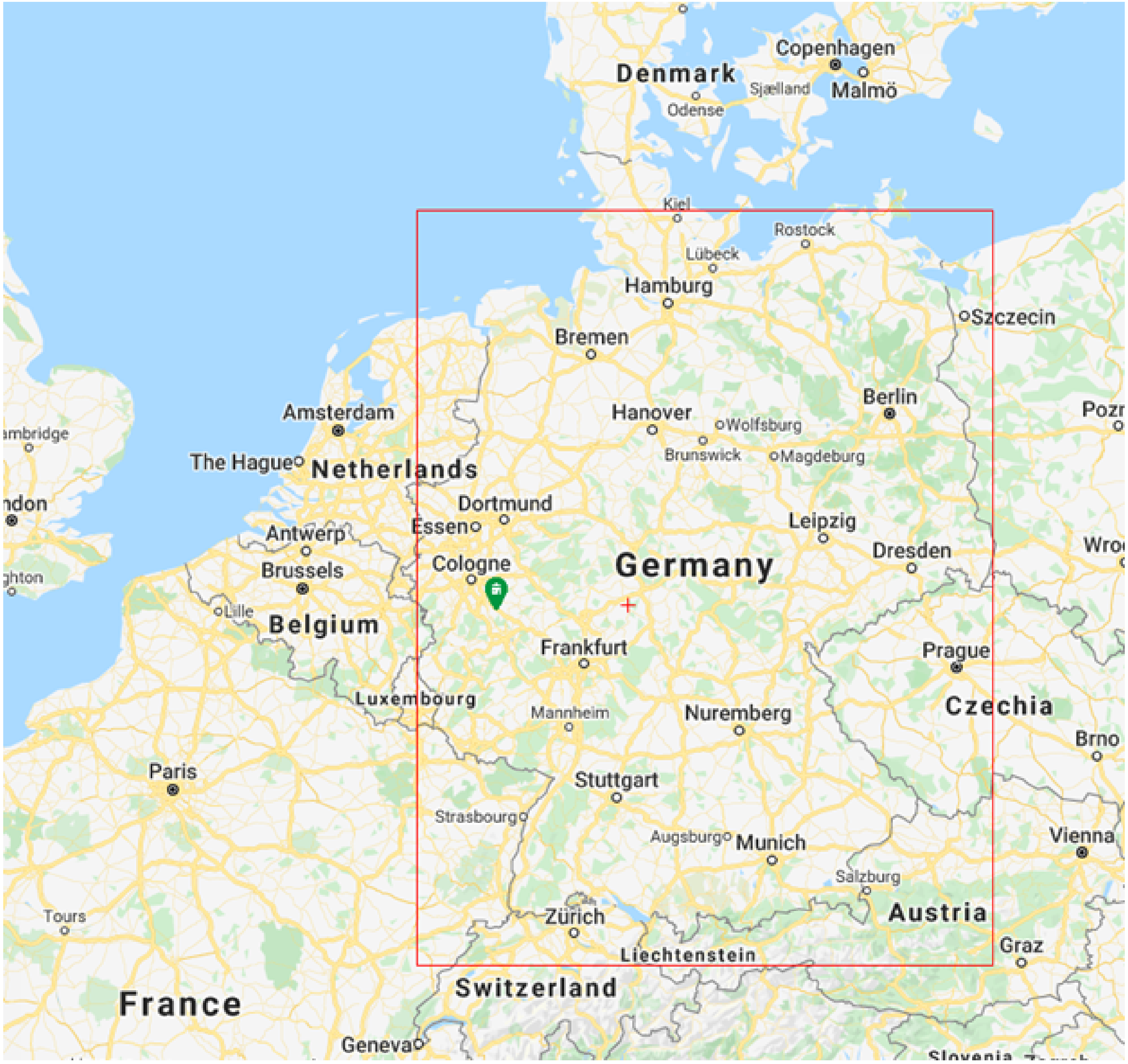
Max Zoom Scale 24 Apply

Default Zoom Scale 13 Apply

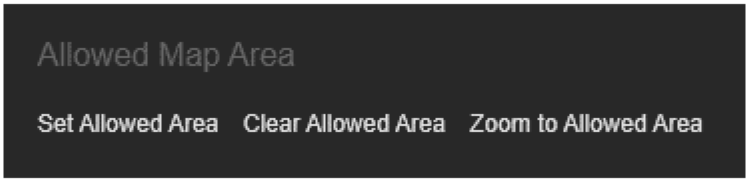
Options	Description
Min Zoom Scale	Specifies the minimum zoom scaling. The value should be in the range [0, 24].
Max Zoom Scale	Specifies the maximum zoom scale. The value should be in the range [0, Max Zoom Scale].
Default Zoom Scale	Specify the default zoom scale when opening the map. The value should be in the range [Min Zoom Scale, Max Zoom Scale].
Apply	Click this button to apply the corresponding zoom scaling.

Allowed Map Area

The allowed map area delimits the area in which the user can move and zoom. It is marked with a red rectangle.

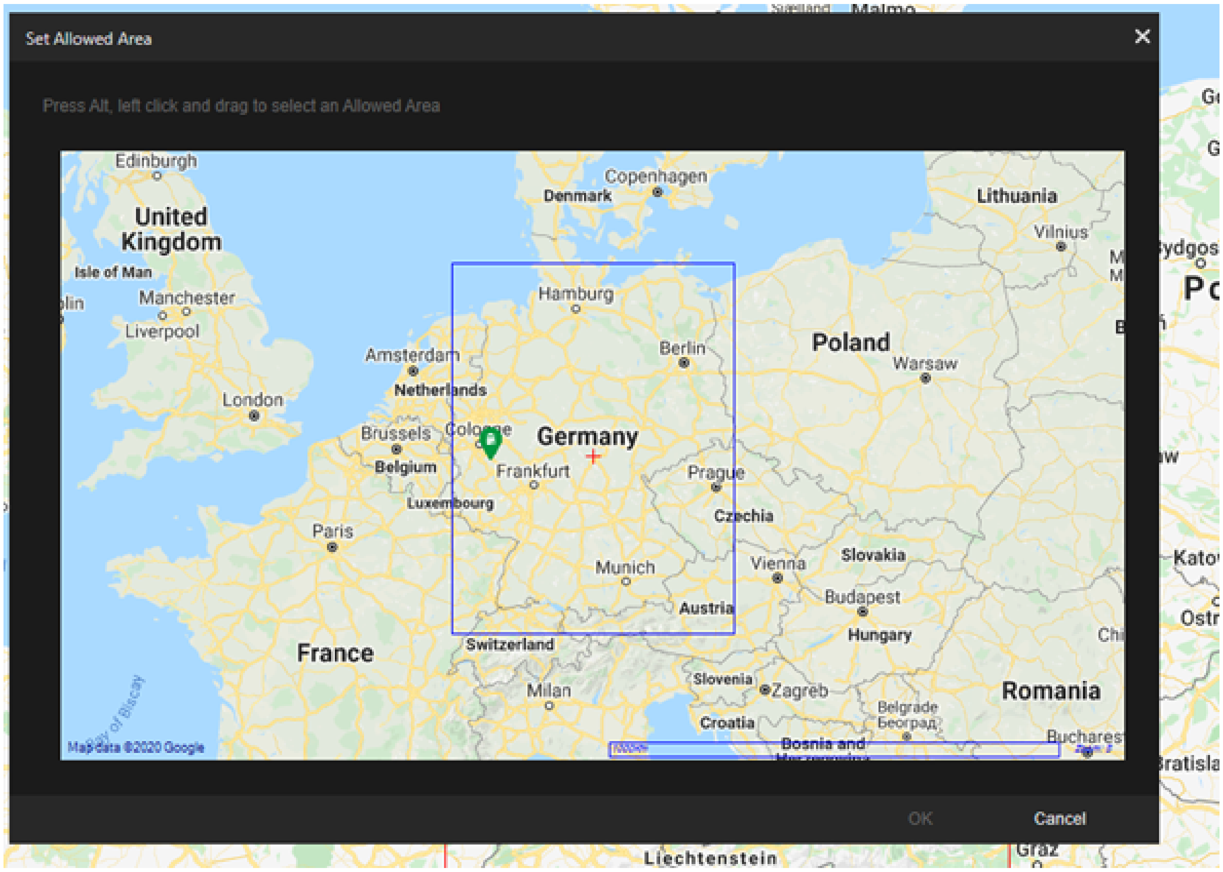


The following buttons are available for editing the allowed map area:



Options	Description
Set Allowed Area	Click this button to set the allowed map area.
Clear Allowed Area	Click this button to delete the allowed map area.
Zoom to Allowed Area	Click this button to zoom in on the allowed map area to be able to check it.

When you click the **Set Allowed Area** button, the following dialog box opens:

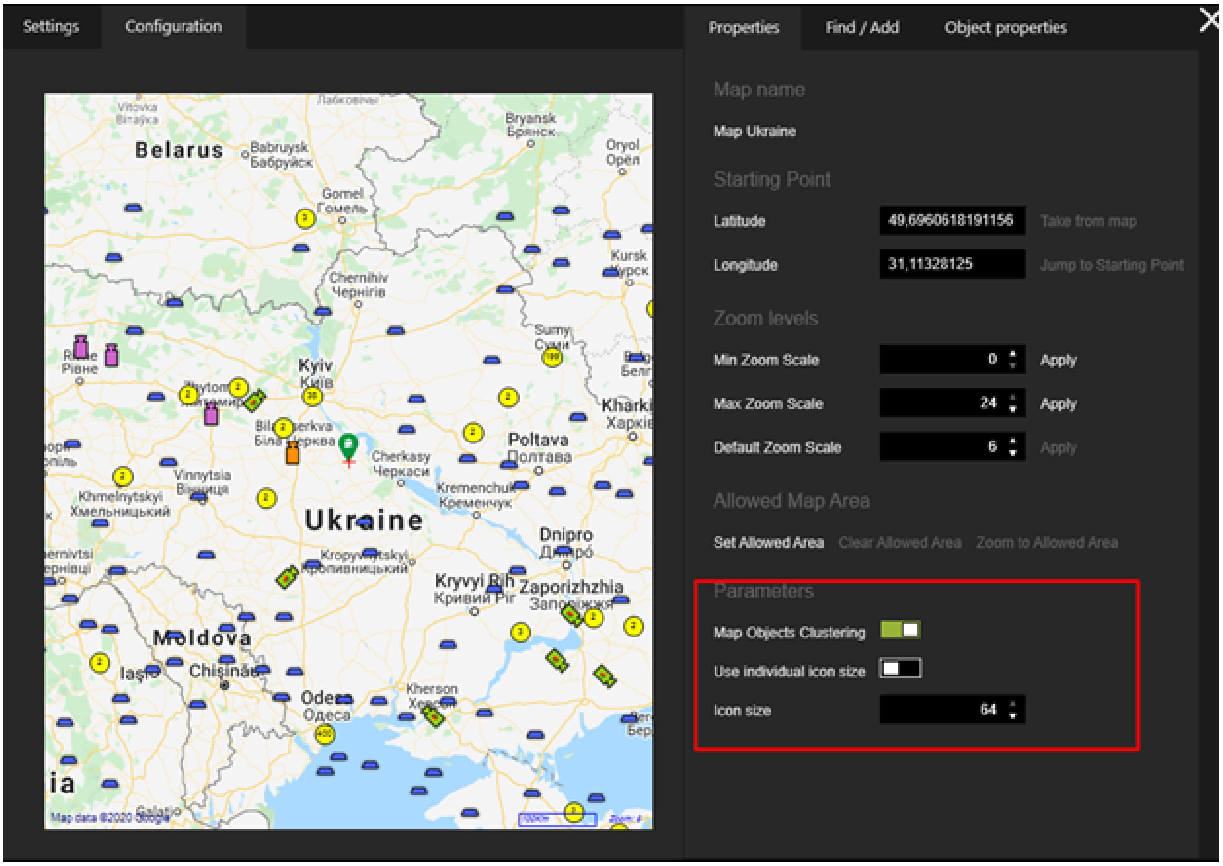

Set Allowed Area

Press Alt, left click and drag to select an Allowed Area

Hold down the ALT-key and the left mouse button and select the allowed map area by dragging the mouse pointer. Click the **OK** button to apply the changes or the **Cancel** button to reject the changes.

Parameters

In the **Parameters** settings area, you can define settings for the display of map objects in the GIS map control.



Map name

Map Ukraine

Starting Point

Latitude 49,6960618191156 Take from map

Longitude 31,11328125 Jump to Starting Point

Zoom levels

Min Zoom Scale 0 Apply

Max Zoom Scale 24 Apply

Default Zoom Scale 6 Apply

Allowed Map Area

Set Allowed Area Clear Allowed Area Zoom to Allowed Area

Parameters

Map Objects Clustering ●

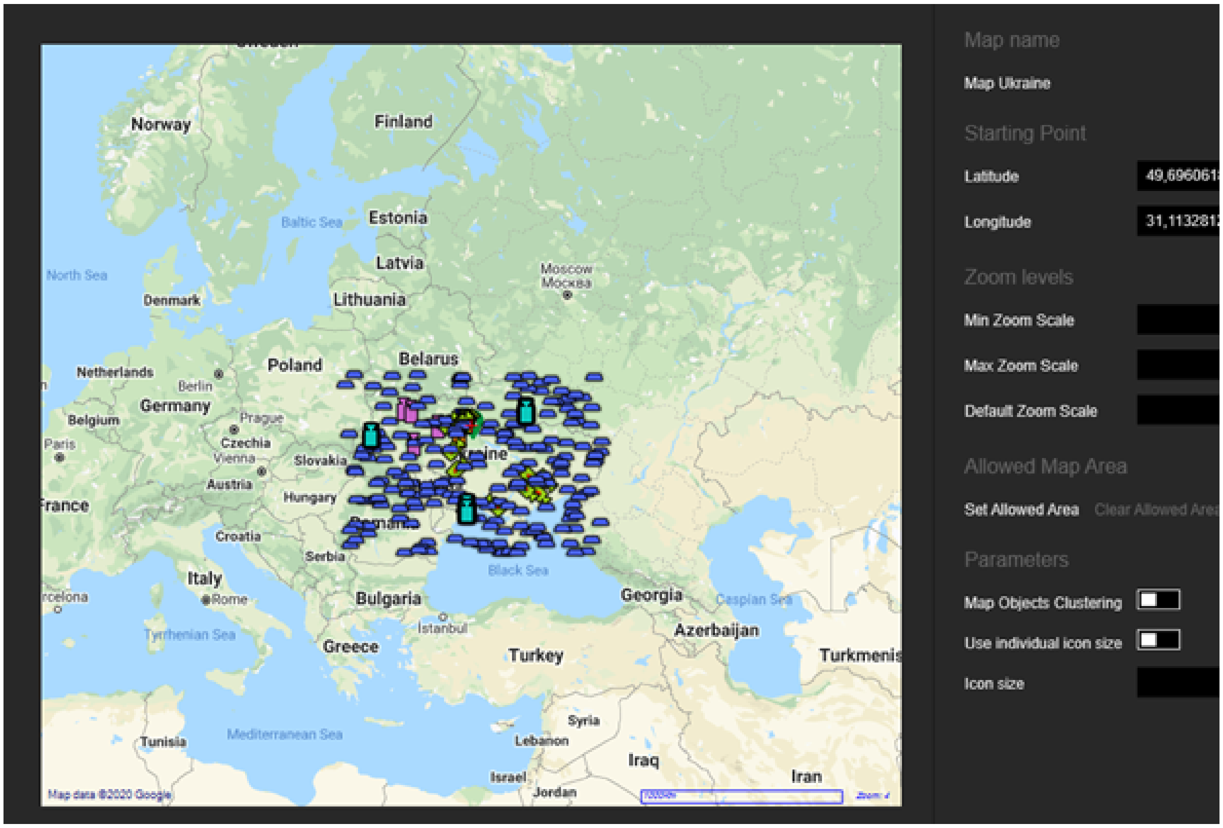
Use individual icon size ○

Icon size 64

Options	Description
Map Objects Clustering	Use this slider to enable or disable the grouping mechanism for Map objects of the GIS map. If the option is enabled, adjacent map objects will be merged into map object groupings to avoid overlapping.
Use individual icon size	Activate this slider to override the global size of map object symbols and map object grouping defined in the system settings and use an individual symbol size. This overriding of the settings can be done individually for each GIS map.
Icon size	Specify the individual symbol size for map objects and map object groupings. Changing this parameter can affect the grouping of map objects.

Map Objects Clustering

If the GIS map contains many map objects in certain regions, map objects may overlap at low zoom settings:



Map name

Map Ukraine

Starting Point

Latitude 49,696061

Longitude 31,113281

Zoom levels

Min Zoom Scale

Max Zoom Scale

Default Zoom Scale

Allowed Map Area

Set Allowed Area Clear Allowed Area

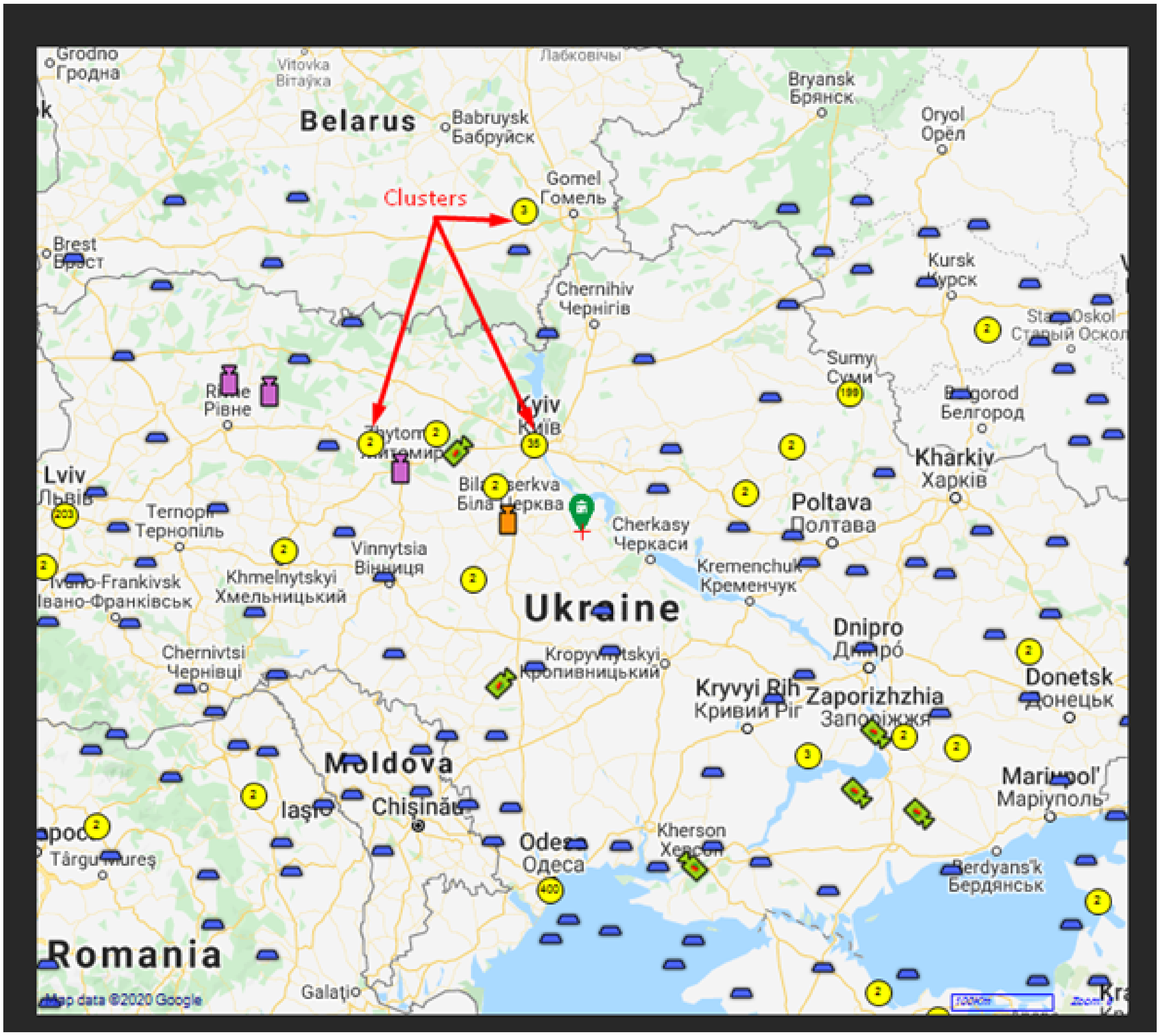
Parameters

Map Objects Clustering □

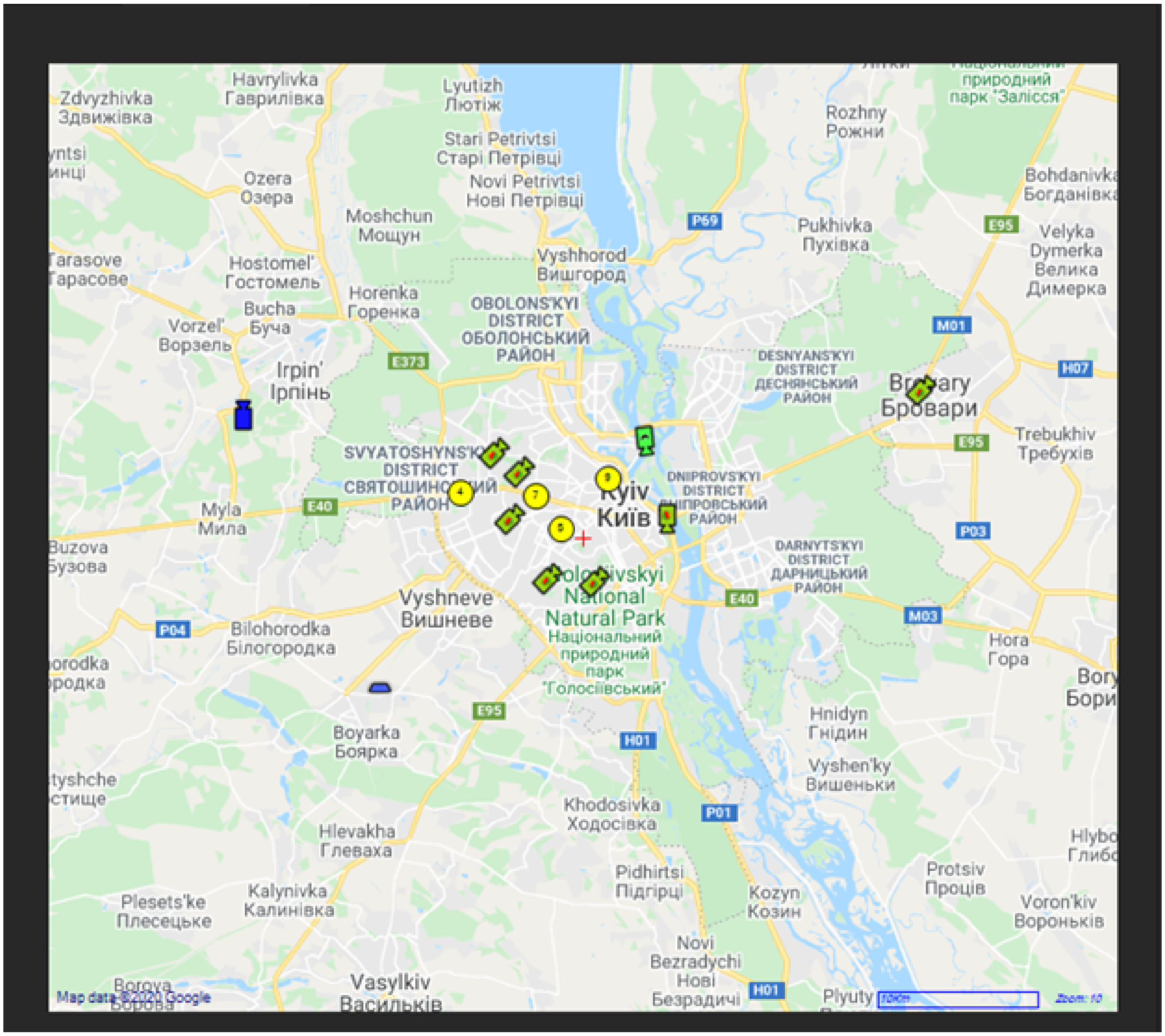
Use individual icon size □

Icon size

If the **Map Objects Clustering** option is enabled, all neighboring map objects are merged into one map object group. To zoom in and view all map objects contained in a grouping individually, the user can click on the respective grouping.

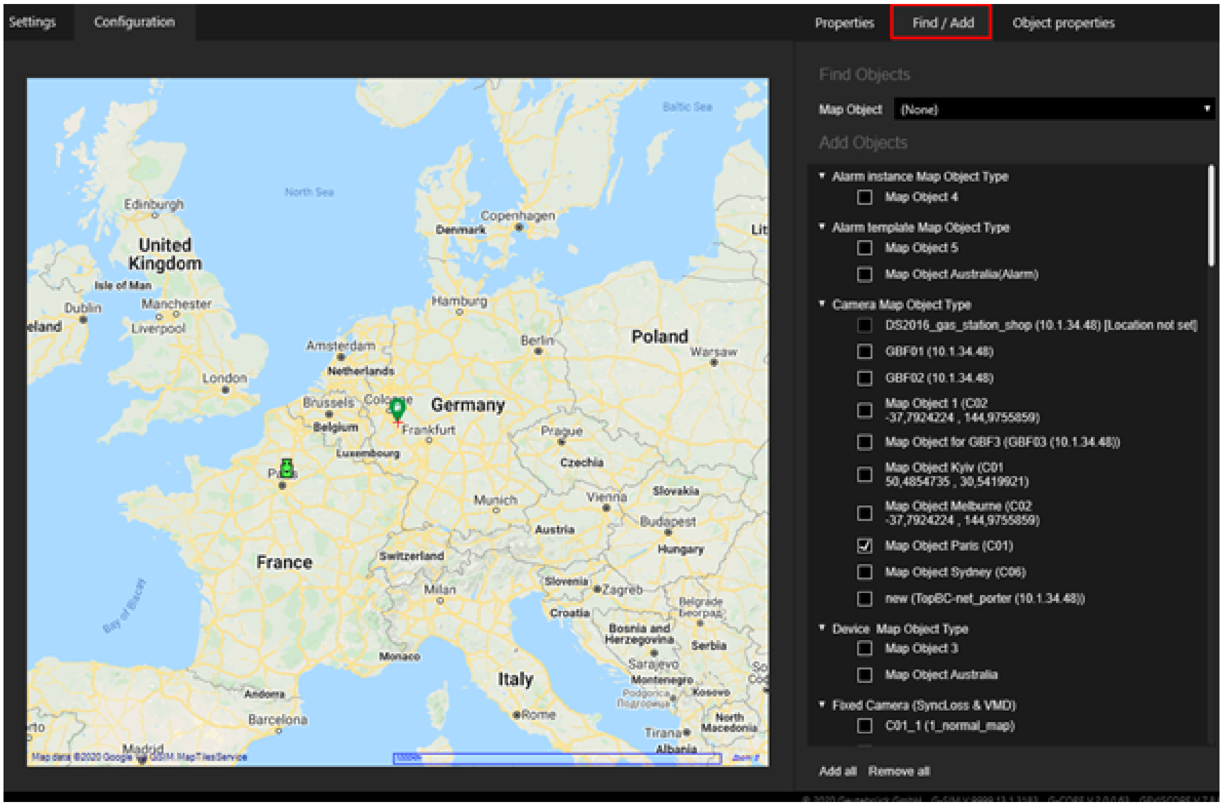


Sometimes it is not possible to display all map objects of a grouping in one view. In this case, smaller map object groupings are displayed:



Find / Add

The **Find / Add** tab contains the following setting areas **Find Objects** and **Add Objects**.



Find Objects

Map Object (None)

Add Objects

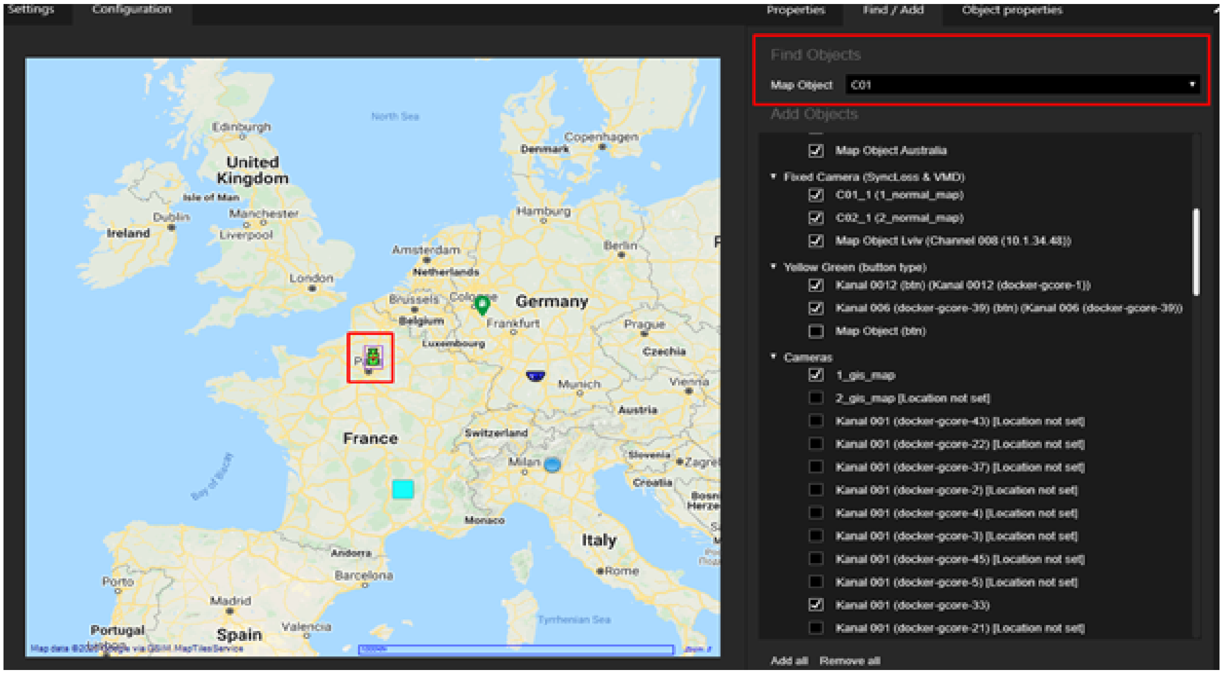
- Alarm instance Map Object Type
  - □ Map Object 4
- Alarm template Map Object Type
  - □ Map Object 5
  - □ Map Object Australia(Alarm)
- Camera Map Object Type
  - □ DS2016_gas_station_shop (10.1.34.48) [Location not set]
  - □ GBF01 (10.1.34.48)
  - □ GBF02 (10.1.34.48)
  - □ Map Object 1 (C02 -37,7924224 , 144,9755859)
  - □ Map Object for GBF3 (GBF03 (10.1.34.48))
  - □ Map Object Kyiv (C01 50,4854735 , 30,5419921)
  - □ Map Object Melburne (C02 -37,7924224 , 144,9755859)
  - ☑ Map Object Paris (C01)
  - □ Map Object Sydney (C06)
  - □ new (TopBC-net_porter (10.1.34.48))
- Device Map Object Type
  - □ Map Object 3
  - □ Map Object Australia
- Fixed Camera (SyncLoss & VMD)
  - □ C01_1 (1_normal_map)

Add all Remove all

Find Objects

The Map Object drop-down lists contains the associated map objects. Select a map object from the list to display it on the map in the control area. Found map objects are marked with a purple frame.

If the found map object is in a map object grouping, the map is zoomed to Max Zoom Scale.



Find Objects

Map Object: C01

Add Objects

- ☑ Map Object Australia
- Fixed Camera (SyncLoss & VMD)
  - ☑ C01_1 (1_normal_map)
  - ☑ C02_1 (2_normal_map)
  - ☑ Map Object Lviv (Channel 008 (10.1.34.48))
- Yellow Green (button type)
  - ☑ Kanal 0012 (btn) (Kanal 0012 (docker-gcore-1))
  - ☑ Kanal 006 (docker-gcore-39) (btn) (Kanal 006 (docker-gcore-39))
  - □ Map Object (btn)
- Cameras
  - ☑ 1_gis_map
  - □ 2_gis_map [Location not set]
  - □ Kanal 001 (docker-gcore-43) [Location not set]
  - □ Kanal 001 (docker-gcore-22) [Location not set]
  - □ Kanal 001 (docker-gcore-37) [Location not set]
  - □ Kanal 001 (docker-gcore-2) [Location not set]
  - □ Kanal 001 (docker-gcore-4) [Location not set]
  - □ Kanal 001 (docker-gcore-3) [Location not set]
  - □ Kanal 001 (docker-gcore-45) [Location not set]
  - □ Kanal 001 (docker-gcore-5) [Location not set]
  - ☑ Kanal 001 (docker-gcore-33)
  - □ Kanal 001 (docker-gcore-21) [Location not set]

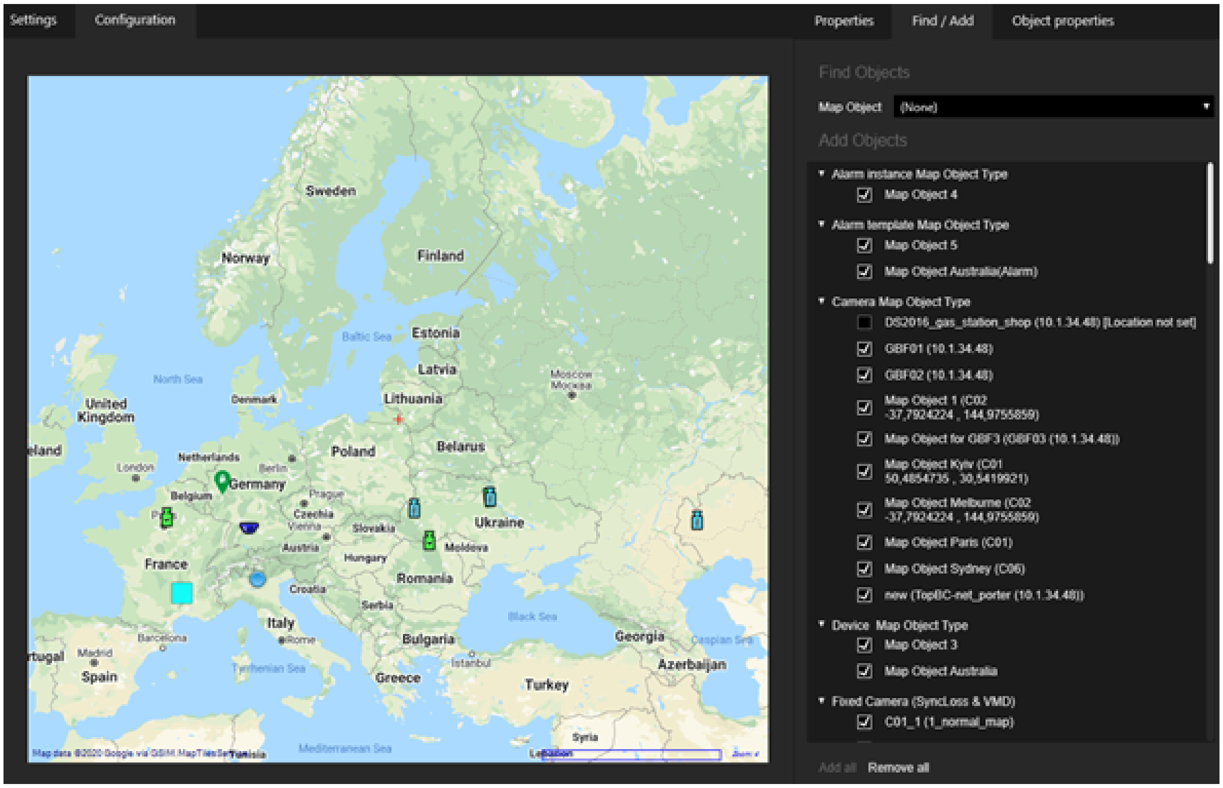
Add Objects

In this settings area you can add or remove map objects in the map by selecting or deselecting the respective map objects in the list. The Add all and Remove all buttons allow you to add or remove all map objects in the list with one click.

When adding map objects, you must keep the following in mind:

- Only Map objects that have geographic coordinates (locations) can be added to the map.
- If a Allowed Map Area is set, only map objects with geographic coordinates (locations) within the allowed map area can be added to the map.

The added map objects are displayed in the GIS map control:



Find Objects

Map Object (None)

Add Objects

- Alarm instance Map Object Type
  - ☑ Map Object 4
- Alarm template Map Object Type
  - ☑ Map Object 5
  - ☑ Map Object Australia(Alarm)
- Camera Map Object Type
  - ☐ DS2016_gas_station_shop (10.1.34.48) [Location not set]
  - ☑ GBF01 (10.1.34.48)
  - ☑ GBF02 (10.1.34.48)
  - ☑ Map Object 1 (C02 -37,7924224 , 144,9755859)
  - ☑ Map Object for GBF3 (GBF03 (10.1.34.48))
  - ☑ Map Object Kyiv (C01 50,4854735 , 30,5419921)
  - ☑ Map Object Melburne (C02 -37,7924224 , 144,9755859)
  - ☑ Map Object Paris (C01)
  - ☑ Map Object Sydney (C06)
  - ☑ new (TopBC-net_porter (10.1.34.48))
- Device Map Object Type
  - ☑ Map Object 3
  - ☑ Map Object Australia
- Fixed Camera (SyncLoss & VMD)
  - ☑ C01_1 (1_normal_map)

Add all Remove all

Object Properties

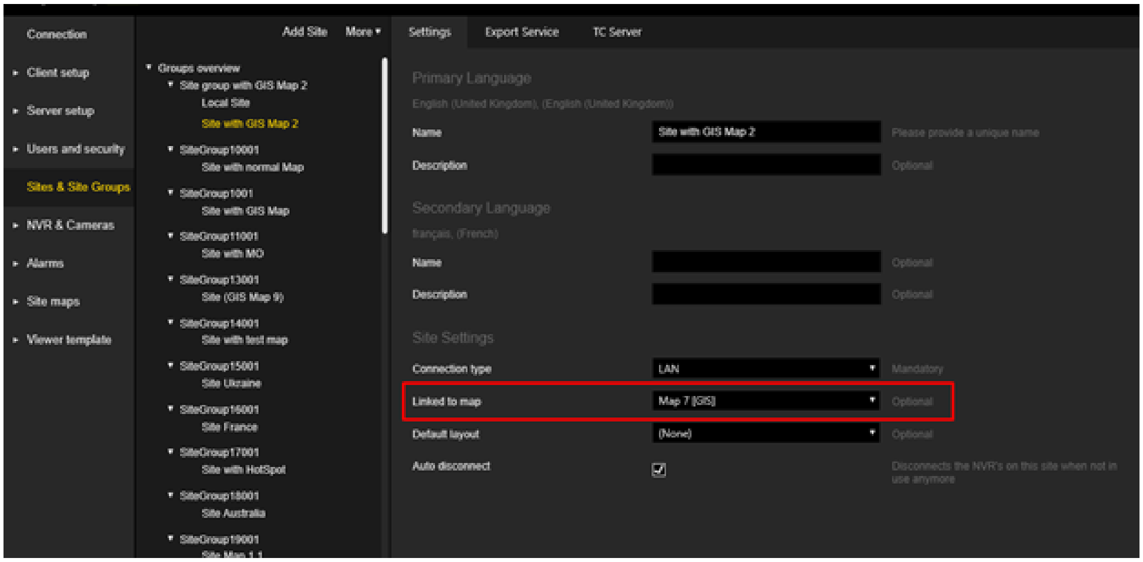
Click on a map object in the GIS map control to view its properties in the **Object properties** tab.

You can only edit the **Primary Map Name** setting.

Usage

GIS maps can be used in all areas where normal maps can be used.

- Linking to a site:



Primary Language
English (United Kingdom), (English (United Kingdom))

Name: Site with GIS Map 2 — Please provide a unique name

Description: — Optional

Secondary Language
français, (French)

Name: — Optional

Description: — Optional

Site Settings

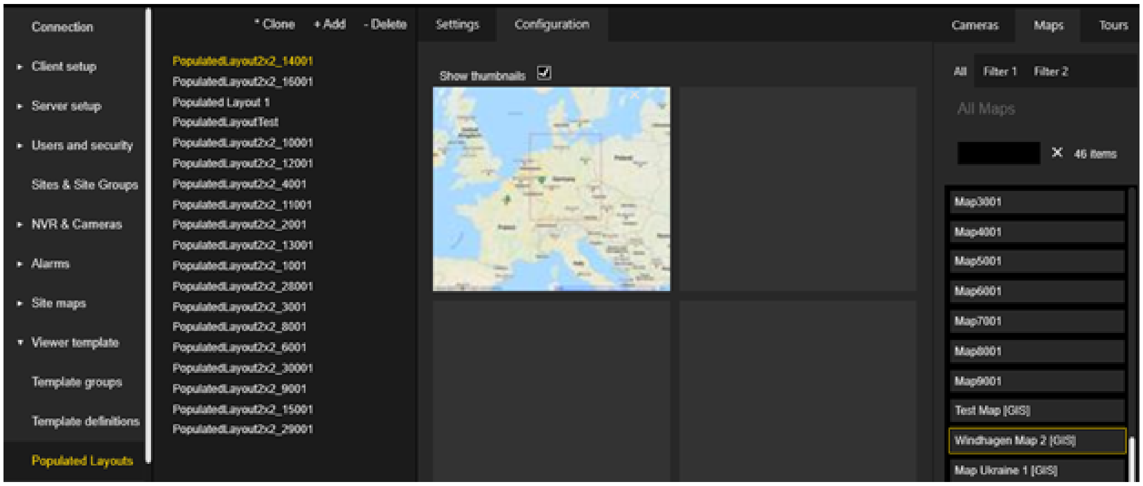
Connection type: LAN — Mandatory

Linked to map: Map 7 [GIS] — Optional

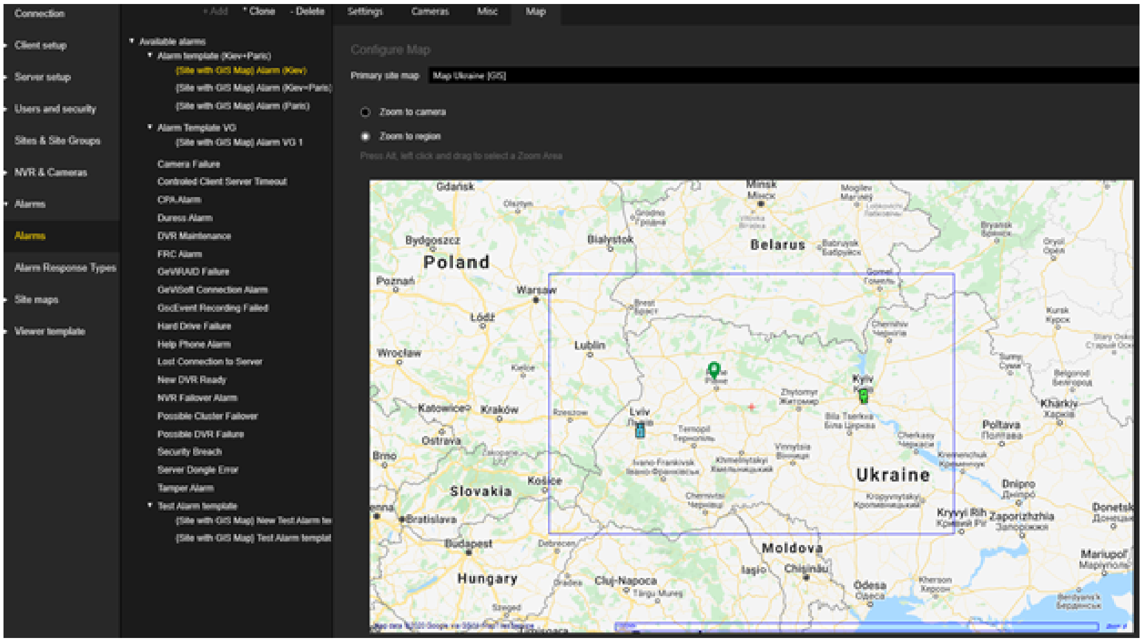
Default layout: (None) — Optional

Auto disconnect: ☑ — Disconnects the NVR's on this site when not in use anymore

- Adding to populated or linked layouts:



- Use in the alarm instance:



Configure Map

Primary site map: Map Ukraine [GIS]

○ Zoom to camera

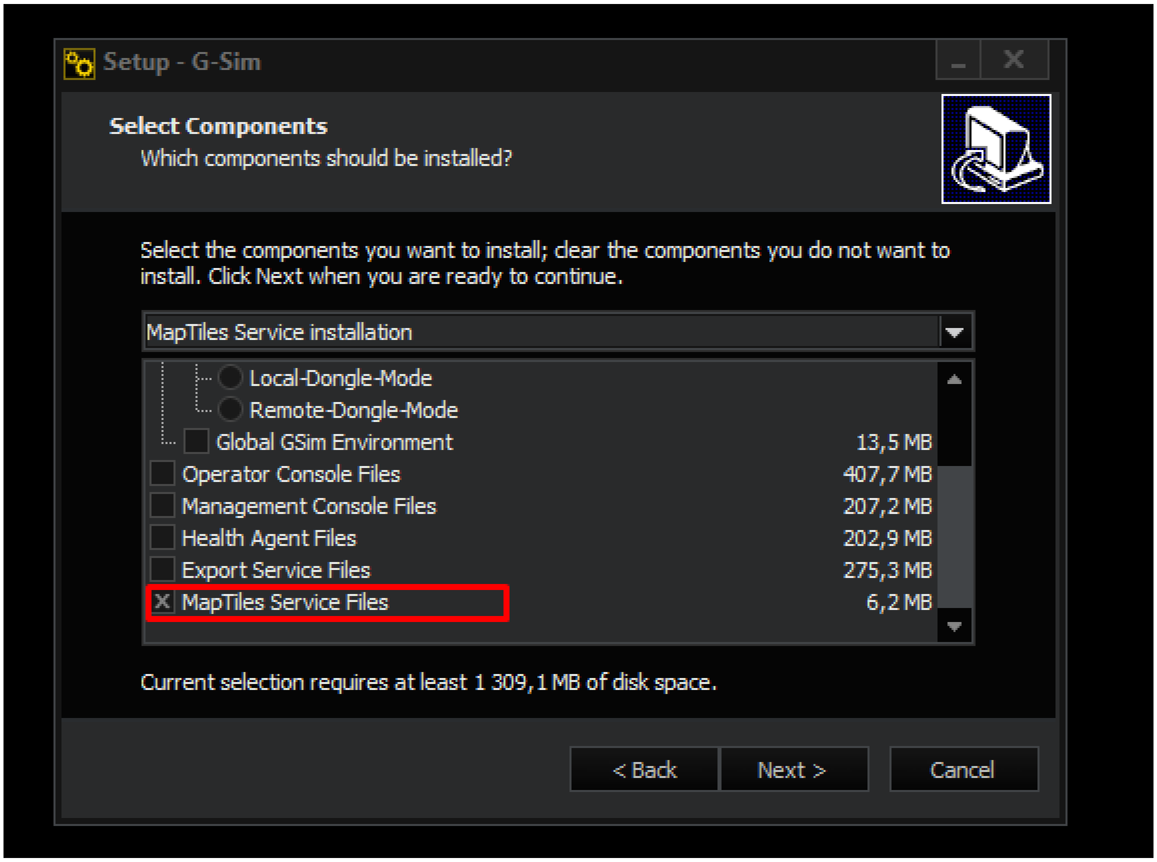
● Zoom to region

Press Alt, left click and drag to select a Zoom Area

Technical Aspects

MapTiles Service

The MapTiles Service is a separate component of G-SIM. It can be installed via the G-SIM installer.



Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

MapTiles Service installation

○ Local-Dongle-Mode	
○ Remote-Dongle-Mode	
□ Global GSim Environment	13,5 MB
□ Operator Console Files	407,7 MB
□ Management Console Files	207,2 MB
□ Health Agent Files	202,9 MB
□ Export Service Files	275,3 MB
☒ MapTiles Service Files	6,2 MB

Current selection requires at least 1 309,1 MB of disk space.

If the **GIS Maps MapTiles Service address** setting in the system settings is filled in, the GIS Map controller makes requests to the MapTiles Service instead of making requests directly to the GIS Map provider.

If the MapTiles Server is not used, the map download is performed by the OpCon or ManCon when the map is to be displayed. Only the map tiles that belong to the currently displayed region will be downloaded. The OpCon or ManCon should have access to the Internet in this case.

If the MapTiles server is used, then it downloads the map tiles on the requests from the ManCon or OpCon. In this case only the MapTiles server needs internet access.

If the MapTiles server is used and the GIS map provider is MapTiles package and the MapTiles package is downloaded to the MapTiles server computer (the MBTiles package can be obtained from the site **https://open-maptiles.com/downloads/planet/**), then the MapTiles server does not need access to the Internet.

A MapTiles Service can be used for different G-SIM servers with different GIS maps settings.

The MapTiles Service has a fast in-memory cache for storing the most recently requested map tile images. When a request for a map tile image is received, the image is first searched in the in-memory cache. This approach can speed up the retrieval of map tile images and reduce the number of requests to GIS maps providers.

The MapTiles Service has a cache database for storing map tiles images.

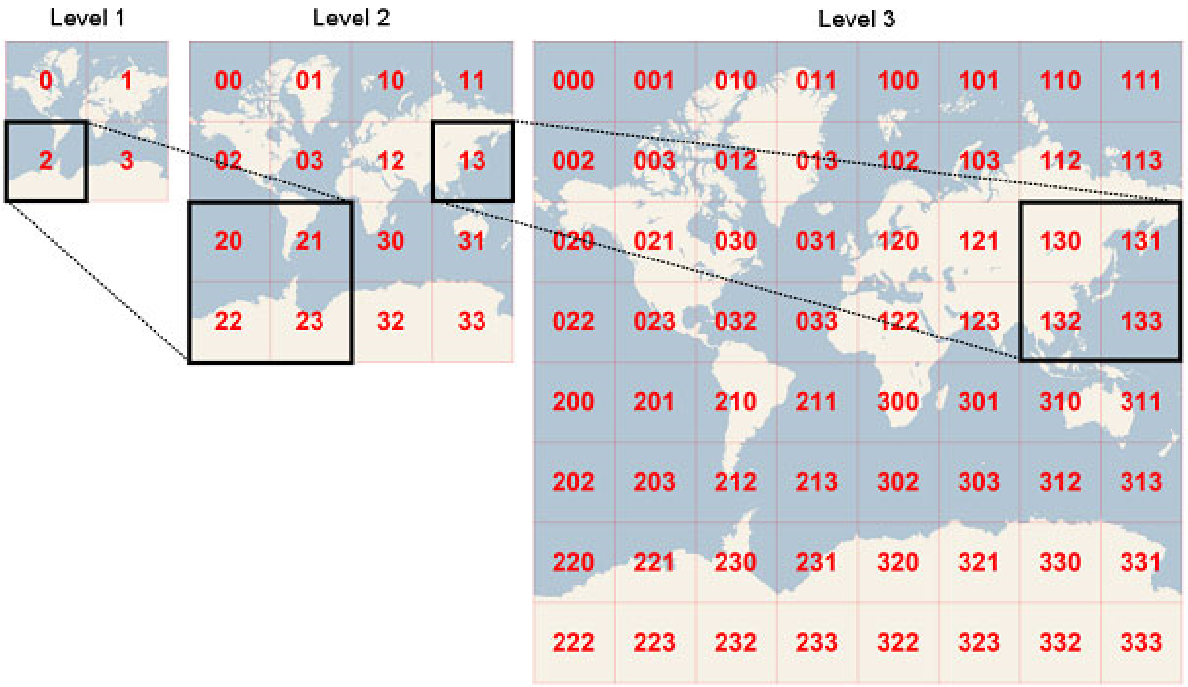
- In **Cache only** mode, the MapTiles Service tries to get the map tile images from the cache database.
- In **Server and cache** mode, the MapTiles Service tries to get the map tile images from the cache database first. If the map tile image is not available in the cache database, the MapTiles Service makes a request to the GIS map provider. When the map tiles image is received from the GIS map provider, it is stored in the cache database.

For some GIS maps providers, the cache database is not used due to the legal aspects.

The MapTiles Service can be used to build a secure environment where only computers with the MapTiles Service have access to the Internet.

Map Tile Images

The GIS Map control uses the map tile approach to create a result image of the current map view. In this case, the entire world is sliced into a square matrix. Each matrix cell contains a separate image called a map tile. The number of rows/-columns depends on the set zoom level. The value of the zoom level is in the range [0,24]. A higher zoom level value means a more detailed view of the map.



Each map tile image is requested from the GIS map provider. Query parameters are: Zoom level and cell coordinates. For some GIS map providers, the GIS maps provider key is also added to the query parameters.

The main advantage of this approach is the reuse of map tile images when the user changes the current map view (which reduces the number of requests to the GIS map provider).

If the request for a map tile image fails, the GIS map control uses the corresponding part of the map tile image of the lower zoom level. This is possible because the GIS Map control uses the Mercator projection to display the 3D world on a 2D surface.

Although the Mercator projection significantly distorts the scale and area (especially near the poles), it has two important properties that outweigh the scale distortion:

- This is a conformal projection, which means that the shape of relatively small objects is preserved. This is especially important when displaying aerial images, as we want to avoid distorting the shape of buildings. Square buildings must appear square, not rectangular.
- It is a cylindrical projection, which means that north and south are always straight up and down, and west and east are always straight left and right.

For more information, click on the following link: **https://en.wikipedia.org/wiki/Tiled_web_map**

Cache

The GIS-Map control has two levels of caching of map tile images:

- In-memory cache: the GIS map control stores the most recently retrieved map tile images in the in-memory cache. When the GIS map control needs a map tile image to display, it first searches the in-memory cache.
- Cache database: the GIS map control has a cache database for storing map tile images.

Some GIS map providers do not use the cache database for legal reasons.

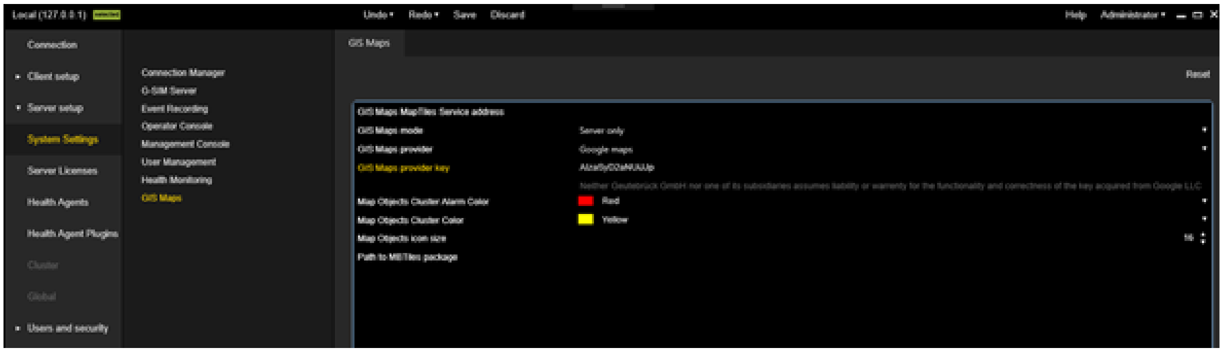
GIS Map Provider

The GIS map control can use different GIS map providers. The following providers are already implemented: Open Street Maps, Google Maps, Bing Maps.

The GIS map control is open for using own GIS map providers.

System Settings

The following **System Settings** can be configured for GIS maps. These settings are applied to all GIS map controls in Management Consoles and Operator Consoles.



GIS Maps MapTiles Service address

GIS Maps mode: Server only

GIS Maps provider: Google maps

GIS Maps provider key: AIzaSyD2aNUiUp

Neither Geutebruck GmbH nor one of its subsidiaries assumes liability or warranty for the functionality and correctness of the key acquired from Google LLC

Map Objects Cluster Alarm Color: 🟥 Red

Map Objects Cluster Color: 🟨 Yellow

Map Objects icon size: 16

Path to MBTiles package

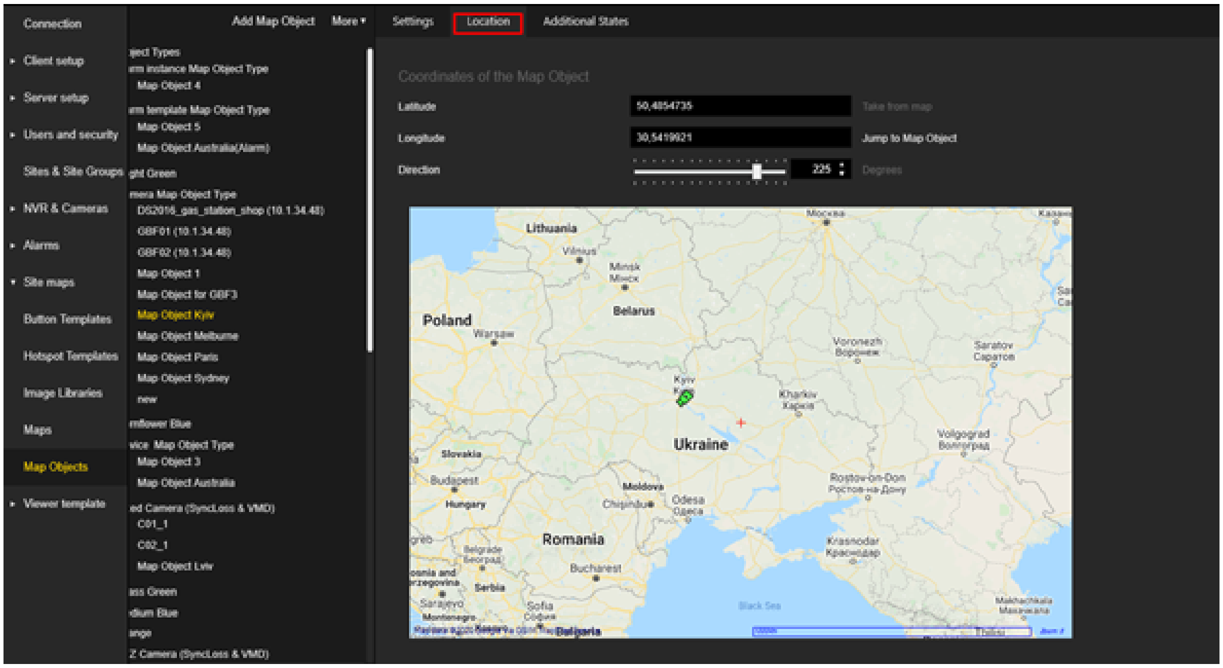
Setting	Description
GIS Maps MapTiles Service Adress	IP or hostname of the computer on which the MapTiles service is installed. The MapTiles Service acts as a proxy between the GIS map controller and the GIS map provider. When the address is specified, the GIS map control makes a request to the map tile service each time it needs a map tile image. The MapTiles Service uses the **GIS Maps provider**, **GIS Maps provider key**, **GIS Maps mode**, and **Path to MBTiles package** settings to obtain MapTiles images.

Setting	Description
	ⓘ **The MapTiles package provider is only available if the address of the Map Tile service is specified.**
GIS Maps mode	Three modes are available: - **Server only**: In this mode, the GIS map control makes a request to the map provider each time it needs a map tile image. If the request is successful, the MapTile image is displayed in the GIS Map control. If the request is not successful, an error message is displayed in the GIS Map control. - **Server and cache**: In this mode, the GIS Map control makes a request to the cache database each time it needs a MapTile image. If the request is not successful, the GIS map control makes a request to the map provider. If the request is successful, the MapTile image is added to the cache database and displayed in the GIS map control. If the request is not successful, an error message is displayed in the GIS Map control. - **Cache only**: This is the "Offline" mode. The GIS Map control attempts to retrieve the MapTile image from the cache database. If the MapTile image is retrieved, it is displayed in the GIS Map control, otherwise an error message is displayed in the GIS Map control. ⓘ **The Server and cache and Cache only options are not available for the Google Maps and Map Tiles Package provider.**
GIS Maps Provider	Select the provider to request map tiles images for GIS map control. Available providers are **Google maps**, **OpenStreetMap maps** and **Map tiles package**. The name of the provider is displayed at the bottom of the GIS map control.
GIS Maps Provider Key	Enter the license key for your maps provider. This setting is mandatory for the Google Maps provider. The key can be requested via https://developers.google.com/maps/documentation/maps-static/get-api-key.

Setting	Description
Map Objects Cluster Alarm Color	Defines the color for the icon of a map object cluster when one of the associated map objects is in alarm.
Map Objects Cluster Color	Defines the color for the symbol of a map object group.
Map Objects Icon Size	Defines the icon size of all GIS map objects and map object groups. ℹ **Changing the icon size may affect the grouping of map objects.**
Path to MBTiles package	The path to the MBTiles DataSet file on the computer running the MapTiles Service. This package will be used as offline tile source. This setting is mandatory for the MapTiles package provider. The MBTiles package can be obtained from the website https://openmaptiles.com/downloads/planet/. The MapTiles package provider supports both raster and vector datasets for MapTiles.

Map Object Settings

The map object settings for the GIS map are located in the **Map Objects** view in the **Location** tab.



Coordinates of the Map Object

Latitude 50,4854735

Longitude 30,5419921

Direction 225

Coordinates

If the trigger type of the selected map object type is **Camera** and the linked camera has coordinates, these are automatically used for the map object and the **Latitude** and **Longitude** fields and the **Take from map** button are disabled.

If the fields are still filled in, you can specify the **Latitude** and **Longitude** manually or click the **Take from map** button.

- The valid range for **Latitude** is [-90,90].
- The valid range for the **Longitude** is [-180,180].

Direction

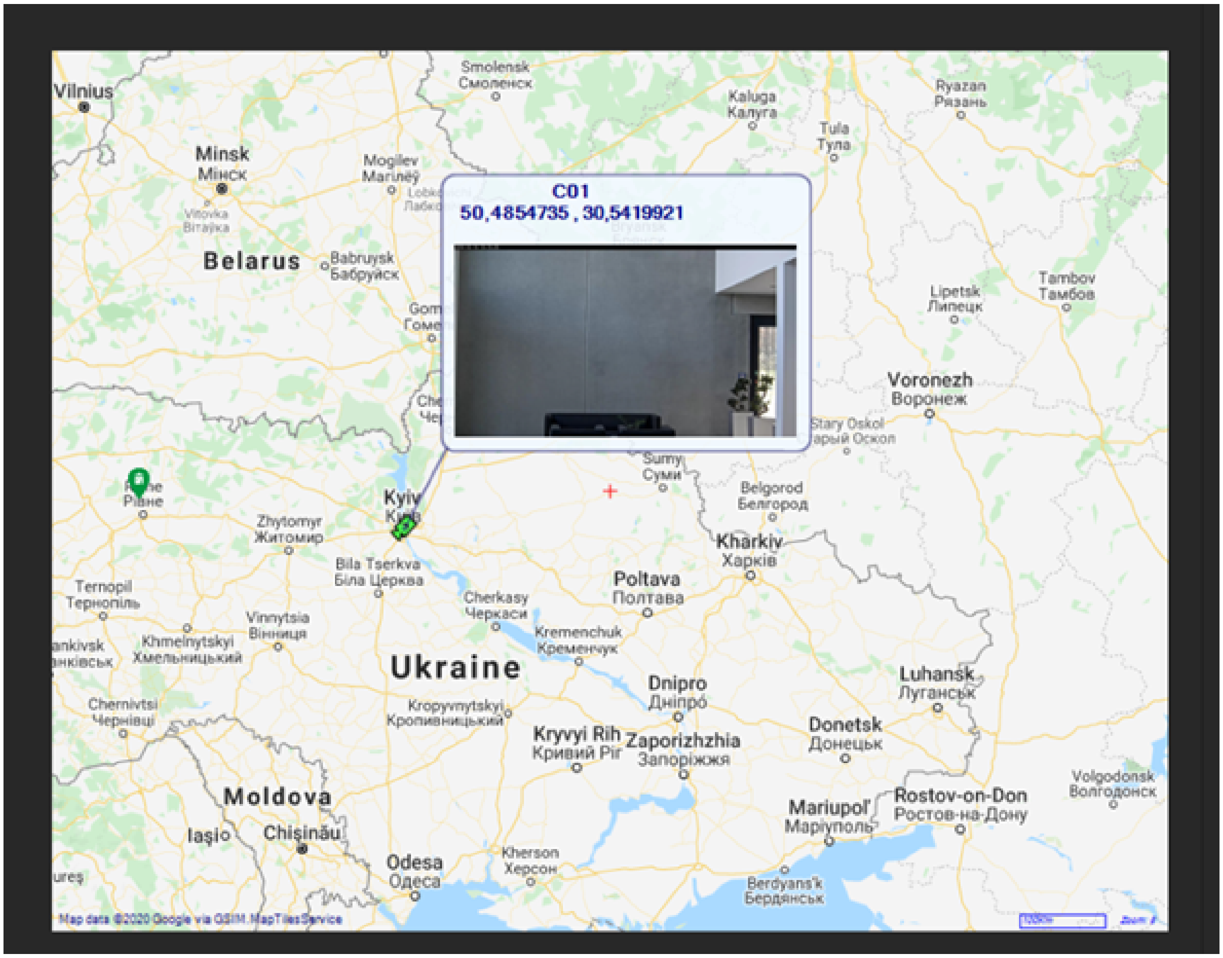
Direction can be set only for map objects whose display type is **Image**.

The valid range for is [-360,360] degrees.

This setting is displayed directly in the preview of the GIS map control.

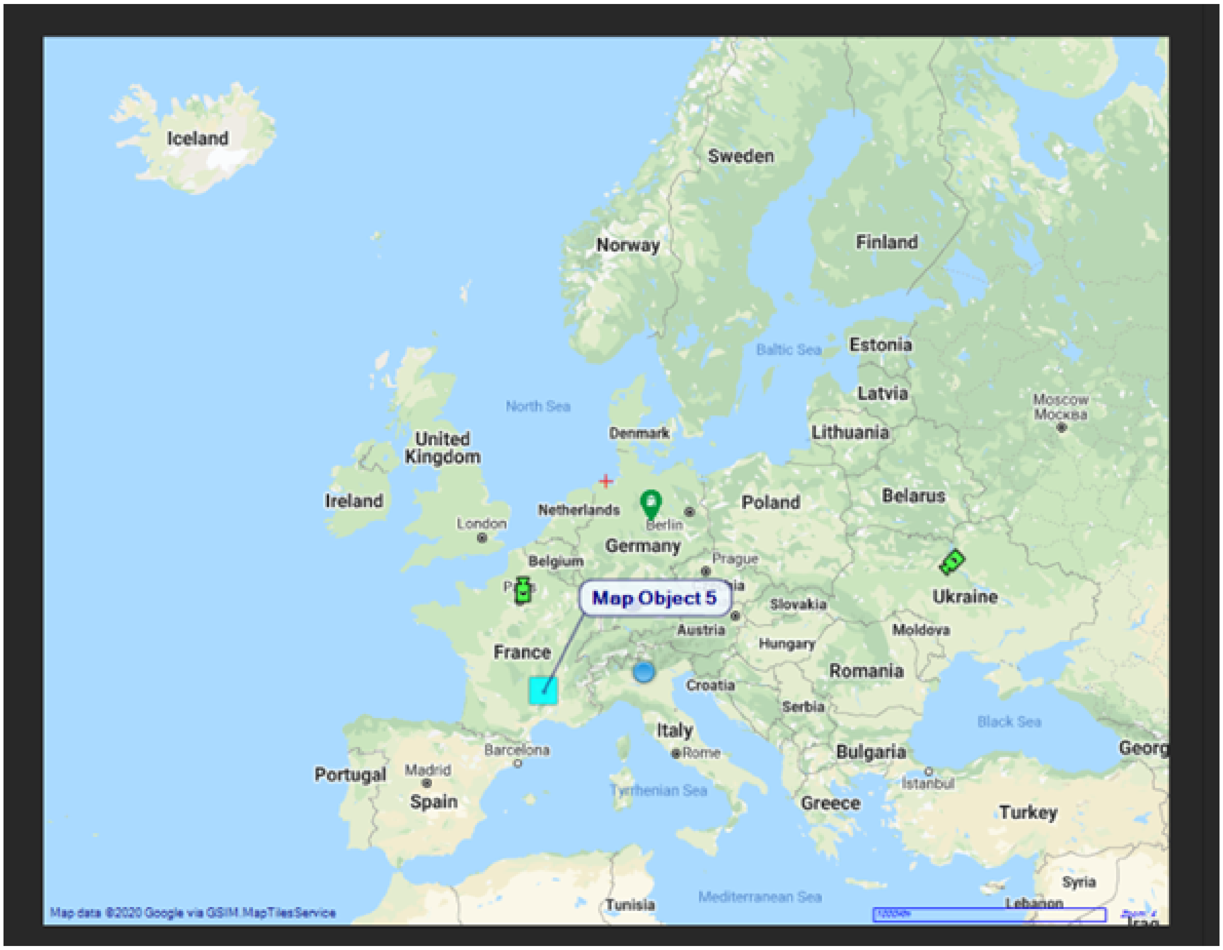
Object Tooltip

If the trigger type of the Map object type is **Camera**, the text in the tooltip is formatted according to the **Display Name Map** camera setting (see **Mediasources**). If present, a camera preview image is also displayed.

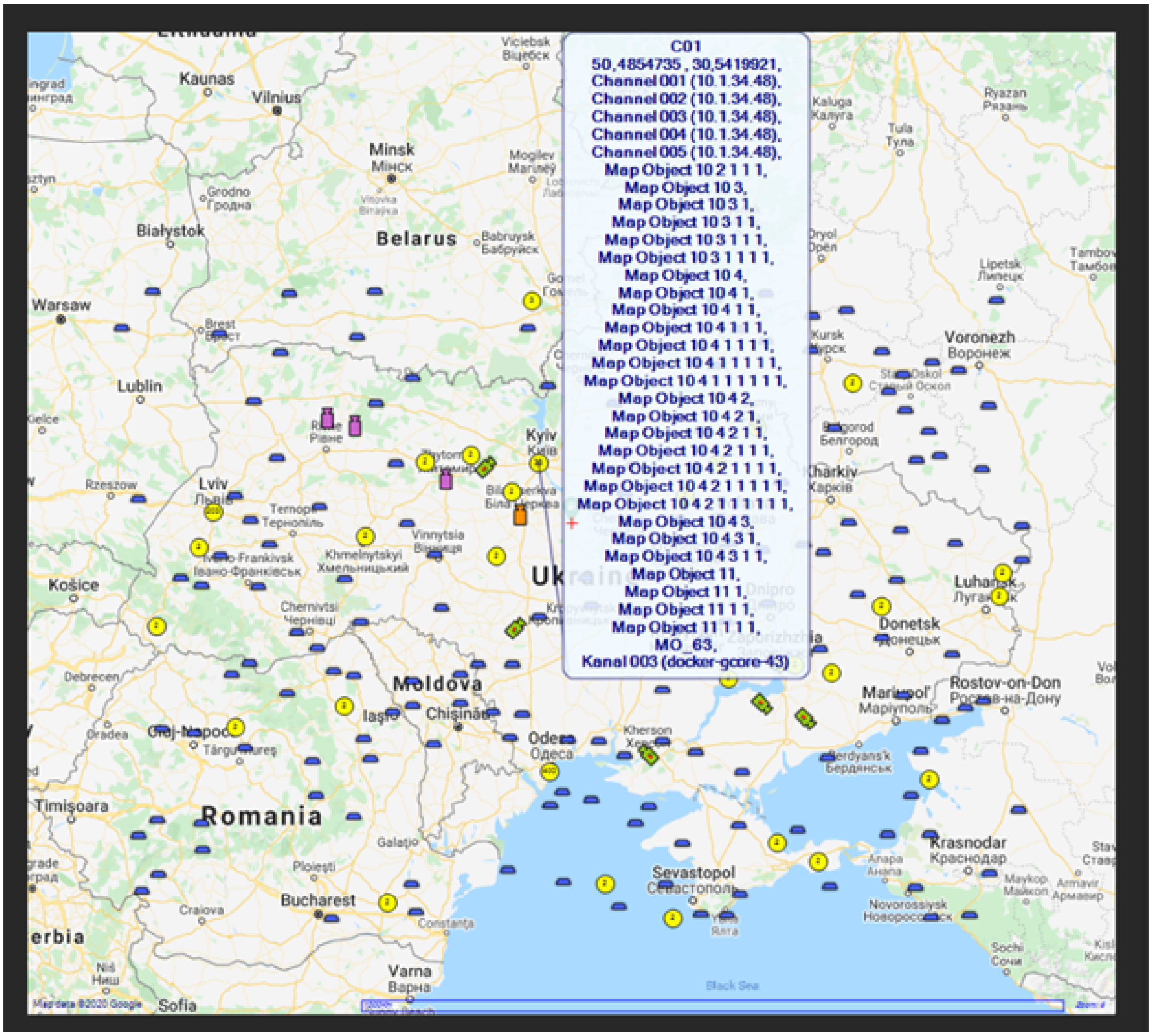


C01
50,4854735 , 30,5419921

If the trigger type of the Map object type is **Alarm / AlarmInstance / SystemComponent / None**, the name of the Map object is displayed.



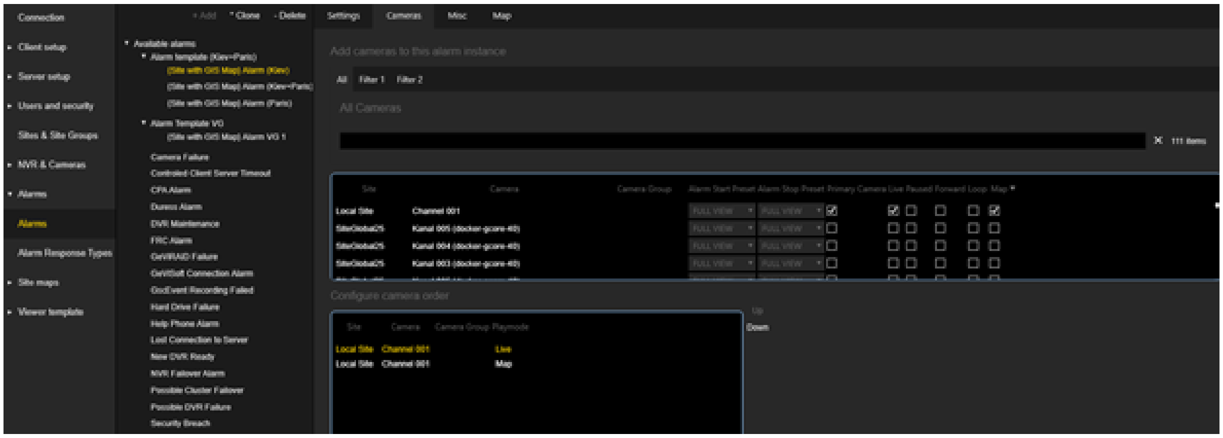
When map objects are merged into the map object grouping, the names of the map objects that are in the grouping are displayed in the tooltip.



C01
50,4854735 , 30,5419921,
Channel 001 (10.1.34.48),
Channel 002 (10.1.34.48),
Channel 003 (10.1.34.48),
Channel 004 (10.1.34.48),
Channel 005 (10.1.34.48),
Map Object 10 2 1 1 1,
Map Object 10 3,
Map Object 10 3 1,
Map Object 10 3 1 1,
Map Object 10 3 1 1 1,
Map Object 10 3 1 1 1 1,
Map Object 10 4,
Map Object 10 4 1,
Map Object 10 4 1 1,
Map Object 10 4 1 1 1,
Map Object 10 4 1 1 1 1,
Map Object 10 4 1 1 1 1 1,
Map Object 10 4 1 1 1 1 1 1,
Map Object 10 4 2,
Map Object 10 4 2 1,
Map Object 10 4 2 1 1,
Map Object 10 4 2 1 1 1,
Map Object 10 4 2 1 1 1 1,
Map Object 10 4 2 1 1 1 1 1,
Map Object 10 4 2 1 1 1 1 1 1,
Map Object 10 4 3,
Map Object 10 4 3 1,
Map Object 10 4 3 1 1,
Map Object 11,
Map Object 11 1,
Map Object 11 1 1,
Map Object 11 1 1 1,
MO_63,
Kanal 003 (docker-gcore-43)

Alarm Instance Settings

GIS Maps can be used for both **Viewer Group** and **Tab View** alarm presentation mode. GIS maps and regular maps can be combined in a single alarm instance.



Site	Camera	Camera Group	Alarm Start Preset	Alarm Stop Preset	Primary Camera	Live	Paused	Forward	Loop	Map
Local Site	Channel 001		FULL VIEW	FULL VIEW	☑	☑	☐	☐	☐	☑
SiteGlobal25	Kanal 005 (docker-gcore-40)		FULL VIEW	FULL VIEW	☐	☐	☐	☐	☐	☐
SiteGlobal25	Kanal 004 (docker-gcore-40)		FULL VIEW	FULL VIEW	☐	☐	☐	☐	☐	☐
SiteGlobal25	Kanal 003 (docker-gcore-40)		FULL VIEW	FULL VIEW	☐	☐	☐	☐	☐	☐

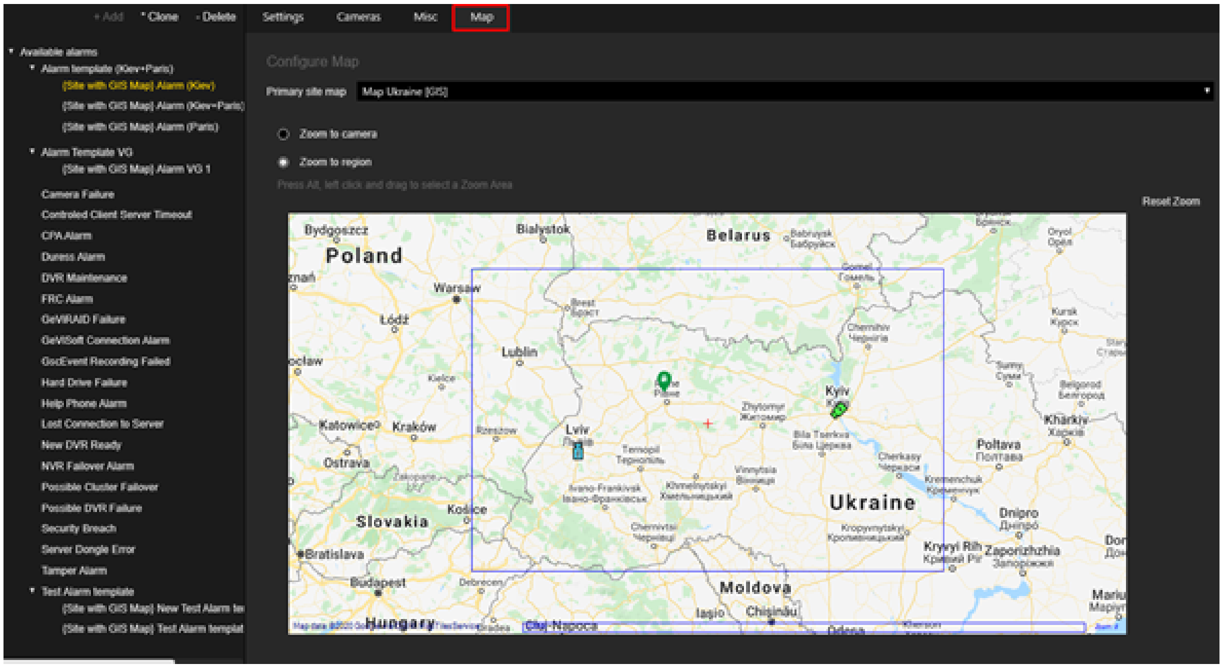
Site	Camera	Camera Group	Playmode
Local Site	Channel 001		Live
Local Site	Channel 001		Map

To determine which map to display, the following algorithm is used:

1. Determine the Map object with the **Camera** trigger type to which the current camera is associated.
2. Determine the primary Map value of the Map object.

GIS Map can be selected as the primary location map on the Map tab. This map will be used for each camera with the **Map** playback mode.

Select the GIS map that contains all map objects tagged to the cameras of the alarm instance with the Map playback mode.



Primary site map: Map Ukraine [GIS]

○ Zoom to camera

● Zoom to region

Press Alt, left click and drag to select a Zoom Area

The following options are possible for the zoom settings:

Option	Description
Zoom to camera	The map of the primary location is placed in the viewer, centered on the camera and zoomed to the maximum zoom level of the GIS maps. The zoom level can be overridden with the **Override default zoom level** check box.
Zoom to region	The map of the primary location is placed in the viewer and zoomed to the specified zoom area. To set the zoom area, hold down the ALT key and the left mouse button and drag the mouse cursor.

Map Objects

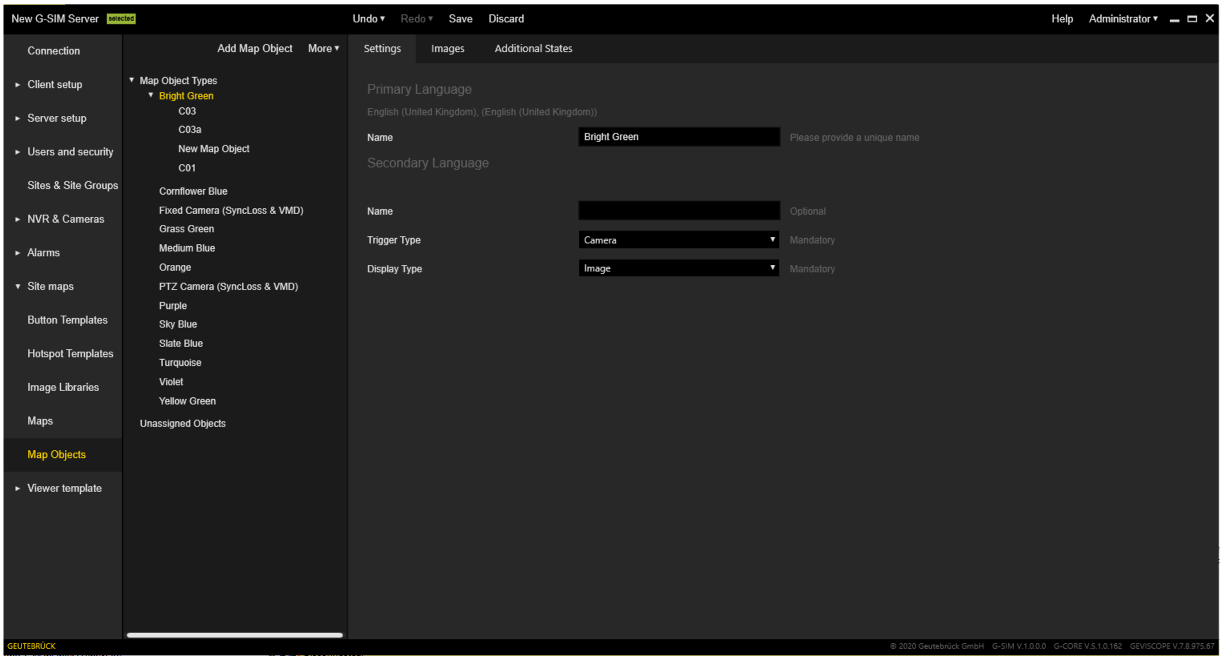
The menu has a tree view with the following structure:

- Top-level nodes: Map Object Types (contains existing map object types) and Unassigned Objects (contains map objects that have been added to the map but not assigned to a specific type).
- Map Object Type nodes: These nodes represent map object types, and each has map objects as child nodes.
- Map Object nodes: These nodes are instances of map objects types and represent map objects that were added to the map.

Settings

The Settings tab allows the user to specify the Name (for primary and secondary language), Trigger Type and Display Type.

You can define the description of a button in two places. In the Settings tab, if you have selected the option Button as Display Type. In the Additional States tab, if you have selected the option Button in the Configure Image or Button area.
If you have defined the description of the button in both places, the description you have defined in the Settings tab will be overlapped by the description in the Additional States tab.
Therefore, be sure to define the description of the button in only one place.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Bright Green — Please provide a unique name

Secondary Language

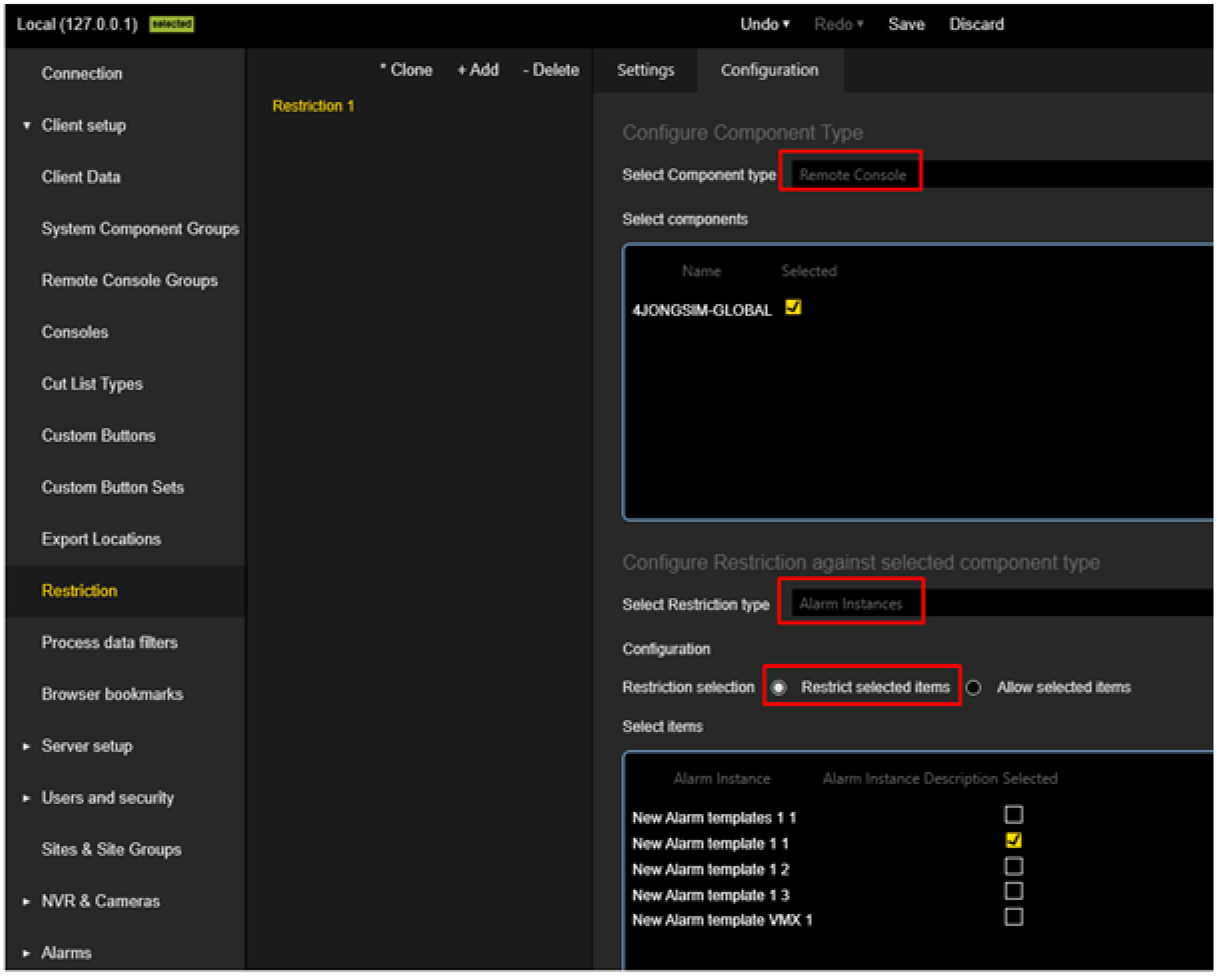
Name: — Optional

Trigger Type: Camera — Mandatory

Display Type: Image — Mandatory

Alarm Logic

To limit alarms by displaying them only on specific RemCons, alarm templates / instances for the specific ReCons can be restricted in the Management Console **Restriction** view.



Configure Component Type

Select Component type: Remote Console

Select components

Name	Selected
4JONGSIM-GLOBAL	☑

Configure Restriction against selected component type

Select Restriction type: Alarm Instances

Configuration

Restriction selection ● Restrict selected items ○ Allow selected items

Select items

Alarm Instance	Alarm Instance Description	Selected
New Alarm templates 1 1		□
New Alarm template 1 1		☑
New Alarm template 1 2		□
New Alarm template 1 3		□
New Alarm template VMX 1		□

Navigate into the restrictions **Configuration** tab.

As **Component type** select Remote Console. Select the Remote Console which should be restricted in the section below.

Than select for **Select Restriction type Alarm Instances**.

The appropriate radio button on the **Restriction Selection** group chooses to restrict or allow items .

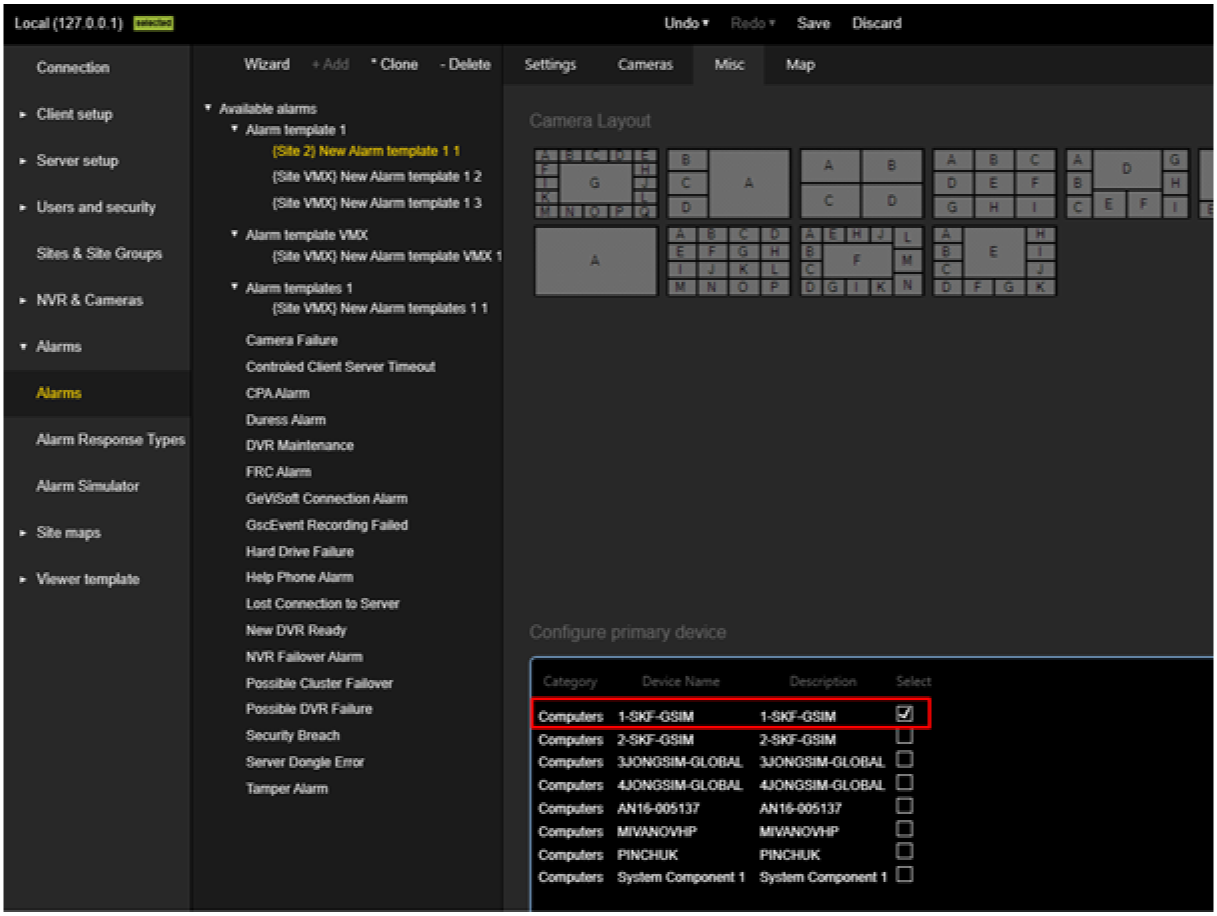
If **Restrict selected items** is selected, the alarm templates / instances selected below will be hidden.

If **Allow selected items** is selected, the alarm templates / instances selected below will be shown.

Primary Device

Primary Devices can be used to create Map Objects with the system component **Trigger Type**. If an Alarm with primary device is triggered, then all Map Objects with the System Component **Trigger Type** that are linked to this device will be entered in Alert-On state. So they will flash on the map.

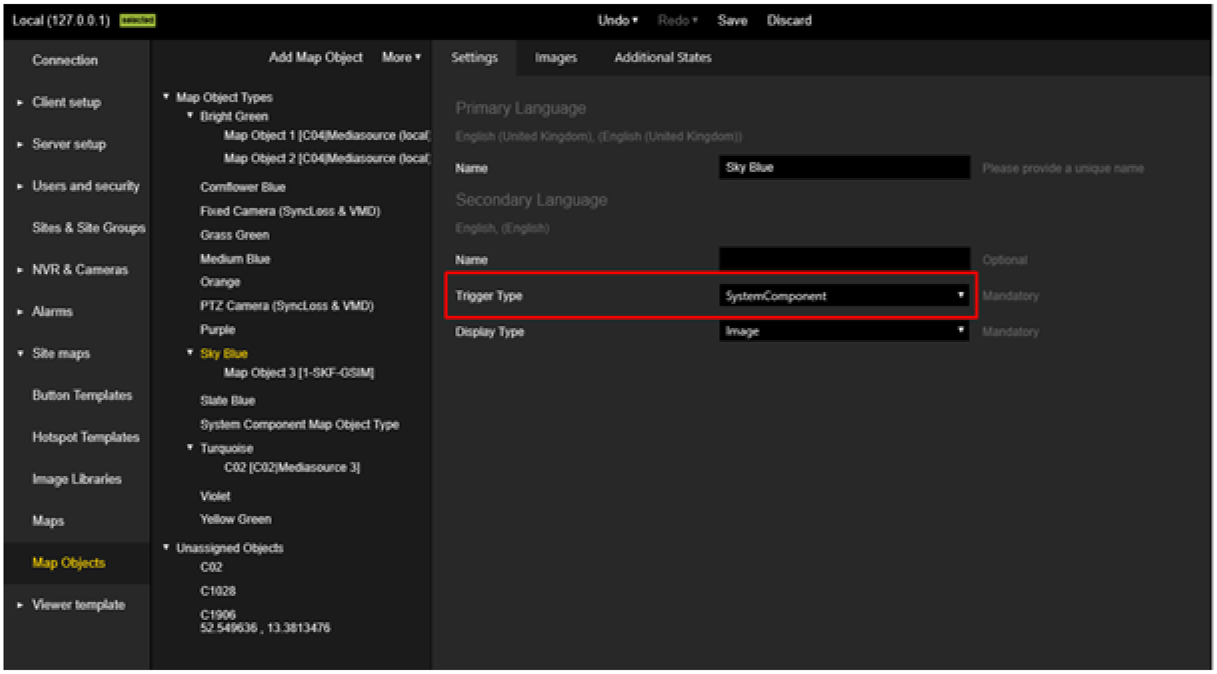
A Primary Device can be added to alarm template / instances in the Management Console via the **Misc** Tab. By selecting a device in the **Configure primary device**box the device will be added to the alarm template / instance as primary device.



Category	Device Name	Description	Select
Computers	1-SKF-GSIM	1-SKF-GSIM	☑
Computers	2-SKF-GSIM	2-SKF-GSIM	□
Computers	3JONGSIM-GLOBAL	3JONGSIM-GLOBAL	□
Computers	4JONGSIM-GLOBAL	4JONGSIM-GLOBAL	□
Computers	AN16-005137	AN16-005137	□
Computers	MIVANOVHP	MIVANOVHP	□
Computers	PINCHUK	PINCHUK	□
Computers	System Component 1	System Component 1	□

For each Map Object Type a trigger can be selected that determines when Map Objects belonging to this Map Object Type switch to alarm mode.

In the **Settings** tab of the Map Object Type select the **Trigger Type System Component**.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Sky Blue — Please provide a unique name

Secondary Language

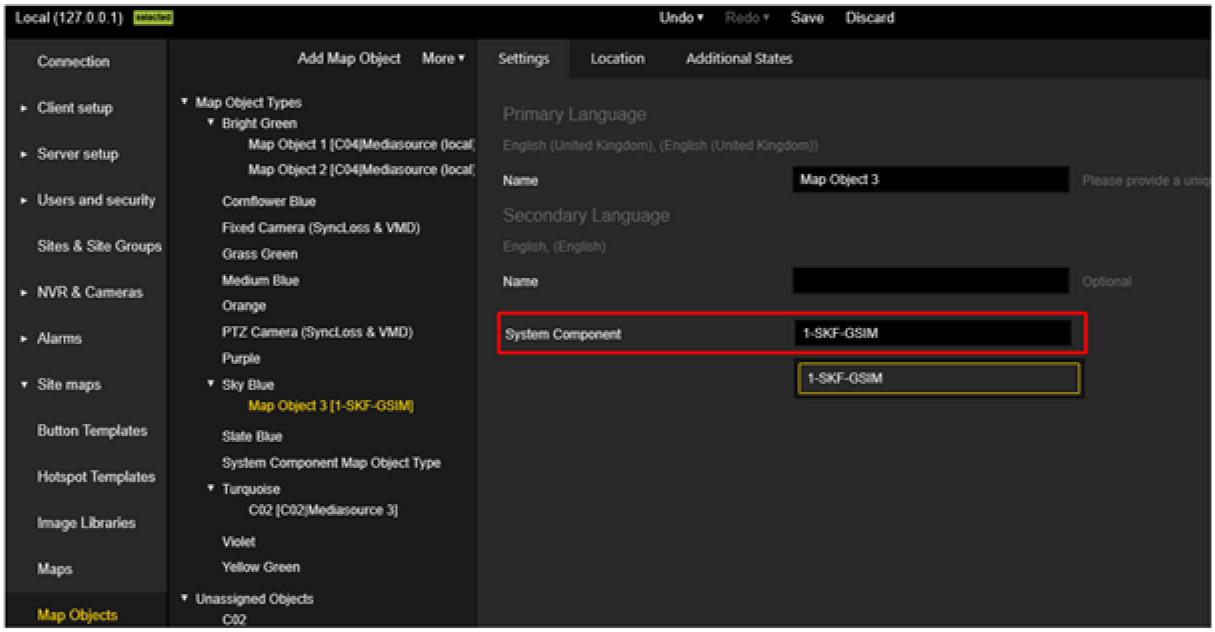
English, (English)

Name: — Optional

Trigger Type: SystemComponent ▾ — Mandatory

Display Type: Image ▾ — Mandatory

In the **Settings** Tab of the Map Object itself select as **System Component** the primary device.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Map Object 3 — Please provide a uniq

Secondary Language

English, (English)

Name: — Optional

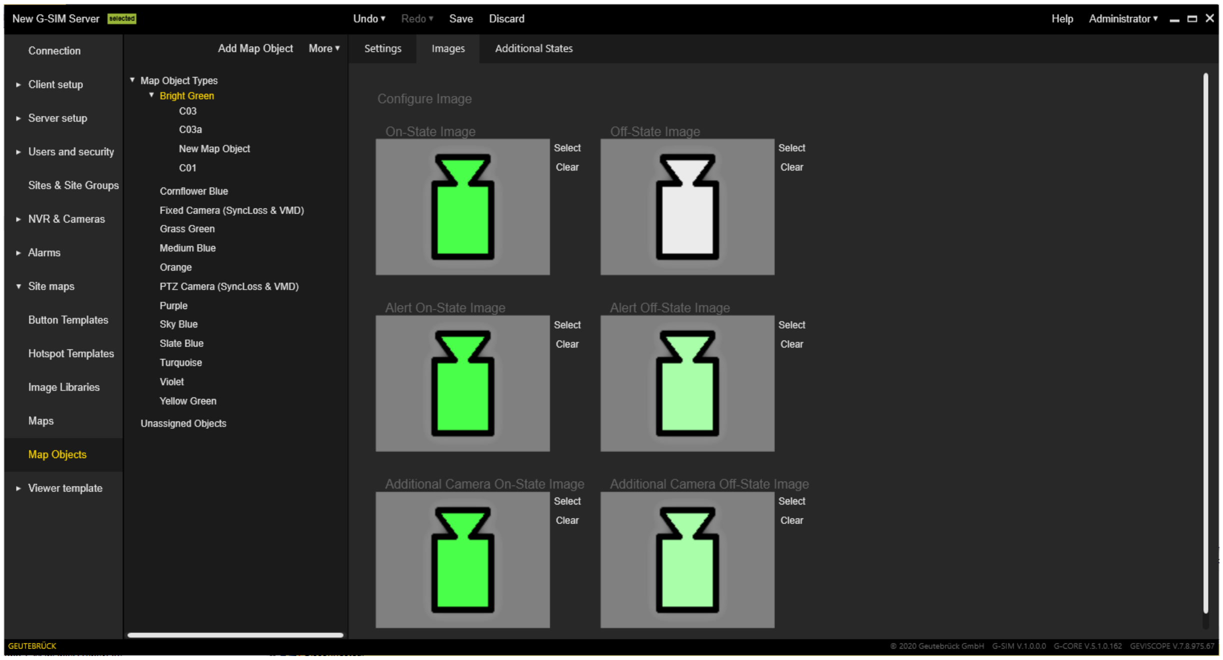
System Component: 1-SKF-GSIM

1-SKF-GSIM

Images

The **Images** tab allows the user to set images of map objects of the selected type for different states:

- On
- Off
- Alert On
- Alert Off
- Additional Camera On
- Additional Camera Off



Additional States

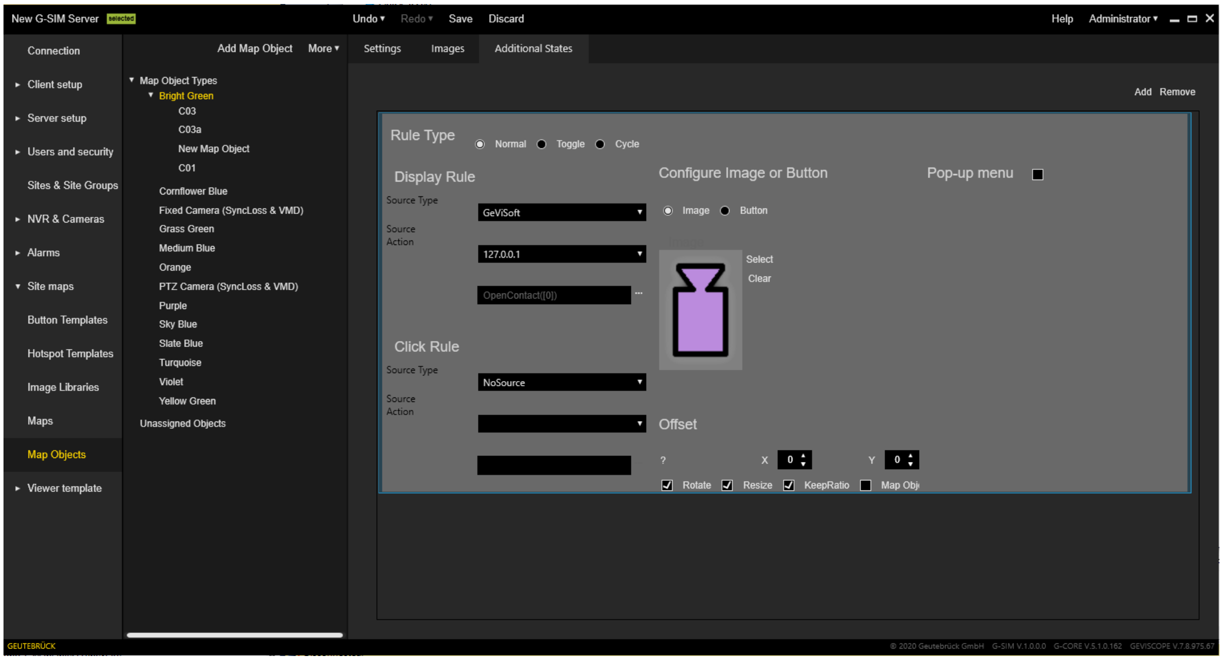
The **Additional States** tab allows the user to configure additional states for map object types.

Additional states can be added or removed using the **Add** or **Remove** buttons in the upper right corner.

The Additional State tab consists of six areas:

- Rule Type
- Display Rule
- Click Rule

- Configure Image or Button
- Pop-up menu
- Offset



Rule Type ● Normal ○ Toggle ○ Cycle

Display Rule
Source Type: GeViSoft
Source: 127.0.0.1
Action: OpenContact([0])

Configure Image or Button ● Image ○ Button

Pop-up menu □

Click Rule
Source Type: NoSource
Source:
Action:

Offset
? X 0 Y 0
☑ Rotate ☑ Resize ☑ KeepRatio □ Map Obj

You can define the description of a button in two places. In the Settings tab, if you have selected the option Button as Display Type. In the Additional States tab, if you have selected the option Button in the Configure Image or Button area.
If you have defined the description of the button in both places, the description you have defined in the Settings tab will be overlapped by the description in the Additional States tab.
Therefore, be sure to define the description of the button in only one place.

Rule Type

There are three rule types for additional states: Normal, Toggle and Cycle.

Select a rule type depending on the intended use and what type of source is used for the state changes.

Display Rule

The Display Rule area contains the following settings:

Settings	Description
Source Type	The source type for a display rule depends on the rule type. The following source types are available: • NoSource • GeViSoft • GeViScope • AlarmType The rule type **Toggle** cannot have **Alarm Type** as source.
Source / Action	Depending on the selected source type, the Source drop-down field lists the possible sources and the Action drop-down field lists the corresponding actions.

Click Rule

The Click Rule area contains the following settings:

Settings	Description
Source Type	The source type for a click rule depends on the rule type. The following source types are available: • NoSource • GeViSoft • GeViScope • AlarmType The rule type **Toggle** cannot have **Alarm Type** as source.
Source / Action	Depending on the selected source type, the Source drop-down field lists the possible sources and the Action drop-down field lists the corresponding actions.

Pop-Up Menu

When you have specified a click rule, you can define an additional pop-up menu that explains what the click rule does. To do this, select the checkbox **Pop-up menu**.

This pop-up menu and the text defined there will be displayed when someone right-clicks on the state image.

Edit Instance Definition

Note that only the appropriate type is defined in these settings. For an actual instance to react as desired, you must go to the instance definition of the map object and edit it there (to do this, expand the type in the type list to go to the instance definition).

For example, for a toggle connected to a digital input on a DVR, you must go to the instance, select the appropriate display rule and click the action. A dialog box will appear where you must enter the relevant details such as DVR name and Digital Input number.

Camera-Linked States

Additional states can be linked to a camera (e.g. video synchronisation failed). Currently, **BlockingFilter** is the only action where you can choose whether to link to a camera.

In camera-linked states, the source (DVR) and the global channel number of the camera are extracted from the camera - no parameters need to be filled in. This is also the case with **BlockingFilter**, where **Connect Camera** is selected.

In the case of the selected **BlockingFilters** action connected to the camera, the filter is appended with the camera channel number. If the definition is **BlockingFilterDeactivate("[DISARM_[cam]]])**, the instance for camera 303 in its display rule will be **BlockingFilterDeactivate("DISARM_303")**.

Note that the text [cam] is automatically generated when [link camera] is selected. The correct event name on the DVR is **DISARM_303**.

This is another example that demonstrates why it is important to complete your DVR configuration and setup before starting configuration in G-SIM.

The parameters of actions that are not camera linked are not automatically filled in, even if some of the actions for the map object type are camera linked.

For example, if a video synchronisation failed and you set the digital output, the parameters for the failed synchronisation are extracted from the camera, but you need to set the parameters for the digital output.

Parameters

Parameters used in the map object type template are used as variables: If you have a digital input(0) and a digital output(0) set, this means that you want to use the same contact number for both the input and the output. You also have the option to specify only one contact ID.

Use two different numbers in the template if you want them to be different in implementation.

The number can be any number. If it is a "global" contact that should be the same for all implementations, specify the correct contact ID from the beginning. It is used as the default ID in the implementation and is correct for all implementations of this card object type.

The same applies to the source of the additional states, as described above for simple parameters. The source selected in the template is used as a variable in the implementations. If all actions have the same source, select the same source for all in the template. If you want the source for implementations to be the same, select the correct source in the template as it is used as the default.

You can provide your own images or choose from our large image archive (library).

Offset

Once you have selected an image, you can use the X and Y offset values to move it away from the associated map object image (by default it is located in the centre of the image and at the top of the image). In relation to the linked object image, you can also allow rotation (Rotate), resizing (Resize) and ratio behavior when resizing (KeepRatio).

When the Map Object check box is selected, the selected click rule is triggered when the operator clicks on the image of the associated map object. This is useful if the state image is very small and difficult to click on, or if a particular action is required when the map object itself is clicked on.

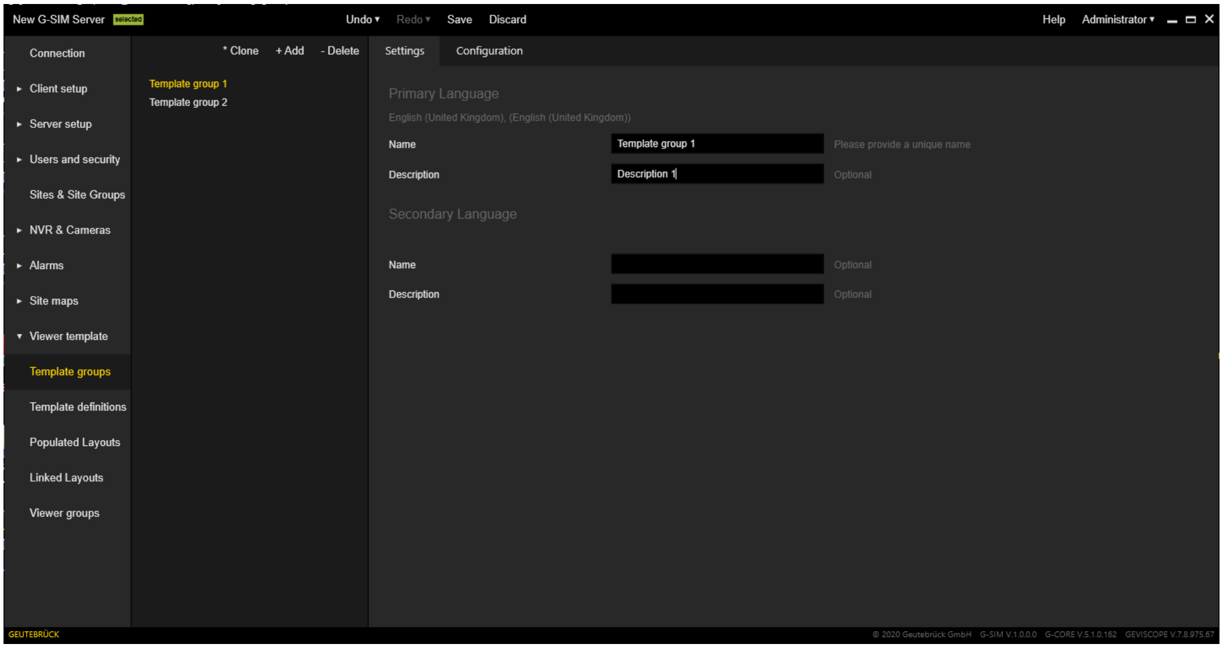
Viewer Template

Template Groups

The Template groups view allows the user to manage the template groups.

Settings

The Settings tab contains name and description fields for both the primary and secondary language.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name: Template group 1 — Please provide a unique name

Description: Description 1 — Optional

Secondary Language

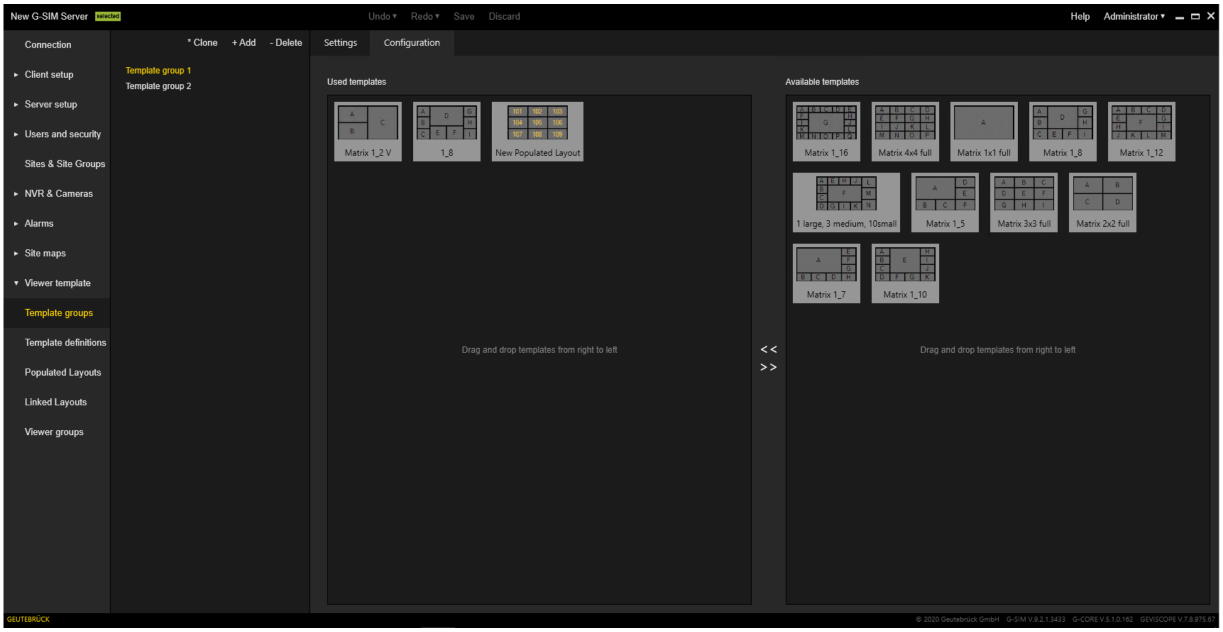
Name: — Optional

Description: — Optional

Configuration

The **Configuration** tab contains a layout selector that allows you to configure template groups with layouts. It consists of two areas:

- **Used templates**: Contains layouts that are assigned to the selected template group.
- **Available templates**: Contains all layouts that can be assigned to the selected template group.



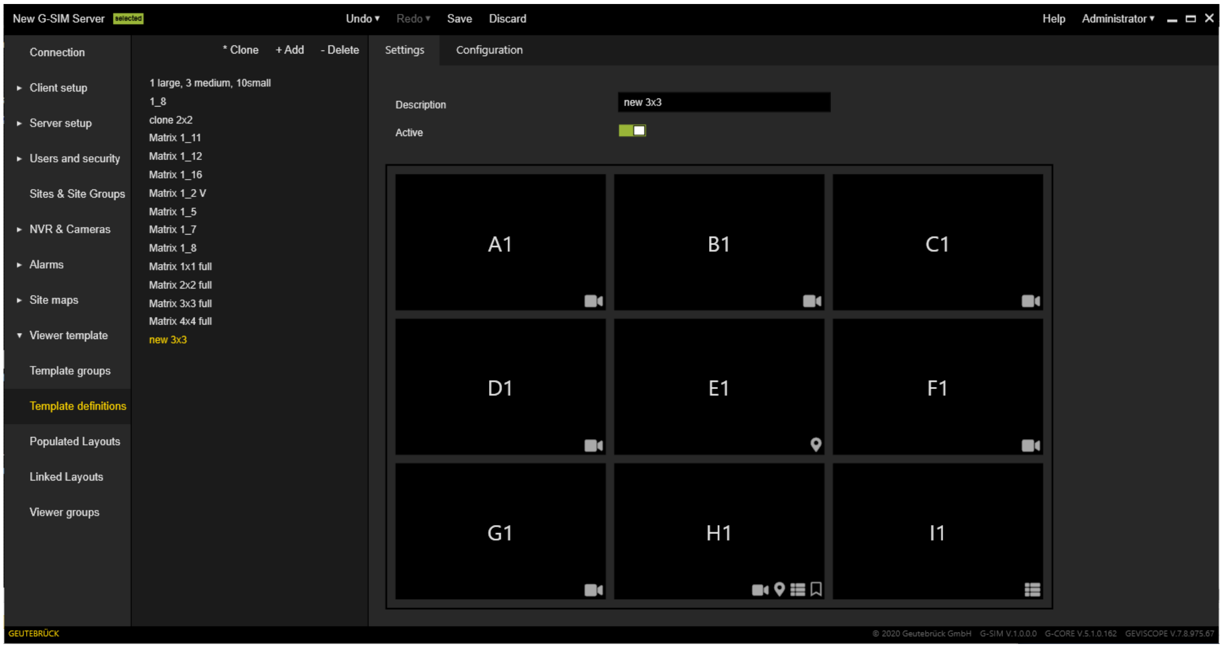
Template Definitions

The **Template definitions** view allows the user to configure predefined layouts or create new layouts.

Settings

The **Settings** tab contains the following settings:

- **Description**: Allows the user to configure the description for the selected layout.
- **Active**: The switch enables or disables the selected layout.

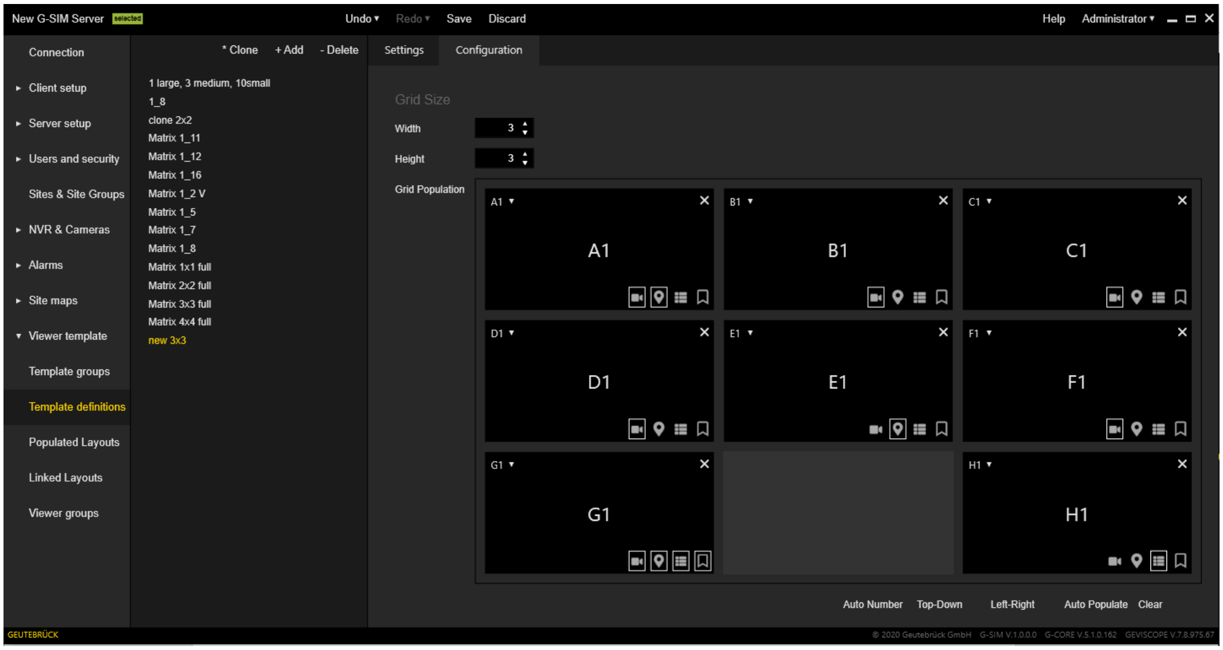


Description: new 3x3

Active: ●

Configuration

The **Configuration** tab contains the following settings:



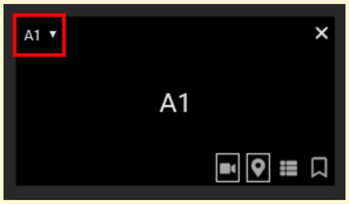
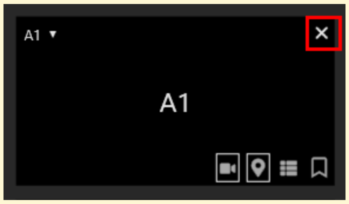
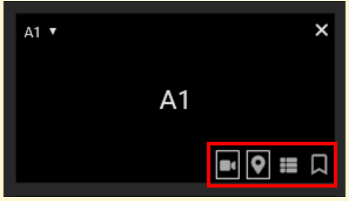
Width 3

Height 3

Settings	Description
Width / Height	Defines the grid resolution of the editor. A higher resolution allows you to configure more complex layouts.
Grid Population	An editor that allows you to configure the selected layout and set the number of viewers and content restrictions.
Auto Number	Automatic assignment of viewer numbers in an appropriate order.
Top-Down / Left-Right	Assign viewer numbers in an appropriate order.
Auto Populate	Fills all grid cells with a viewer cell.
Clear	Removes all viewer cells from the grid.

Viewer cell

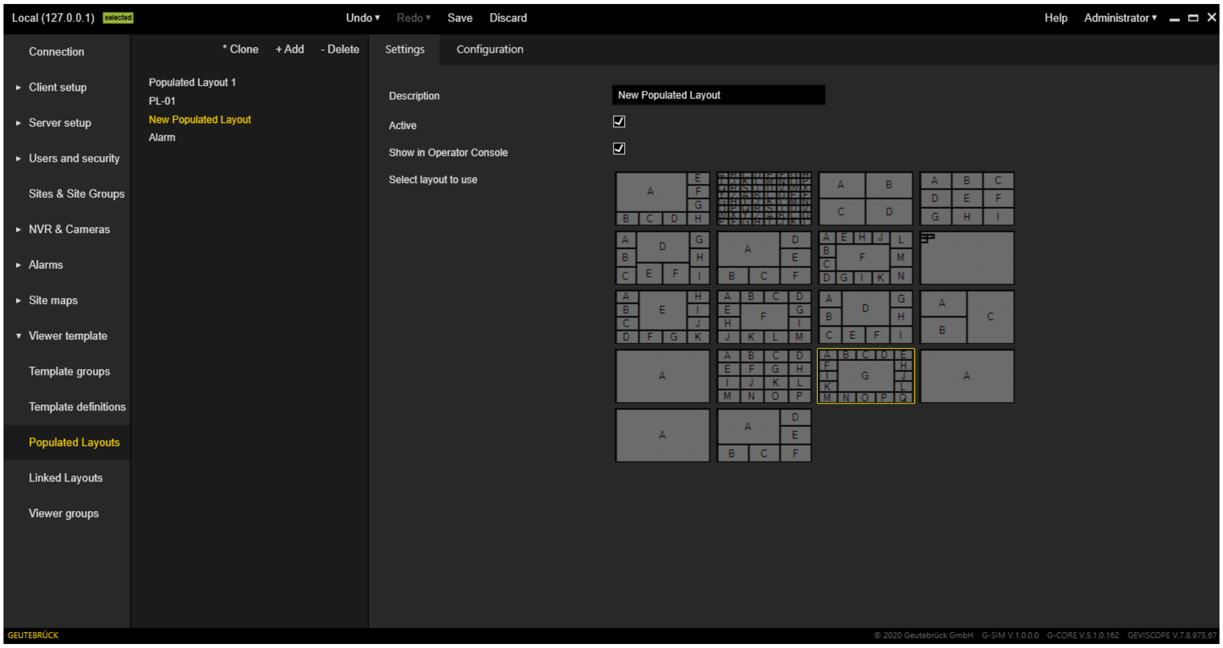
The viewer cell contains the following elements:

Element	Description
Viewer number selector  	Allows the user to select viewer number from the list of available numbers.
Close button  	Removes the viewer cell from layout.
Buttons for allowed content types  	When a button is pressed, it means that the appropriate content type is allowed. • Video • Map • List • Browser bookmark

Populated Layouts

Settings

The **Settings** tab contains the following settings:



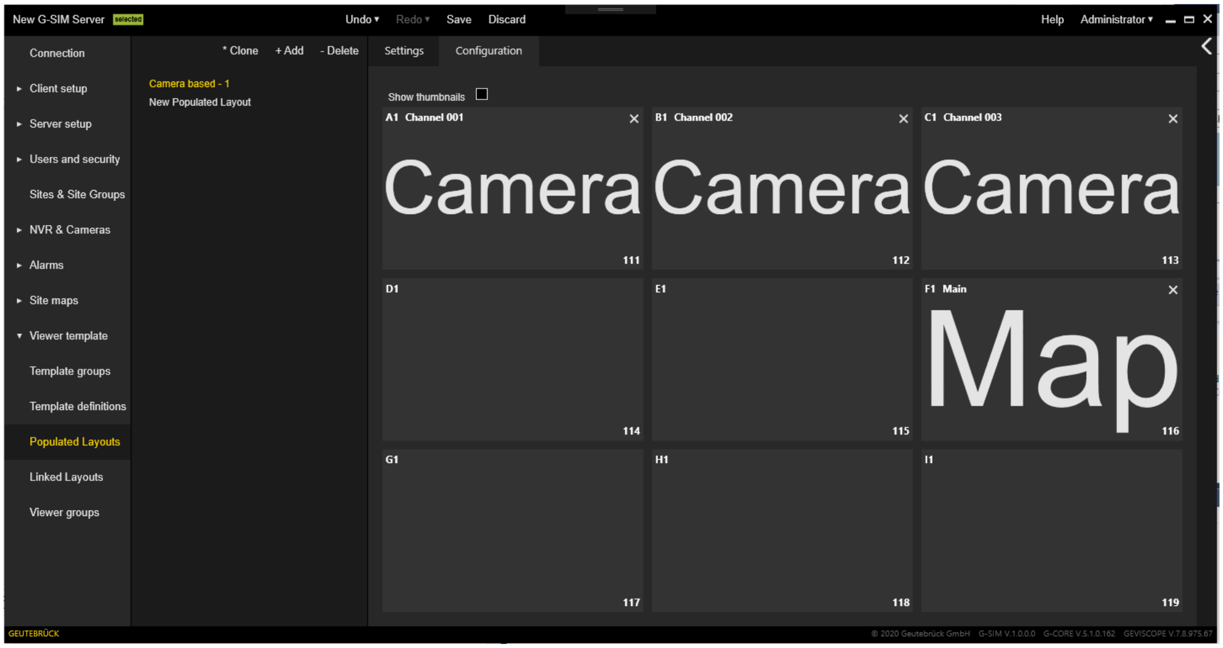
Populated Layout 1
PL-01
New Populated Layout
Alarm

Description: New Populated Layout
Active: ☑
Show in Operator Console: ☑
Select layout to use

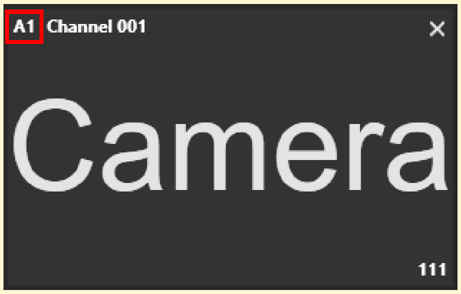
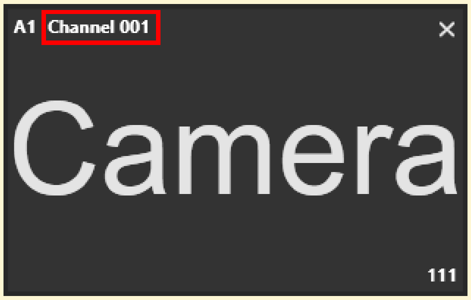
Settings	Description
Description	Allows the user to configure the description for the selected populated layout.
Active	Select the checkbox to activate the populated layout.
Show in Operator Console	Allows you to use the layout in the template selector.
Select layout to use	Allows the user to select already defined template definitions.

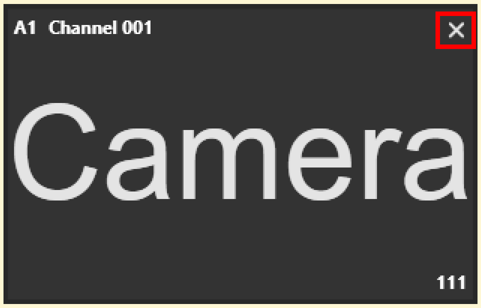
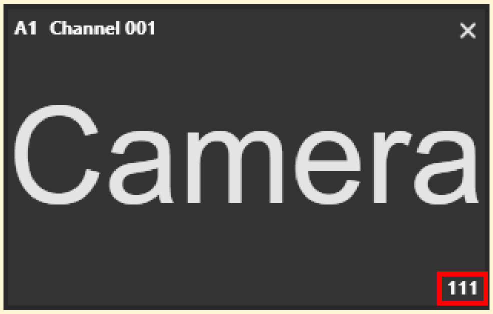
Configuration

The **Configuration** tab contains a layout editor that is used to configure the contents of the viewer.



A single viewer contains:

Element	Description
	Viewer number
	Content name / description

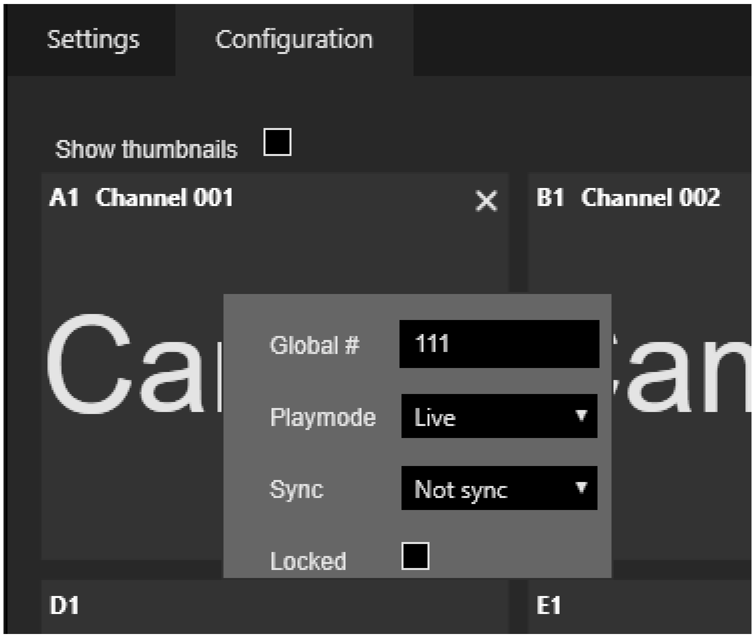
Element	Description
	Clear button Removes content from a viewer.
	Global number

If the contents of the viewer have a reference image, it can be displayed by selecting the **Show thumbnail** checkbox.

The viewer configuration is performed in the following ways:

- The viewer content is moved by a drag and drop action from the contents list to a viewer.
- Global number (**Global #**), **Playmode**, **Sync** and locking is configured through

a context menu on each single viewer.



Show thumbnails ☐

Global # 111

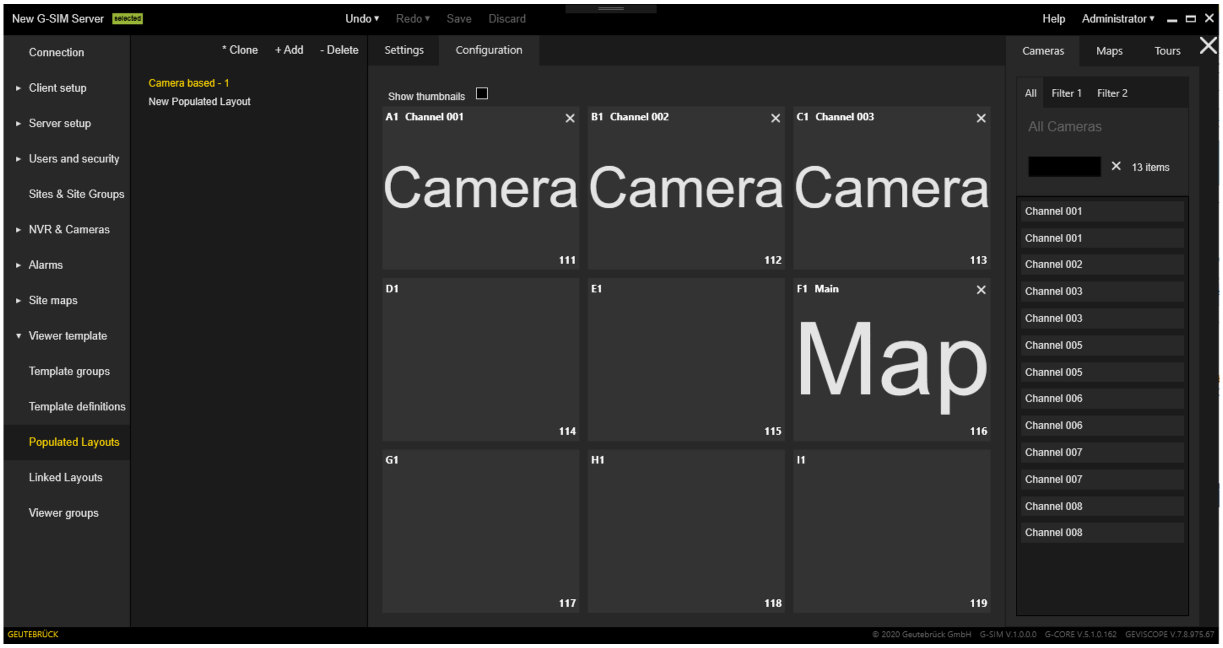
Playmode Live

Sync Not sync

Locked ☐

Content List

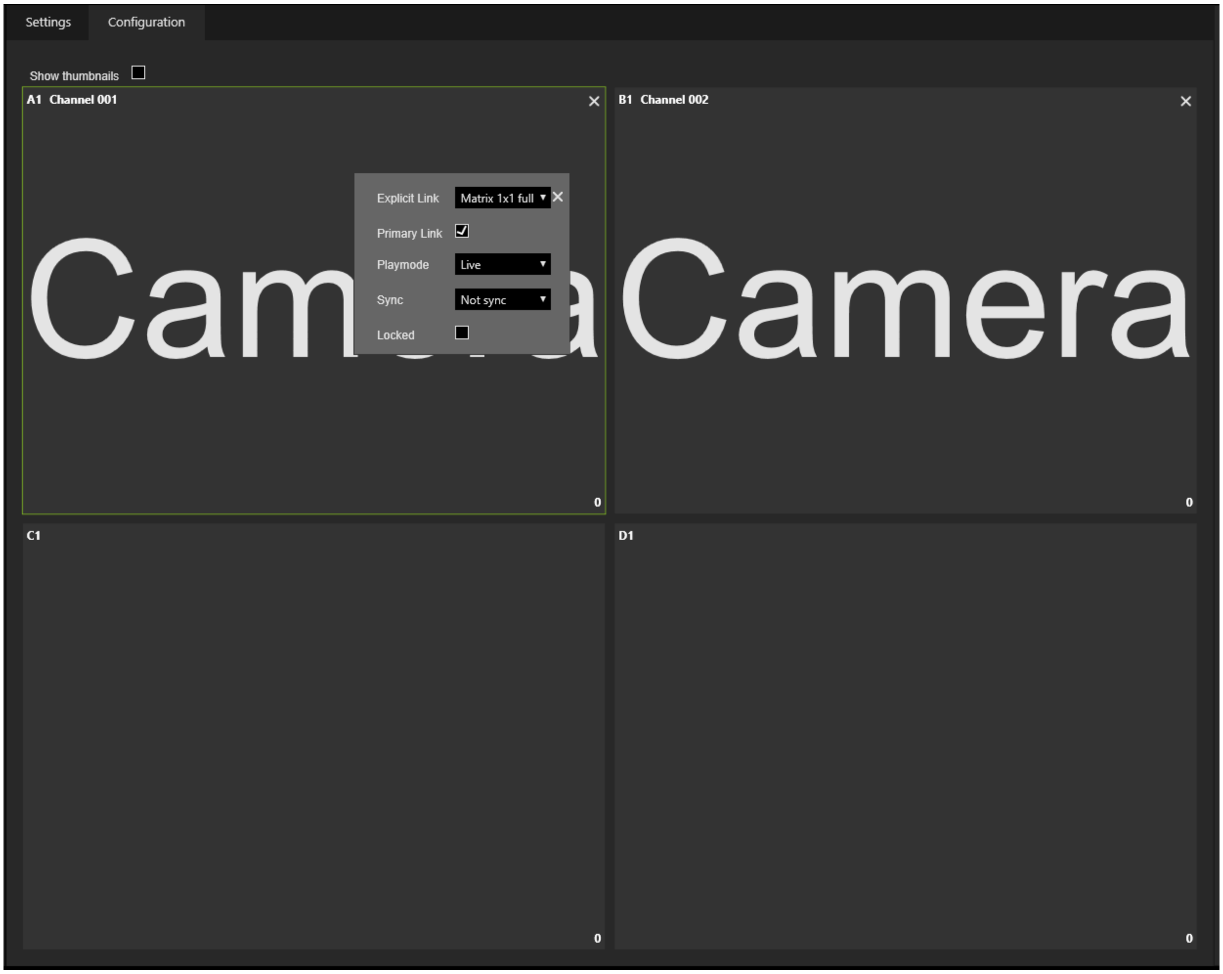
The content lists area is visible when the **Configuration** tab is visible. It can be expanded and collapsed. Content lists contain tabs with media contents that can be dropped on a viewer. Each contents tab has filter tabs.



Linked Layouts

The configuration of linked layouts has the same interface as populated layouts.

The configuration for an **Explicit Link** or **Primary Link** is done via a context menu on a single viewer.



Show thumbnails ☐

Explicit Link: Matrix 1x1 full ▾

Primary Link ☑

Playmode: Live ▾

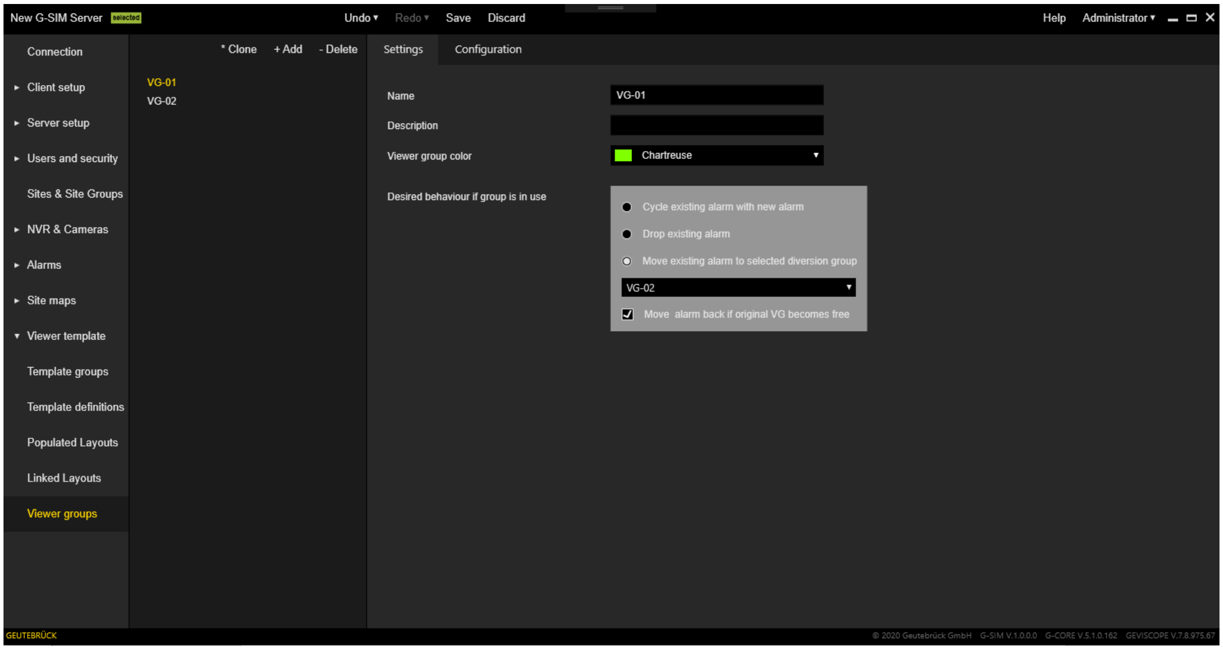
Sync: Not sync ▾

Locked ☐

Viewer Groups

Settings

The **Settings** tab contains the following settings:



Name: VG-01

Description:

Viewer group color: 🟩 Chartreuse ▾

Desired behaviour if group is in use

- ● Cycle existing alarm with new alarm
- ● Drop existing alarm
- ○ Move existing alarm to selected diversion group
- VG-02 ▾
- ☑ Move alarm back if original VG becomes free

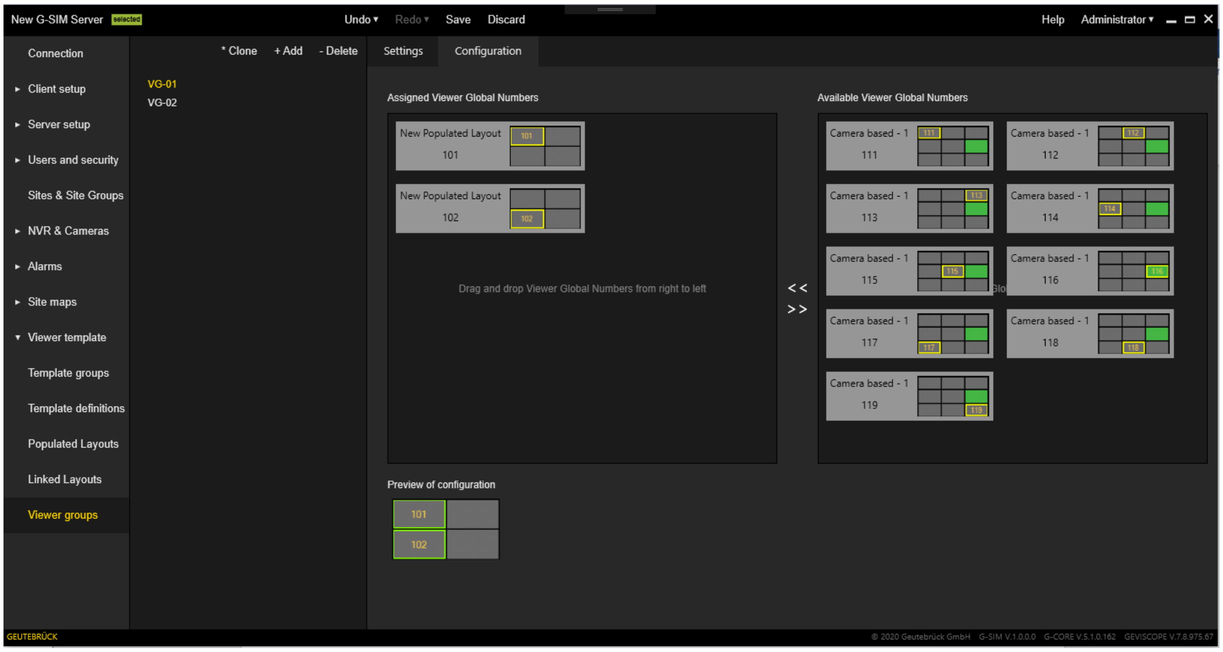
Settings	Description
Name	Sets the name of the selected viewer group.
Description	Sets the description of the selected viewer group.
Viewer group color	Sets the color of the frame of a viewer assigned to the selected viewer.
Desired behaviour if group is in use	Allows the user to select one of three alarm behaviors.

Configuration

The **Configuration** tab consists of several areas:

- Assigned Viewer Global Numbers
- Available Viewer Global Numbers
- Preview of configuration

Use the Viewer Selector to assign an available viewer from the **Available Global Viewer Numbers** area to the selected group **Assigned Global Viewer Numbers**. The **Preview of configuration** area shows the configuration of the viewer that has been added.



Drag and drop Viewer Global Numbers from right to left

Operator Console

The Operator Console (OpCon) is the main user interface for individual control, viewing and monitoring of video streams, site maps and resources. It is equipped with the appropriate permissions for the respective user or site.

Function Overview

Product Features

One of the main foci of the system instant access to live video from any of the connected cameras, without being overwhelmed with the detail of where and how to find them. Playback of recorded footage or PTZ-control of selected cameras is also possible for users with the appropriate access rights. Cyclic camera sequences (Guard-Tours) may be created to allow for controlled viewing of multiple cameras from various sites in one display window (viewer).

Flexible alarm handling allows the system administrator to configure various alarms (from the system components, cameras, NVRs, networks, servers, storage devices, etc.) to monitor the total health of the system and the video network. Each alarm-type may have specific handling procedures associated with it to assist in resolving possible problems.

Designated users may assign tasks to other users or user-groups, which can be tracked, transferred and managed through the user interface. Tasks may also be linked to sites, site-groups, or cameras, to allow immediate access to live camera signals or recorded footage. For non task-related communication, simple messaging is incorporated for instant collaboration between users and user groups.

All user and system events are recorded in the Audit Log, which may be queried, viewed and printed.

System Features

Feature	Description
Central Control	**Total Control Over Who May Do What** The G-SIM Maintenance Console allows the system administrator to configure many system parameters, and to allow or disallow access to any functionality on a per-user basis. Any changes to user-rights or permissions are immediately permeated to all open Operator Console. **High Level of Redundancy and Robustness** As the system will most probably be operational 24/7, a high level of redundancy is imperative. Most parts of the system may be disconnected, downed, re-started, and even replaced, with minimal effect on the rest of the system. There are also numerous options for installation redundancy, with various combinations of NVR, channel, and camera fail-over possible. **Various Connection Methods** Connections to sites can be via most network types (e.g. LAN, WAN, ISDN), with configurable site usage limitations per connection method.
LAN/WAN-Based Operator Console	**Unique User Interface** Configurable, flexible user interface, which allows the display of maps, video, lists or information on virtually any part of the screen. Depending on the strengths and abilities of your graphics card, the interface may be displayed on up to four screens (even with varying screen resolutions). Any screen layout may be stored and retrieved at a later stage. The user interface is highly intuitive, and implicitly "knows" what the user may intend when using drag-and-drop to display item. **Site List**

Feature	Description
	The site list (which may be filtered by status or site group), gives access to site maps and site cameras and also indicates if sites are being accessed. **Camera List** The camera list may be filtered by functional group, site, usage, or availability. Each camera in the list may be viewed, reviewed, viewing may be blocked (for selected users or user groups), controlled, transferred, and much more. Additional information for each camera contains detail such as description and type. It also dynamically shows the camera status, including how and by whom it is being used. Cameras may also be part of private or public Guard-Tours. The Check-Camera feature allows the user quickly to compare the current camera signal with the previously recorded reference frame. **Navigational Maps** Hyper-linked user-definable maps facilitate maximum flexibility and ease-of-use, allowing multiple representations of site networks and cameras on sites. A Map may be used to view site-maps, or a camera on a site, or to find the position of any particular camera on a site. The maps also allow direct access to camera functions or information and indicate any pending camera-linked alarm conditions. (Maps are displayed at optimal sizes and may also be zoomed dynamically.)
Health Monitoring	Note that this is not health monitoring in the sense of Systems Management or some other discipline which focuses on health only — we are here talking about the G-SIM specific health, as outlined in the following list. • A combination of centralised and decentralised system-wide monitoring is used continuously to keep track of the health of the various system parts and equipment. • Alarm generation is totally configurable and customizable to react to status changes, triggered events, or even complex state sequences. Alarms may be designated to specific user groups. Each type of alarm may have an action-list linked to it through which the progress of the alarm handling

Feature	Description
	can be traced. Pending alarms which are associated with cameras are also indicated on the maps. • Step-by-step tracking of alarm procedure completion is managed via the alarm-list. Alarms may also be transferred between users for handling. • The health monitoring architecture allows for diverse types of user defined health events and alarms; from system security related information to hardware failure information. Examples of such events could be: Aggregated video sync-loss, HDD failure, RAID status, etc. • The system can be tailored to meet almost any health monitoring related need via SNMP intergation.
Auditing	Every system action, user interaction or user response is recorded in the central Audit Log. The logged items include: system start-up and shut-down; system problems; user logins and login attempts; camera access; configuration changes; task handling; alarm handling; etc.

Fundamentals

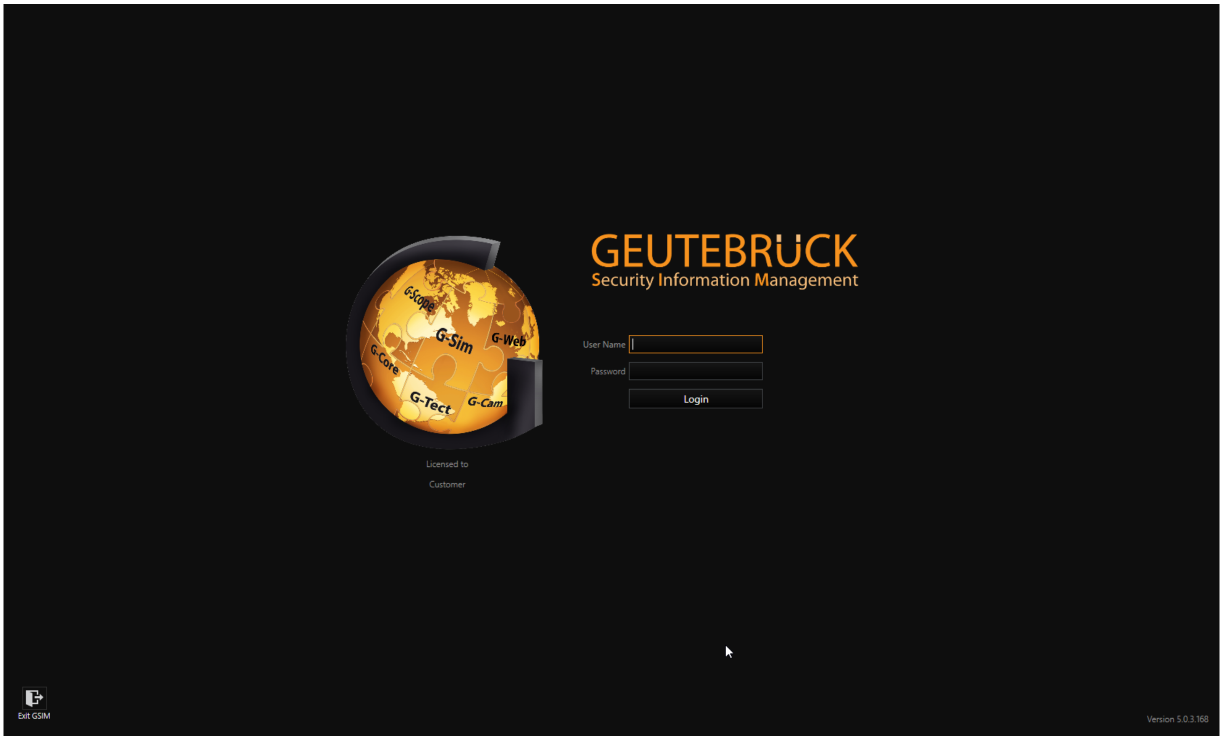
This chapter covers the basics of getting started with the G-SIM Operator Consoleand will introduce you to the main interface elements of the system. Guidelines and tips are given on using different navigation tools, and how to perform common tasks quickly. Some aspects of the main interface, e.g. the Lists, will be described in more detail in following chapters.

Login and Logout

Because program functionality is dependent on the privileges assigned to a user, and all user activity is logged as part of an audit process, the log-in process is an important part of G-SIM usage. It is therefore essential that users log out when they are not using the system, and that every operator only uses the system when logged in with his or her own credentials.

Login

After a system start-up, or when a user has logged out, you will be presented with a log-in screen containing the following fields:



G-SIM uses a five step initialisation and authentication process after start-up. A progress bar will indicate the authentication stage which may be:

- **Connecting**
- **Loading Initial Data**
- **Logging In**
- **Signing In**
- Loading Your Profile

Connecting

During this phase the application is connecting to the main G-SIM server. This process might take several seconds, but if it fails to complete there might be a network connection problem, or the server might be down. A "Connection Failed" message will be displayed, and an eight second countdown will begin before the application will retry to connect to the server. Make sure you are connected to the local network. Contact your designated system administrator if you suspect a server problem.

Loading Initial Data

After a successful connection, the application will receive initial data from the server to facilitate the rest of the initialisation and authentication process.

Logging In

Enter your user name and password in the appropriate fields and click the **Login** button, or press **Enter**. Remember that the Password is case sensitive.

ⓘ **After three unsuccessful tries to log in, your account will be locked by the server, and an alarm will be generated. The system administrator will have to unlock your account before you will be granted access again**

During this stage a login request will be sent to the server and the application will wait for validation. If the entered User Name or Password is incorrect, an Access Denied message will be displayed. If access was granted, the system will continue to sign in.

Signing In

Your privileges and other user-specific information are sent from the server to the local system. The main interface will be populated with this data.

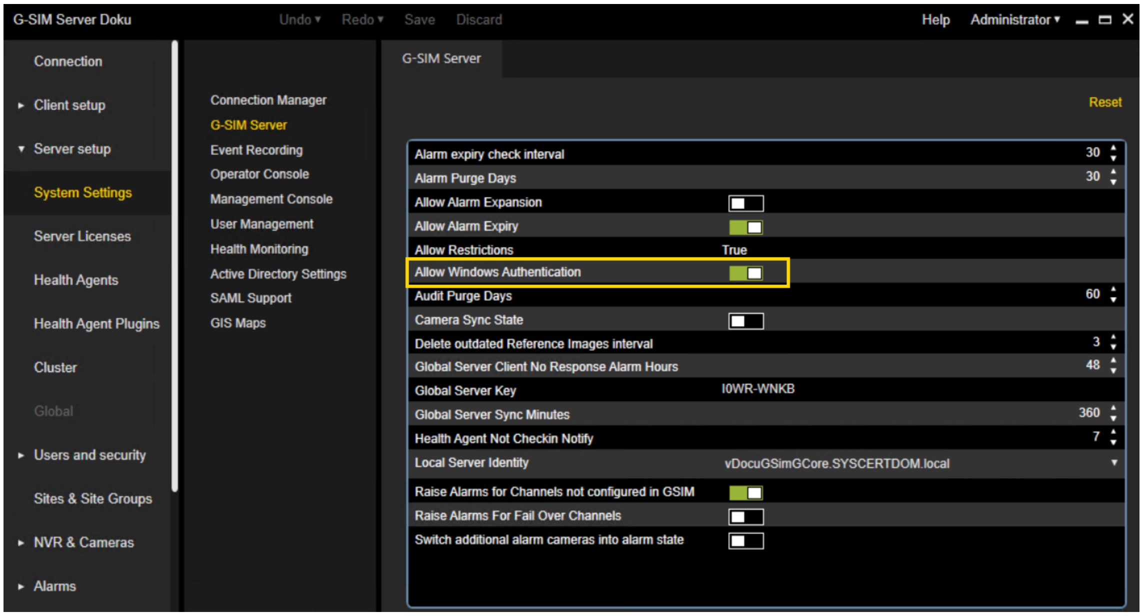
During this process your profile is applied to the user interface. The main interface will be displayed once all the necessary data are processed.

Automatic Login via Windows Authentication

To use the automatic login via Windows authentication for the OpCon, some settings in the ManCon and OpCon have to be configured beforehand.

Allow Windows Authentication in ManCon

1. Open the ManCon.
2. Open the **Server setup** drop-down menu in the sidebar.
3. Click on **System Settings** and then on **G-SIM Server**.
4. Activate **Allow Windows Authentication**.

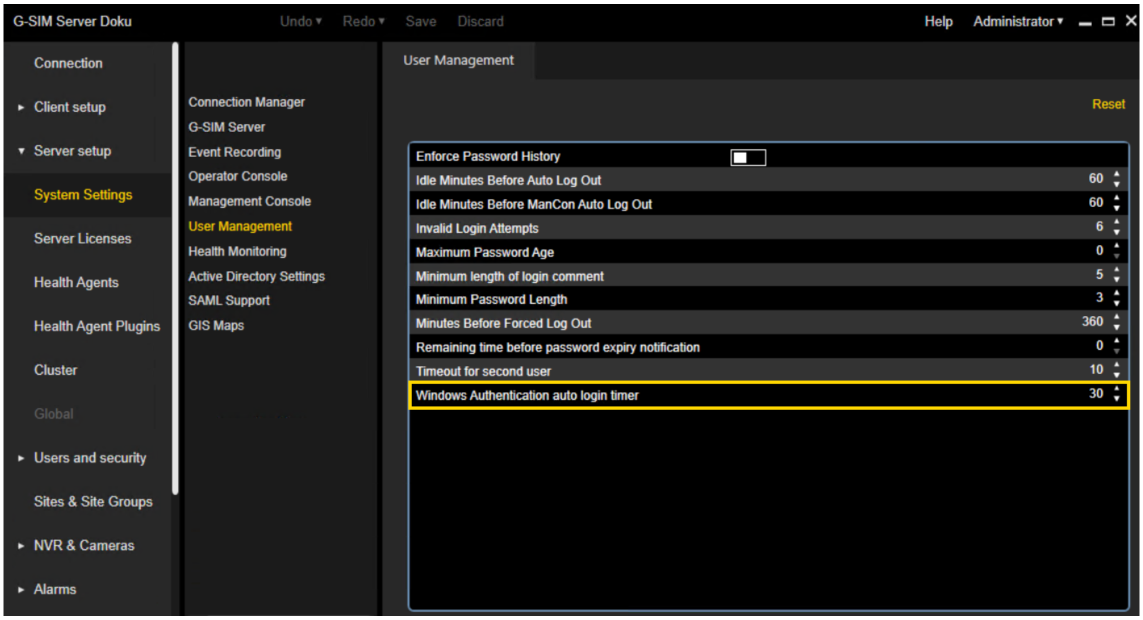


Alarm expiry check interval	30
Alarm Purge Days	30
Allow Alarm Expansion	☐
Allow Alarm Expiry	☑
Allow Restrictions	True
Allow Windows Authentication	☑
Audit Purge Days	60
Camera Sync State	☐
Delete outdated Reference Images interval	3
Global Server Client No Response Alarm Hours	48
Global Server Key	I0WR-WNKB
Global Server Sync Minutes	360
Health Agent Not Checkin Notify	7
Local Server Identity	vDocuGSimGCore.SYSCERTDOM.local
Raise Alarms for Channels not configured in GSIM	☑
Raise Alarms For Fail Over Channels	☐
Switch additional alarm cameras into alarm state	☐

5. Click on **Save**.

Set Windows Authentication Auto Login Timer in ManCon

1. Open the ManCon.
2. Open the **Server setup** drop-down menu in the sidebar.
3. Click on **System Settings** and then on **User Management**.
4. To specify the preferred time in seconds after which you want to be automatically logged into the OpCon via Windows authentication, set the **Windows Authentication auto login timer**.

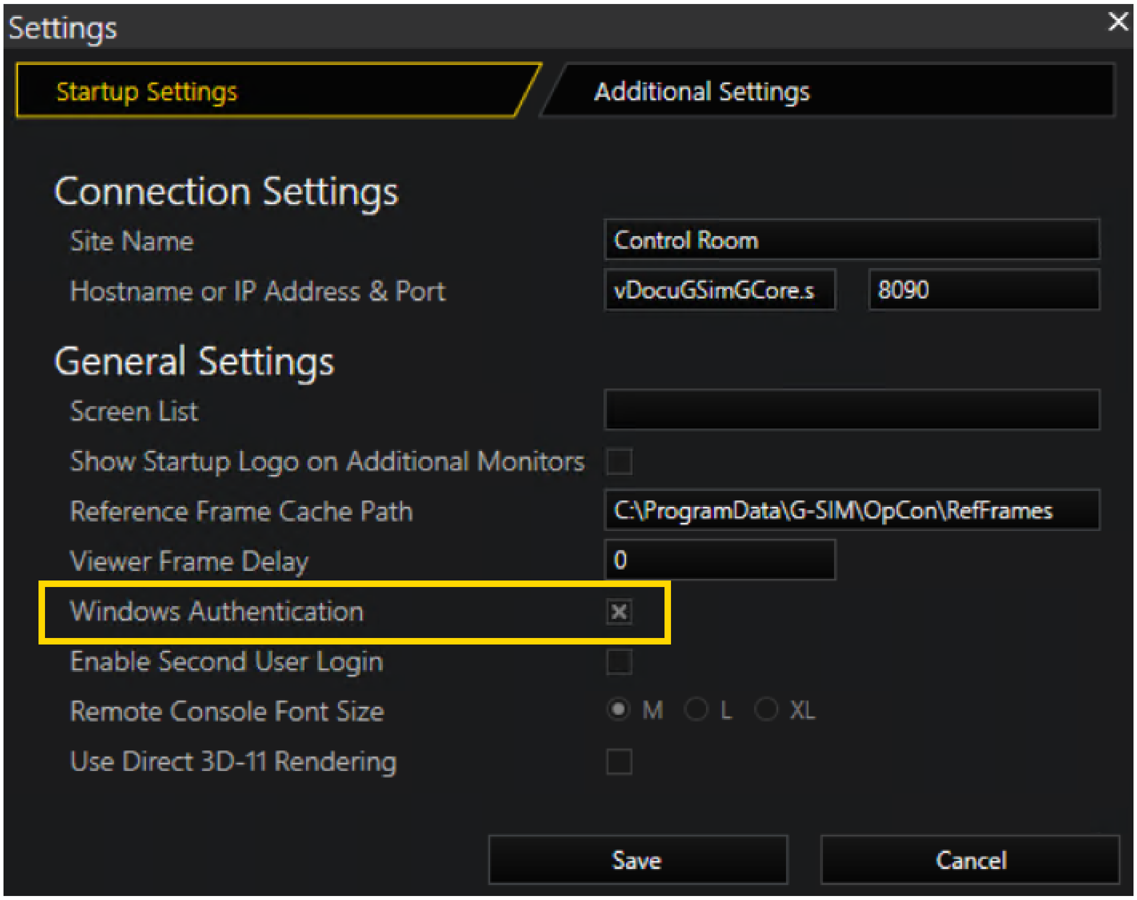


Enforce Password History	□
Idle Minutes Before Auto Log Out	60
Idle Minutes Before ManCon Auto Log Out	60
Invalid Login Attempts	6
Maximum Password Age	0
Minimum length of login comment	5
Minimum Password Length	3
Minutes Before Forced Log Out	360
Remaining time before password expiry notification	0
Timeout for second user	10
Windows Authentication auto login timer	30

5. Click on **Save**.

Activate Windows Authentication in OpCon

1. Open the OpCon.
2. In the OpCon login window, click on **Settings**. The **Settings** window opens.
3. In the **Startup Settings** tab under **General Settings**, activate **Windows Authentication**.



Settings

Startup Settings | Additional Settings

Connection Settings

Site Name: Control Room

Hostname or IP Address & Port: vDocuGSimGCore.s 8090

General Settings

Screen List:

Show Startup Logo on Additional Monitors ☐

Reference Frame Cache Path: C:\ProgramData\G-SIM\OpCon\RefFrames

Viewer Frame Delay: 0

Windows Authentication ☒

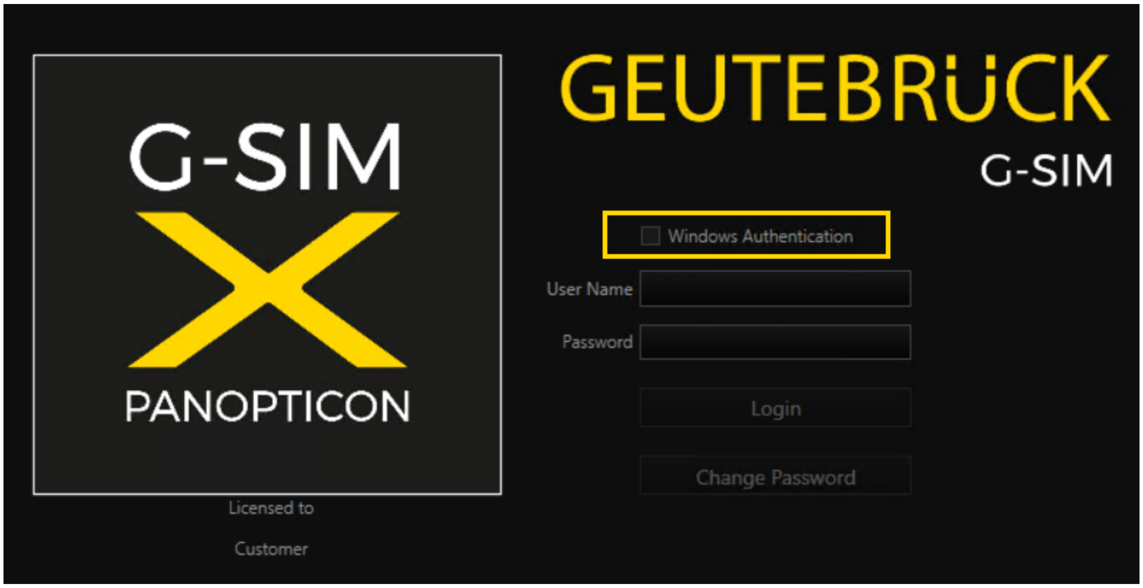
Enable Second User Login ☐

Remote Console Font Size ● M ○ L ○ XL

Use Direct 3D-11 Rendering ☐

4. Click on **Save**. The OpCon login window opens.

5. Activate **Windows Authentication**.



The **User Name** appears in the corresponding field and, if set previously, the Windows authentication auto login timer appears as well and is counted down. Afterwards, you will be logged into the OpCon automatically.

If the Windows Authentication check box is deactivated again, User Name and timer disappear, and you have to log in manually.

Application Start-Up

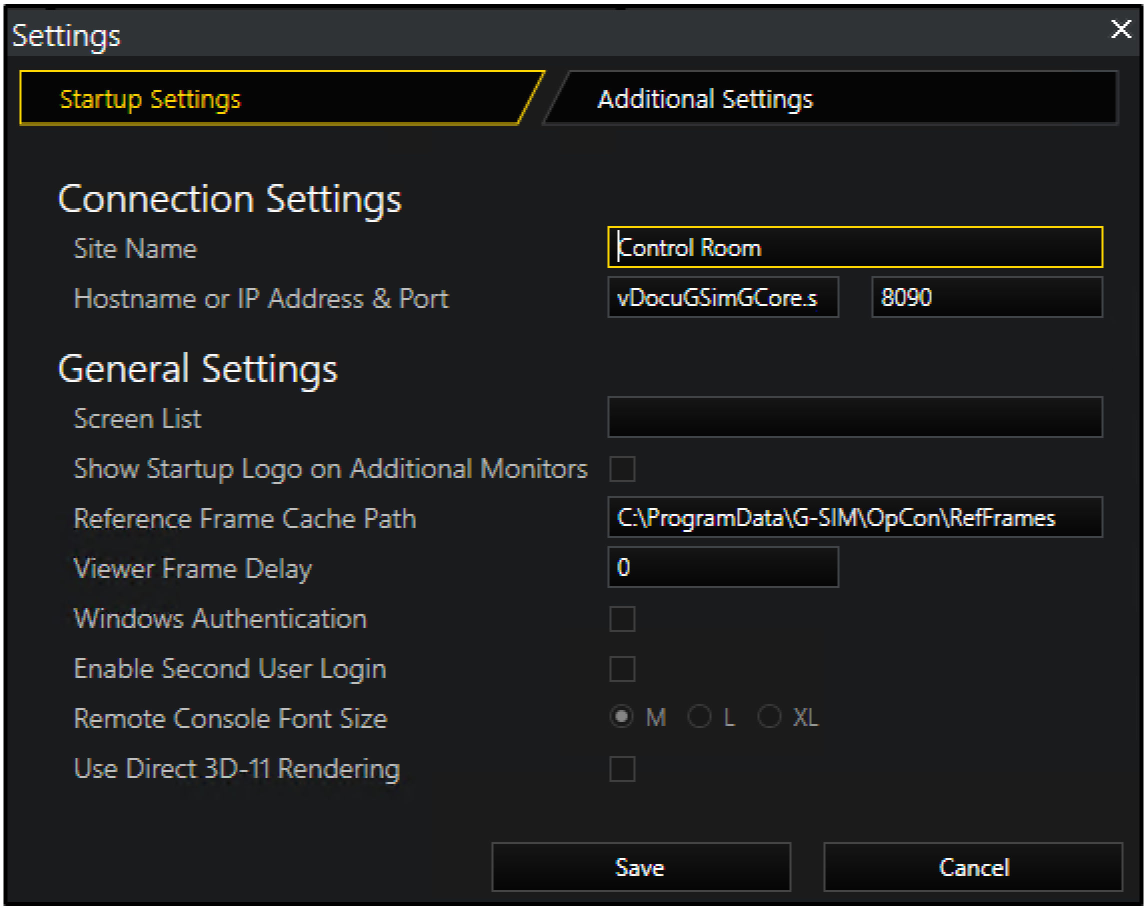
Starting for the First Time

If you have never used G-SIM before, the application will start up with the default view. You will see the empty default Viewer layout, with the Tabbed Lists on the right of the screen.

Settings

Startup Settings

Under the tab **Startup Settings** you can configure the following settings:



Settings

Connection Settings

Site Name: Control Room

Hostname or IP Address & Port: vDocuGSimGCore.s 8090

General Settings

Screen List:

Show Startup Logo on Additional Monitors □

Reference Frame Cache Path: C:\ProgramData\G-SIM\OpCon\RefFrames

Viewer Frame Delay: 0

Windows Authentication □

Enable Second User Login □

Remote Console Font Size ● M ○ L ○ XL

Use Direct 3D-11 Rendering □

Connection Settings:

Setting	Description
Site Name	Descriptive name of the Operator Console which will be used in debug output and log traces.
Hostname or IP Address & Port	Hostname/IP address and port of G-SIM server.

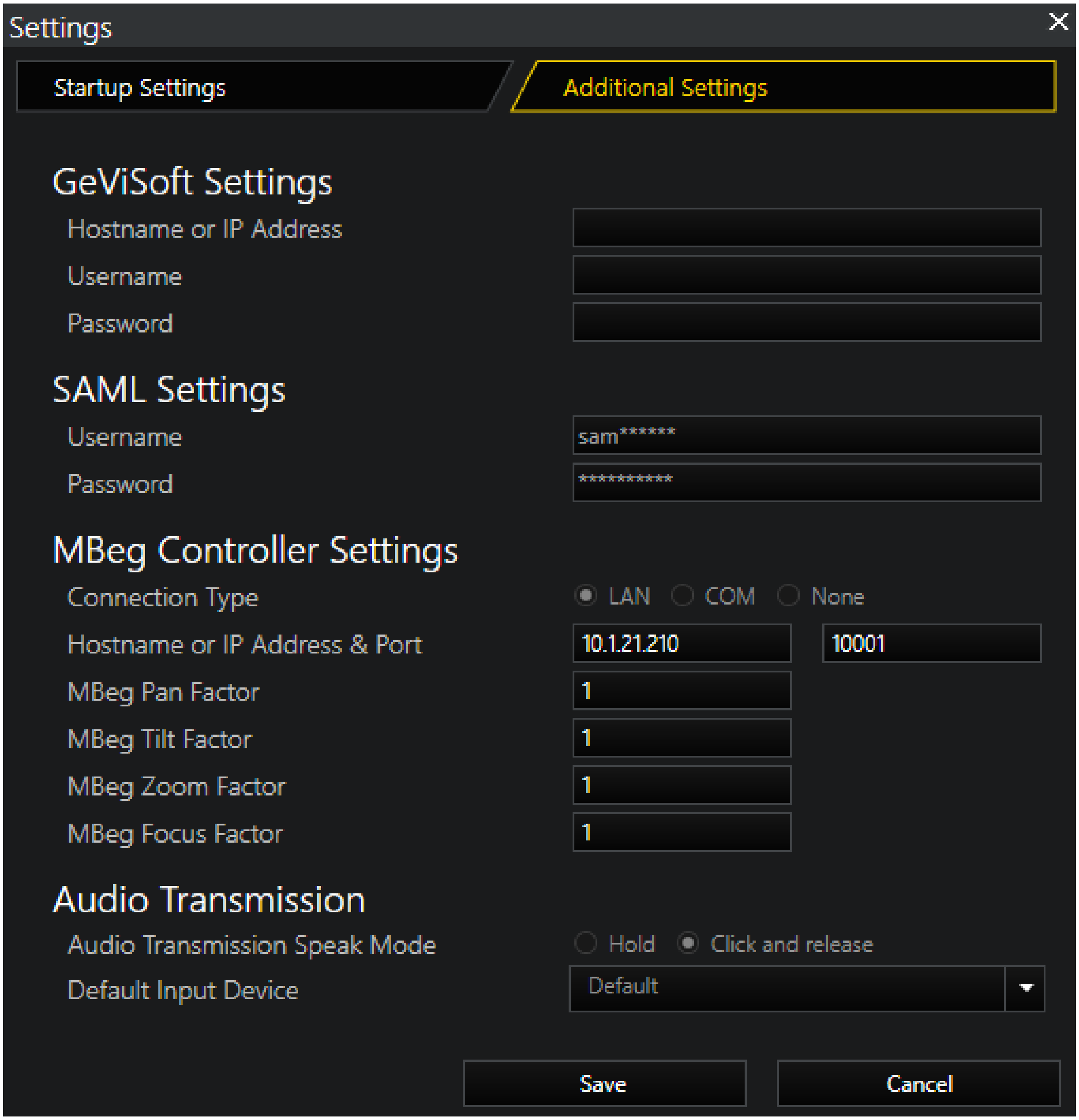
General Settings:

Setting	Description
Screen List	Comma separated list of monitor numbers which are used in Operator Console. Main Operator Console screen will be shown on the first monitor of this list. Operator Console supports up to 4 monitors. If this field is empty, then first 4 monitors will be used in Operator Console.
Show Startup Logo on Additional Monitors	If checkbox is checked then startup logo will be shown on all monitors until Operator Console will be logged in and user profile is loaded.
Reference Frame Cache Path	Path to the folder where camera reference frames are stored.
Viewer Frame Delay	Set livestream frame delay (in milliseconds) parameter for the video viewers.
Windows Authentication	If checkbox is checked and G-SIM Server has Active Directory license, then Windows user can be used to login in Operator Console. Windows user must be included in domain and Active Directory synchronization must be configured in Management Console.

Setting	Description
Enable Second User Login	If checkbox is checked, then second user can log in simultaneously with first user in Operator Console.
Remote Console Font Size	Select relative font size which is used for texts in the Remote Console.
Use Direct 3D-11 Rendering	If checkbox is checked, then Direct 3D-11 rendering is used to render frames in the video viewers.

Additional Settings

Under the tab **Additional Settings** you can configure the following settings:



GeViSoft Settings

Hostname or IP Address

Username

Password

SAML Settings

Username: sam******

Password: **********

MBeg Controller Settings

Connection Type: ● LAN ○ COM ○ None

Hostname or IP Address & Port: 10.1.21.210 10001

MBeg Pan Factor: 1

MBeg Tilt Factor: 1

MBeg Zoom Factor: 1

MBeg Focus Factor: 1

Audio Transmission

Audio Transmission Speak Mode: ○ Hold ● Click and release

Default Input Device: Default

GeViSoft Settings:

Setting	Description
Hostname or IP Address	Hostname /IP address of the GeViSoft server.
Username	Name of the GeViSoft server.

Setting	Description
Password	Password of the GeViSoft server.

SAML Settings:

The SAML Settings section is only visible if SAML Authentication was selected during the installation of G-SIM. Additionally, you have to make sure that the SAML service is running. For further information see SAML Authentication**.**

Setting	Description
Username	Name of G-SIM user which is used to connect to G-SIM server by G-SIM SAML Web API.
Password	Password of G-SIM user which is used to connect to G-SIM server by G-SIM SAML Web API.

MBeg Controller Settings:

Setting	Description
LAN	MBeg is connected via network. When this option is selected, the following settings appear: • Hostname or IP Address & Port (should be provided) • MBeg Pan Factor • MBeg Tilt Factor • MBeg Zoom Factor • MBeg Focus Factor
COM	MBeg is connected via Com port. When this option is selected, the following settings appear: • Com Port (should be selected) • MBeg Pan Factor

Setting	Description
	• MBeg Tilt Factor • MBeg Zoom Factor • MBeg Focus Factor
None	MBeg is not connected to Operator Console. When this option is selected, all other MBeg settings are hidden.

Audio Transmission:

Setting	Description
Audio Transmission Speak Mode	There are two options: • **Hold**: Voice is transmitted while button is pressed. • **Click and release**: First click activates voice transmission. Second click deactivates voice transmission.
Default Input Device	Select the microphone to be used for the voice transmission.

For detailed information see **Speak**.

Configuring an Initial View

Every time you start the application, what you see will be determined by a number of factors. If you have not selected a Default Layout, the system will start up with the interface as follows:

- If no-one else logged in on the same machine since you logged out and it is less than two hours since your last log-in. If either of these is not true, your default layout will be used.
- If you do not have a default defined, and no-one else has logged in on that machine, then your previous layout will be used, even it is more than two hours since you logged out.

- If the system would have given you your default layout but you don't have one, the first template in the template list will be applied, with no viewers or maps having any content.

You can save your favourite layouts (which includes viewer content, cameras, etc.) for future use and choose one of them as a Default Layout. This will override any saved previous state and instead show the selected Favourite Layout (including screen layout and video) every time you log in. See **The Toolbar**. Favourite Layouts are set up per user.

You can also configure the Viewer grid layouts for all screens. See **The Toolbar**.

Logout

✕ You can log out by either clicking the Log Out button on the right-hand side of the application toolbar, or by closing the main application window (click the Close button in the window header). The preferred method would be to use the Log Out button which will show the log-in interface again, making it easy for the next user to start using the system.

If you log out or if a G-SIM session was terminated in any way, the system will revert to its previous state (i.e. the Viewers and open List will still display the same video and information) when you log in again, unless you have selected a Default View. You may therefore log out if you want to leave the system unattended for a few minutes, and just log in again to continue where you have left off.

A user will be logged out in the following scenarios:

- If the application timed out due to inactivity (default is 1 minute, and this has to be activated and configured in the Management Console).
- If a forced log-out time was specified in the Management Console.
- If a user clicked on the Log Out button in the toolbar.
- If a user closed the G-SIM application (e.g. by clicking the Close button in the top right corner).
- If G-SIM lost contact with the main database, the user will be logged out if the application can't reconnect during the grace period.
- If a user changed the language.

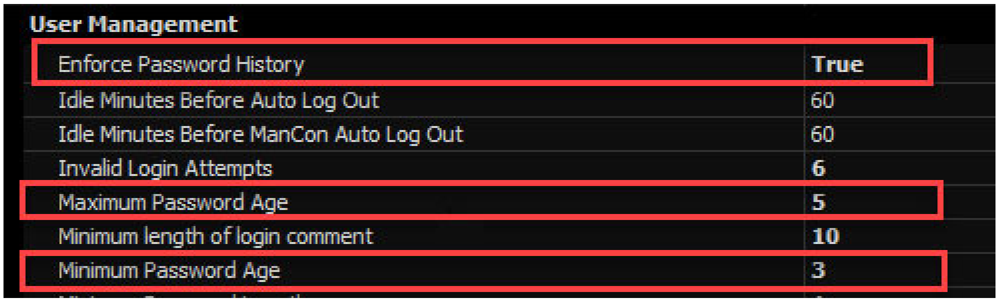
- If there is a pending update of the Operator Console and the user agrees to the update.

Change Password

Management Console (ManCon)

System Settings

Server Setup > System Setting > All Settings contains three new configuration options.



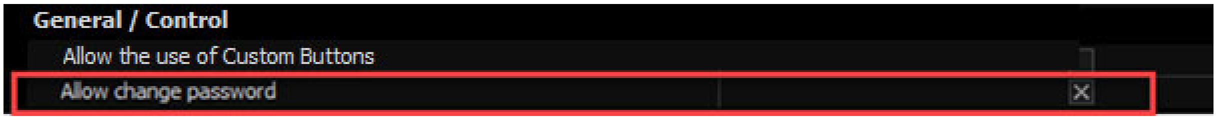
User Management

Enforce Password History	True
Idle Minutes Before Auto Log Out	60
Idle Minutes Before ManCon Auto Log Out	60
Invalid Login Attempts	6
Maximum Password Age	5
Minimum length of login comment	10
Minimum Password Age	3

Settings	Description
History of enforce password	This safety setting defines whether the system saves the previous password. If this setting is TRUE, the user cannot use the last password to create a new password.
Maximum Password Age	This safety setting defines the period (in days) for which a password can be used before the user must change the password. You can set the password so that it expires after a number of days greater than 1, or you can define that the password never expires, by setting the number of days to 0.
Minimum Password Age	This safety setting defines the period (in days) for which a password must be used before the user is notified.

User Privileges

User and Security > User > Privileges contains a new right.

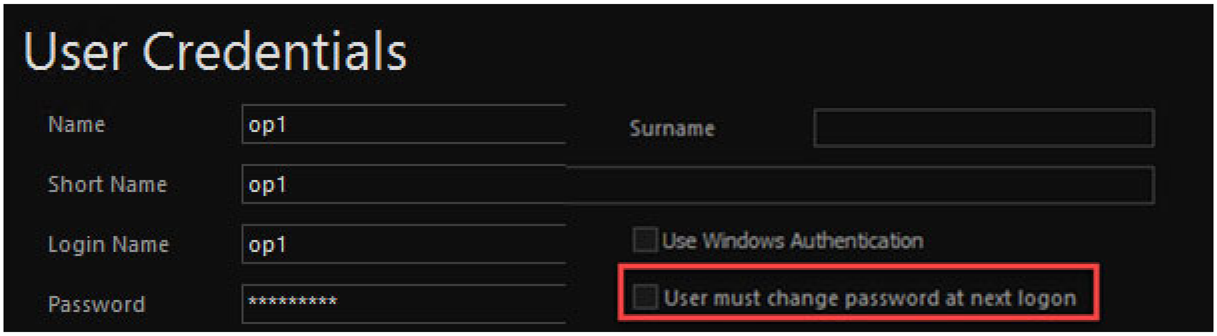


General / Control

Allow the use of Custom Buttons	□
Allow change password	☒

Settings	Description
Allow change password	This safety setting makes it possible to change the password on the login screen or in the main screen of the Operator Console.

And in the access data under **User and Security** > **User** > **User Credentials**, there is a new setting.



User Credentials

Name: op1

Surname:

Short Name: op1

Login Name: op1

Password: *********

□ Use Windows Authentication

□ User must change password at next logon

Settings	Description
User must change password at next logon	This safety setting defines that the password must be changed at the next logon.

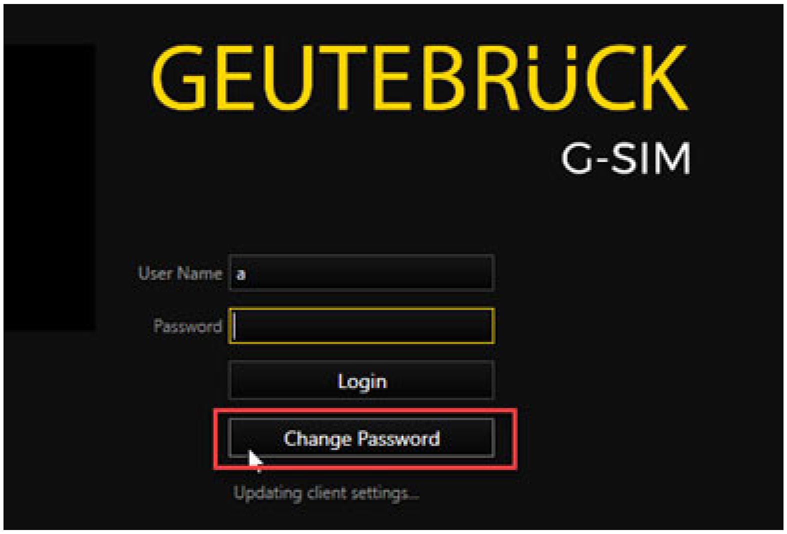
Operator Console (OpCon)

Change Password for User

The user can change their own password in the Operator Console in two ways (when they have the necessary privilege):

On the Login Screen

The **Change password** is activated once the user name has been entered.



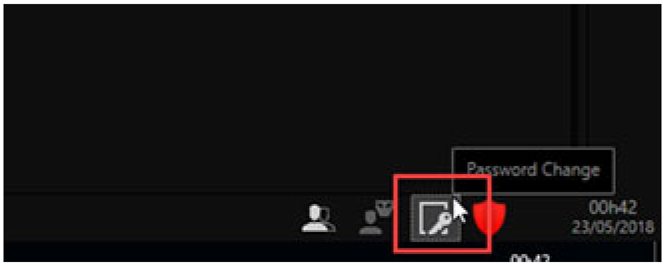
User Name a

Password

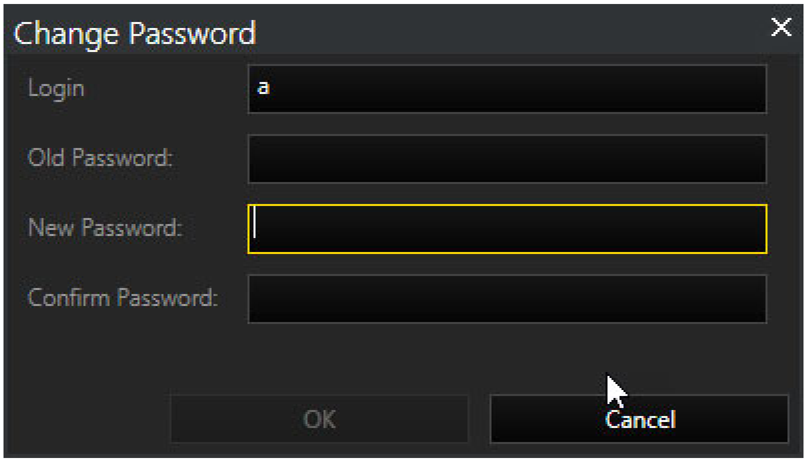
Updating client settings...

In the Main Operator Console Window

After clicking on the **Change password** button, the corresponding dialog is shown.



This dialog prompts the input of the old password:



Change Password

Login a

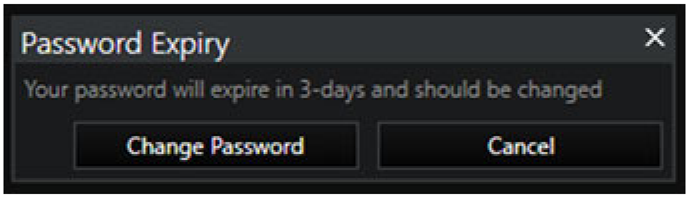
Old Password:

New Password:

Confirm Password:

Notification of Expiry of the Password

You are notified when your password will soon expire. The time at which the notification is shown depends on the setting **Minimum Password Age**. This notification is shown after each login.

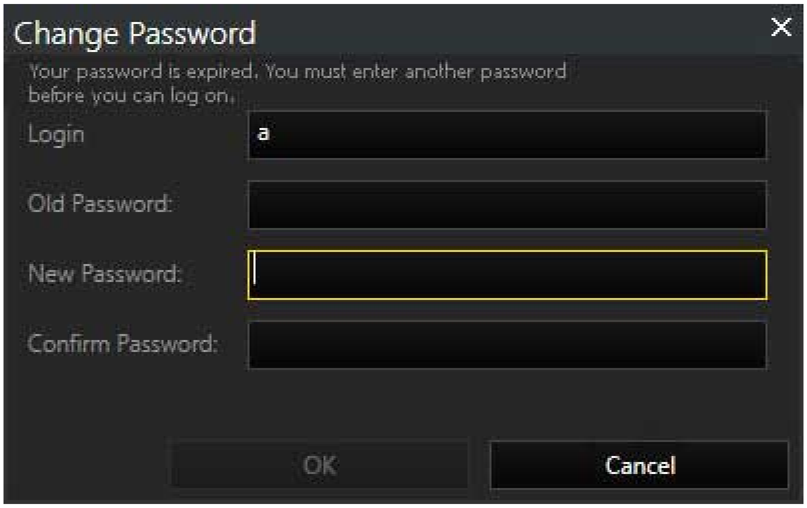


Password Expiry

Your password will expire in 3-days and should be changed

Expiration of the Password

If your password has expired, the system shows the **Change password** dialog. The time at which the notification is shown depends on the setting **Maximum Password Age**.



Change Password

Your password is expired. You must enter another password before you can log on.

Login a

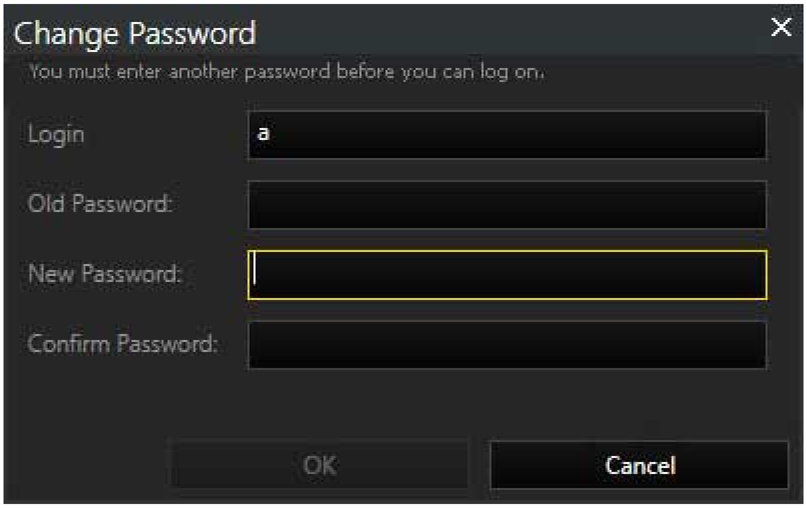
Old Password:

New Password:

Confirm Password:

Mandatory Password Change

If the control box **User must change password at next logon** is activated, the **Change password** dialog is shown.



Change Password

You must enter another password before you can log on.

Login: a

Old Password:

New Password:

Confirm Password:

Main Interface

The G-SIM Operator Interface will run on a computer with up to four monitors attached. For manned consoles, the main monitor (screen 1, as configured within the operating system) will always display the main interface with a toolbar and the Lists panel that gives you access to different items like cameras, alarms etc. The optional second, third and fourth monitors will display only additional viewer windows (Viewers). Unmanned consoles will never display the toolbar, lists, or any other interactive user interface component.

The main interface consists of four main areas:

1. Toolbar. The toolbar contains buttons that allow you to configure the main application, such as modifying the screen layout, clearing all Viewers, controlling Remote Consoles, switching to Alarm View when applicable, silencing audible alarms, logging out, and displaying the About window (click on "G-SIM" to see it).

2. Tabbed Lists. Tabbed Lists are the core of control over the Operator Console and contain all system items the user may use, e.g. Alarms, Cameras and Tours. Lists may be docked on either the left or right hand side of monitor 1, and the Menu Tabs can be displayed next to or above the Lists (this is part of template configuration, done by the administrator). As operator, however, you can move the lists to either the right or the left by means of the mirrored template view, via the Customize | General menu. This is also where top or side tabs are set.

3. Viewers. A central area divided into a number of smaller Viewer windows.

4. Status Bar. The status bar below the Lists displays the name of the currently logged-in user, the license state, and the date and time. If applicable, MBeg Controller status and fail-over information is also shown here.

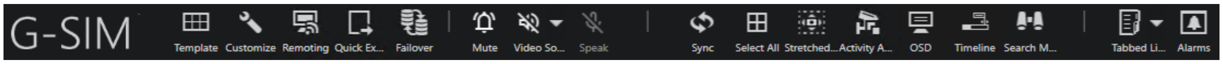
The license status is indicated using symbols:

🛡	Gray symbol: The dongle is present. Normal condition, all licenses available
🛡	Yellow symbol: Dongle not available. G-SIM starts now to count down 30 days until it turns off.
🛡	Red symbol: Dongle not available. An indication is given shortly before expiry of the 30-day license that G-SIM will soon be shut down.
🛡	Blue symbol: Dongle available again. G-SIM now counts up to 30 days and switches to gray.

If a version is installed for which no valid license is present, the same procedure takes place even though a dongle is present. The same also applies if the dongle is broken.

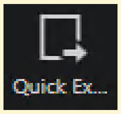
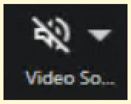
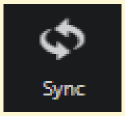
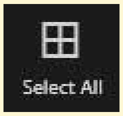
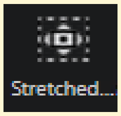
Toolbar

Some of the toolbar functions are permission-based, which means that they will only be visible to a user that possesses the necessary privileges to access their functionality.



The toolbar contains the following buttons:

Button	Description
Template	The **Template** button opens a new dialog for different layouts of the Operator Console.
Customize	The **Customize** button opens a new dialog for various modifications of the Operator Console.
Remoting	The **Remoting** button opens a new dialog for screen layout configuration of Remote Consoles.

Button	Description
	This button opens the **Quick Export** dialog window. You can perform an export or create a cut list from cameras which are shown in the viewers.
	The Reporting button opens the **Reporting** dialog window. In this window you can generate reports about alarms based on different criteria.
	The Failover button opens the dialog that displays the states of all NVRs in the system.
	The **Mute** button mutes alarms.
	The **Video Sound** button mutes video sounds.
	The **Speak** button enables or disables the microphone, facilitating audio transmission to a camera equipped with a speaker.
	The **Sync** button turns on/off viewer synchronization mode for all/selected viewers. The first selected viewer will be the master viewer. All other viewers will get play mode and time stamp from the master viewer.
	The **Select All** button selects all viewers of the current screen.
	The **Stretched View** button turns on/off the **Stretched View Mode**. In stretched mode, the video frames of the camera fill all the viewer, and the viewer header is hidden. When stretched mode is off, the video frames of the camera are stretched accordingly to the camera type aspect ratio, and the viewer header is shown.

Button	Description
Activity A...	With the **Activity Areas** button turned on, areas with activities are marked within the viewer.
OSD	The **OSD** button opens the **OSD settings** dialog window where you can select which information (camera name and time, event information, viewer number) should be shown in the viewers.
Timeline	The **Timeline** button turns on/off the timeline. When it is off, the buttons which activate play modes are shown directly in the selected viewer.
Search M...	The **Search Mode** button enables you to perform a MOS (Motion On Screen) search. When the Search Mode is on, you can set up zones in the viewers where the search will be performed and get results.
Tabbed Lists	The **Tabbed Lists** button is used for showing/hiding the tab page lists and for changing tab page and lists items.
Alarms	The **Alarms** button shows/hides the alarm screen when alarms with automatic display are present.
Camera Check	The **Camera Check** button opens the dialog that displays the result of the camera check.

Template

Definition of templates:

You can define templates and use them for various purposes. Some work best for operational use, some for auditing purposes, some for video walls, some for different screen sizes, etc. The options are self explanatory, other than the reason for "Reconnect All". In our experience, some combinations of network equipment and configurations seem to freeze some connections arbitrarily. If that happens, you can use this button as a workaround until the network issue is sorted out (whether it is configuration, firmware upgrade, or some other cause).

Definition of screens:

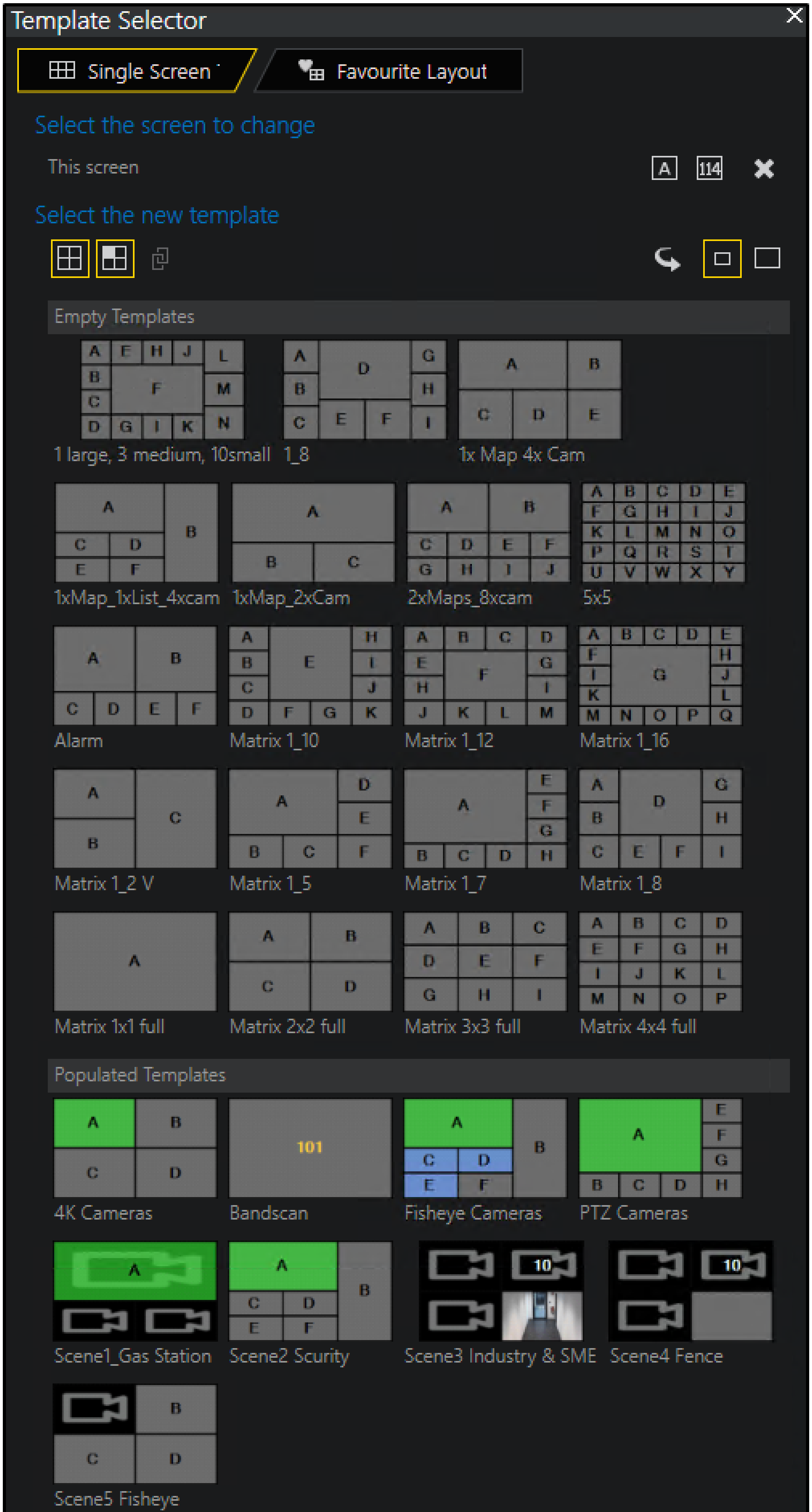
Additionally, you can define the screens (and their order) on which the user interface should start up. This allows some screens to be used for non-G-SIM functionality. An example would be if G-SIM was integrated to a fire alarm system. The fire alarms could be displayed in G-SIM, and only if necessary for further intervention would the user then switch to the fire alarm system on another screen. In such a way one can keep one screen open for other systems which are not used that often, while still using most of the screens for the monitoring functionality which G-SIM provides.

To open the associated dialog, click on **Template**, which contains tabs for **Single Screen Templates** and **Favorite Layouts**.

Single Screen Templates

Under the **Single Screen Templates** tab, you have the following options:

- Select any template on this tab to immediately change the view of the selected screen in the Operator Console.
- Identify and delete the viewers of the template.
- Show or hide empty or filled templates or linked layouts.
- Change the alignment of the templates.



Template Selector

Select the screen to change

This screen

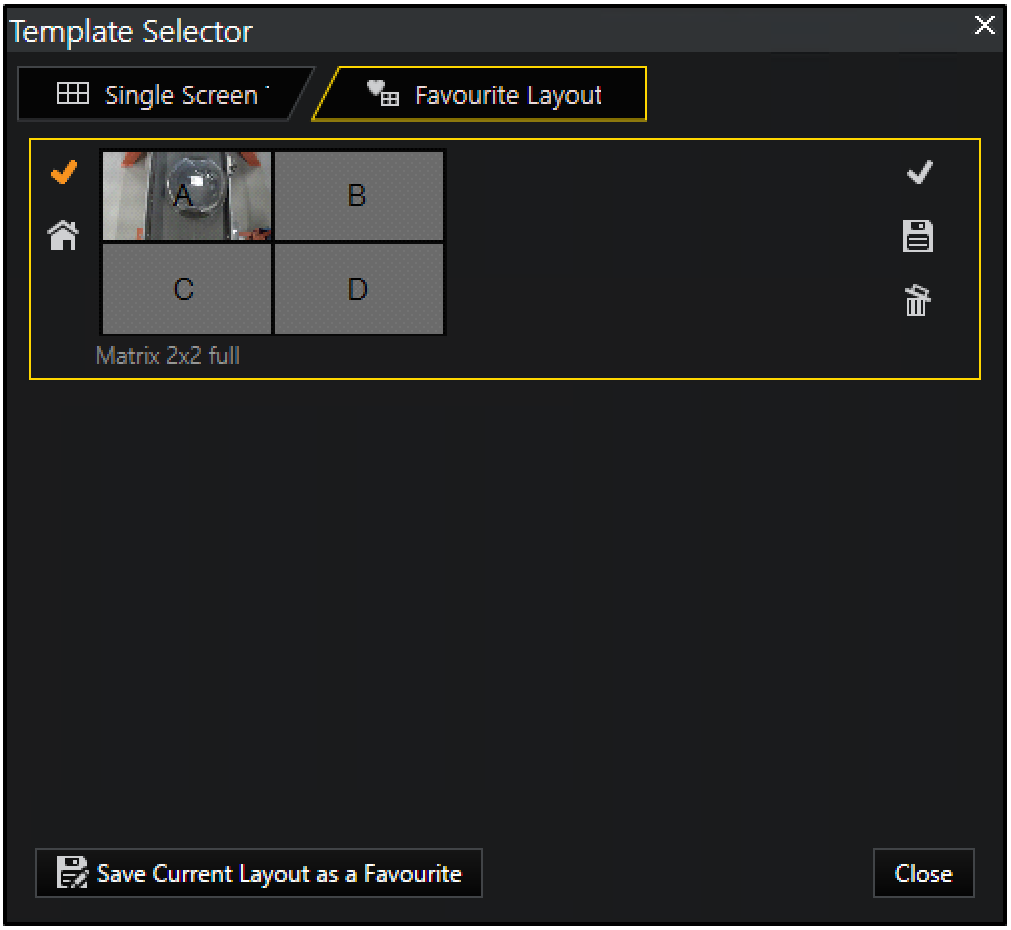
Select the new template

Favourite Layouts

You can save and recall a specific set of viewers and maps as a favorite. The difference between templates and favorites is that favorites include the content whereas a template is simply an empty layout.

A favorite set as default will be used when you start up G-SIM. In this way you can always start your shift with a certain layout already populated if necessary.

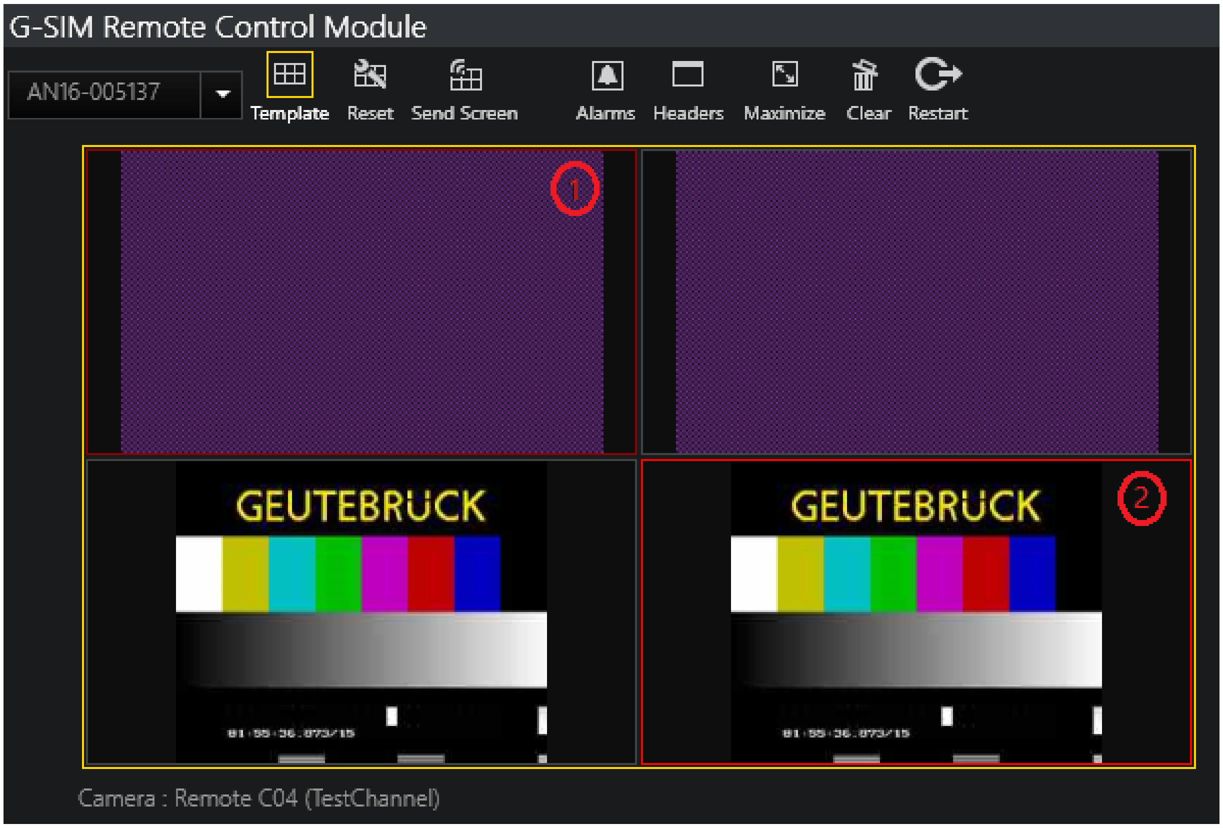
You can save the current layout and restore it later as a favorite. To make the layout appear in the list, click on **Save Current Layout as a Favourite** and give it a name.



Maps and Tours in Populated Layouts

Remote Control:

- Guard tours are marked in purple.
- Cameras and maps have a preview image shown.
- Locked viewers (not selected ①; selected ②) have a red border with a brighter color if set.
- Drag and drop and clear is not enabled for locked viewers.

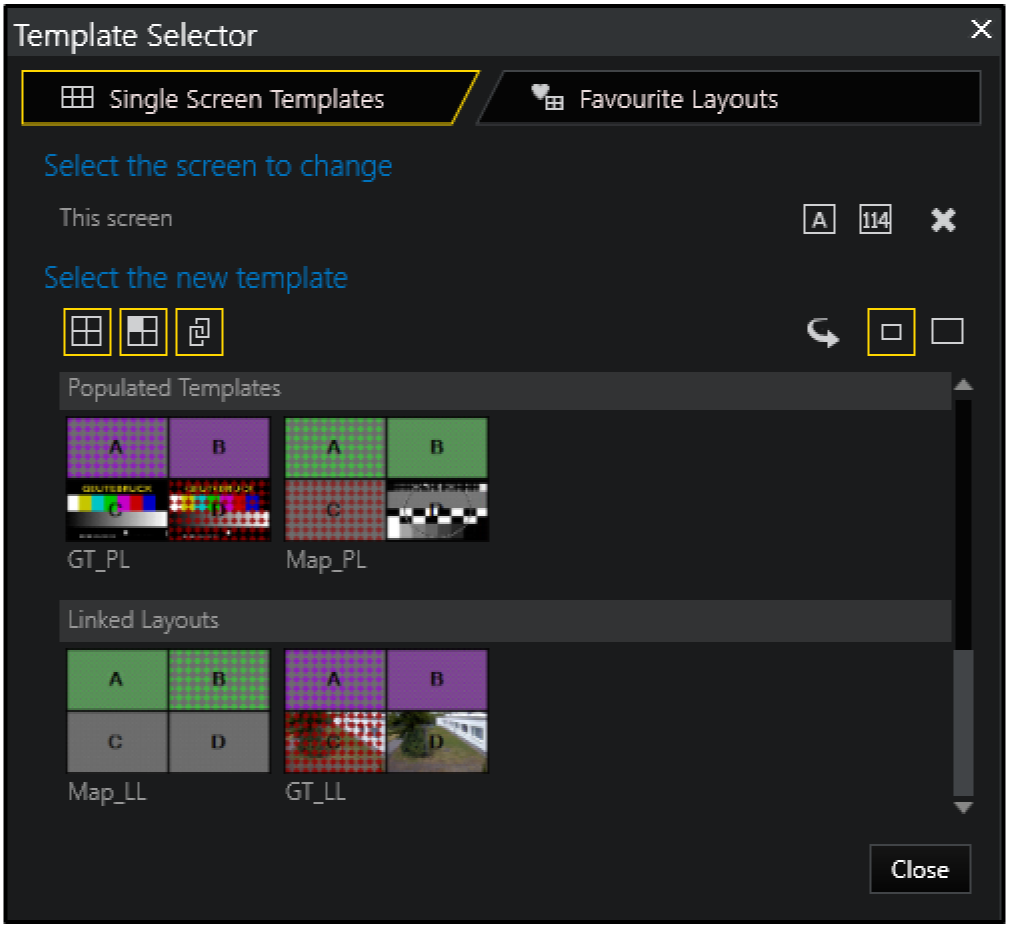


Camera : Remote C04 (TestChannel)

Template Selector:

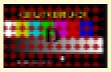
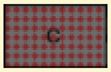
The template selector is used for selecting screen templates for both the Remote Consoles and the current Operator Console.

The **Populated Templates** and **Linked Layouts** sections also display the content as configured in the Management Console.



Guard Tours, maps and cameras are marked as follows:

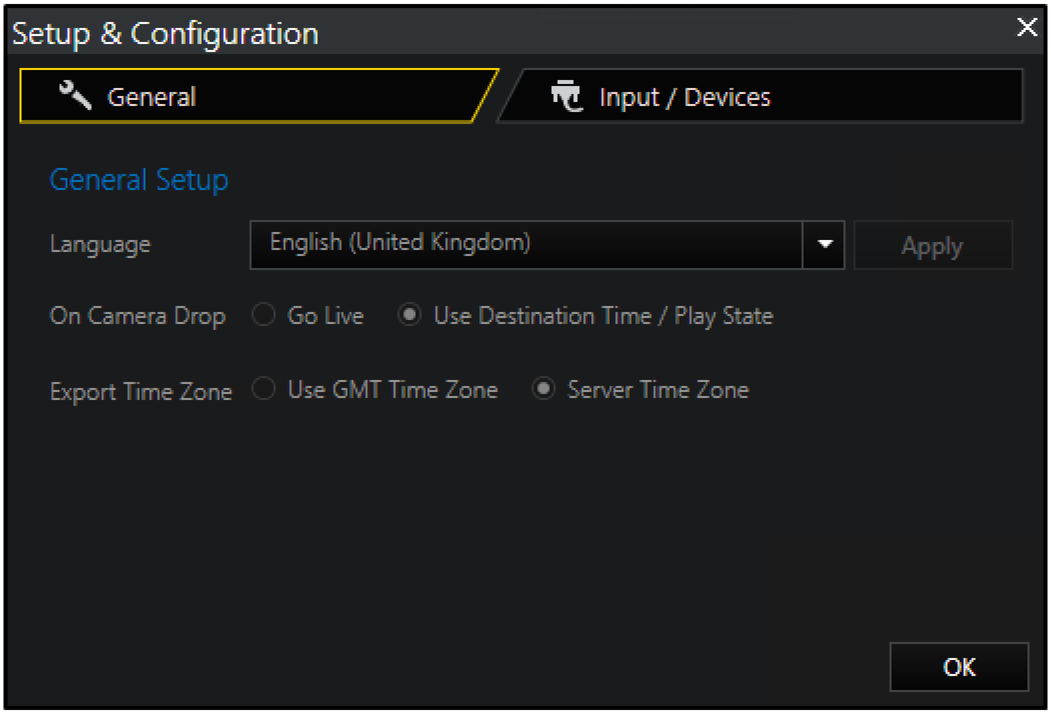
Marking	Description
🟪 B	Guard Tour
🟪 A	Guard Tour (locked)
🟩 B	Map
🟩 A	Map (locked)

Marking	Description
	Camera
	Camera (locked)
	Empty
	Empty (locked)

Customize

To customize settings, click on **Customize**. The associated dialog box with the tabs **General** and **Input / Devices** opens.

Under the tab **General**, you can make the general settings for language and time.



General Setup

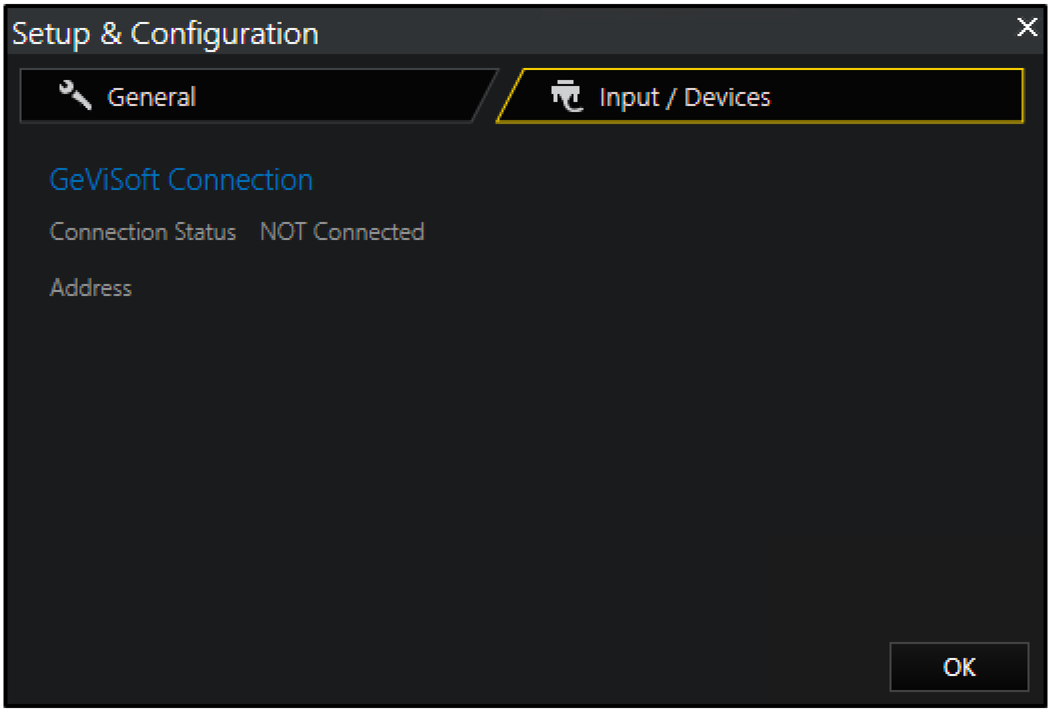
Language: English (United Kingdom)

On Camera Drop: ○ Go Live ● Use Destination Time / Play State

Export Time Zone: ○ Use GMT Time Zone ● Server Time Zone

Under the tab **Input / Devices** there are the following options.

They are only displayed if you have installed devices such as an MBeg controller or GeViSoft.



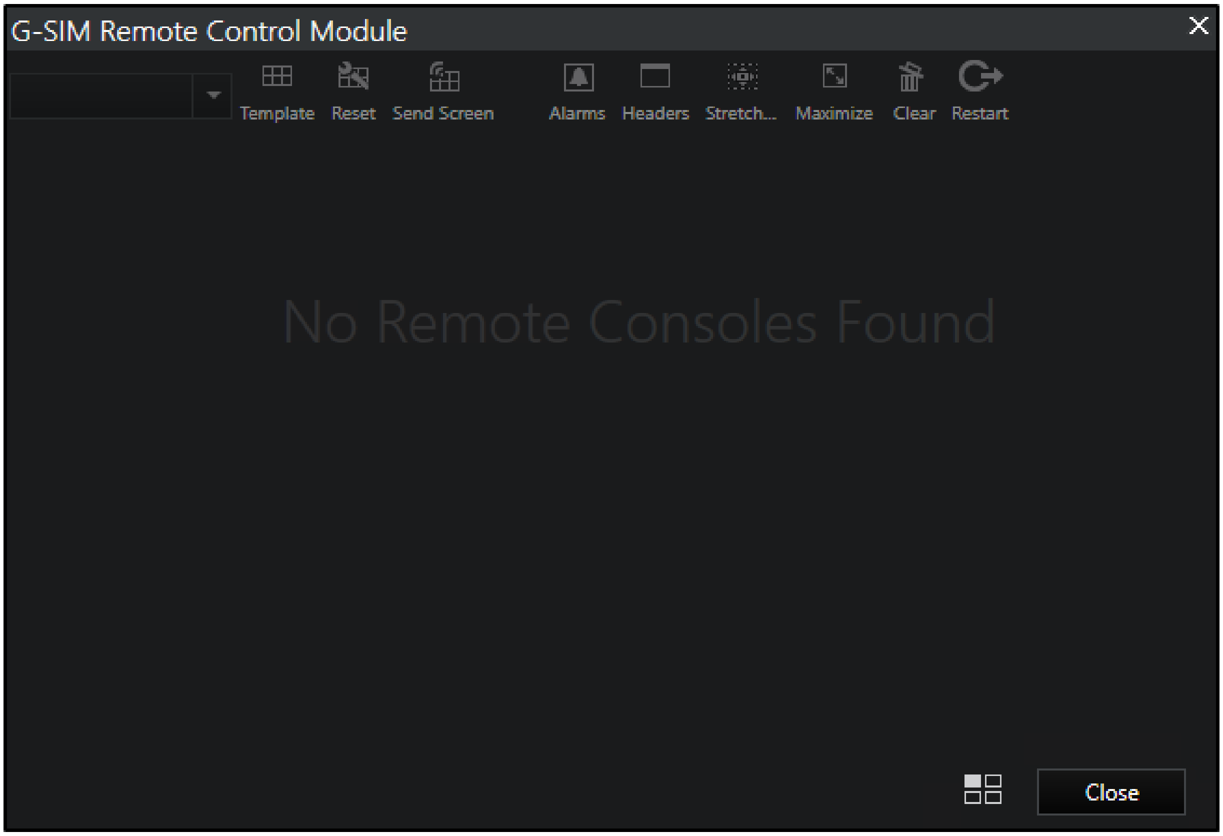
GeViSoft Connection

Connection Status NOT Connected

Address

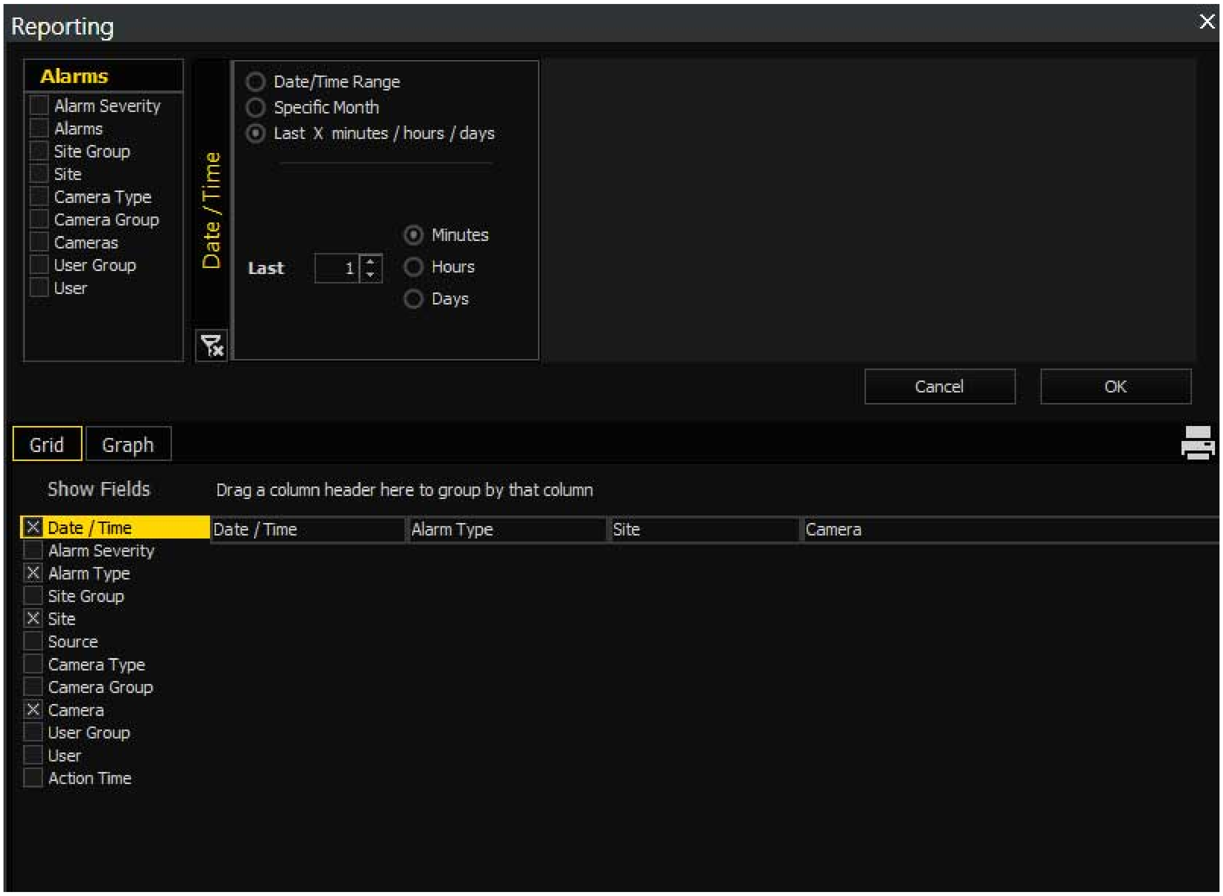
Remoting

The **Remoting** button allows you to configure the screen layout for any Remote Console as well as to save favorite screen setups for them. See **Remote Consoles** for detailed information on Remote Consoles and their remote control.



Reporting

The **Reporting** button opens the dialog for reporting alarms. Here, you can set user-defined filters to create alarm reports.



Alarms

- □ Alarm Severity
- □ Alarms
- □ Site Group
- □ Site
- □ Camera Type
- □ Camera Group
- □ Cameras
- □ User Group
- □ User

Date / Time

- ○ Date/Time Range
- ○ Specific Month
- ● Last X minutes / hours / days

Last 1

- ● Minutes
- ○ Hours
- ○ Days

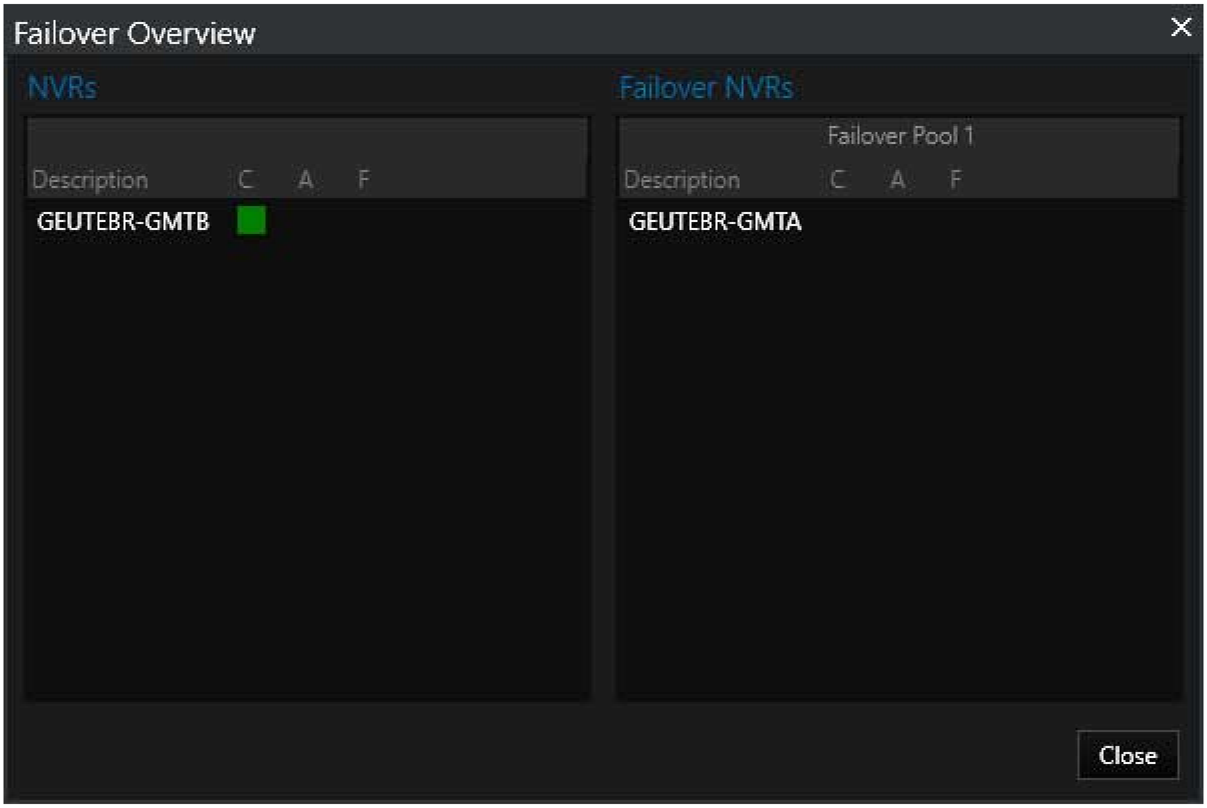
Show Fields

- ☒ Date / Time
- □ Alarm Severity
- ☒ Alarm Type
- □ Site Group
- ☒ Site
- □ Source
- □ Camera Type
- □ Camera Group
- ☒ Camera
- □ User Group
- □ User
- □ Action Time

Date / Time	Alarm Type	Site	Camera

Failover

The **Failover** button opens the **Failover Overview** dialog.



Description	C	A	F
GEUTEBR-GMTB	🟩		

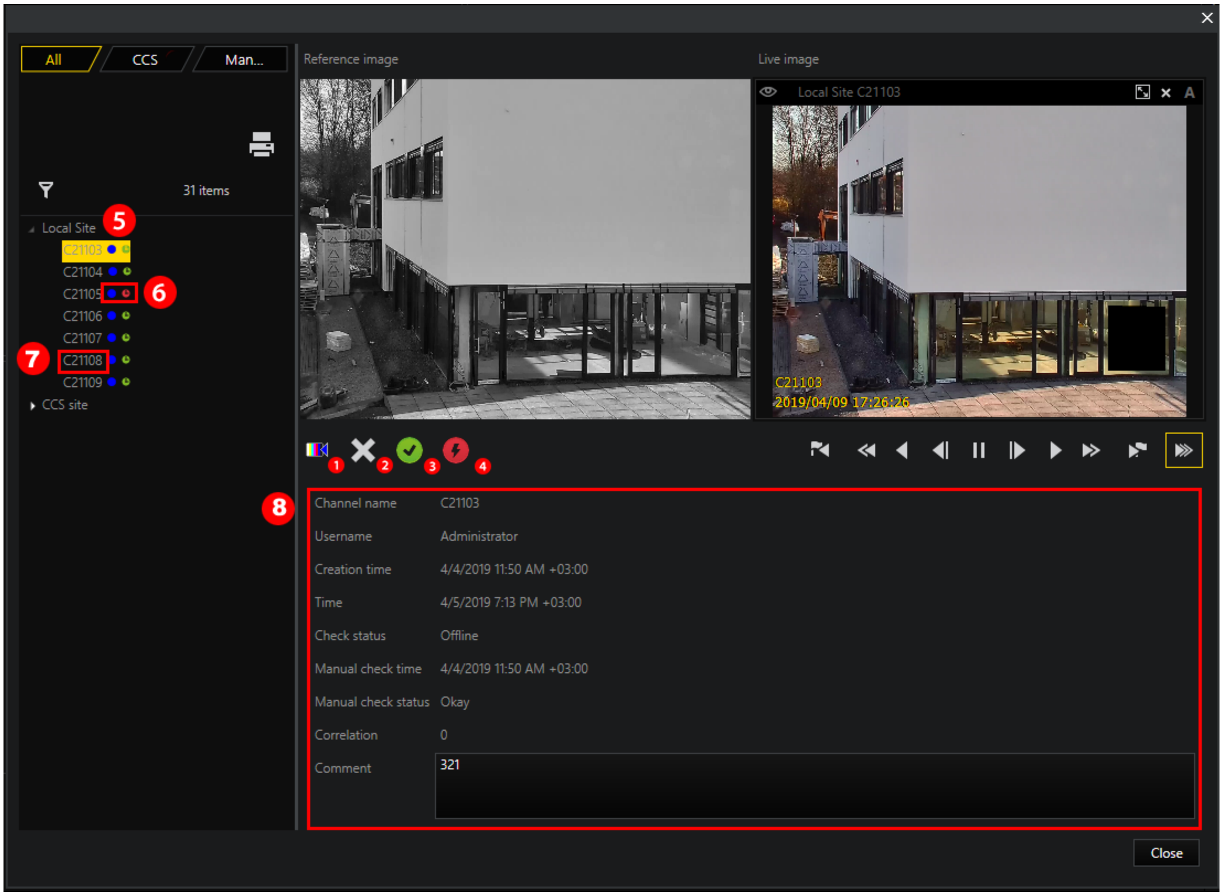
	Failover Pool 1		
Description	C	A	F
GEUTEBR-GMTA			

Here the states of all NVRs in the system can be displayed in a graphical view:

State	Description
C (Connected)	Indicates whether the recorder is connected or not.
A (Available)	Indicates that the recorder is a spare and ready to handle a failover.
F (Failover)	Indicates that another recorder is in a failover state and handled by this recorder.

Camera Check

The **Camera Check** button opens the dialog that displays the result of the camera check.



Channel name	C21103
Username	Administrator
Creation time	4/4/2019 11:50 AM +03:00
Time	4/5/2019 7:13 PM +03:00
Check status	Offline
Manual check time	4/4/2019 11:50 AM +03:00
Manual check status	Okay
Correlation	0
Comment	321

Marking	Description
1	With this button you can turn an image from the livestream into a reference image. The service immediately applies it for comparison.
2	With this button you can remove a reference image.
3	With this button you can set the manual status to "OK" by clicking this button.
4	With this button you can set the manual status to "Not OK" by clicking this button.
5	Indication of the camera location.

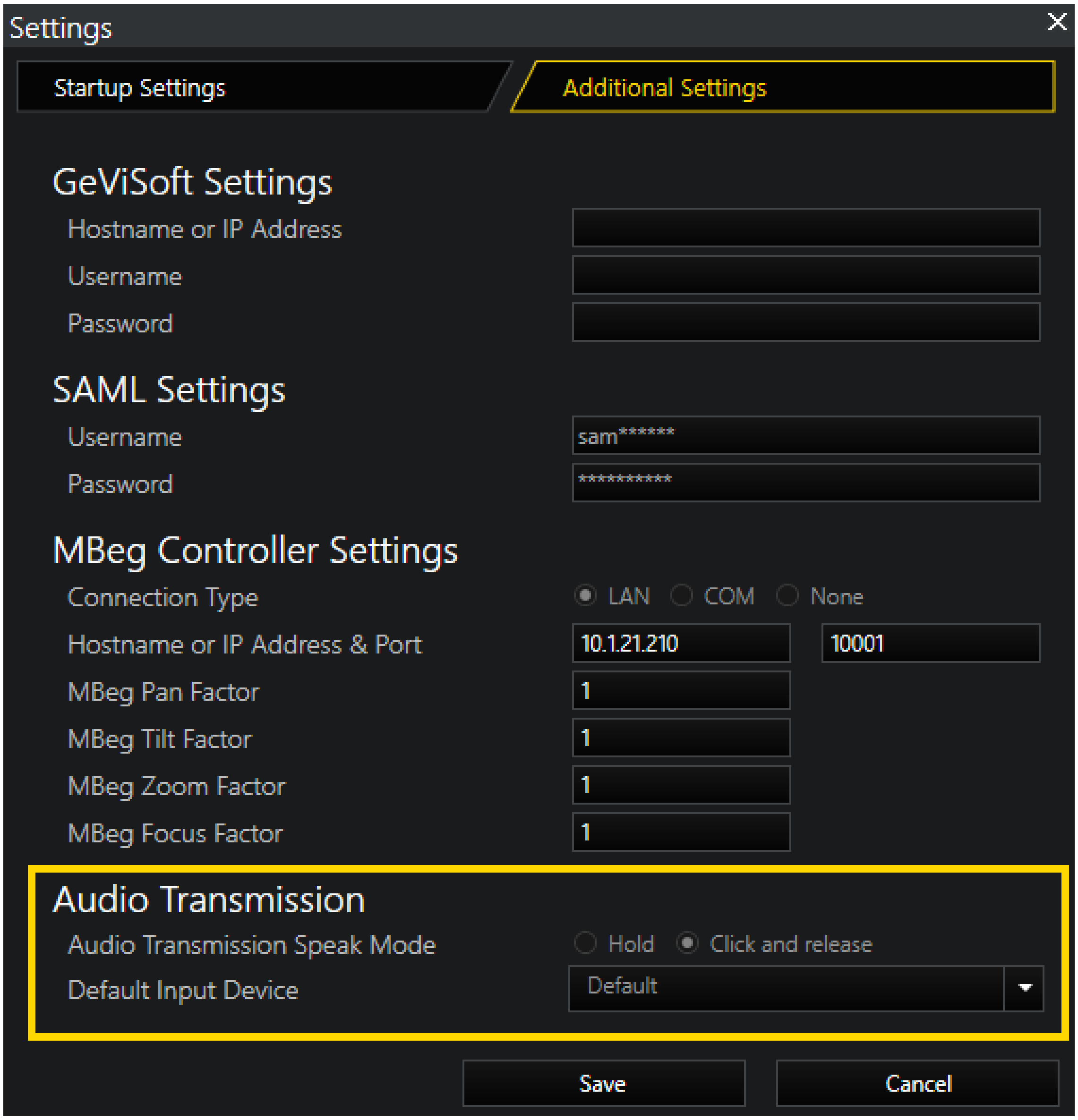
Marking	Description
6	LEDs indicating the camera status: • Green: camera status okay • Red: camera status failed • Grey: camera status unknown • Blue: camera status offline
7	Indication of the camera name.
8	Information on the selected camera is displayed.

Speak

The **Speak** button is an integral part of the 2-way audio transmission feature. It empowers the operator to transmit audio through a microphone to a camera. This is applicable to cameras that are configured with the ONVIF plugin and are equipped with either an internal or an external speaker.

How to configure the input device:

1. Open the **Settings** in the OpCon log in window and navigate to **Additional Settings** > **Audio Transmission**.



Settings

Startup Settings | Additional Settings

GeViSoft Settings

Hostname or IP Address

Username

Password

SAML Settings

Username: sam******

Password: **********

MBeg Controller Settings

Connection Type: ● LAN ○ COM ○ None

Hostname or IP Address & Port: 10.1.21.210 10001

MBeg Pan Factor: 1

MBeg Tilt Factor: 1

MBeg Zoom Factor: 1

MBeg Focus Factor: 1

Audio Transmission

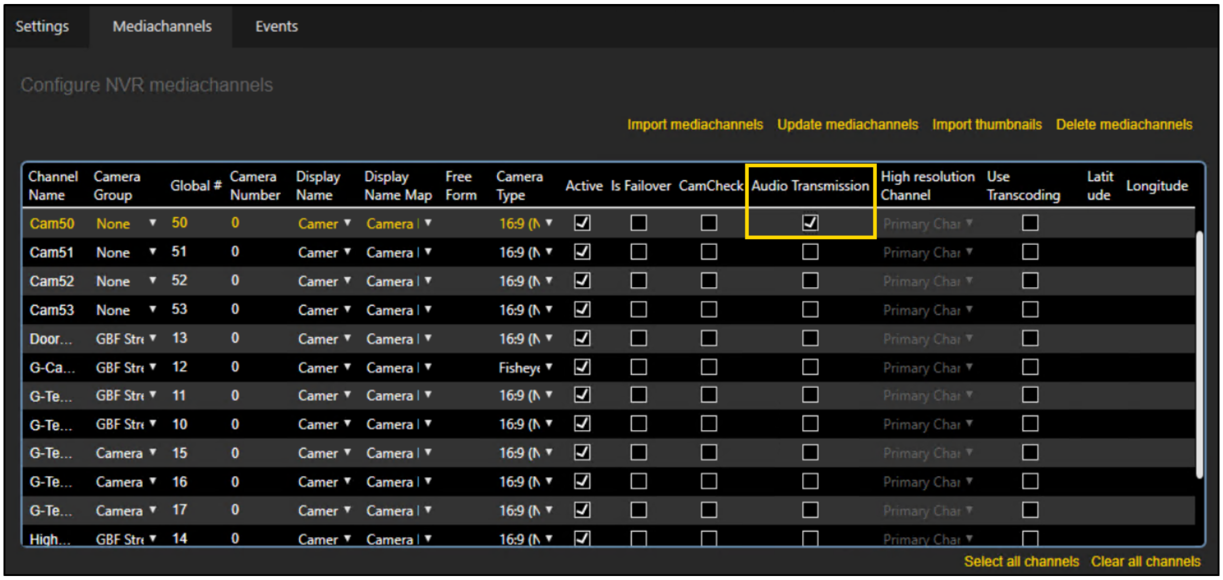
Audio Transmission Speak Mode: ○ Hold ● Click and release

Default Input Device: Default

2. Select the **Audio Transmission Speak Mode** to configure the **Speak** button behavior. You have two options here:
   - **Hold**: Voice is transmitted while button is pressed.
   - **Click and release**: First click activates voice transmission. Second click deactivates voice transmission.
3. In the **Default Input Device** drop-down menu, select the default microphone.

How to set up the camera for audio transmission:

In the ManCon interface, in the section **NVR & Cameras** > **Mediasources** > **Recorder** > **Mediachannels**, ensure that the camera (either possessing a speaker or connected to one) is marked as capable of **Audio Transmission**.



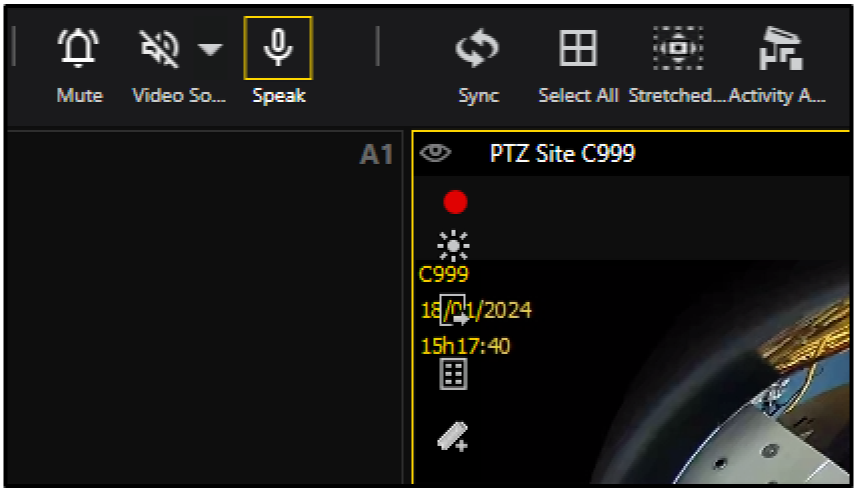
Configure NVR mediachannels

Channel Name	Camera Group	Global #	Camera Number	Display Name	Display Name Map	Free Form	Camera Type	Active	Is Failover	CamCheck	Audio Transmission	High resolution Channel	Use Transcoding	Latitude	Longitude
Cam50	None ▾	50	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	☑	Primary Char ▾	□		
Cam51	None ▾	51	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
Cam52	None ▾	52	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
Cam53	None ▾	53	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
Door...	GBF Stre ▾	13	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
G-Ca...	GBF Stre ▾	12	0	Camer ▾	Camera I ▾		Fisheye ▾	☑	□	□	□	Primary Char ▾	□		
G-Te...	GBF Stre ▾	11	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
G-Te...	GBF Stre ▾	10	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
G-Te...	Camera ▾	15	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
G-Te...	Camera ▾	16	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
G-Te...	Camera ▾	17	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		
High...	GBF Stre ▾	14	0	Camer ▾	Camera I ▾		16:9 (N ▾	☑	□	□	□	Primary Char ▾	□		

Indication of the status of the Speak button:

The **Speak** button is normally grayed out. It is only active if a camera capable of audio transmission is selected in a viewer. If you select such a camera and click the **Speak** button, the icon changes from a muted icon to an active microphone icon. Additionally, a blinking red recording symbol appears in the viewer.

It is not possible to select multiple viewers simultaneously for multicast or broadcast audio.

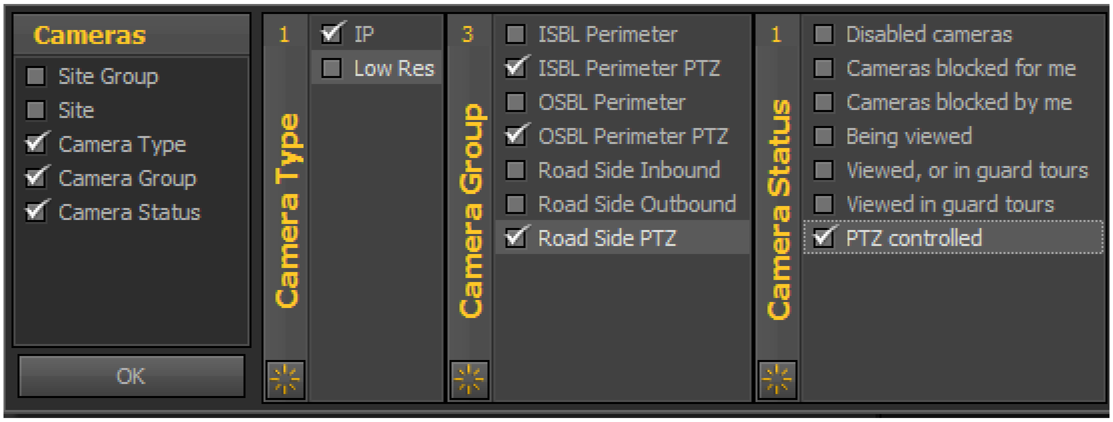


Filtering

Filtering is a core aspect of G-SIM, and is one of its foundations. To see why this is so, imagine going to a public library that you know has a book you want to read, but all you can remember is the author's name. When you arrive, their classification system is down, so you have no way of finding where in the library the book is. Sifting through potentially tens of thousands of events in G-SIM to find the one you are interested in is a task of similar proportion.

The traditional method of dealing with such large volumes of data is to make use of a data base (DB). This is all very well, and DBs are powerful indeed, but there is a problem: how do you tell the DB that it must look for certain information for you?

G-SIM has a very powerful filtering mechanism to cope with this. We have designed a query builder which knows how the DB is designed, and which gives you a simple, yet powerful interface to the DB's capabilities without having to know anything about SQL. The following screen shot shows how such a filter is defined in the G-SIM GUI.



Cameras

□ Site Group
□ Site
☑ Camera Type
☑ Camera Group
☑ Camera Status

OK

Camera Type 1

☑ IP
□ Low Res

Camera Group 3

□ ISBL Perimeter
☑ ISBL Perimeter PTZ
□ OSBL Perimeter
☑ OSBL Perimeter PTZ
□ Road Side Inbound
□ Road Side Outbound
☑ Road Side PTZ

Camera Status 1

□ Disabled cameras
□ Cameras blocked for me
□ Cameras blocked by me
□ Being viewed
□ Viewed, or in guard tours
□ Viewed in guard tours
☑ PTZ controlled

This is an example from the Cameras list (See **Tabbed Lists** and **The Camera List**). Since G-SIM filters are all defined in the same way, it does not matter which filter we use for the example.

You define a filter by clicking on one of the two filter buttons at the top of your list.

Once you have chosen a filter, you can press the filter icon to open the query builder. That then brings up the initial pane from which you can make one or more selections. The query builder is intelligent, in that it will not allow you to multi-select when that doesn't make sense, e.g. the in the far right of the above example, a camera can only be in one of those states, so you can only choose one.

In the above example, we chose Camera Type, Group, and Status. Each click opened up a filter detail pane related to that selection. Once you are happy with the filter definition, press OK to apply it. This will update the contents of the list to only those which match your filter criteria.

Press to clear your choices for any particular pane. The number displayed in the top of each filter criterion pane shows how many items in that pane's list have been chosen. In this example it's not particularly useful, but in large lists it will be of great value.

It may help to see the filters as incremental: each option you choose narrows the field further. When you start with just cameras, there could be thousands. Then if you choose camera type, the number drops. It drops further when you choose which camera group and status. In this way you can quickly go from a list containing thousands of entries to one containing just a few. Of course, this depends on how well your initial classification was done.

Also note that some lists that you filter are dynamic (for example you want every alarm in the past 30 minutes). To deal with such cases, press the refresh button to get the latest data.

Within the filtered results you can sort by clicking on column headings as required. Another trick is if you want to filter by cameras currently being viewed, just click on the view status icon to sort by viewed cameras.

Note Regarding Number of Items Returned

As useful and as powerful as filters are, it doesn't help you to receive a massive list as your filter output. In order both to speed up getting the result and keeping your results manageable, our filter lists contain no more than 2,000 elements.

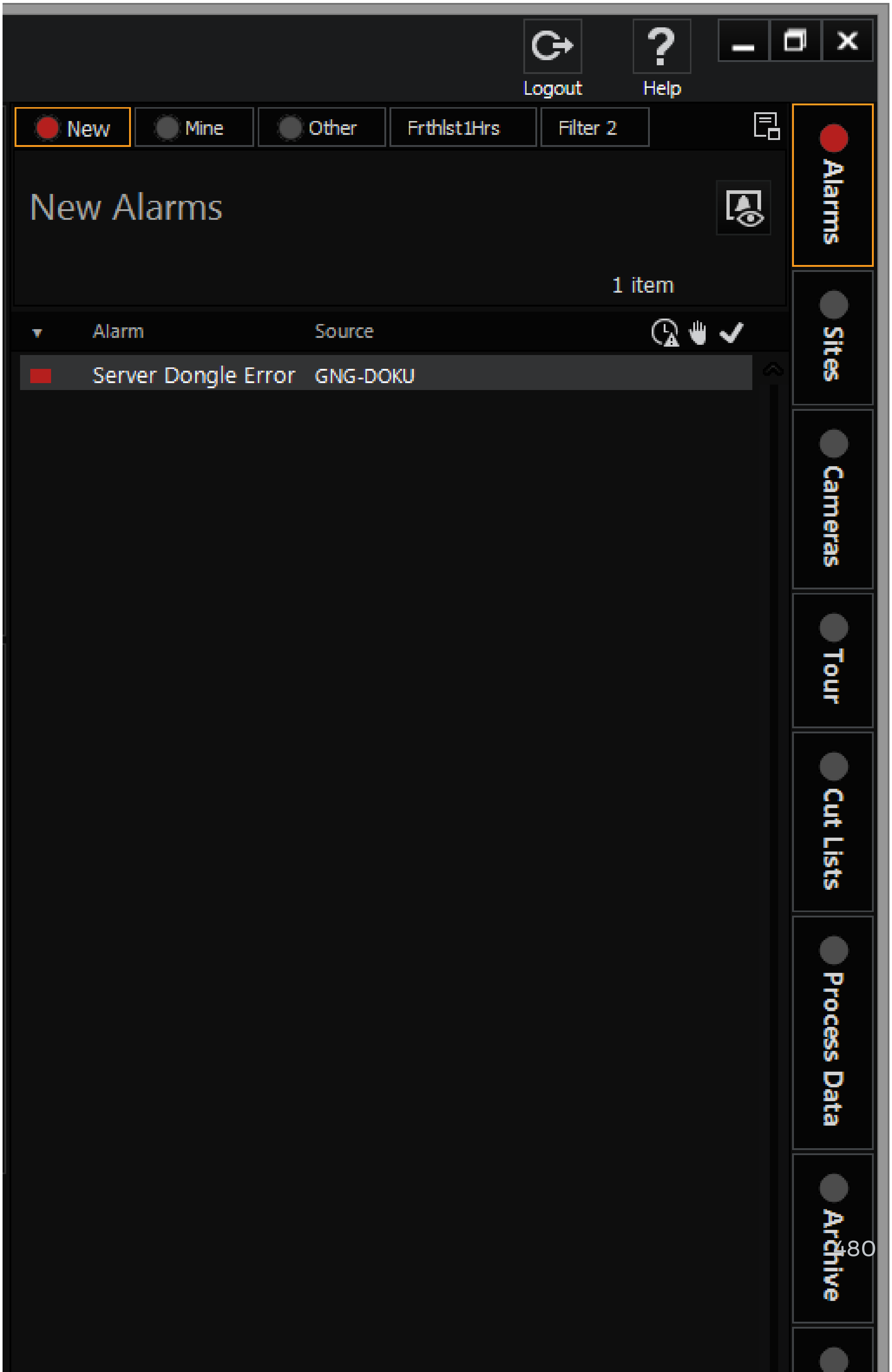
Notes for Alarm and Audit Log Filters

When you have applied a filter, the print button becomes visible. Useful though they are (page scaling, watermark, search,...) the options are mostly self-explanatory. The following should be highlighted, though:

Detail: Toggles whether to show only summaries, or detail on each alarm (not applicable to Audit Log entries).

/ **Export / Mail:** Each of these buttons has a drop-down list allowing you to choose the file format before choosing where to save to mail the file.

Tabbed Lists



New Alarms

1 item

Alarm	Source
Server Dongle Error	GNG-DOKU

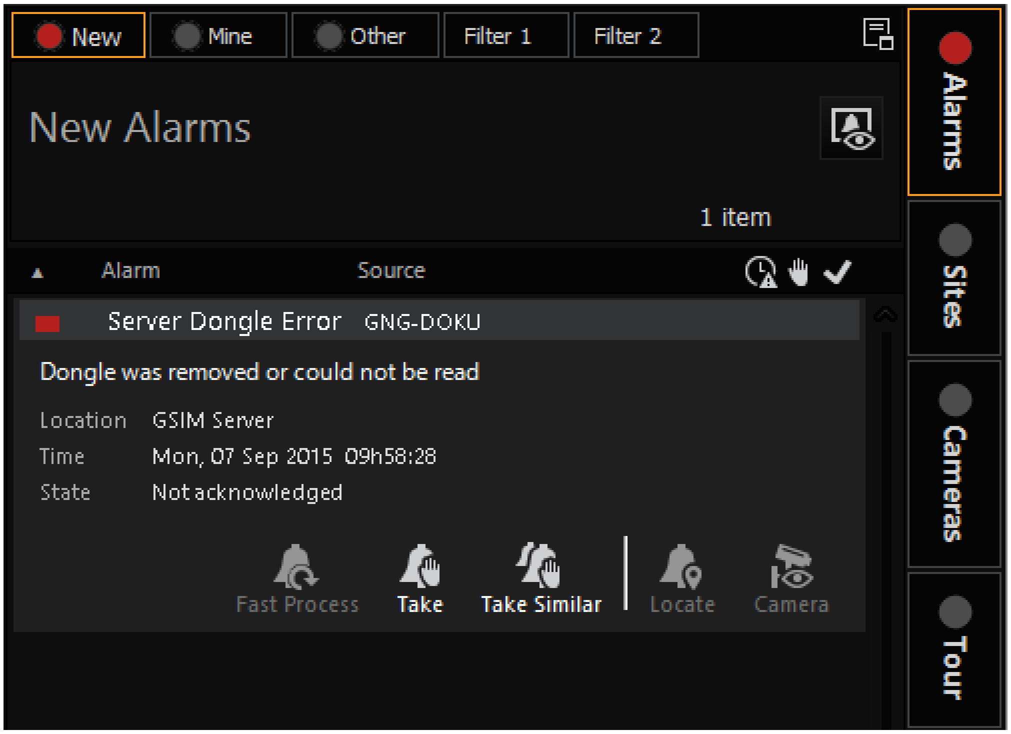
Operational data in G-SIM are displayed as Lists that are accessed through the Menu Tabs. By default the Menu Tabs and Lists are displayed on the right hand side of monitor 1, unless you have decided to mirror your template. Lists can be displayed either on the left or right hand side of the main interface, while the Menu Tabs may be positioned beside or above the Lists. Not all Lists may be visible to all users because of individual user privilege settings.

These Lists form the core control of the G-SIM Operator Interface and contain all system items you may want to use or access, e.g. Alarms, Sites, Cameras, VideoTools, Tours, Events, Users, Tasks, Messages, or Audit Log items (each has a dedicated chapter). Items may be dragged from these Lists to populate Viewers, for example be it to view a camera Live, to get a map of a site or to handle an Alarm. In the rest of this chapter we will focus on the generic aspects that are applicable to most of the Lists.

List Layout

All the Lists available to a specific user are grouped on one of the Main Tabs, and by clicking the corresponding tab, its List will be displayed. At the top of most Lists is a set of filter buttons that can be used to filter the list content. Depending on the list, the first is usually "All", which is an unfiltered list, followed by two filters that you can define. See **Filtering** for more on filtering.

The items in the list are each displayed as a line of text giving the most essential information about the item. Clicking on an item will expand it to reveal a Detail Card with information about the item.



New Alarms

1 item

Server Dongle Error GNG-DOKU

Dongle was removed or could not be read

Location GSIM Server
Time Mon, 07 Sep 2015 09h58:28
State Not acknowledged

Many items have detail that might in turn also contain one or more lists, e.g. the Detail Card of a Camera may contain a list of users who currently have viewers attached to the camera, as well as a list of currently playing Tours which contain this camera. Most of the items in these Detail Card lists are again objects that might be used in drag-and-drop operations.

> Example For example: if a user is viewing a camera, his/her name will appear in the Users List in the Camera Detail, and you may drag that user's name from here to the Msg Tab to send the user a message.

The text colors of list items indicate intrinsic (fixed) properties of the item, e.g. in the Camera List the different camera positions are indicated by different colored text.

An item's state is indicated by a series of State Icons displayed to the right of the item's colored band. Some items may hold only single states, e.g. in the Users List a user is logged in or not, and this state is indicated by an icon. Cameras in the Camera List can display the view state (if viewed by any users), blocked state, available state etc. These state icons will be discussed in detail for each List in subsequent chapters, but a rule of thumb is that an icon with a small figure in the left corner indicates that you (the current logged in user) are the owner. E.g. a screen icon in the camera list indicates that the camera is viewed by a user. A screen icon with a figure in the corner indicates that you are viewing that camera.

Below are state icons associated with cameras:

🖥	**Viewed.** The camera is currently being viewed by someone
🖥	**Viewed by me.** You (the logged in user) are currently viewing the camera
🚫	**Blocked to me.** The camera is blocked by someone, and you may not view it at this stage
🚫	**Blocked by me.** You (the logged in user) blocked this camera

Applying Filters to a List

Most Lists may be filtered by at least one filter criterion. A filter is set by clicking on the filter box and selecting an option from the list of available criteria, as explained in detail in **Filtering**.

Pressing a key while the filter list is open will select the first item in the list starting with this letter. This is useful in long sorted criteria lists, e.g. selecting a site in the camera list. You can also use arrow keys or the mouse wheel to scroll through a filter list.

Incremental Search in Lists

In the Site List the incremental search facility is very useful to find a specific site by simply starting to type the site name while the list has focus (for example positioning the mouse cursor over the list). All letters pressed within 1 second from each other will be added to the current search, and a new search will start after a 1 second delay. For example: pressing 'B', 'A', 'L' with less than a 1 second delay between each letter will select the first word starting with 'BAL'. If you type 'B', 'A', wait 1 second and then press 'L', the first item starting with 'BA' will be selected, and thereafter the first item starting with 'L' will be selected.

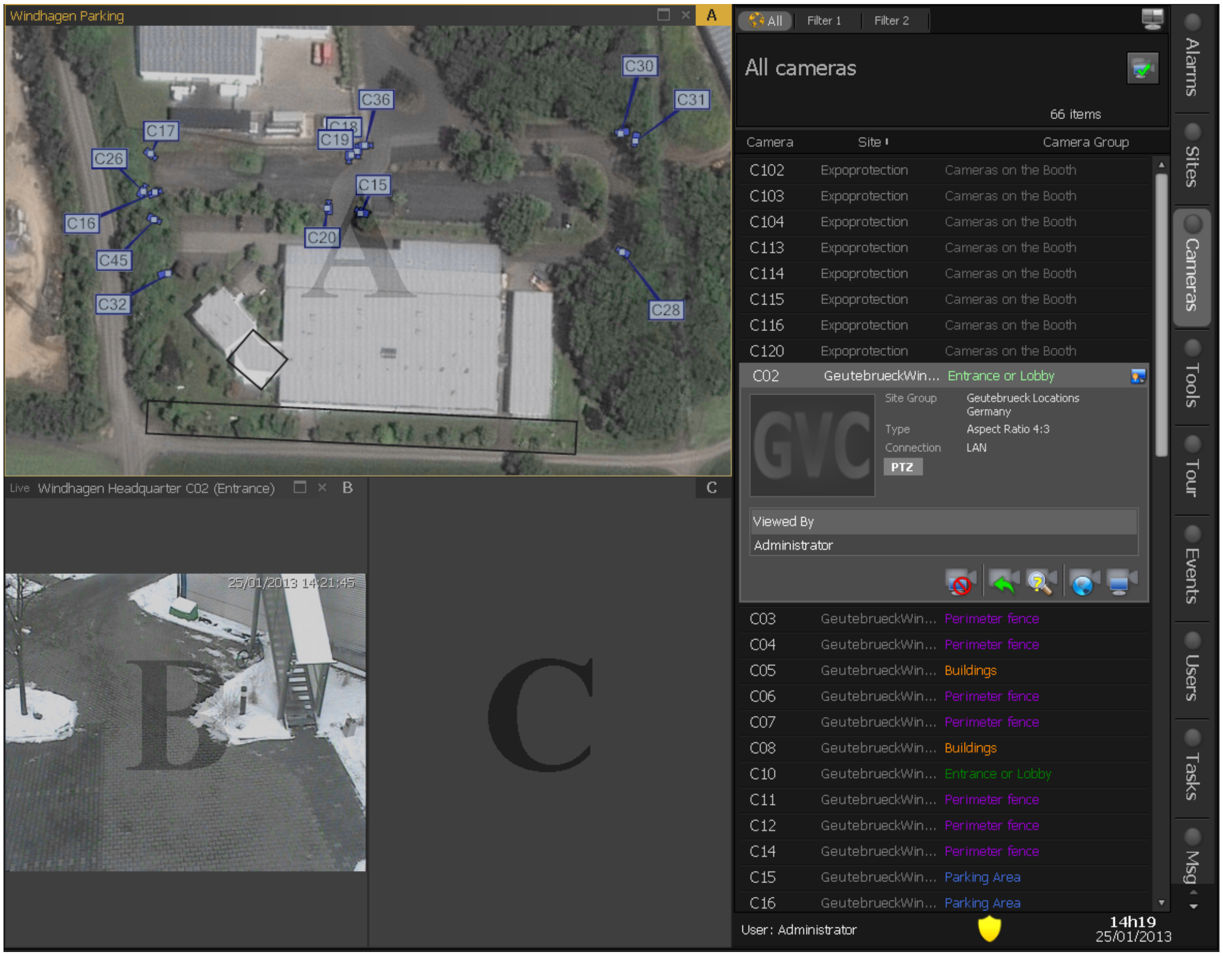
The arrow keys may be used to select a list item in close proximity of the previous selection. The mouse wheel may also be used to scroll through a list if you want to select an item using the mouse.

Multi-Selection in Lists

Some of the lists (e.g. the alarm and cameras lists) and some of the filter criteria (e.g. selecting users to block from viewing a camera) allow the user to select more than one item and then batch process all the selected items. It is sometimes very useful to be able to handle a batch of new alarms that were generated because of a recurring failure, or to add a group of cameras to a Tour by selecting them all, then dragging them to the GT.

Viewers

Viewers refer to all the windows except the group of Tabbed Lists as described above. These windows can be used to dock and view video streams, maps or Lists. The whole main interface area not used for Lists or the main toolbar consists of Viewer windows. Viewers fill the whole screen area of any second, third or fourth monitors. Each Viewer window has a single-digit identifier displayed in its top right corner. The actual size and layout of Viewer windows can be customised, as described elsewhere in this chapter (see **Toolbar**).



All cameras

66 items

Camera	Site	Camera Group
C102	Expoprotection	Cameras on the Booth
C103	Expoprotection	Cameras on the Booth
C104	Expoprotection	Cameras on the Booth
C113	Expoprotection	Cameras on the Booth
C114	Expoprotection	Cameras on the Booth
C115	Expoprotection	Cameras on the Booth
C116	Expoprotection	Cameras on the Booth
C120	Expoprotection	Cameras on the Booth
C02	GeutebrueckWin...	Entrance or Lobby

Site Group: Geutebrueck Locations Germany
Type: Aspect Ratio 4:3
Connection: LAN
PTZ

Viewed By
Administrator

Camera	Site	Camera Group
C03	GeutebrueckWin...	Perimeter fence
C04	GeutebrueckWin...	Perimeter fence
C05	GeutebrueckWin...	Buildings
C06	GeutebrueckWin...	Perimeter fence
C07	GeutebrueckWin...	Perimeter fence
C08	GeutebrueckWin...	Buildings
C10	GeutebrueckWin...	Entrance or Lobby
C11	GeutebrueckWin...	Perimeter fence
C12	GeutebrueckWin...	Perimeter fence
C14	GeutebrueckWin...	Perimeter fence
C15	GeutebrueckWin...	Parking Area
C16	GeutebrueckWin...	Parking Area

User: Administrator

14h19
25/01/2013

To populate a Viewer with a video, map or List, you can use either the keyboard or the mouse. Some List items (Cameras, Tours, and Maps) have in their detail view a View button which may be used to dock that item on a Viewer. The description of this button depends on the item: Show on Map in the case of a site, View Live in the case of a camera and View Tour in the case of a Tour. After clicking any of these buttons the unique identifying letter of each Viewer will be enlarged and overlaid over the Viewer window (as shown in the image above). On your keyboard, press the identifier of the Viewer you want to use — the selected item will then be displayed at that position. Alternatively simply click on the viewer.

Lists can also be copied to a Viewer window (the original list will always stay in the Tabbed List group). This is useful if you always want to have an Alarm List open, if you want your List of Tasks in a separate window, etc. To copy a List to a viewer, click the **Dock List** button at the top of the List next to the tabs, and select a Viewer by typing its letter as before. Or you can just drag the List's tab and drop it on the Viewer.

A Viewer may very easily be populated using the mouse by dragging an item from a List and dropping it on the Viewer window. An item may be dragged without its detail being displayed - the above mentioned method using the keyboard can only be accomplished if the Detail Card is expanded, because you need to click a button on the Card. If the detail is displayed, you can start to drag the item by grabbing any part of it. You can also copy a list to a Viewer by grabbing it in the header section and dropping it on a Viewer. Starting a drag operation in the List body will obviously drag a list item and not the List itself.

You can use drag & drop either to copy a viewer's content or to move the viewer. To copy, click on the content then drag it and drop it where you want the copy displayed. To move it, drag the viewer's header. This is useful if you want to review the footage whilst still viewing it live in the original viewer.

The result of a drag-and-drop operation depends on the item being dragged and the current content of the viewer it is dropped on. If a camera is dropped on an empty viewer, the live video will be displayed, whereas if it's dropped on a viewer containing a map, that camera's position will be highlighted on the map (even if the map containing that camera has to be loaded).

The mouse cursor will always give an indication of the kind of item being dragged, and will change to show the action that will be performed if dropped on a specific viewer.

The detail of how to control cameras with the viewer interface and other topics are explained in detail in the chapter on Cameras. See **Viewing Camera Footage**.

General Navigation

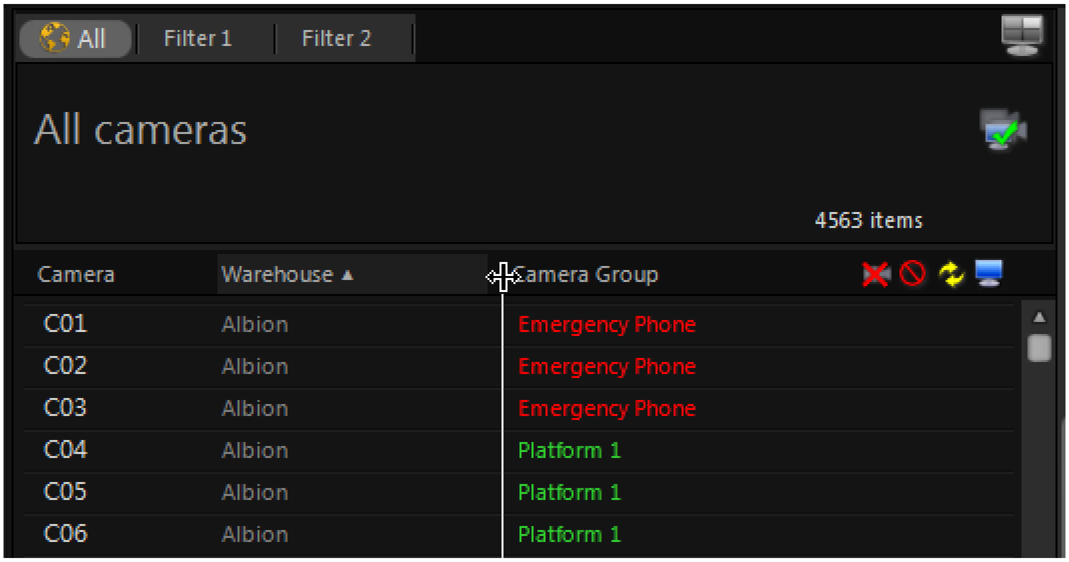
The G-SIM Management Console is mainly a drag-and-drop interface, meaning that you can perform most tasks by dragging items with the mouse from one position and dropping them somewhere else to perform a certain task. The outcome of these drop actions will be the most logical action under the circumstances, and will be ignored if no action is possible. Many of the navigation details described in the rest of the manual are therefore intuitive if you understand the basic idea of dragging and dropping items. It is more important to grasp the idea and way of thinking behind the interface than to try and memorise all the possibilities to perform a certain task.

Input Focus

When a Viewer, List or input box has focus, then all keyboard and mouse wheel events are directed to it. To shift the input focus to a Viewer, you simply click with the mouse in the viewer. The outside frame and identifier of a viewer will be highlighted if it has input focus. If recorded camera footage is reviewed, the viewer must have focus if you want to use the keyboard to control the playback (forward, rewind, pause etc.), or use the mouse wheel to zoom. A map must have focus to use the mouse wheel to pan or zoom. If the mouse cursor is moved over a List, the List will automatically get all mouse wheel events so that the List will scroll up and down when the mouse wheel is used while the cursor is over the List. If you are typing in a text box (e.g. typing a comment for an alarm), the text box will have the input focus, and you will have to click on the List or the List's scroll bar to move the focus back to the List itself.

Resizing Operator Console Card List Columns

Card List Columns may be resized with the mouse by positioning the mouse cursor on the card list header near a column start/end. The cursor will change to indicate a column resize may be performed. Click and drag the mouse to resize the column - a minimum width will be applied to ensure all columns are always visible - a column width cannot be set to zero.



Camera	Warehouse ▲	Camera Group
C01	Albion	Emergency Phone
C02	Albion	Emergency Phone
C03	Albion	Emergency Phone
C04	Albion	Platform 1
C05	Albion	Platform 1
C06	Albion	Platform 1

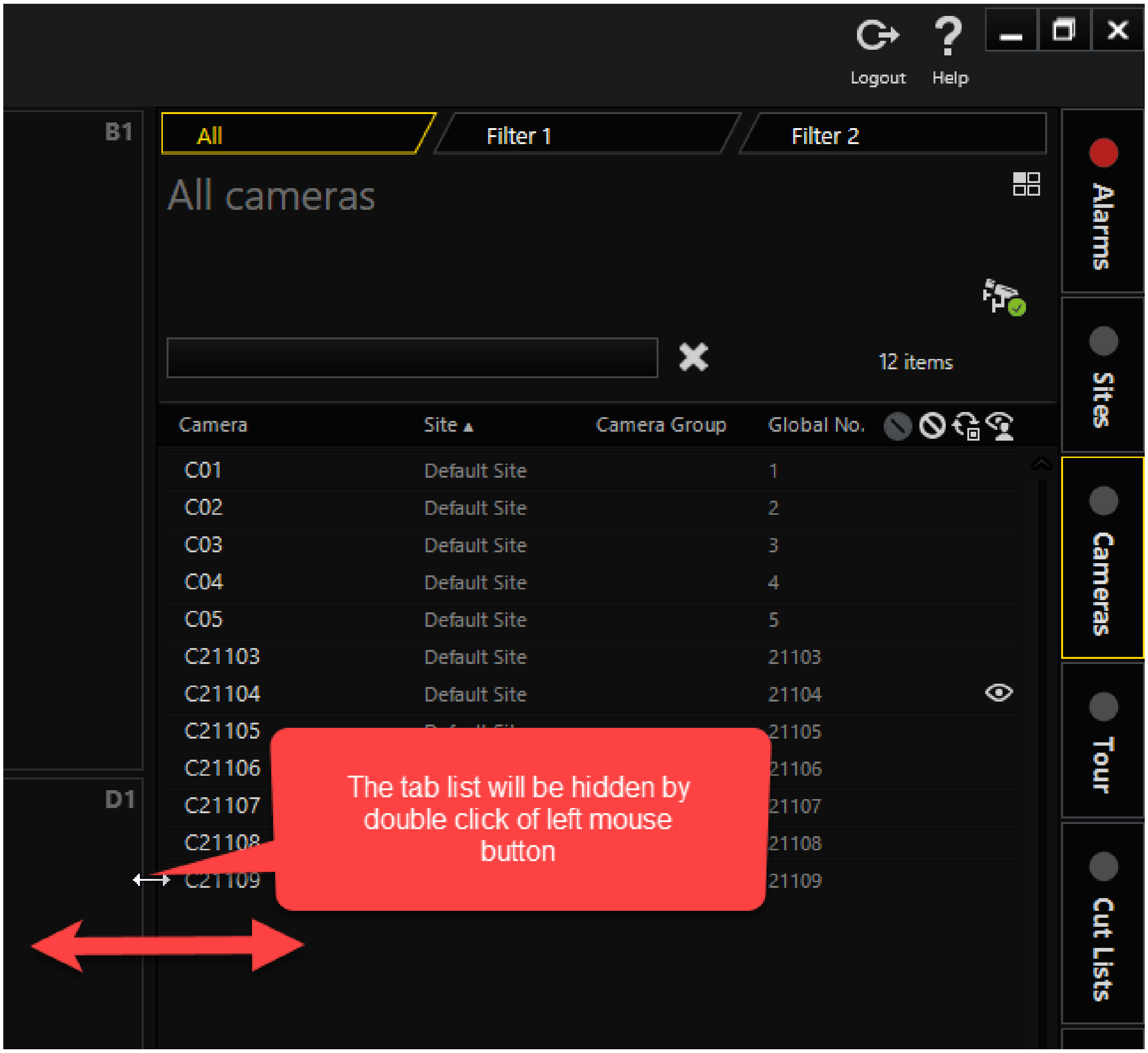
Resizing of Navigation

General

This implementation allows you to resize the menu / timeline and video controls so that you can reduce the space required for the card list/ timeline and video controls and have more space available for the camera.

Different Size of Menu

The operator can use the mouse to resize the card list area to a smaller size.



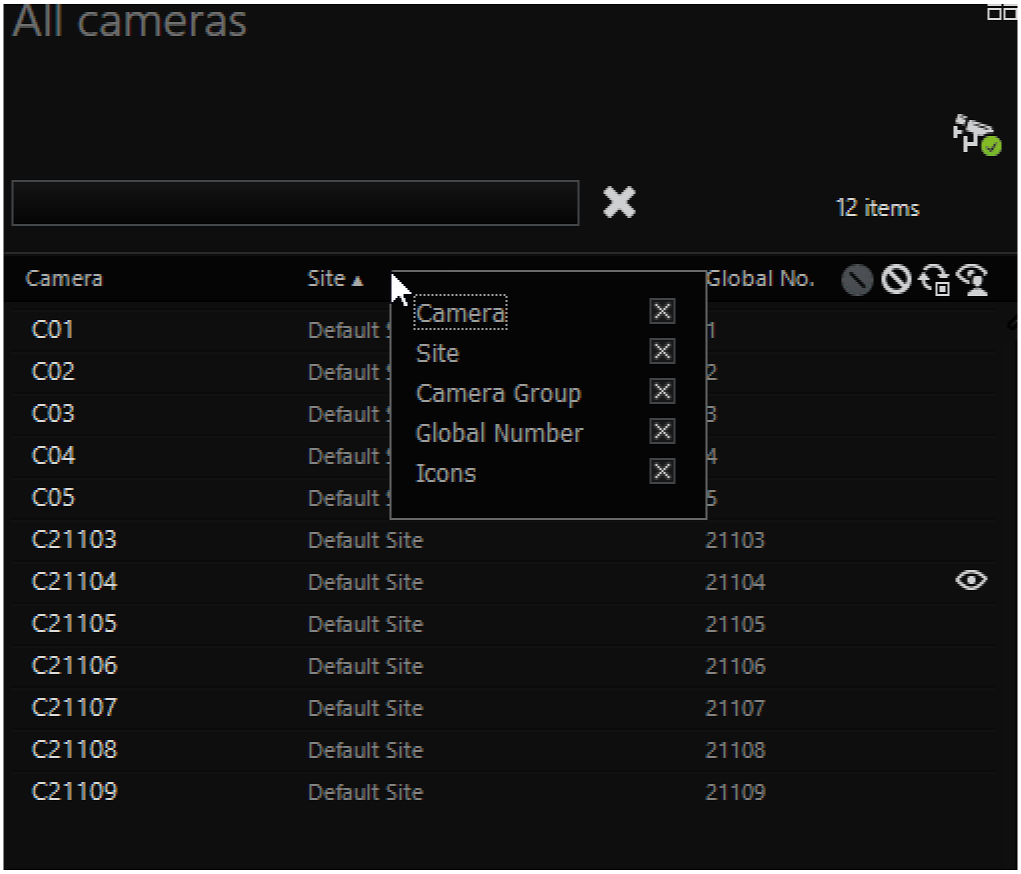
All cameras

12 items

Camera	Site ▲	Camera Group	Global No.
C01	Default Site		1
C02	Default Site		2
C03	Default Site		3
C04	Default Site		4
C05	Default Site		5
C21103	Default Site		21103
C21104	Default Site		21104
C21105	Default Site		21105
C21106			21106
C21107			21107
C21108			21108
C21109			21109

The tab list will be hidden by double click of left mouse button

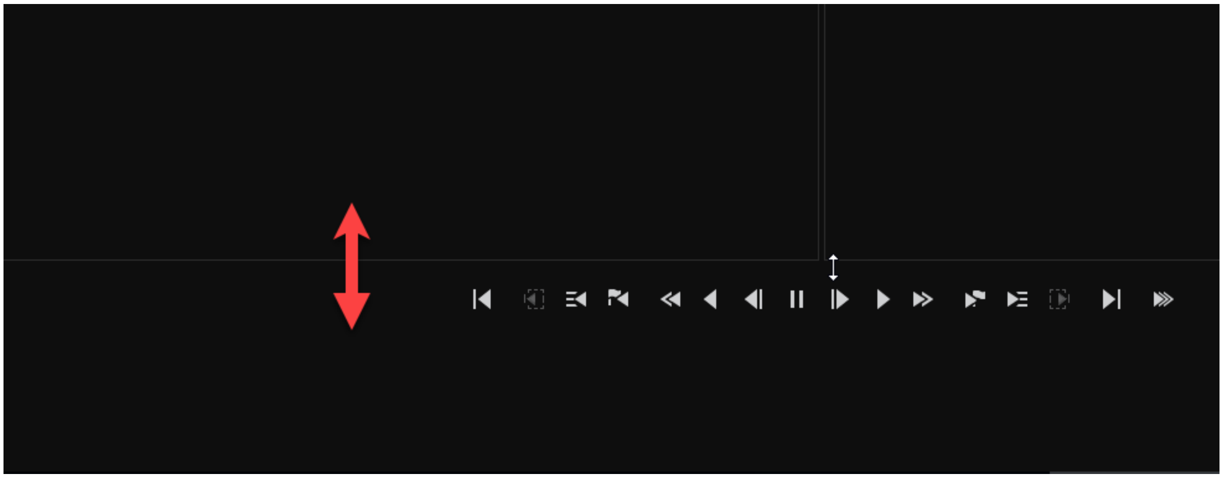
The maximum width value is 30% of the width of the operator console. The minimum width value is 15%. The tab list can be hidden by double-clicking with the left mouse button. The operator can enable the tab list from main menu. The operator can select which columns are visible in the card list for each navigation tab. Click with the right mouse button on the card list header for the context menu.



Camera	Site ▲	Global No.
C01	Default	1
C02	Default	2
C03	Default	3
C04	Default	4
C05	Default	5
C21103	Default Site	21103
C21104	Default Site	21104
C21105	Default Site	21105
C21106	Default Site	21106
C21107	Default Site	21107
C21108	Default Site	21108
C21109	Default Site	21109

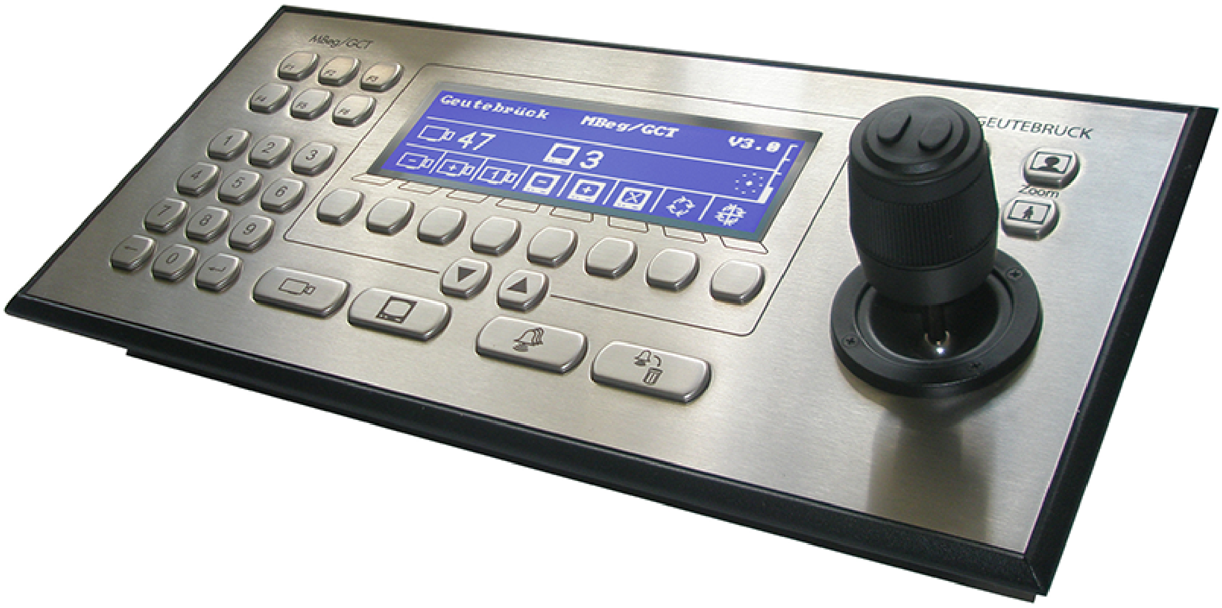
Different Size of Timeline and Video Controls

The operator can use the mouse to resize the timeline and video controls. The minimum height is the value if the video controls are still present without the timeline. The maximum size is the value of the current height.



Using an MBeg Controller

An MBeg Controller is a multi-function operator keyboard, developed specifically for operating video matrices and camera remote control systems.



Although the actual MBeg hardware is aimed at different (non-G-SIM) installations and it does not cater for all the system requirements of G-SIM, we nevertheless use it to the fullest extent.

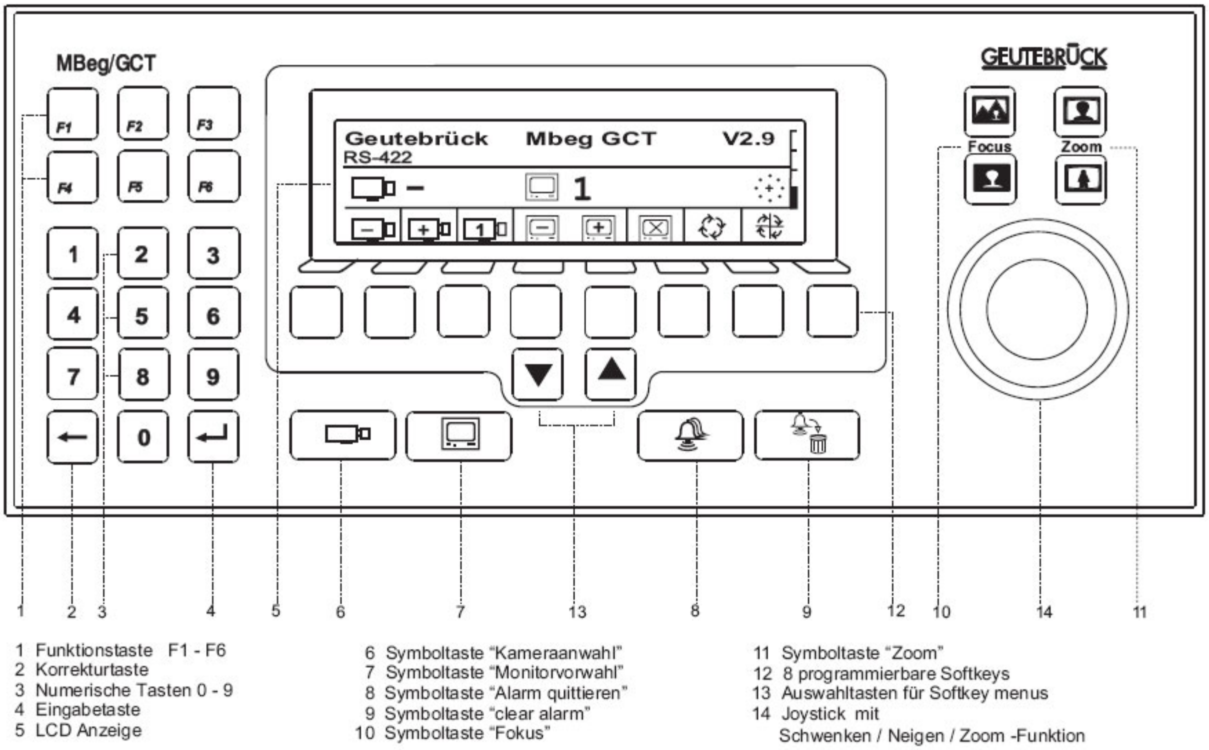
The MBeg is a very good PTZ controller and when used in conjunction with a mouse for camera selection, it becomes extremely useful. Furthermore, all the playback functionality is supported as well. Although not recommended as the only way of selection, the MBeg can be used to select a camera and viewer to display it in, and then control it if required.

Traditionally the MBeg keyboard is used (via GeViSoft) to control alarm-handling as well, but only has the ability to acknowledge the most recent alarm, and optionally “Quit” it (or in G-SIM terms, Complete it). This is obviously very limiting, as G-SIM caters for multiple alarms of a single type to exist simultaneously, and also facilitates the enforcement of alarm-handling procedures and user feedback, all of which is quite impossible with only the joystick controller. That said, we do allow for the acknowledgement of any alarm, and even the Completing of it with the MBeg, as long as there are no specific handling actions for that type of alarm.

The current implementation of the MBeg with G-SIM does not require the configuration of GeViSoft.

Operator Console Interaction

Although it is highly recommended to use a mouse and keyboard for selection in G-SIM, it is possible to use the MBeg for most screen interactions and navigation.


MBeg/GCT
GEUTEBRÜCK
F1
F2
F3
F4
F5
F6
1
2
3
4
5
6
7
8
9
0
Geutebrück Mbeg GCT V2.9
RS-422
1
Focus
Zoom
1 2 3 4 5 6 7 13 8 9 12 10 14 11
1 Funktionstaste F1 - F6
2 Korrekturtaste
3 Numerische Tasten 0 - 9
4 Eingabetaste
5 LCD Anzeige
6 Symboltaste "Kameraanwahl"
7 Symboltaste "Monitorvorwahl"
8 Symboltaste "Alarm quittieren"
9 Symboltaste "clear alarm"
10 Symboltaste "Fokus"
11 Symboltaste "Zoom"
12 8 programmierbare Softkeys
13 Auswahltasten für Softkey menus
14 Joystick mit
Schwenken / Neigen / Zoom -Funktion

Softkeys (13). These 8 keys are assigned to trigger the 8 function displayed directly above them on the screen in the 4 different Softkey Menu. The Softkey Menus can be selected by using the up (▴) and down (▾) arrows (directly underneath the Softkeys), as well as an additional Softkey Menu for each for the 4 Symbol Keys.

Symbol Keys (6-9). These keys are used to select specific elements or perform specific tasks within G-SIM:

- "Camera Select" is used to select the Camera List
- "Monitor Pre-Select" is used to make the Viewers available for selection using the Joystick
- "Acknowledge Alarm" is used to select New Alarms in the Alarm List
- "Clear Alarm" (not used).

Focus and Zoom Symbol Keys (10-11). The “Focus” keys focus the camera that is currently selected in the Viewer. The “Zoom” keys control the zoom of the currently selected camera in the same way the mouse wheel does.

Joystick (14). Joystick with Pan/Tilt/Zoom function.

Selecting a Viewer

1. Select the Alarms List by pressing the “Acknowledge Alarm” symbol key.
2. Use the Softkeys #3 and #4 to scroll through the New Alarms.
3. Press Softkey #7 under the “Apply and Close” symbol to Acknowledge an Alarm.

Selecting a Camera from the Camera List

1. Select the Camera List by pressing the “Camera Select” symbol key
2. Use the Joystick to scroll through the list. Pressing the Joystick slightly up or down will scroll through the list one item at a time; pressing the Joystick all the way up or down will scroll a whole page at a time.
3. Press Softkey #7 under the “Apply and Close” symbol to send the Camera to the selected Viewer.

Selecting an Alarm from the Alarm List

Remember: The MBeg controller does not allow complex alarm handling, as needed with most alarms.

1. Select the Alarms List by pressing the “Acknowledge Alarm” symbol key.
2. Use the Softkeys #3 and #4 to scroll through the New Alarms.
3. Press Softkey #7 under the “Apply and Close” symbol to Acknowledge the Alarm.

Take/acknowledge/complete an alarm

The following buttons on the MBeg may be used to take/acknowledge/complete an alarm:

- the "Enter" key on the num pad
- the second-from-right "soft key"

- the left main Alarm button. This 3 buttons will therefore always do the same thing.

The result of pressing any one of the above buttons depends on the current state of the alarm

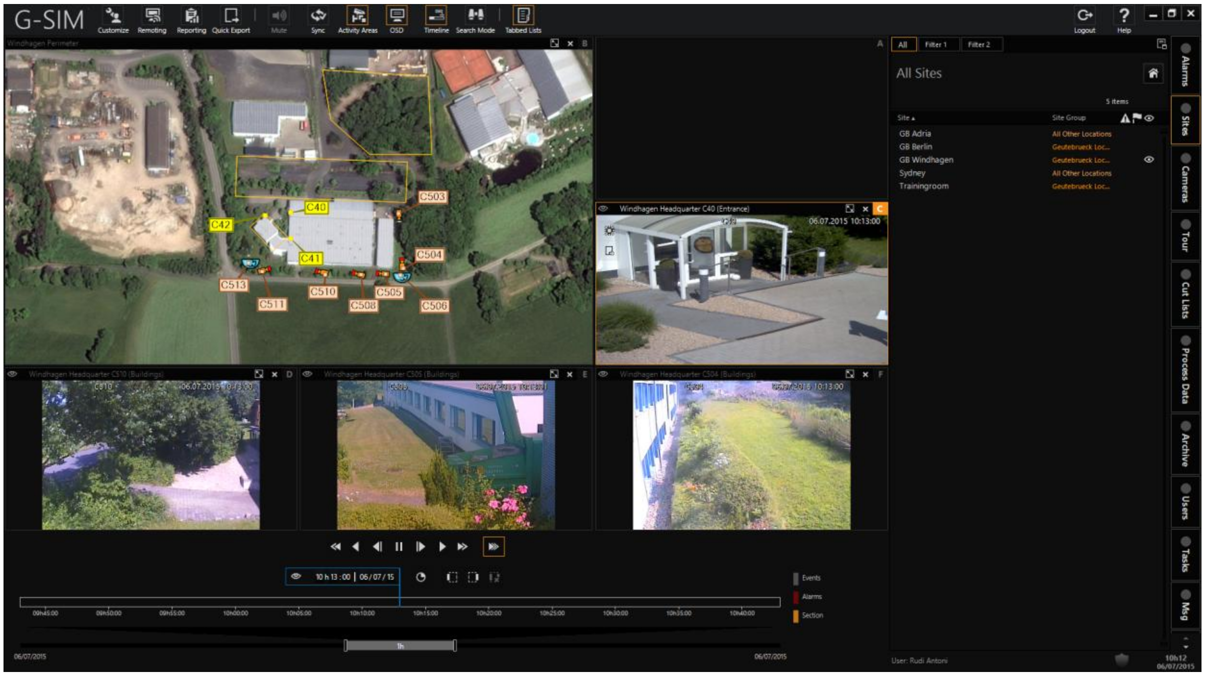
- If an alarm may be fast processed, it takes and completes the alarm

OTHERWISE (not fast process)

- Take/Acknowledge an Alarm which was not acknowledged yet
- Complete and Alarm which was already acknowledged - the first time you click it the alarm will be acknowledged, and the same card will stay selected. If you click it again, the alarm will be completed and removed from the list and the next alarm will be selected. If you just want to take the alarm but not complete it, you can click the button once, move to the next alarm etc.

The F3 key will show the Alarm pop-up screen (alarm detail). It will not remove the screen again because you may move to another alarm and click it again to add this alarm as a tab to the Alarm Screen.

Sites



All | Filter 1 | Filter 2

All Sites

5 items

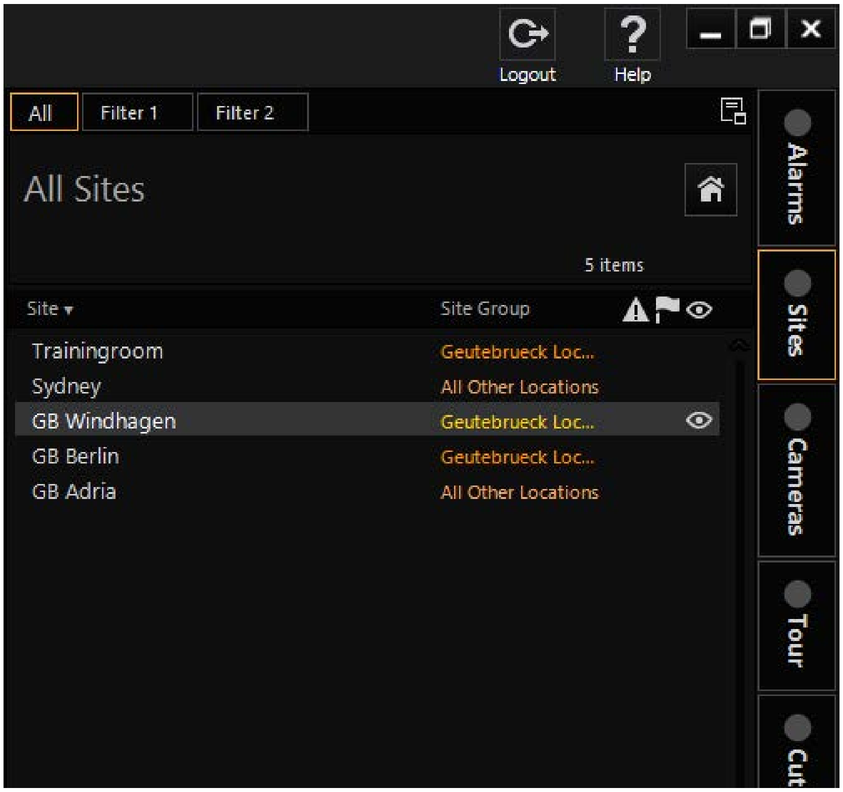
Site ▲	Site Group	⚠ ⚑ 👁
GB Adria	All Other Locations	
GB Berlin	Geutebrueck Loc...	
GB Windhagen	Geutebrueck Loc...	👁
Sydney	All Other Locations	
Trainingroom	Geutebrueck Loc...	

A site is a logical (and usually physical) grouping of cameras which may be accessed via the Sites List. Every site may belong to a Site Group further to simplify sorting and referencing. For example, for a rail customer, Sites would be train stations while the Site Groups specify on which railway line a particular station is.

The physical representation of a site is a map — therefore if a site is dropped on a viewer, a map of the site will be displayed. See **Maps** for more on maps.

Site List

The Site List gives you quick access to available sites. Each row in the list represents one site and displays the site name, site group and a series of state icons to indicate sites with active video connections as well as possible connection problems.



Site ▾	Site Group	⚠ 🚩 👁
Trainingroom	Geutebrueck Loc...	
Sydney	All Other Locations	
GB Windhagen	Geutebrueck Loc...	👁
GB Berlin	Geutebrueck Loc...	
GB Adria	All Other Locations	

Filter and Search

Site filters are configured exactly as per **Filtering**. The following points are highlighted.

A site may be easily selected in the Site List by starting to type the site's name while the list has input focus. See **Main Interface** for more on incremental searches in Lists.

Buttons

Button	Description
⧉	Pressing this button allows you to dock a copy of the site list in a viewer.
🏠	Pressing this button is a short cut to display the installation's home site map.

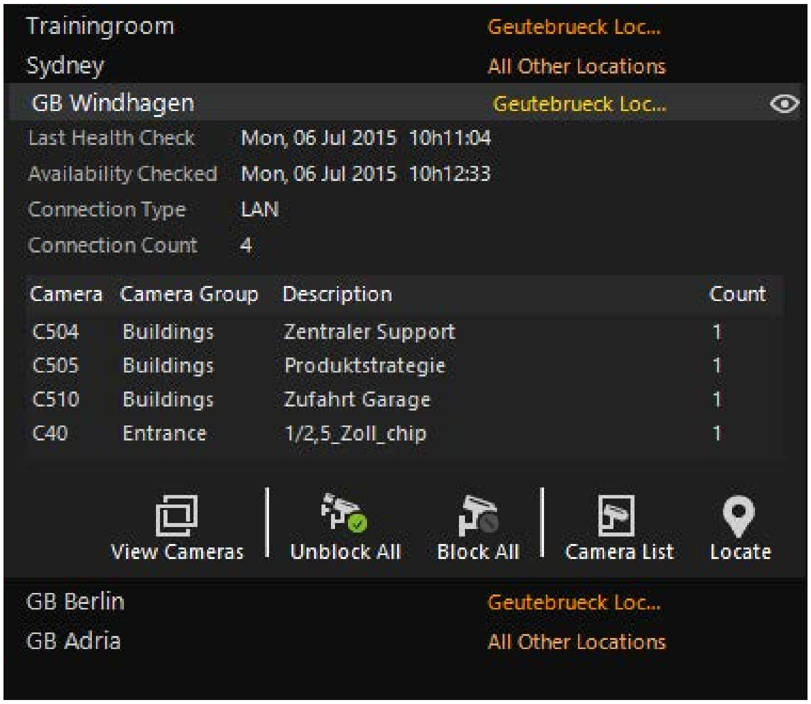
Site Status

The third column in the list shows the current activity and status of each site which include sites with open video connections and sites with connection problems.

Icon	Status	Description
👁	Viewed	The site has one or more open video connections. By selecting the site you will be able to see which cameras on the site are being accessed, and by how many users.
⚑	Health Check Overdue	The site's health agent did not contact the server within the pre-set time for health agent check-ins. The "Last Health Check" entry on the site detail card will show the date and time the last contact was made by the health agent (see Site Detail later in this chapter). This flag will only be displayed to users with the "Show Site Critical Flag" privilege (typically administrators and maintenance personnel).
⚠	Some Cameras (NVRs) Unavailable	Some of the cameras on the site are not available, owing to problems connecting to one or more NVRs. This flag will only be displayed to users with the "Show Site Critical Flag" privilege.
⚠	All Cameras (NVRs) Unavailable	All cameras on the site are not available due to connection problems to the NVR's. If a site has only one NVR this flag will be displayed if it cannot be connected to. This flag will only be displayed to users with the "Show Site Critical Flag" privilege.

Site Detail

A site may be selected in the Site List either by clicking on the desired item or by starting to type the name of the site while the site list has input focus (see **Main Interface**). After selecting a specific site item (row) in the list, the following detail will be displayed for that particular site:



Trainingroom	Geutebrueck Loc...
Sydney	All Other Locations
GB Windhagen	Geutebrueck Loc...

Last Health Check	Mon, 06 Jul 2015 10h11:04
Availability Checked	Mon, 06 Jul 2015 10h12:33
Connection Type	LAN
Connection Count	4

Camera	Camera Group	Description	Count
C504	Buildings	Zentraler Support	1
C505	Buildings	Produktstrategie	1
C510	Buildings	Zufahrt Garage	1
C40	Entrance	1/2,5_Zoll_chip	1

GB Berlin	Geutebrueck Loc...
GB Adria	All Other Locations

Details

Detail	Description
Last Health Check	Time and date of the last health check
Connection Type	The connection type will usually be LAN Local Area Network or ISDN Integrated Services Local Network. **If the Connection Type is ISDN, be aware that only limited connection to it will be possible. Not only may the initial connection to a camera on the site be slow, but the total number of video streams that may be viewed from the site will be limited, meaning that you may not be able to access a camera on an ISDN site if there are open connections to such a site.**
Active cameras	For the active cameras, the number of connections is also shown in the list. The list is updated dynamically. It can thus detect if a camera in this site group is being viewed or no longer being viewed by a user.

Buttons

The following action buttons are available on the Site Detail Card. If a viewer is selected which already contains some other content, it will be replaced. This option will only be available to users with the "View Site Map" privilege.

Settings	Description
View Cameras	Show all cameras from the site.
Unblock all	The button allows you to cancel the blocking of any cameras you blocked on this site. i **This option is only available to users with the Block Camera privilege.**
Block all	Allows you to block access to all the cameras of the selected site. i **This option is only available to users with the Block Camera privilege.**
Camera list	This takes you to the **Cameras** tab where it creates a camera filter showing a summary of the current connections to this site.
Locate	This button allows you to display an overview map of the site in the viewer of your choice. When you click the button all viewer windows will display their unique letter identifiers. It may be used in three different ways: • Press the corresponding key on the keyboard to place the map in the viewer • Click with the mouse in the viewer. • Drag the button to the viewer where you want the map to be displayed.

Blocking and Unblocking All Cameras on Site

Camera blocking allows a sufficiently-privileged user to prevent any other user or group of users to access the cameras on a site. This may be required to ensure fast and dedicated access to the camera footage (especially if there are bandwidth limitations to the site) or to isolate a site in the case of an emergency.

To block the cameras, click the Block All Cameras on Site button and select a user or group of users from the user filter. If it is not necessary to block the whole site, consider blocking only a single camera or smaller selection of cameras. This may be done from the Camera List (see **Camera Detail**).

Use the Unblock All Cameras on Site button to unblock all blocked cameras on a site. This function may be used even if a single camera or a subset of cameras was blocked on the site.

ℹ **Blocking and unblocking of cameras is only available to users with the Block Camera privilege.**

Dragging and Dropping Sites

Dragging a Site Item

A site drag may be initiated from:

- A site item in the Site List
- The site name of a camera listed in the "Cameras Viewed by User" list on a User Detail Card (in a User List)
- A site in a Tour's detail (in a Tour List) - start the drag on the site name of a camera entry
- A site attached to a Task (Task detail card in the Task List)
- A site attached to an alarm (Alarm detail Card in the Alarm List)

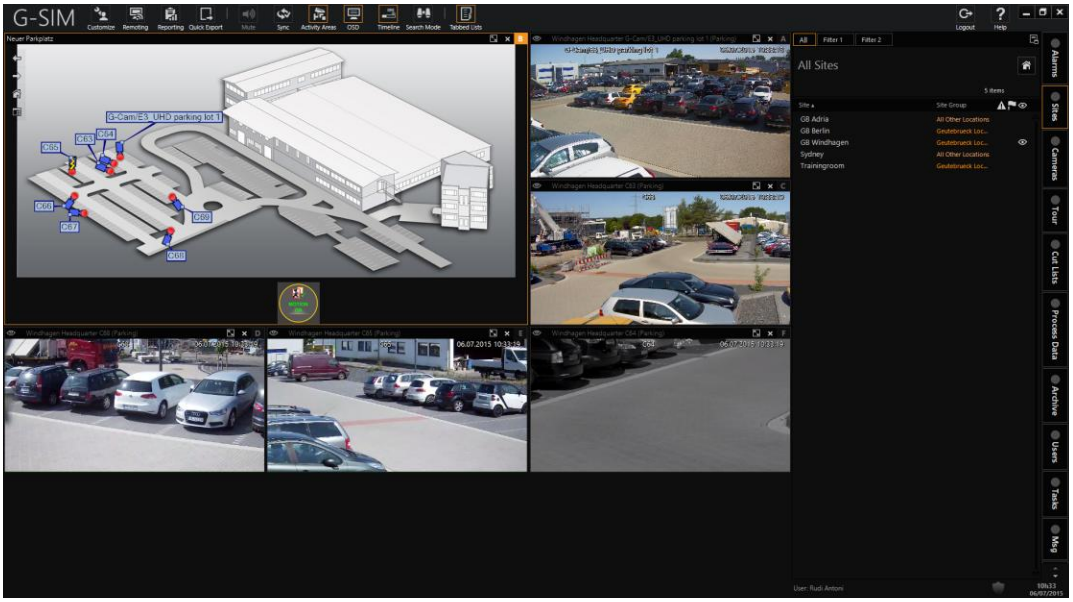
Dropping a Site Item

A site item may be dropped onto:

- An empty viewer to display a map of the site. If a map is not available, the top level map of the whole network will be displayed.
- A viewer already containing a map to replace it with a map of the dropped site.
- A viewer containing a camera (video stream) to replace it with a map.

- A Site List to select the dragged site and show its detail (if the list contains the site, i.e. not filtered).
- The Cameras Tab to switch to the Camera List and display a list of all cameras on the site.
- A Camera List (docked in a viewer) to filter the list and display all cameras on the site.
- The Tasks Tab to switch to the Task List, create a new task and link it to the site.
- A new Task Card in the Task List to link the site to the task.

Maps



All Sites

5 items

Site ▲	Site Group
GB Adria	All Other Locations
GB Berlin	Geutebrueck Loc...
GB Windhagen	Geutebrueck Loc...
Sydney	All Other Locations
Trainingroom	Geutebrueck Loc...

Maps are graphical representations of physical or logical groupings of sites and cameras, and are intended to streamline accessing cameras and receiving visual feedback on state changes of map objects. Maps give a visual context to sites and to cameras which would otherwise be very difficult to use.

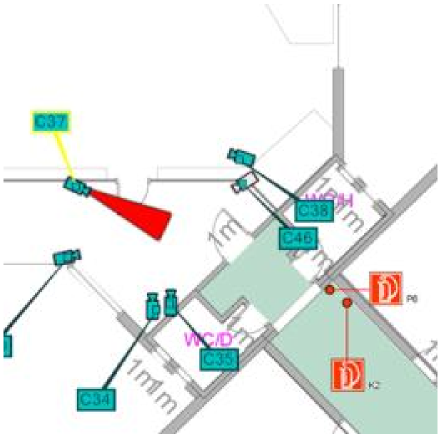
Installations are usually configured with an overview map of the video network which has links (called hotspots) to all the sites. These site maps may then again have links to detail maps or alternative map layouts. Cameras may be directly accessed from the map or from a camera list. Camera detail is also available from cameras on a map by right-clicking.

The same camera may appear on more than one map if it makes sense. At first this may seem strange, but only if you think of all maps as having the same function. It is useful to have different maps for different types of personnel. For example, building maintenance personnel require information on maps that security personnel don't need, and vice versa. Thus two very different maps of the same area could be made. Each would have the same cameras and building outline, for example, but that would be where the similarity ends.

A map of a site may be viewed, drilled into (to show detail for certain map areas), zoomed and panned. If a site is dropped on a map viewer, a map of the site will be displayed. If a camera (or alarm or task with a camera attached to it) is dropped on a map, the position of the camera will be displayed. If the current map does not contain the camera position, the correct map will be loaded.

Maps consist of a background image and objects which G-SIM places on these images. Map objects can represent more than just cameras. For example, a security keypad or a card reader could also be represented on the map. Anything that has a state which can change and is important to know about should be managed by G-SIM. Your administrator could have configured some state changes to be indicated as a colour change of the map object, say between normal and alarm state:

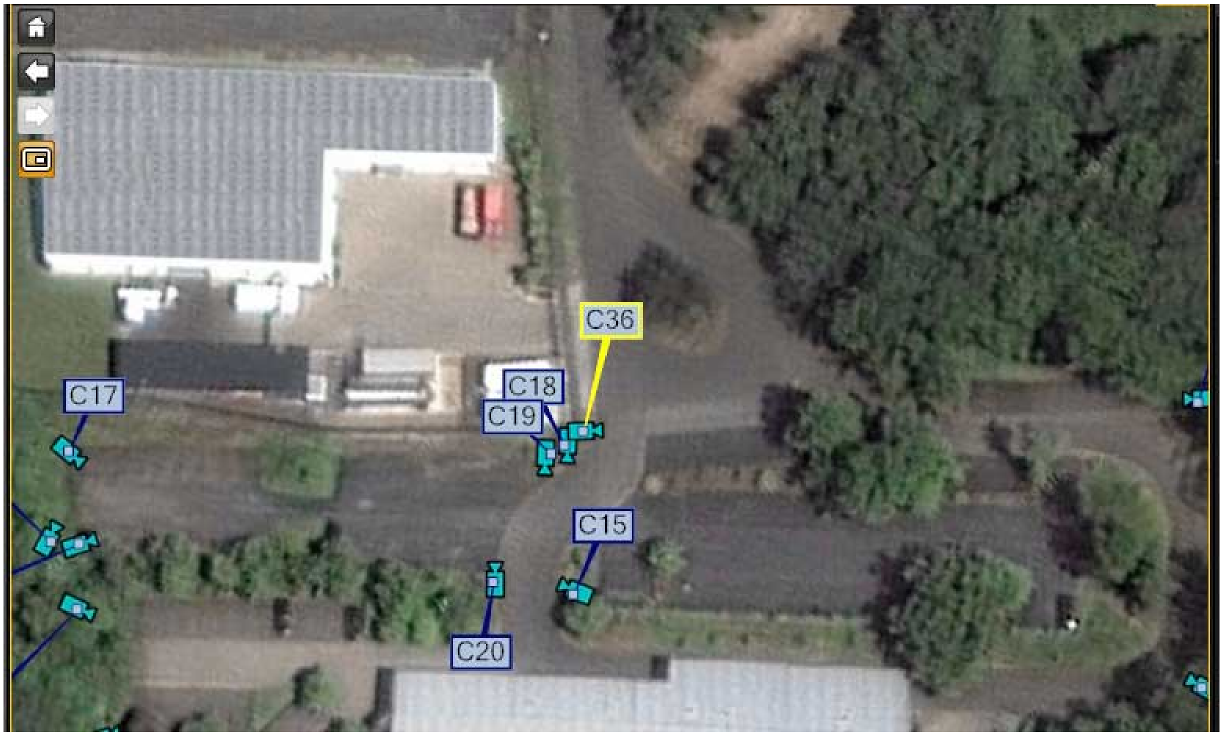
Some states are a bit more specialised (camera sync loss, battery low, etc.), and are best indicated by means of an icon. Your administrator may have configured such map object state symbols. Such symbols would then appear on the map as appropriate.



Mapping in G-SIM

Map functionality is only available to users with the View Site Map privilege.

Maps in G-SIM consist of a hierarchical set of linked images that cover the whole video network. A map may contain hotspots that enable the user to drill down to a detail level. A user may pan and zoom a map by using the mouse and mouse wheel. A "back" option allows you go back to a previous map. Cameras on a map have all the functionality of cameras in the camera list — right-clicking on a camera will display the same camera info card as in the Camera List. A camera may be dragged from a map to a viewer or any other drop position that will accept a camera. See **Cameras** for a detailed description of cameras.



The Overview Map (Home)

The main map is an overview of the entire video network, and will usually not contain any cameras, but only the relative position of sites (and site groups). Clicking a specific site will show the site detail. The main map may be accessed by clicking the Home button above the Site List.

Sites with active alarms will be displayed in red on the main map.

Viewing a Site Map

A site map may be displayed by

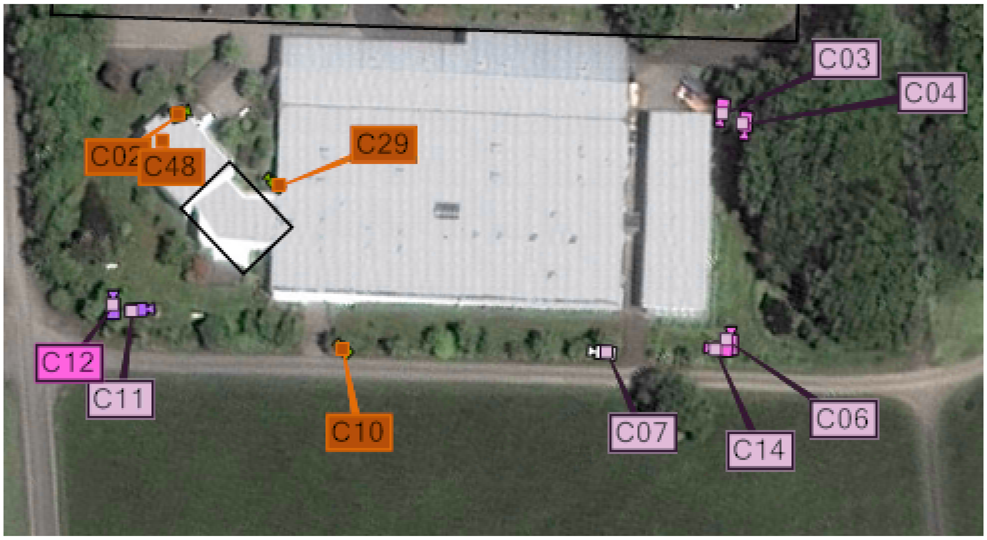
- Clicking on the site name on the main map. The main map will be replaced by a map of the site.
- Dragging a site item from any list to a viewer. In addition to from the Site List, Sites may also be dragged from the item list of a Tour.
- Using the Show on Map button on a Site, Camera, Alarm or Task detail card. This button allows you to display the overview map of the site in the viewer of your choice. The button may be used in three different ways: when you click the button all viewer windows will display their unique letter identifiers.

1. Press the corresponding key on the keyboard to place the map in that viewer.
2. Click with the mouse in the viewer.
3. Drag the button to the viewer where you want the map to be displayed.

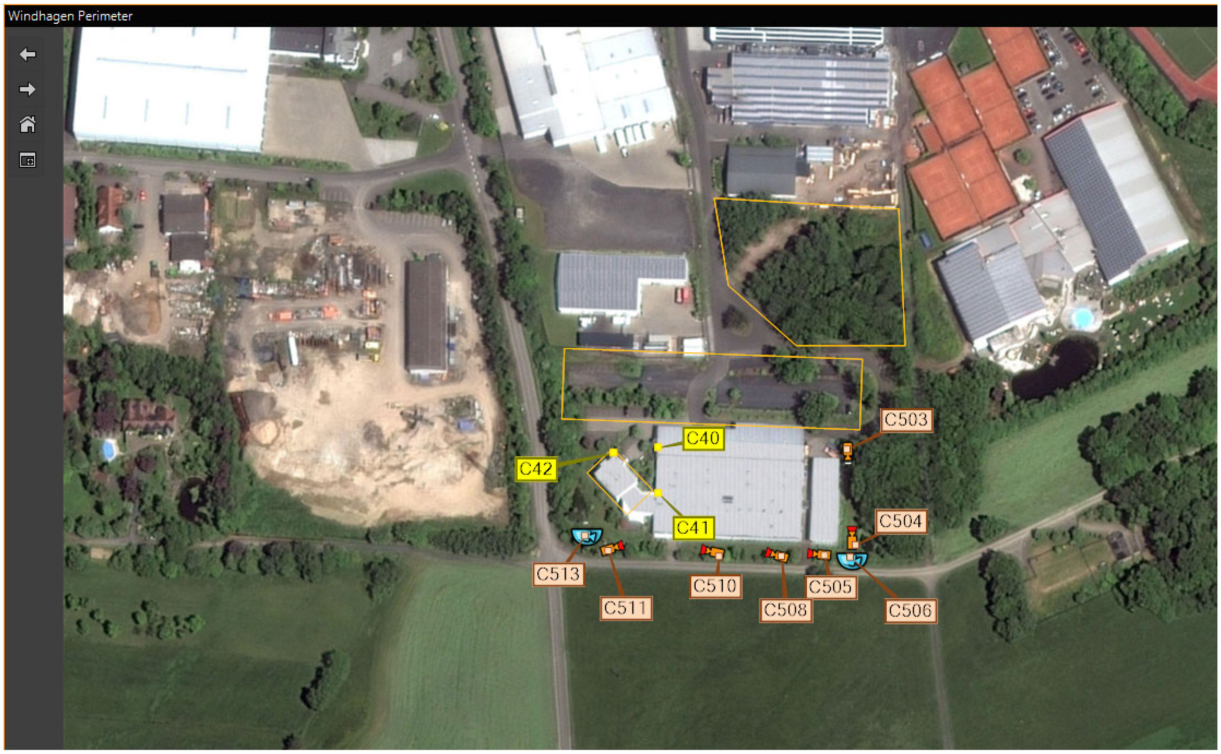
Map Symbols and Colors

Cameras are indicated on maps by a camera symbol and a call-out box containing the camera name. A camera may be in one of four camera states, each indicated by colors defined in the Management Console. The four cameras states are:

1. Normal state
2. Selected state
3. Alarm state (flashing state)
4. Offline state



Navigating Maps

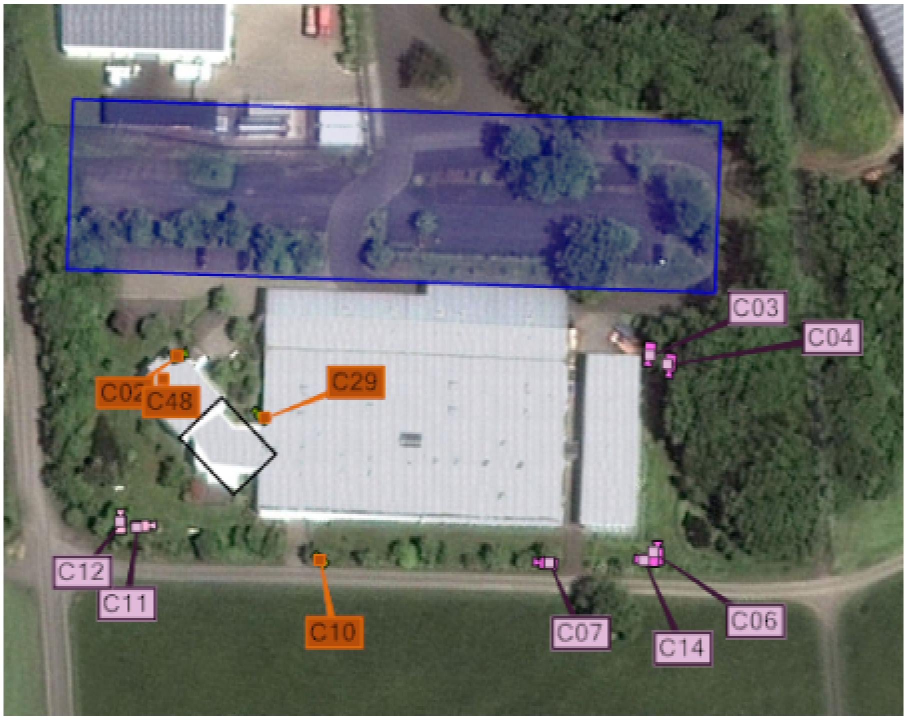


Mouse Cursors Used on Maps

Settings	Description
Default	The default mouse pointer is shown on maps when no selectable elements, such as hotspots or cameras, are present at that position. In this situation, hold the left mouse button to drag and pivot the map, if possible.
Selection	There is a selectable item at the current mouse position. If it is a hotspot (hotspot border highlighted), left click to display the detail map of the hotspot area. If it is a camera, the camera can be dragged onto a viewer, etc. Right click the camera to display the detail view of the camera.
Pivot	This pointer appears when the mouse is over a non-selectable map area and you hold the left mouse button (if the default mouse pointer was shown beforehand). If you move the mouse now, the map is pivoted. Note that maps can sometimes be pivoted in one direction only.
Going to the next level of detail	Maps can contain hotspot areas, which can be used to navigate to other maps or details of the current map. When you move the mouse over these hot spots, the border of the hotspots becomes highlighted. In addition, the "Select" cursor is displayed. Simply left click a hotspot to view the detailed map that is linked with this area.
Zooming and pivoting	You can zoom in and out of the maps using the mouse wheel. How far you can zoom is defined by the zoom limits. To pivot the map, hold the left mouse button and move the mouse. Before you press and hold the left mouse button, the default mouse pointer must be displayed. If this is not the case, you will select a map object or a hotspot (see the table above).

Drilling Down to View Detail

Maps may contain hot-spot areas which will navigate to other maps or detail of the current map. These hot-spots are indicated by a highlighted border when the mouse is moved over them. The mouse cursor will also change to the “Select” cursor when hovered above a hot-spot. Simply left-click a hot-spot to display the detail map linked to that region.



Zoom and Pan

A map may be zoomed by using the mouse wheel. Zoom limits will restrict zooming in and out. To pan, click the left mouse button and hold while moving the mouse. Make sure that the default arrow mouse cursor is displayed before clicking; otherwise your click will either select a map object or a hot-spot. (See the above table).

The Map Toolbar

The following buttons are available on the toolbar to the left of the map control:

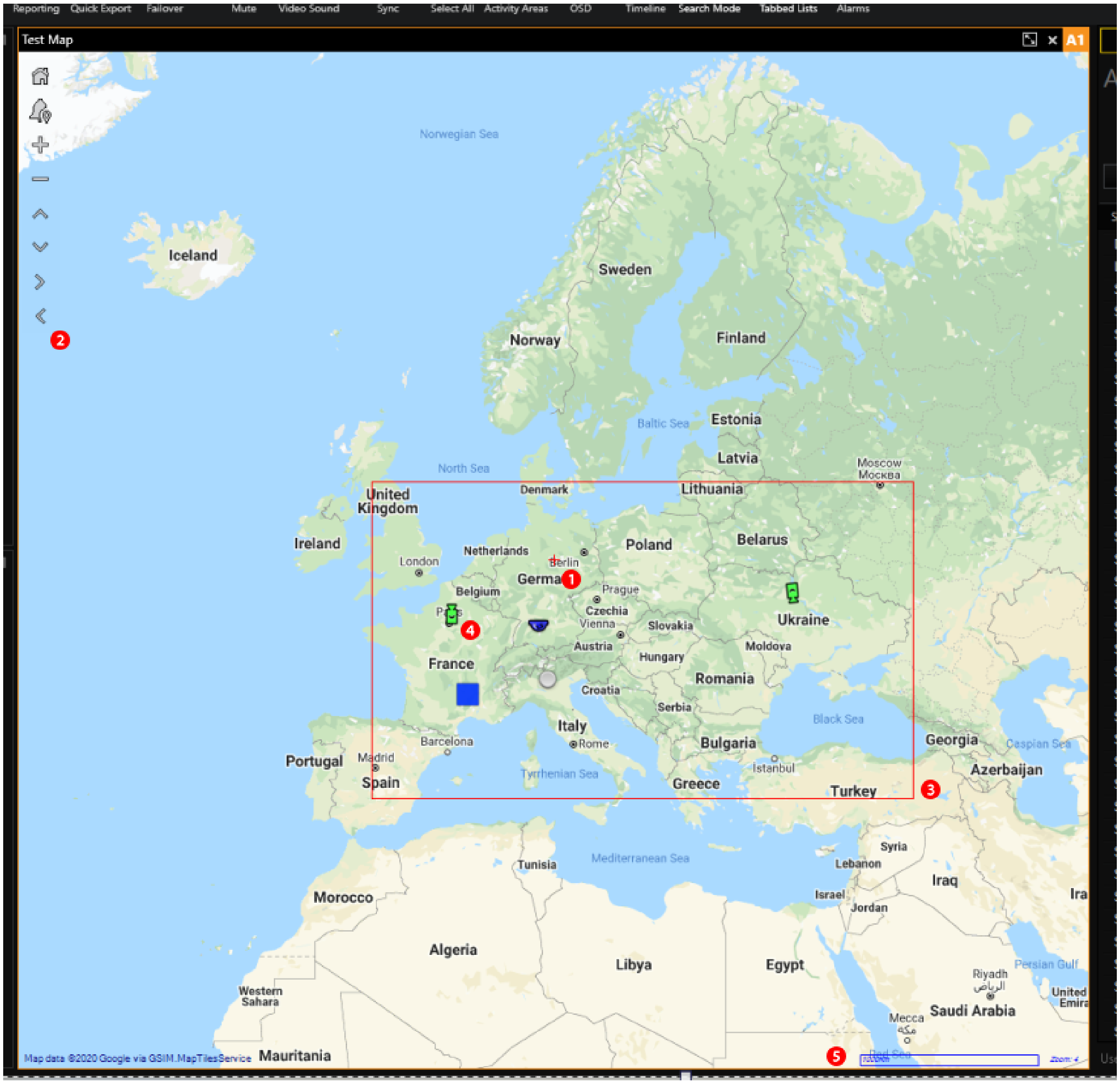
Button	Description
🏠	**Overview map (Home)**: The overview/main map of the video network is displayed. This is usually a map showing all sites and site groups.
←	**Back**: The previously displayed map is shown. You will typically use this button when you have gone to the next level of detail and now wish to return to the next highest level.
→	**Next**: The next previously displayed map is shown. This button is activated once the "Back" button is used. It makes it possible to

Button	Description
	move a step forward in the chronological order of the displayed maps.
▣	**Overview map position**: This option is used to specify the corner of the viewer in which the overview map will be displayed.

GIS Maps

On the GIS Map Control, the operator can see the following information:

- 1 Current map view center (small red cross marker)
- 2 Map Control Panel
- 3 Allowed map area (if any)
- 4 Map objects and their current states
- 5 Name of the map provider, scale and current zoom level



The Map Control Panel contains the following buttons:

Buttons	Explanation
Home	Centers map according to the map's starting point and applies the default zoom level.
Map Related Alarms	Shows the Map Related Alarms Control.

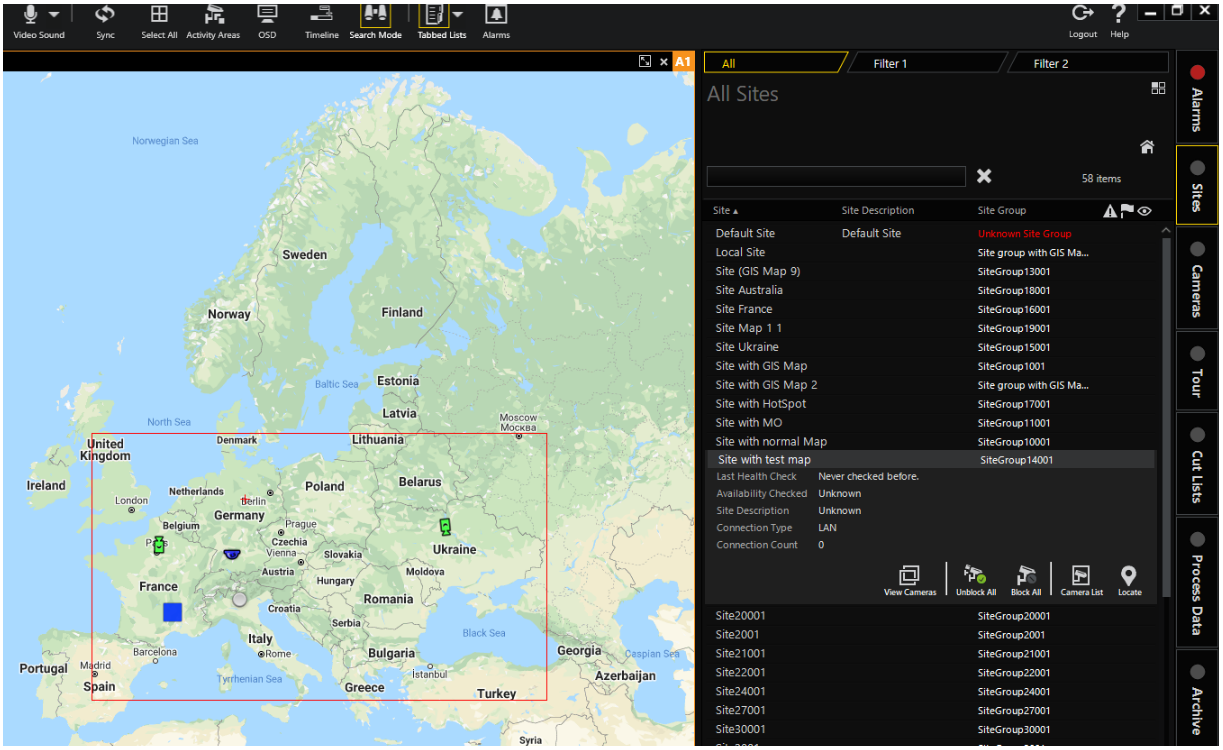
Buttons	Explanation
+/ − Zoom in/Zoom out	Increases/Decreases the current zoom level of the map. The current map zoom cannot be outside [Min Zoom scale, Max Zoom Scale] range.
∧/ ∨/ ›/ ‹ Move up/Down/Right/Left	Moves the current map view. If **Allowed Area** is set, the operator cannot move outside the **Allowed Area** rectangle.

Navigation on the GIS Map:

- Move the current map view by holding the left mouse button and moving the mouse. Alternatively, you can use the Move Up/ Down/Right/Left buttons on the Map Control Panel.
- To zoom in/zoom out the current map view, scroll the mouse wheel. The same can be done with the Zoom In/ Out buttons on the Map Control Panel.

Show GIS Map in Viewer

To show the GIS Map in the viewer, the operator can drag and drop a Site with a linked map to the viewer.



All Sites

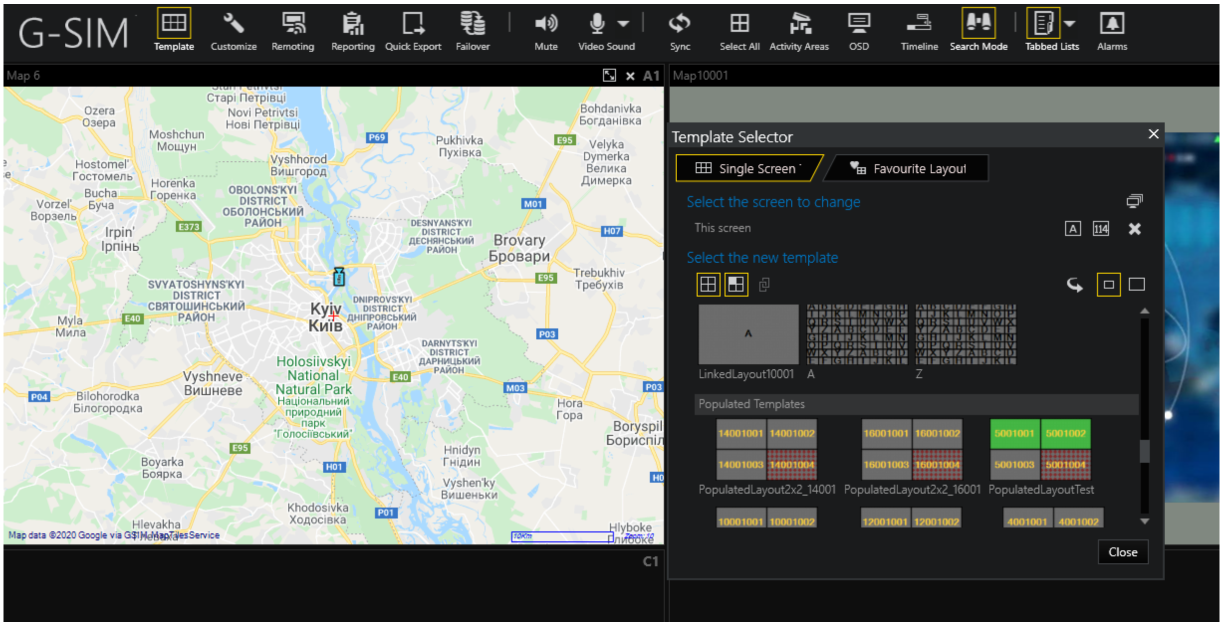
58 items

Site ▴	Site Description	Site Group
Default Site	Default Site	Unknown Site Group
Local Site		Site group with GIS Ma...
Site (GIS Map 9)		SiteGroup13001
Site Australia		SiteGroup18001
Site France		SiteGroup16001
Site Map 1 1		SiteGroup19001
Site Ukraine		SiteGroup15001
Site with GIS Map		SiteGroup1001
Site with GIS Map 2		Site group with GIS Ma...
Site with HotSpot		SiteGroup17001
Site with MO		SiteGroup11001
Site with normal Map		SiteGroup10001
Site with test map		SiteGroup14001
Site20001		SiteGroup20001
Site2001		SiteGroup2001
Site21001		SiteGroup21001
Site22001		SiteGroup22001
Site24001		SiteGroup24001
Site27001		SiteGroup27001
Site30001		SiteGroup30001

Last Health Check: Never checked before.
Availability Checked: Unknown
Site Description: Unknown
Connection Type: LAN
Connection Count: 0

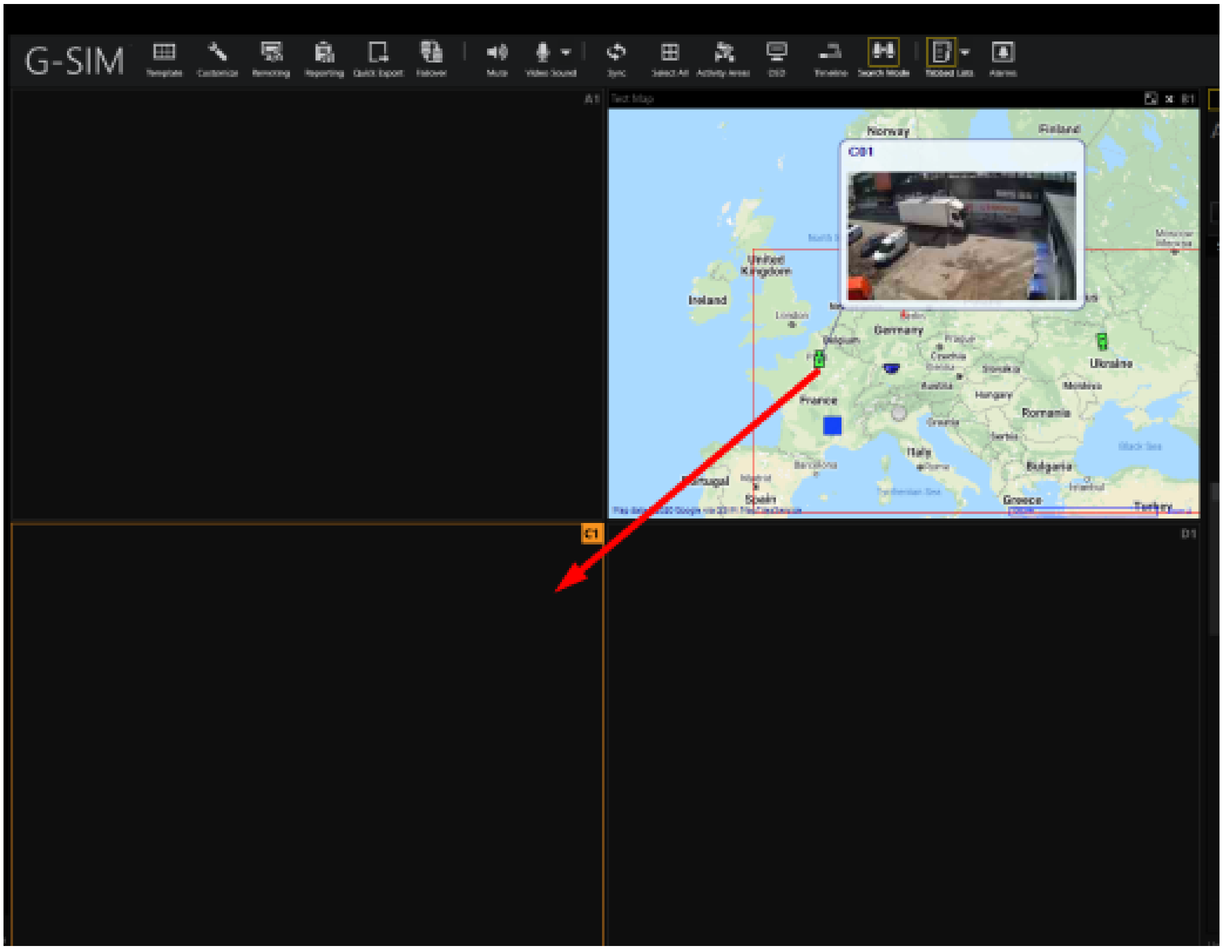
If the viewer is restricted to only showing maps, the operator can drag and drop the camera. In this case the camera's site linked map will be shown in the viewer.

The operator can select **Populated/Linked Layout** that contains the GIS Map.

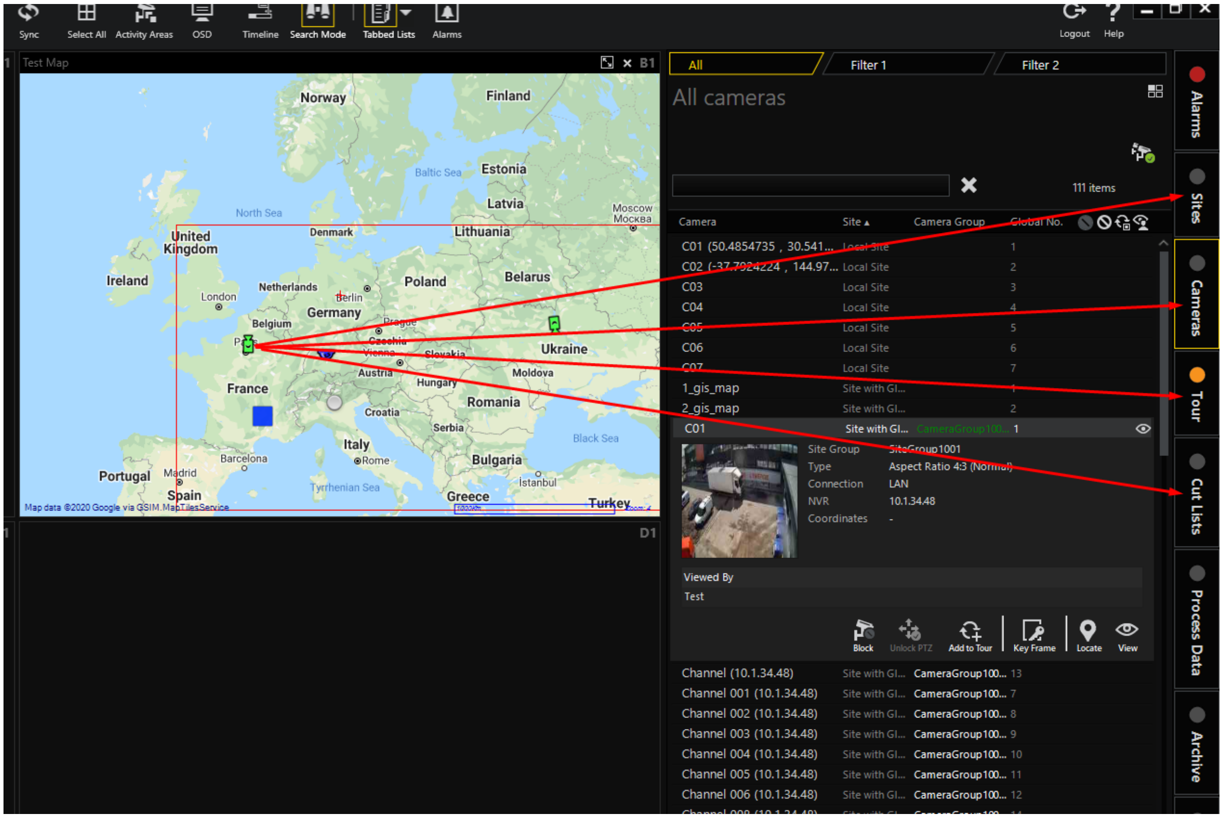


Drag & Drop Camera Map Object from GIS Map

The operator can drag and drop the Camera Map Object from the GIS Map to the viewer. The camera stream will be shown.



The operator can drag and drop the Camera Map Object from the GIS Map to the tabbed lists.



Camera	Site ▲	Camera Group	Global No.
C01 (50.4854735 , 30.541...	Local Site		1
C02 (-37.7924224 , 144.97...	Local Site		2
C03	Local Site		3
C04	Local Site		4
C05	Local Site		5
C06	Local Site		6
C07	Local Site		7
1_gis_map	Site with Gl...		1
2_gis_map	Site with Gl...		2
C01	Site with Gl...	CameraGroup100...	1

Site Group	SiteGroup1001
Type	Aspect Ratio 4:3 (Normal)
Connection	LAN
NVR	10.1.34.48
Coordinates	-

Viewed By

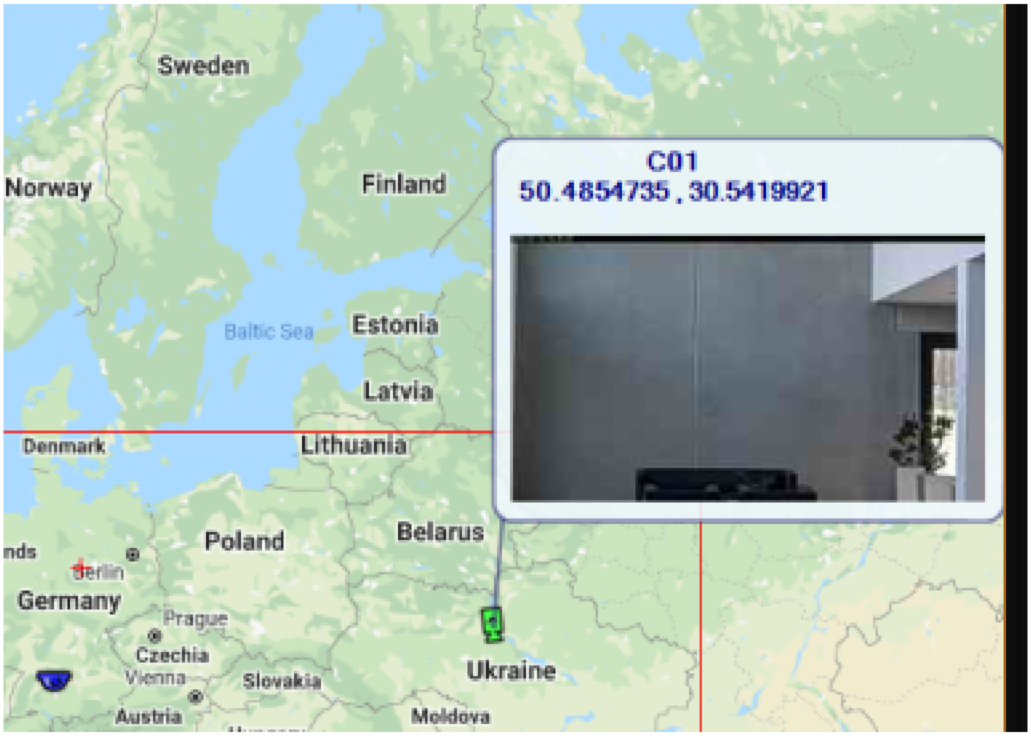
Test

Camera	Site ▲	Camera Group	Global No.
Channel (10.1.34.48)	Site with Gl...	CameraGroup100...	13
Channel 001 (10.1.34.48)	Site with Gl...	CameraGroup100...	7
Channel 002 (10.1.34.48)	Site with Gl...	CameraGroup100...	8
Channel 003 (10.1.34.48)	Site with Gl...	CameraGroup100...	9
Channel 004 (10.1.34.48)	Site with Gl...	CameraGroup100...	10
Channel 005 (10.1.34.48)	Site with Gl...	CameraGroup100...	11
Channel 006 (10.1.34.48)	Site with Gl...	CameraGroup100...	12

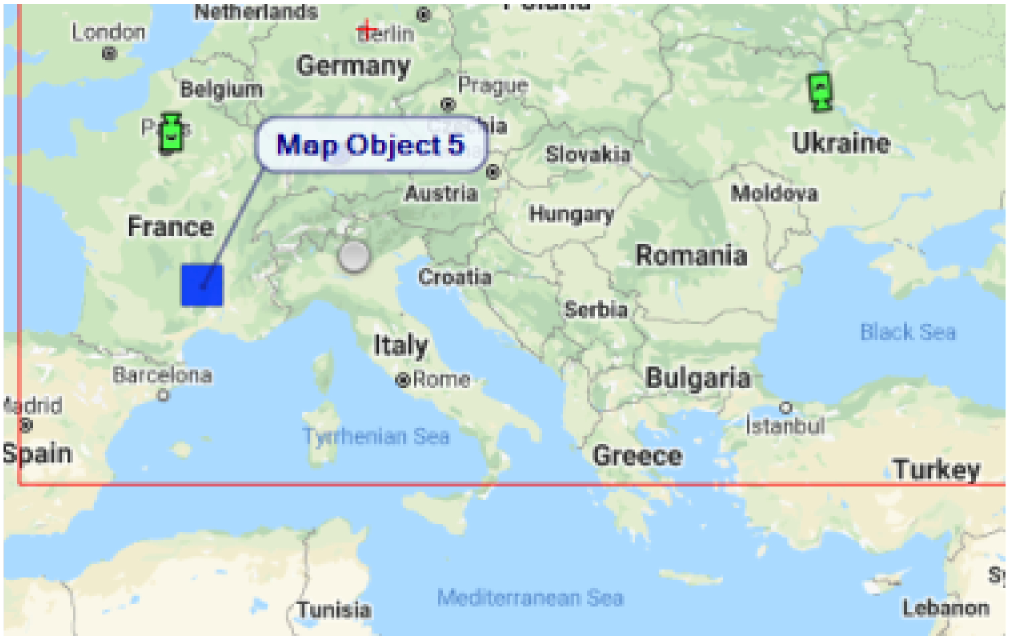
Buttons	Explanation
Sites tab	The camera's site card will be opened.
Cameras tab	The camera's card will be opened.
Tour tab	The camera will be added to the newly created Guard Tour.
Cut Lists tab	If the newly created Cut List exists, the camera will be added to this Cut List. Otherwise a new Cut List with camera will be created.

GIS Map Object Tooltip

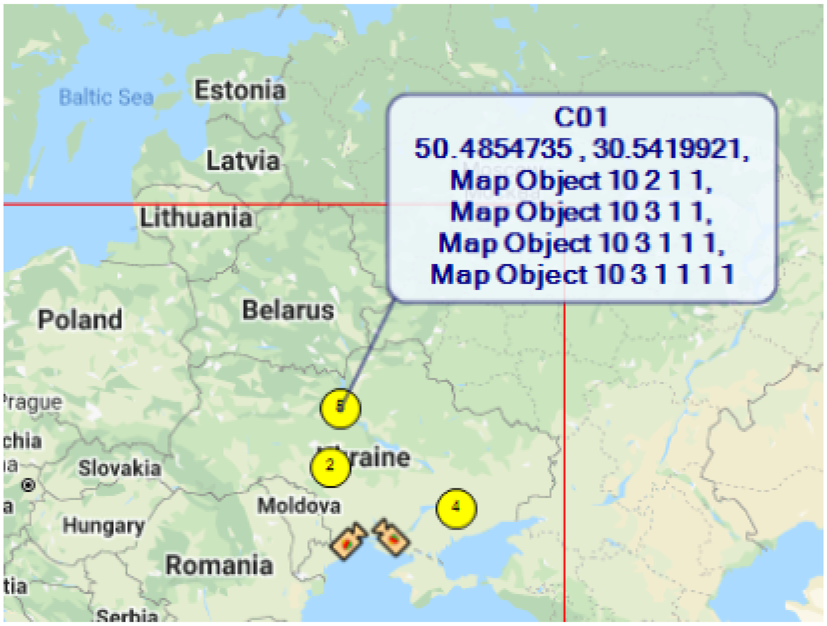
If the trigger type of the Map Object Type is **Camera**, the tooltip text is formatted due to the **Display Name Map** camera setting. If existing, a camera thumbnail image is also shown on the tooltip.



If the trigger type of the Map Object Type is **Alarm**, **AlarmInstance**, **SystemComponent** or **None**, the Map Object name is shown on the tooltip.



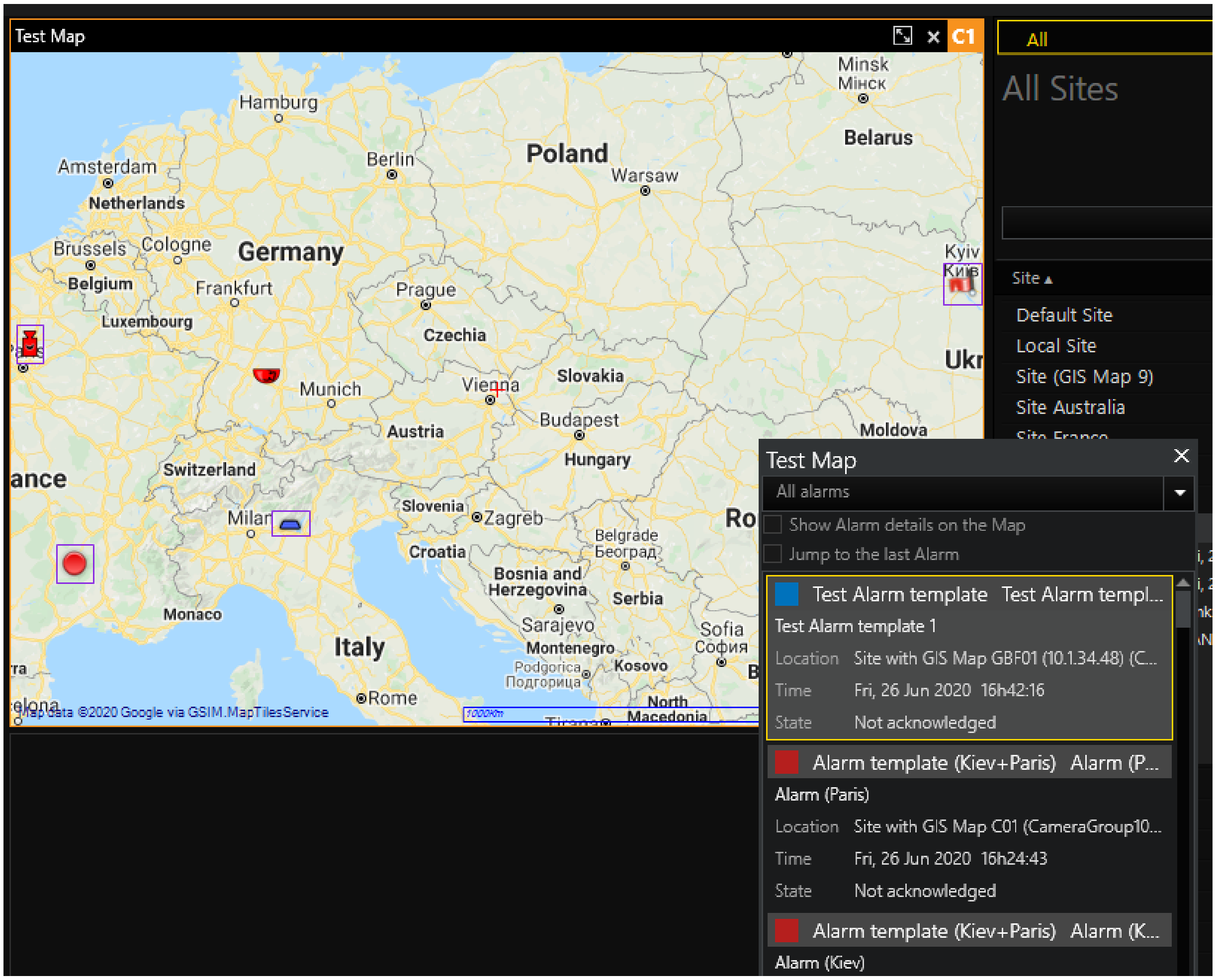
If Map Objects are merged to the Map Objects Cluster, the names of the Map Objects that are in the Cluster are shown on the tooltip.



C01
50.4854735 , 30.5419921,
Map Object 10 2 1 1,
Map Object 10 3 1 1,
Map Object 10 3 1 1 1,
Map Object 10 3 1 1 1 1

GIS Map Objects States

As well as Map Objects on the Regular Map, Map Objects on the GIS Map change their image according to the Map Object states. Image flashing is used to show the Alarm state of the GIS Map Object.



Test Map

All alarms

□ Show Alarm details on the Map

□ Jump to the last Alarm

🟦 Test Alarm template   Test Alarm templ...
Test Alarm template 1
Location   Site with GIS Map GBF01 (10.1.34.48) (C...
Time   Fri, 26 Jun 2020 16h42:16
State   Not acknowledged

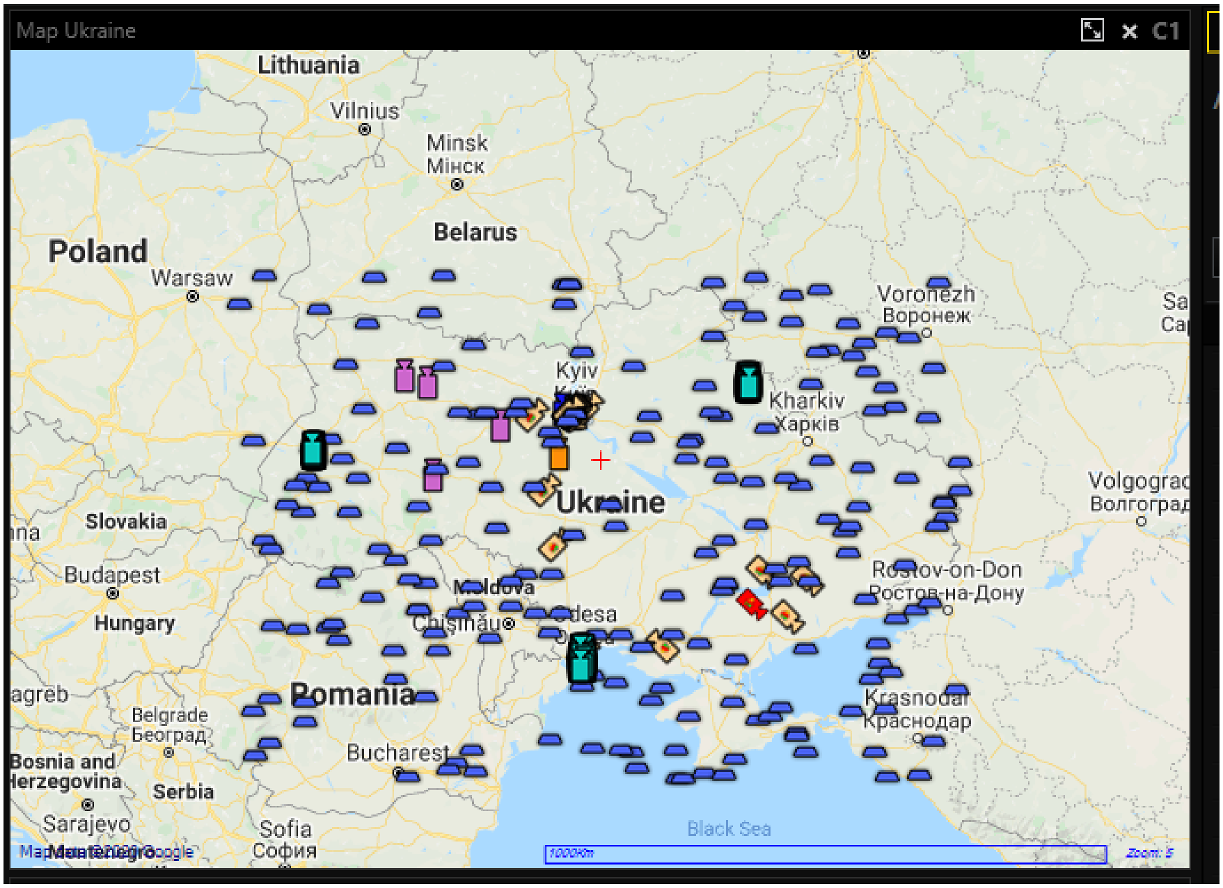
🟥 Alarm template (Kiev+Paris)   Alarm (P...
Alarm (Paris)
Location   Site with GIS Map C01 (CameraGroup10...
Time   Fri, 26 Jun 2020 16h24:43
State   Not acknowledged

🟥 Alarm template (Kiev+Paris)   Alarm (K...
Alarm (Kiev)

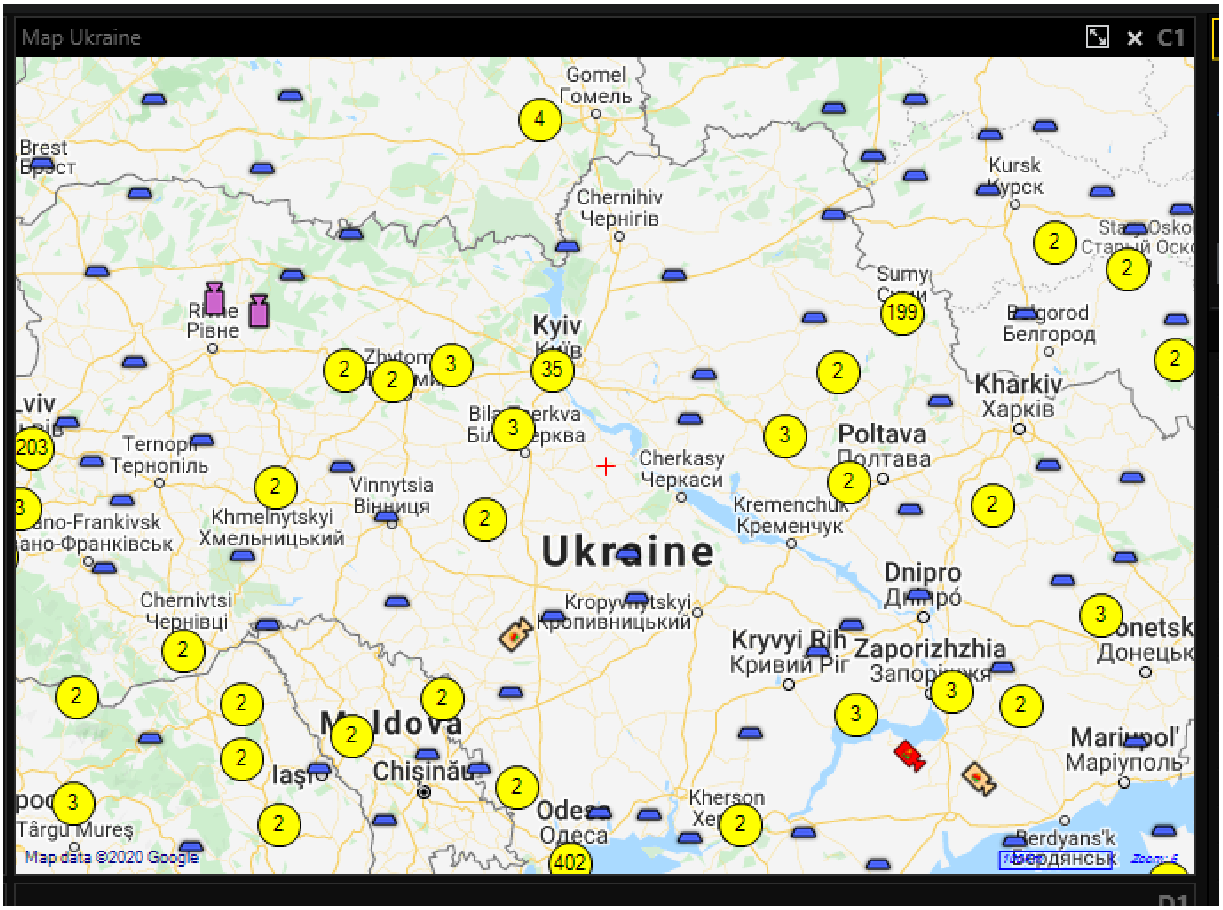
Map Objects **Additional State** settings are not supported for the GIS Maps.

GIS Map Objects Clustering

If GIS Map has a lot of Map Objects in specific region, then on the small Zoom levels Map Objects can overlap each other.



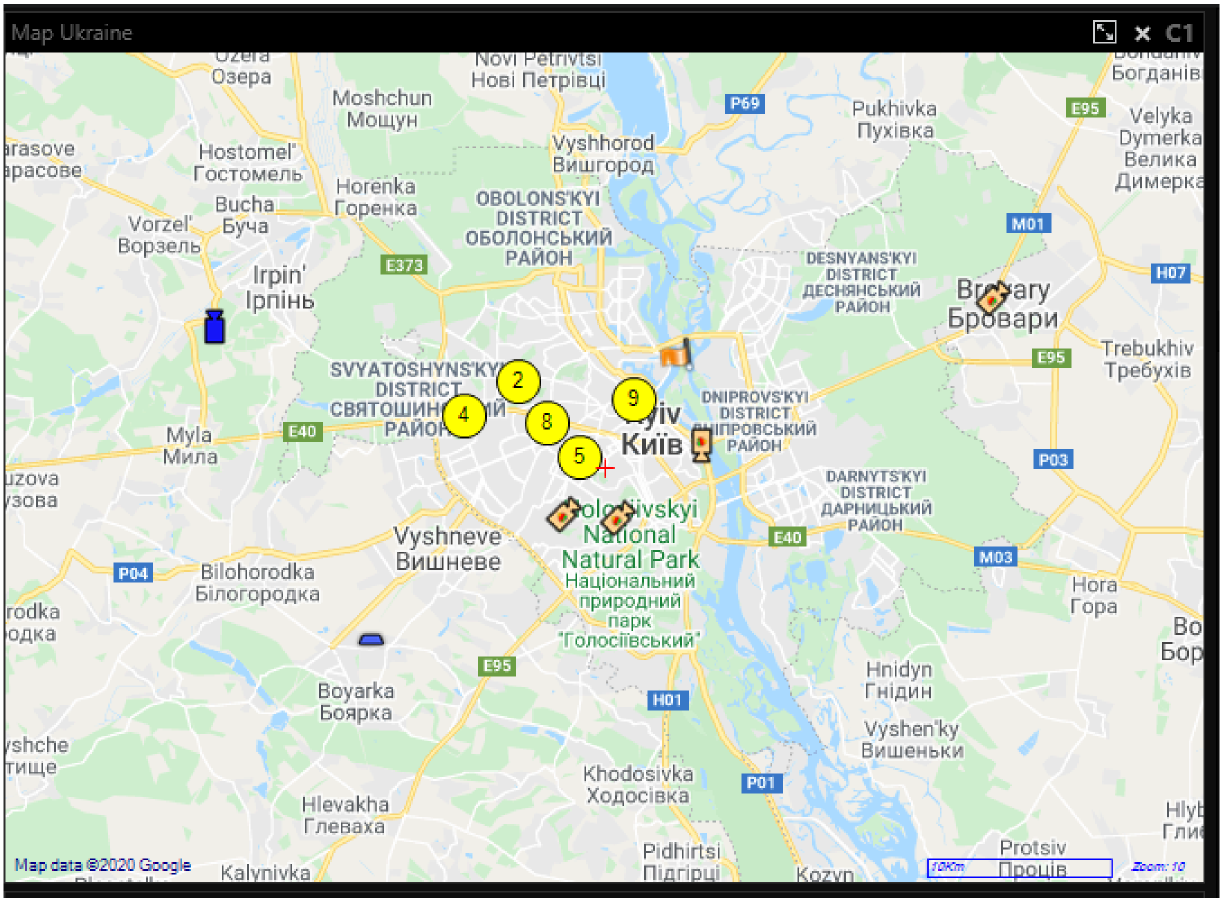
To avoid Map Objects overlapping, Administrator can enable **Map Objects clustering** setting for the specific GIS Map. In this case neighbour Map Objects will be merged to the Map Objects Clusters.



Map Objects Cluster use **Map Objects Cluster Color / Map Objects Cluster Alarm Color** System Settings for the visualization. If **Use individual icon size** GIS Map setting is enabled , then Map Objects Cluster use **Icon size** for the visualization, otherwise **Map Objects icon size** System Setting is used.

On the Map Objects Cluster Icon User can see the number of the Map Objects that are included in this Cluster. Map Objects Cluster’s tooltip contains names of the Map Objects that are included in this Cluster.

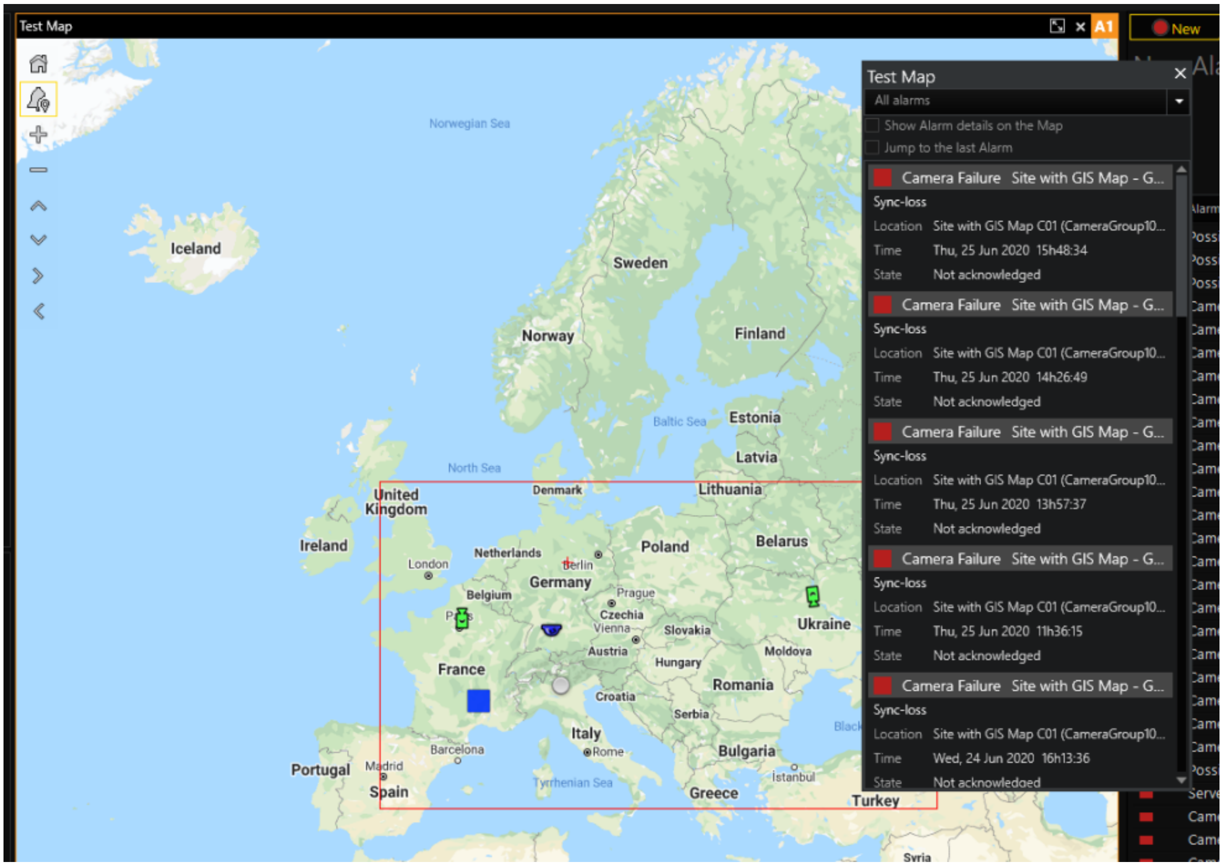
User can click on the Map Objects Cluster to zoom GIS Map to show cluster’s Map Objects. Sometimes is not possible to show all cluster’s Map Objects in one view, in that case smaller Map Objects Clusters will be shown.



Map Objects Clustering is performed whenever User changes current map view (move /zoom map).

GIS Map Related Alarms Control

The operator can click **Map Related Alarms** ( ) to show the **Map Related Alarms Control** window.



Test Map

All alarms

□ Show Alarm details on the Map

□ Jump to the last Alarm

Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...
Time Thu, 25 Jun 2020 15h48:34
State Not acknowledged

Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...
Time Thu, 25 Jun 2020 14h26:49
State Not acknowledged

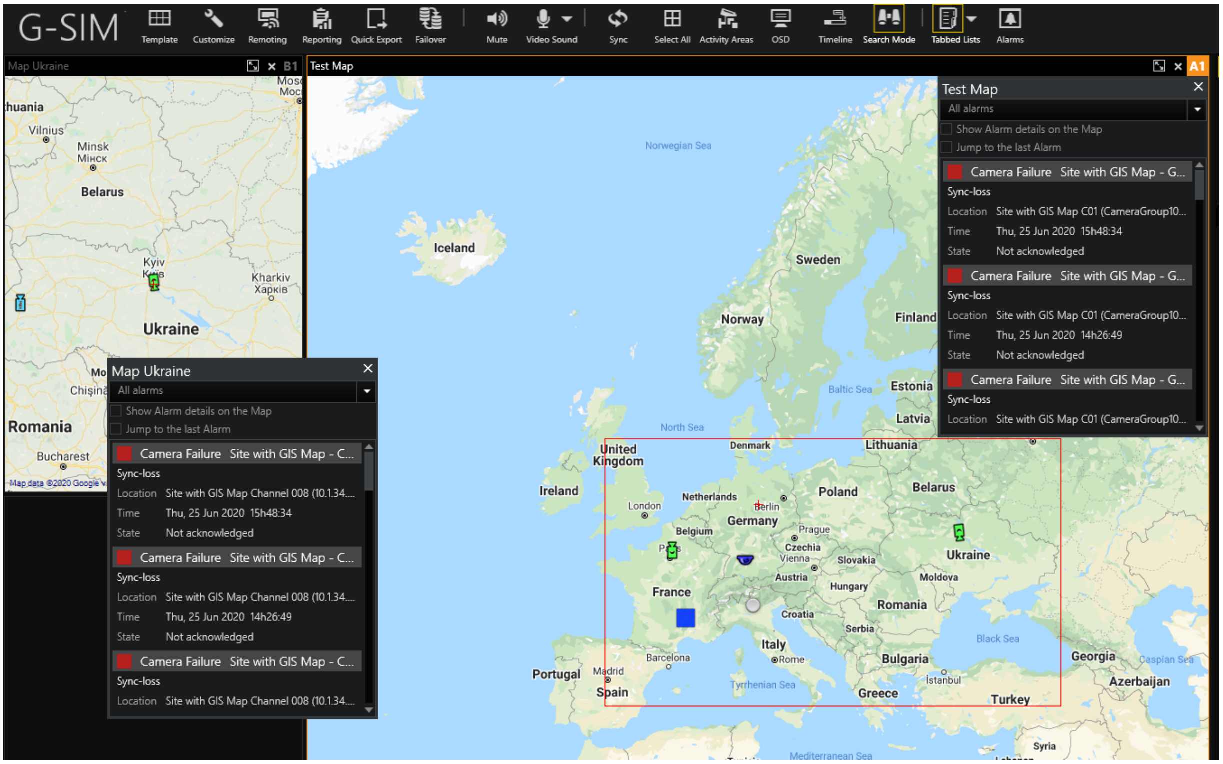
Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...
Time Thu, 25 Jun 2020 13h57:37
State Not acknowledged

Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...
Time Thu, 25 Jun 2020 11h36:15
State Not acknowledged

Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...
Time Wed, 24 Jun 2020 16h13:36
State Not acknowledged

A second click on **Map Related Alarms** ( ) will close the **Map Related Alarms Control** window. The operator can move the **Map Related Alarms Control** window to any accepted place (the map cannot be overlapped).

Every GIS Map has its own Map Related Alarms Control.



Map Ukraine

All alarms

□ Show Alarm details on the Map

□ Jump to the last Alarm

🟥 Camera Failure Site with GIS Map - C...
Sync-loss
Location Site with GIS Map Channel 008 (10.1.34....
Time Thu, 25 Jun 2020 15h48:34
State Not acknowledged

🟥 Camera Failure Site with GIS Map - C...
Sync-loss
Location Site with GIS Map Channel 008 (10.1.34....
Time Thu, 25 Jun 2020 14h26:49
State Not acknowledged

🟥 Camera Failure Site with GIS Map - C...
Sync-loss
Location Site with GIS Map Channel 008 (10.1.34....

Test Map

All alarms

□ Show Alarm details on the Map

□ Jump to the last Alarm

🟥 Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...
Time Thu, 25 Jun 2020 15h48:34
State Not acknowledged

🟥 Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...
Time Thu, 25 Jun 2020 14h26:49
State Not acknowledged

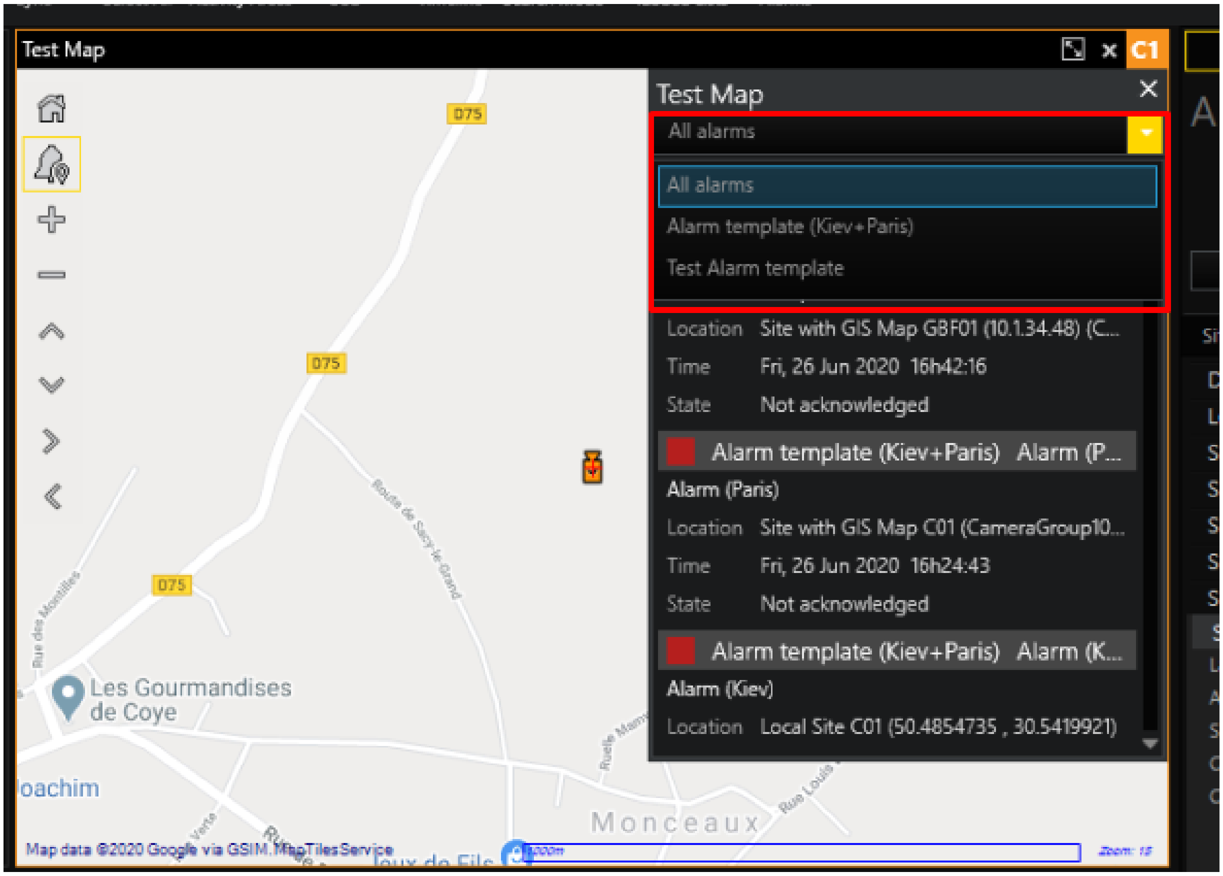
🟥 Camera Failure Site with GIS Map - G...
Sync-loss
Location Site with GIS Map C01 (CameraGroup10...

The Map Related Alarms Control contains the following non completed Camera/System Component alarms:

- Alarm Template is linked to the Map Object that is added on the GIS Map
- Alarm Instance is linked to the Map Object that is added on the GIS Map
- Primary Device of the Alarm Instance is linked to the Map Object that is added on the GIS Map
- Any Camera from the Alarm Instance Cameras is linked to the Map Object that is added on the GIS Map

Whenever a new Map Related Alarm is received by the Operator Console, it will appear on the top of the Map Related Alarms Control list.

The operator can choose which Alarm Types to see in the Map Related Alarms Control.

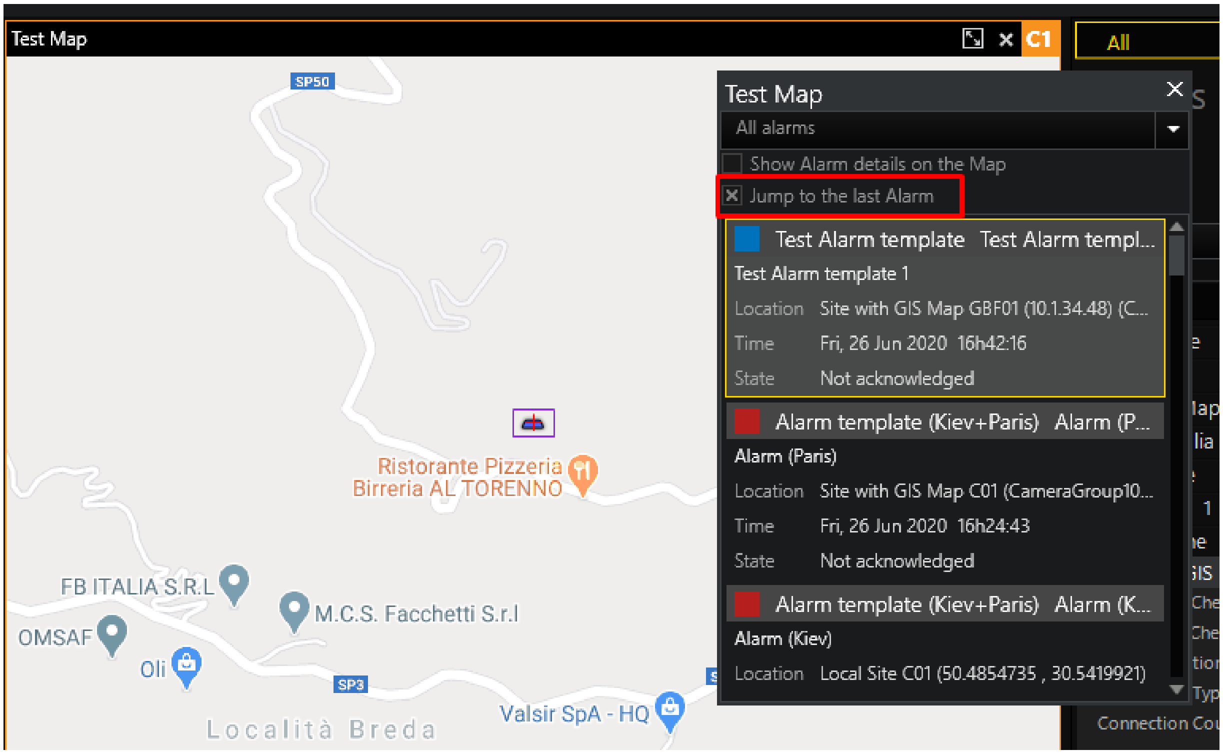


Location Site with GIS Map GBF01 (10.1.34.48) (C...
Time Fri, 26 Jun 2020 16h42:16
State Not acknowledged

🟥 Alarm template (Kiev+Paris) Alarm (P...
Alarm (Paris)
Location Site with GIS Map C01 (CameraGroup10...
Time Fri, 26 Jun 2020 16h24:43
State Not acknowledged

🟥 Alarm template (Kiev+Paris) Alarm (K...
Alarm (Kiev)
Location Local Site C01 (50.4854735 , 30.5419921)

The operator can check the **Jump to the last Alarm** check box. In this case whenever a new Map Related Alarm is received by the Operator Console, it will be selected automatically.



Test Map

All alarms

☐ Show Alarm details on the Map

☒ Jump to the last Alarm

🟦 Test Alarm template Test Alarm templ...
Test Alarm template 1

Location	Site with GIS Map GBF01 (10.1.34.48) (C...
Time	Fri, 26 Jun 2020 16h42:16
State	Not acknowledged

🟥 Alarm template (Kiev+Paris) Alarm (P...
Alarm (Paris)

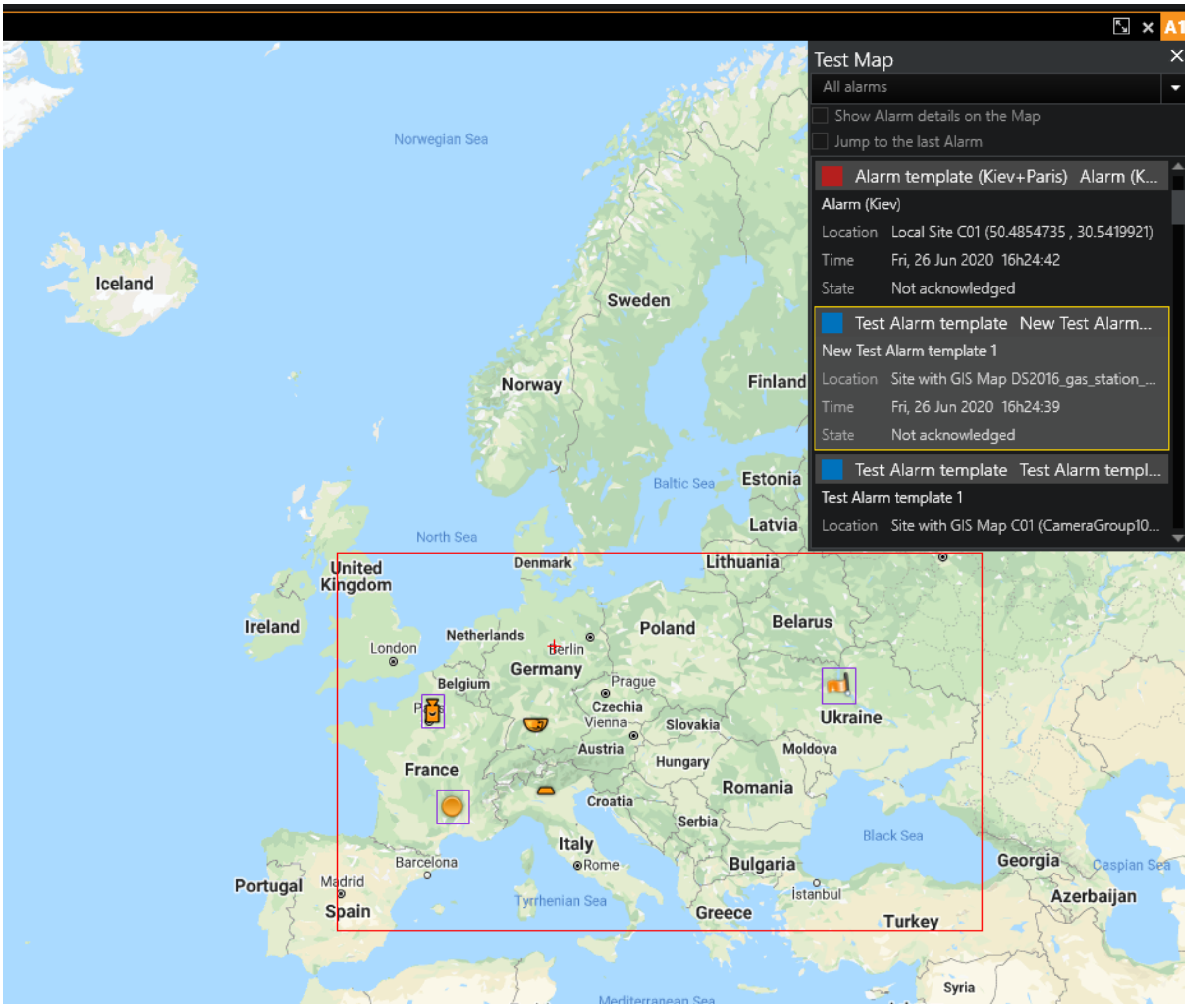
Location	Site with GIS Map C01 (CameraGroup10...
Time	Fri, 26 Jun 2020 16h24:43
State	Not acknowledged

🟥 Alarm template (Kiev+Paris) Alarm (K...
Alarm (Kiev)

Location	Local Site C01 (50.4854735 , 30.5419921)

When an alarm in the Map Related Alarms Control is selected, the following actions will be performed:

All Alarm Related Map Objects will be marked with a purple frame:



Test Map

All alarms

□ Show Alarm details on the Map

□ Jump to the last Alarm

🟥 Alarm template (Kiev+Paris)   Alarm (K...

Alarm (Kiev)

Location   Local Site C01 (50.4854735 , 30.5419921)

Time   Fri, 26 Jun 2020 16h24:42

State   Not acknowledged

🟦 Test Alarm template   New Test Alarm...

New Test Alarm template 1

Location   Site with GIS Map DS2016_gas_station_...

Time   Fri, 26 Jun 2020 16h24:39

State   Not acknowledged

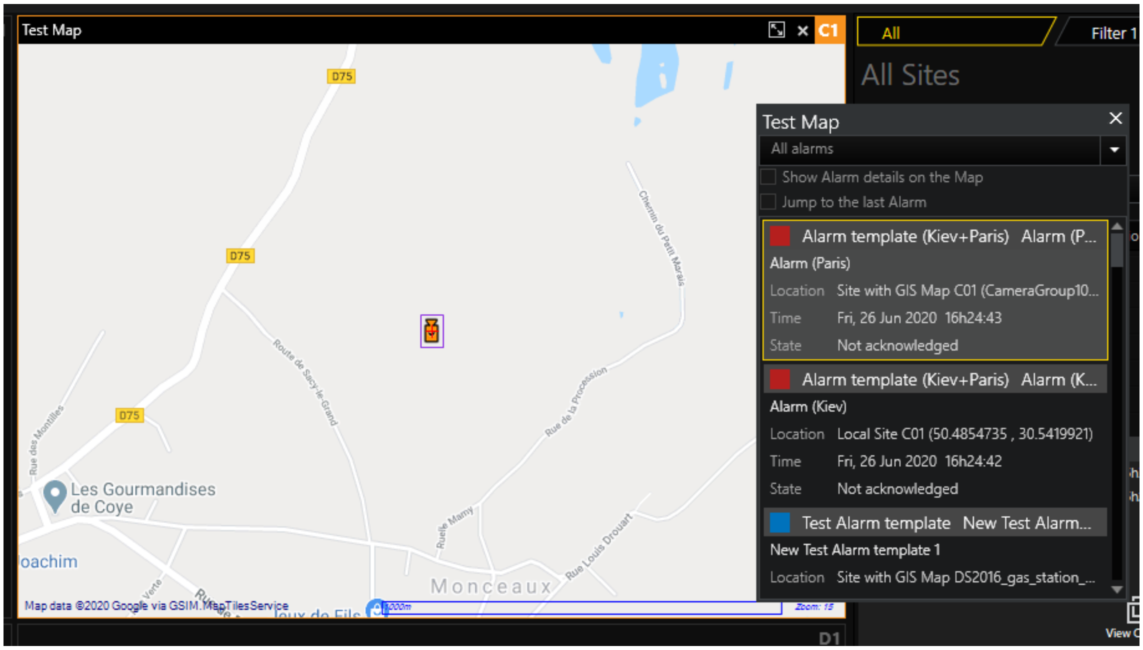
🟦 Test Alarm template   Test Alarm templ...

Test Alarm template 1

Location   Site with GIS Map C01 (CameraGroup10...

The map will be centered and zoomed according to the following rules:

- If the GIS Map contains a Map Object that is linked to the Alarm Primary Camera, the GIS Map will be centered to this Map Object and the Max. Zoom level will be applied.



Test Map

All alarms

□ Show Alarm details on the Map

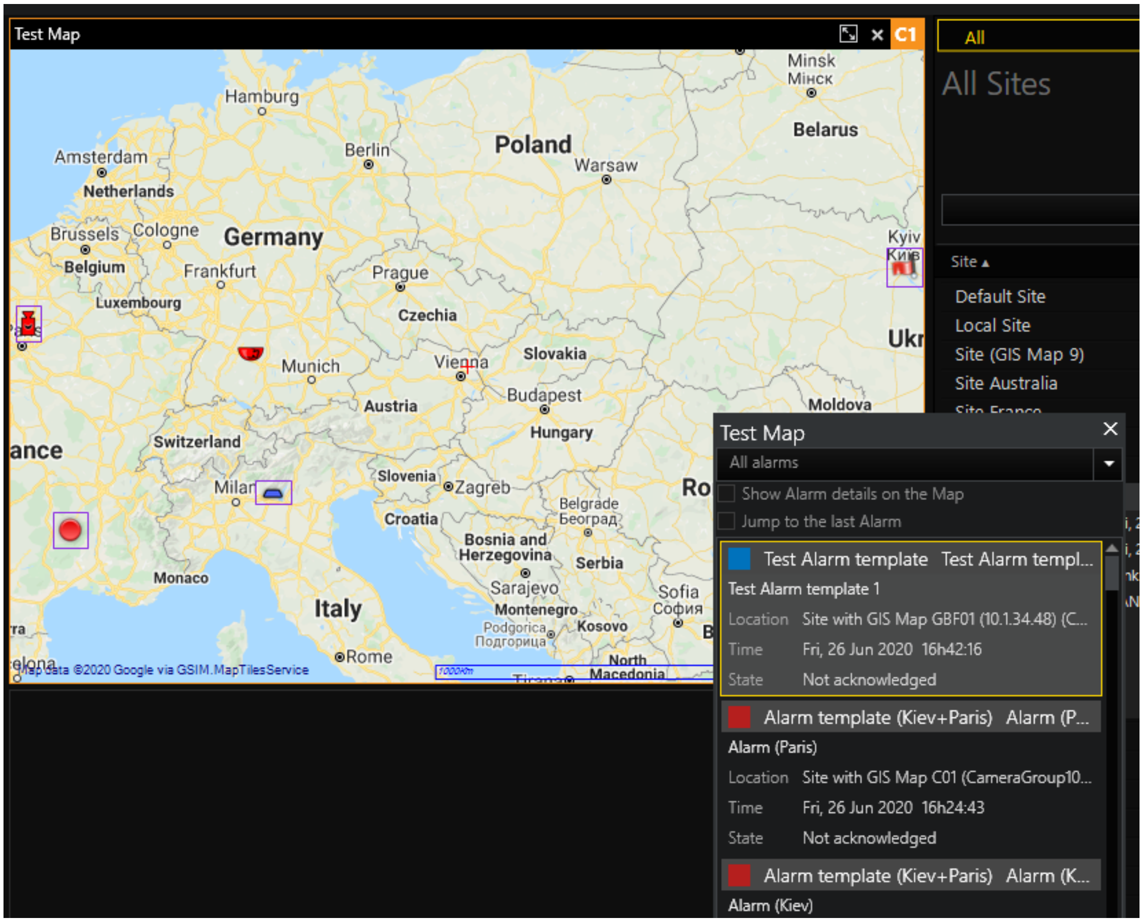
□ Jump to the last Alarm

🟥 Alarm template (Kiev+Paris) Alarm (P...
Alarm (Paris)
Location Site with GIS Map C01 (CameraGroup10...
Time Fri, 26 Jun 2020 16h24:43
State Not acknowledged

🟥 Alarm template (Kiev+Paris) Alarm (K...
Alarm (Kiev)
Location Local Site C01 (50.4854735 , 30.5419921)
Time Fri, 26 Jun 2020 16h24:42
State Not acknowledged

🟦 Test Alarm template New Test Alarm...
New Test Alarm template 1
Location Site with GIS Map DS2016_gas_station_...

- If the GIS Map contains a Map Object that is linked to the Alarm Instance, the GIS Map will be centered to this Map Object and the Max .Zoom level will be applied.
- If the GIS Map contains a Map Object that is linked to the Alarm Type, the GIS Map will be centered to this Map Object and the Max .Zoom level will be applied.
- If the GIS Map contains a Map Object that is linked to the Alarm Primary Device, the GIS Map will be centered to this Map Object and the Max. Zoom level will be applied.
- If the GIS Map contains Map Objects that are linked to the Alarm Cameras, the GIS Map will be centered and zoomed to the rectangle that contains all of these Map Objects.



Test Map

All alarms

□ Show Alarm details on the Map

□ Jump to the last Alarm

🟦 Test Alarm template Test Alarm templ...

Test Alarm template 1

Location	Site with GIS Map GBF01 (10.1.34.48) (C...
Time	Fri, 26 Jun 2020 16h42:16
State	Not acknowledged

🟥 Alarm template (Kiev+Paris) Alarm (P...

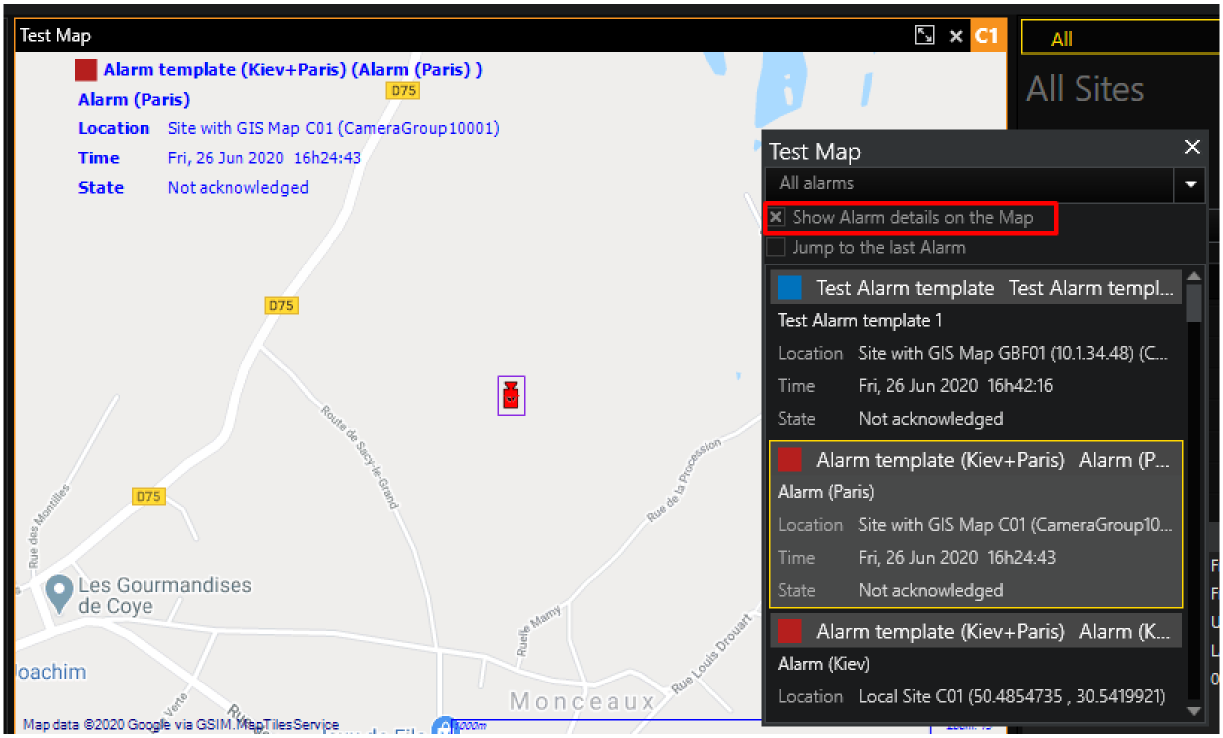
Alarm (Paris)

Location	Site with GIS Map C01 (CameraGroup10...
Time	Fri, 26 Jun 2020 16h24:43
State	Not acknowledged

🟥 Alarm template (Kiev+Paris) Alarm (K...

Alarm (Kiev)

The operator can check the **Show Alarm details on the Map** check box to show **Alarm Severity**, **Name**, **Location**, **Time** and **State** information on the upper left corner of the GIS Map Control.



Test Map

🟥 **Alarm template (Kiev+Paris) (Alarm (Paris))**

Alarm (Paris)	
Location	Site with GIS Map C01 (CameraGroup10001)
Time	Fri, 26 Jun 2020 16h24:43
State	Not acknowledged

Test Map

All alarms

☒ Show Alarm details on the Map

□ Jump to the last Alarm

🟦 Test Alarm template   Test Alarm templ...

Test Alarm template 1	
Location	Site with GIS Map GBF01 (10.1.34.48) (C...
Time	Fri, 26 Jun 2020 16h42:16
State	Not acknowledged

🟥 Alarm template (Kiev+Paris)   Alarm (P...

Alarm (Paris)	
Location	Site with GIS Map C01 (CameraGroup10...
Time	Fri, 26 Jun 2020 16h24:43
State	Not acknowledged

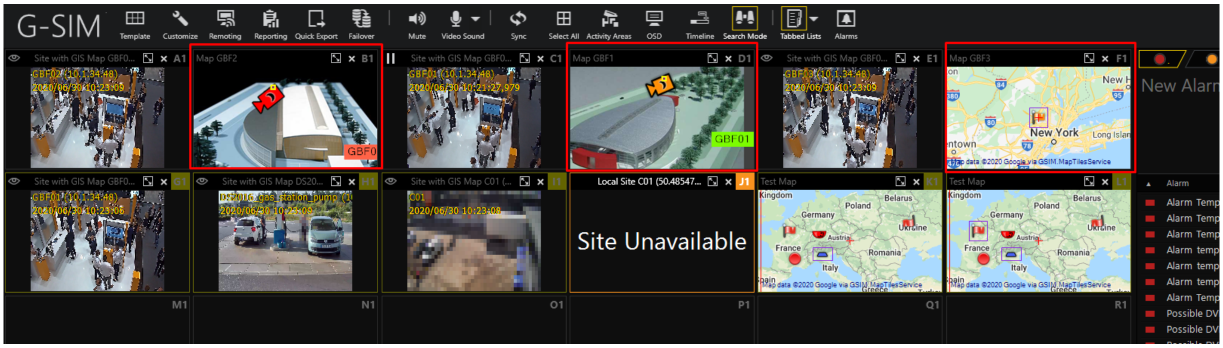
🟥 Alarm template (Kiev+Paris)   Alarm (K...

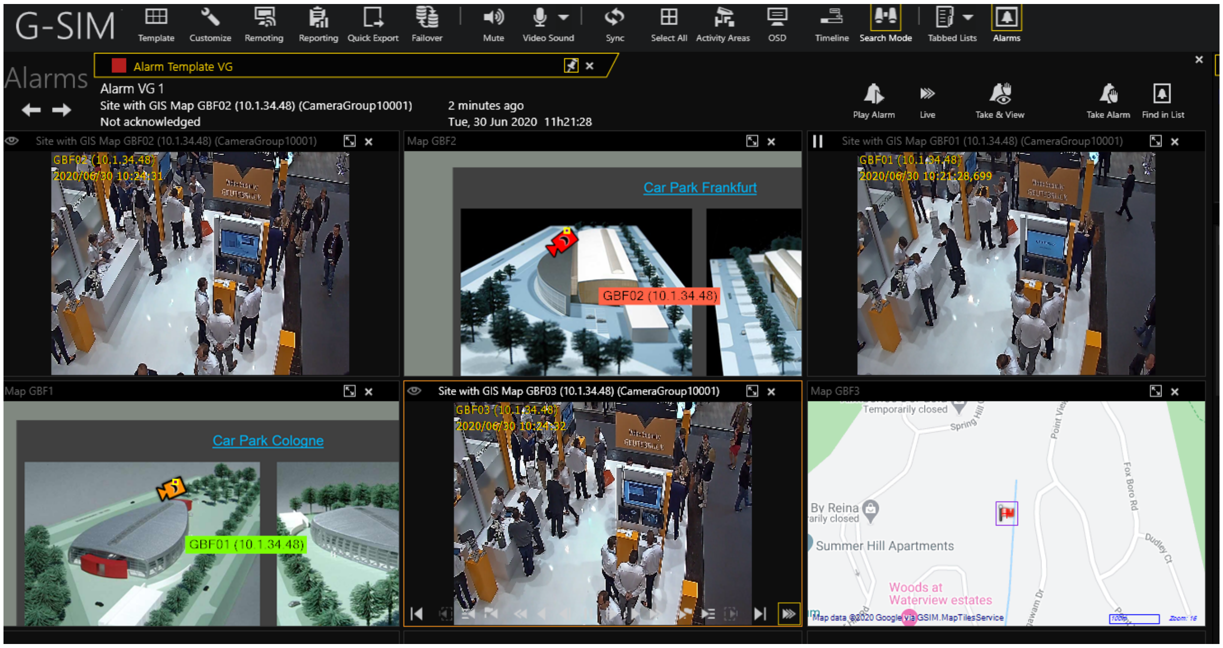
Alarm (Kiev)	
Location	Local Site C01 (50.4854735 , 30.5419921)

Whenever a Map Related Alarm is completed, it will disappear from the Map Related Alarm Control.

Alarm Settings

GIS Maps can be used for both **Viewer Group** and **Tab View** alarm presentation modes. GIS Maps and Regular Maps can be combined in a single Alarm Instance.





Alarms

Alarm Template VG

Alarm VG 1
Site with GIS Map GBF02 (10.1.34.48) (CameraGroup10001)
Not acknowledged

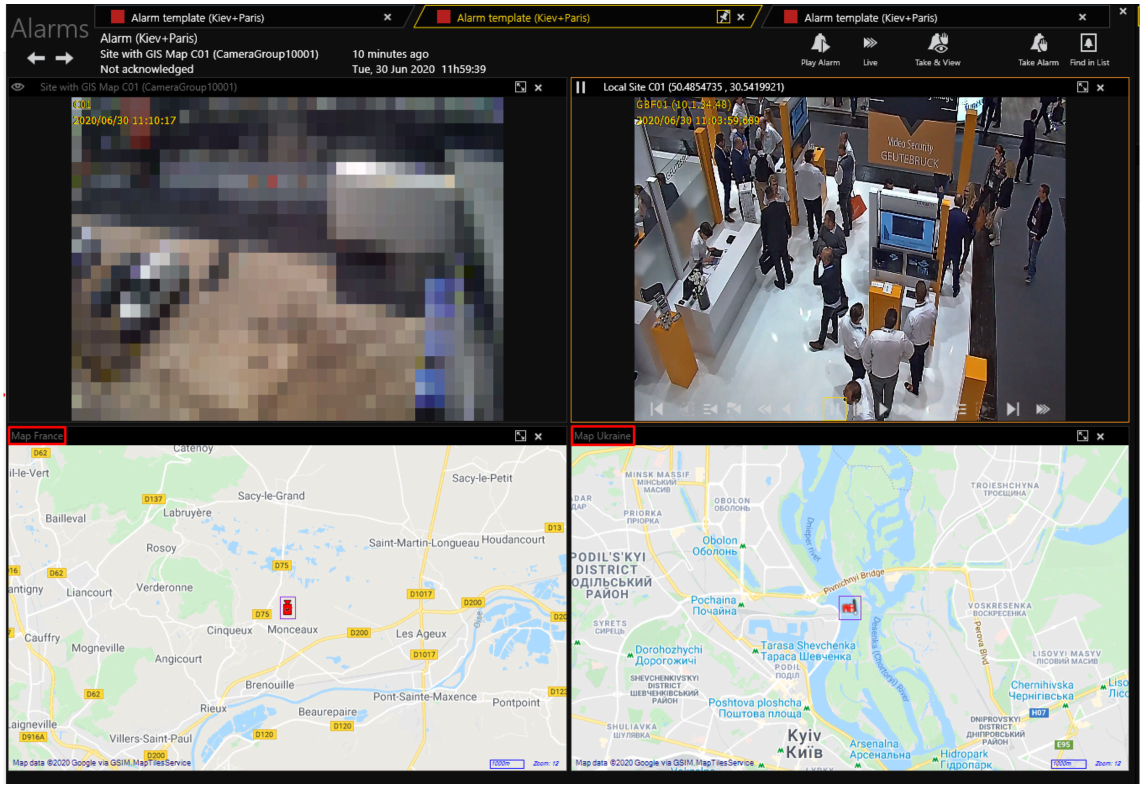
2 minutes ago
Tue, 30 Jun 2020 11h21:28

Whenever camera with playmode **Map** occurs, the next algorithm is used:

If Primary Site Map for the Alarm Instance is (None):

1. Set Map Object with Camera Trigger type where current camera is linked.
2. Get Primary Map value of the Map Object.
3. Show the map in the viewer, centre it to the Map Object and zoom the map

to the Max. Zoom Scale.



Alarm (Kiev+Paris)
Site with GIS Map C01 (CameraGroup10001)
Not acknowledged
10 minutes ago
Tue, 30 Jun 2020 11h59:39

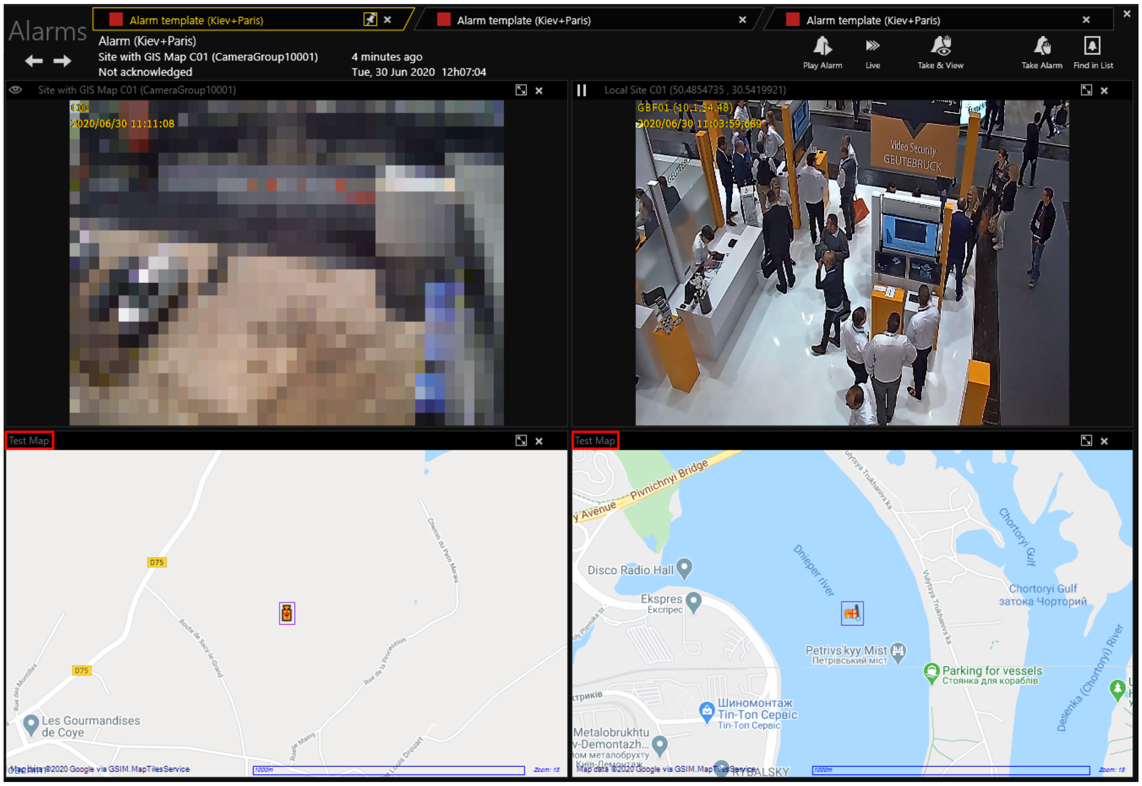
Alarms
Alarm template (Kiev+Paris)
Alarm template (Kiev+Paris)
Alarm template (Kiev+Paris)
Play Alarm
Live
Take & View
Take Alarm
Find in List
Site with GIS Map C01 (CameraGroup10001)
Local Site C01 (50.4854735 , 30.5419921)
2020/06/30 11:10:17
GBF01 (10.1.54.48)
2020/06/30 11:03:59,889
Map France
Map Ukraine
Map data ©2020 Google via GSIM.MapTilesService
Map data ©2020 Google via GSIM.MapTilesService

If Primary Site Map for the Alarm Instance is filled with GIS Map:

This Map will be used for every Camera with Playmode **Map**. It is advised to choose the GIS Map which contains all Map Objects related to the Alarm Instance’s cameras with Playmode **Map**.

According to zoom settings, the following cases are possible:

- **Zoom to camera:** Map is shown in the viewer, centred to the Map Object and zoomed to the Max. Zoom Scale or to the overridden zoom value, if any.



Alarms

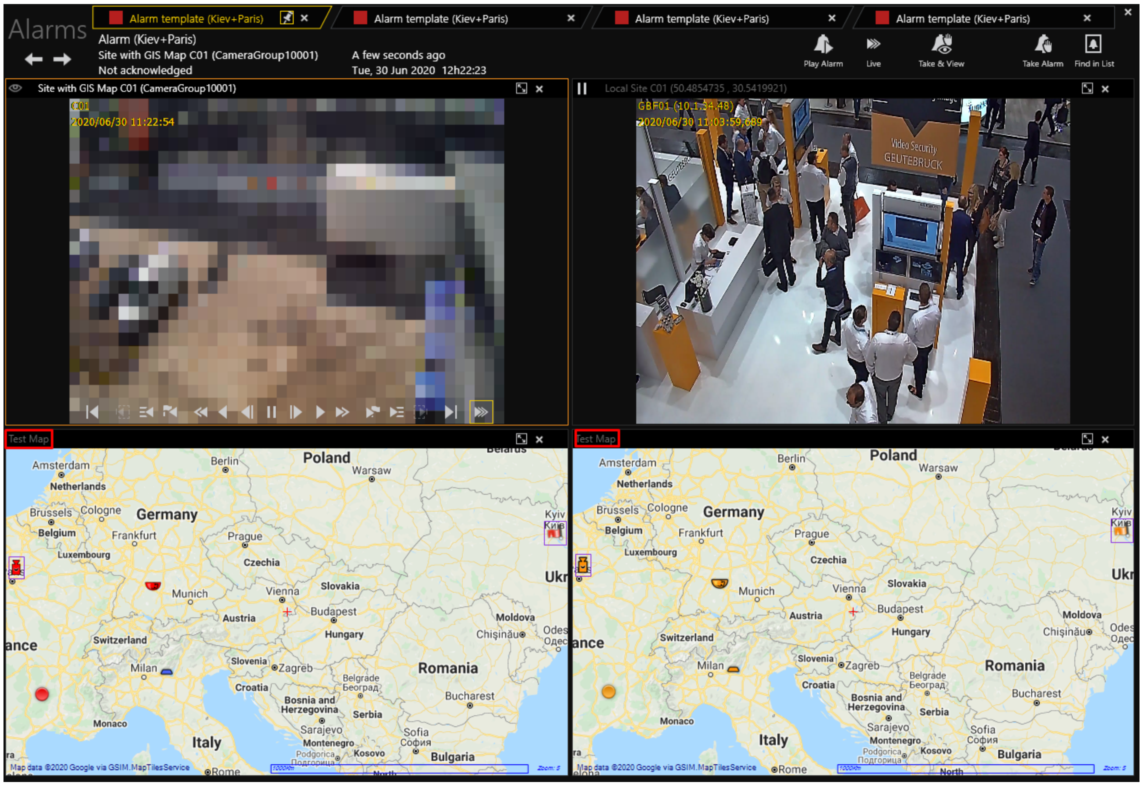
Alarm template (Kiev+Paris)

Alarm (Kiev+Paris)
Site with GIS Map C01 (CameraGroup10001)
Not acknowledged

4 minutes ago
Tue, 30 Jun 2020 12h07:04

- **Zoom to region:** The map is shown in the viewer, centred and zoomed to the specified Zoom Region. It is advised to set **Zoom Region** which contains all the Map Objects related to the Alarm Instance's cameras with Playmode

Map.



Alarm (Kiev+Paris)
Site with GIS Map C01 (CameraGroup10001)
Not acknowledged

A few seconds ago
Tue, 30 Jun 2020 12h22:23

Site with GIS Map C01 (CameraGroup10001)

Local Site C01 (50.4854735 , 30.5419921)

Cameras

Working with cameras is obviously one of the major functions of G-SIM. The term "camera" as used in G-SIM and this manual refers more broadly to the live video stream from a camera than to the actual camera itself. Cameras may be accessed from the Camera List or from a map — both these groupings of cameras allow the same functionality by means of buttons located on the camera detail card, or by means of dragging and dropping. The administrator would have defined groups of cameras according some common factor, e.g. Perimeter Cameras. Furthermore, cameras may be grouped in Tours which allow you to view any number of cameras in a timed sequence. Tours are described separately (see **Guard Tours**).

Cameras may be viewed (live) and, if the user has the necessary privilege, can also be reviewed, meaning it may be paused, a specific date and time searched for, and the recorded footage played backward or forward at different speeds. By blocking camera access to one or more users, exclusive access to a camera or site may be gained. This is useful if bandwidth is limited or an area needs to be isolated during an emergency situations. Apart from being viewed, a camera may be dragged and dropped onto a map, which will highlight the camera position on the map.

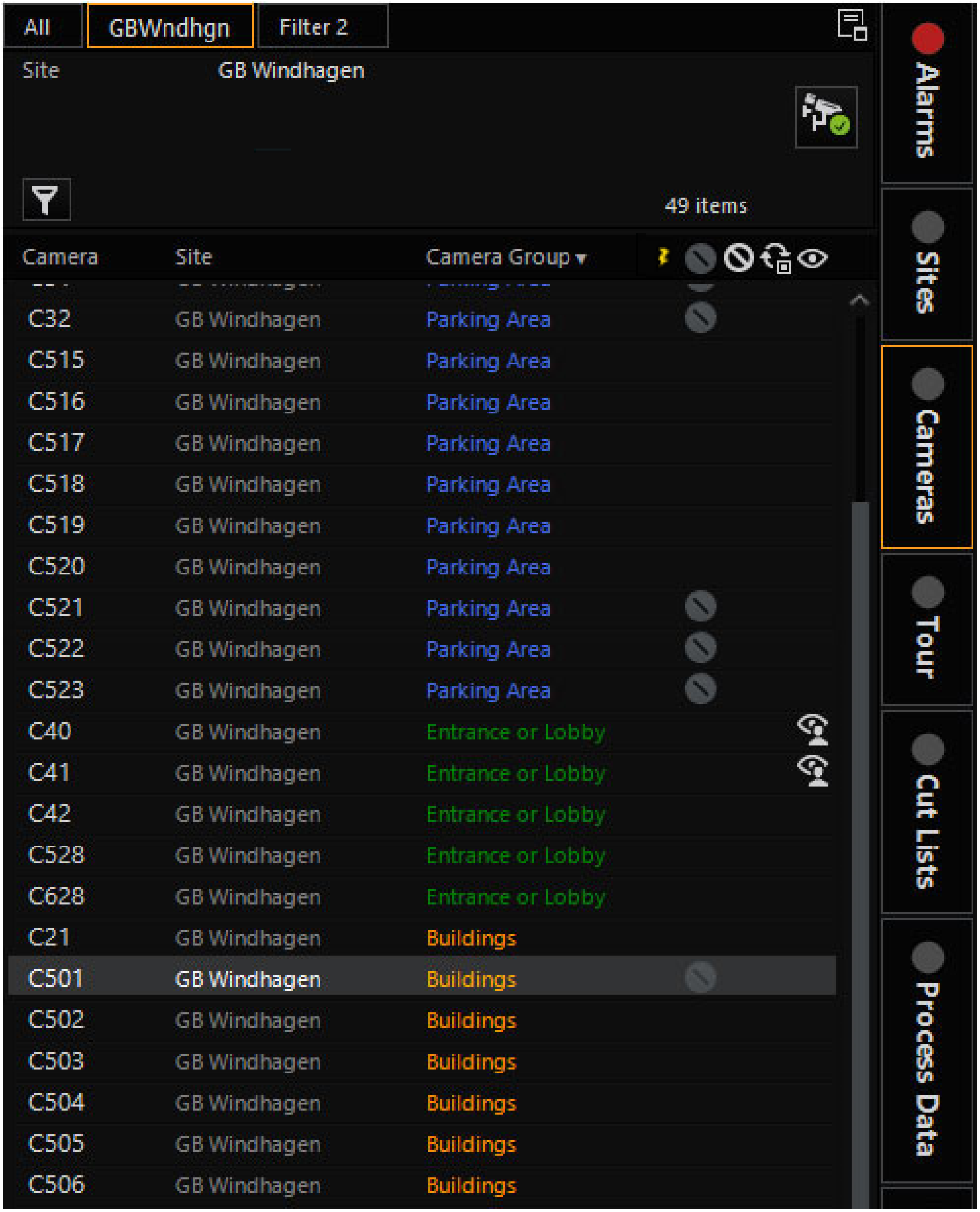
In the Camera List a camera item has a number of state icons that may be displayed with it. These icons are updated in real-time and give an overview of which cameras are being viewed, which are included in active Tours, blocked cameras, etc.

Camera List

The Camera List gives the user quick access to all system cameras, to cameras at a specific site which belong to a specific group, to camera groups, or to cameras in a specific state. Each row in the list represents one camera, and shows the camera name, the site and a series of state icons indicating which cameras are being viewed or are unavailable for viewing. The list is sorted alphabetically according to the site name, and then the camera name.

Because a video network may contain thousands of cameras it makes sense to apply a filter to the camera list based on camera location or camera state. It is easy to get a list of all cameras on a specific site by dropping the site on the camera list tab.

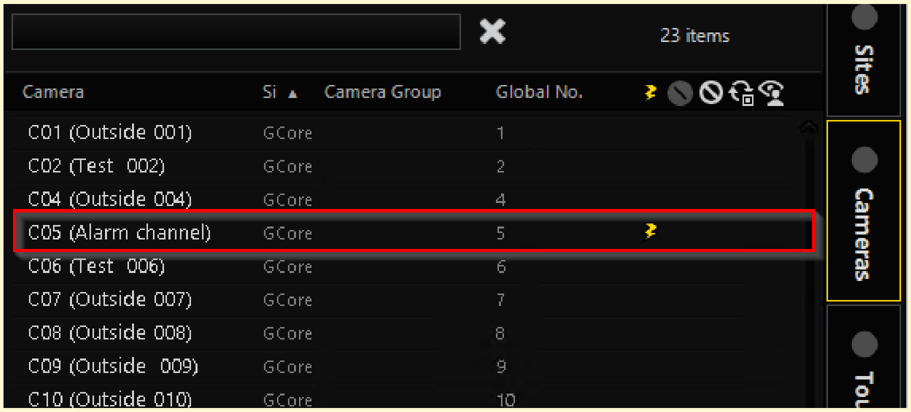
Camera List Layout and Buttons



Site GB Windhagen

49 items

Camera	Site	Camera Group ▾	
C32	GB Windhagen	Parking Area	⊘
C515	GB Windhagen	Parking Area	
C516	GB Windhagen	Parking Area	
C517	GB Windhagen	Parking Area	
C518	GB Windhagen	Parking Area	
C519	GB Windhagen	Parking Area	
C520	GB Windhagen	Parking Area	
C521	GB Windhagen	Parking Area	⊘
C522	GB Windhagen	Parking Area	⊘
C523	GB Windhagen	Parking Area	⊘
C40	GB Windhagen	Entrance or Lobby	
C41	GB Windhagen	Entrance or Lobby	
C42	GB Windhagen	Entrance or Lobby	
C528	GB Windhagen	Entrance or Lobby	
C628	GB Windhagen	Entrance or Lobby	
C21	GB Windhagen	Buildings	
C501	GB Windhagen	Buildings	⊘
C502	GB Windhagen	Buildings	
C503	GB Windhagen	Buildings	
C504	GB Windhagen	Buildings	
C505	GB Windhagen	Buildings	
C506	GB Windhagen	Buildings	

<table>
<tr><th>Button</th><th>Description</th></tr>
<tr><td>⧉</td><td>Dock list</td></tr>
<tr><td>✓</td><td>Enable all cameras I blocked</td></tr>
<tr><td>👁</td><td>Observed</td></tr>
<tr><td>👁</td><td>Observed by me</td></tr>
<tr><td>⟳</td><td>Displayed in tour</td></tr>
<tr><td>⟳</td><td>Displayed by me in tour</td></tr>
<tr><td>⊘</td><td>Blocked for me</td></tr>
<tr><td>⊘</td><td>Blocked by me</td></tr>
<tr><td>⊘</td><td>Deactivated</td></tr>
<tr><td>⚡</td><td>
<p>The Camera Sync State detects the initial state of the camera for G-Core media sources.</p>
<ul>
<li>If the <b>VideoSyncFailed</b> action is detected, it means that the connection to the camera is lost. The Camera Sync State icon is displayed in the camera bar.</li>
</ul>

<p>23 items</p>
<table>
<tr><th>Camera</th><th>Si ▲</th><th>Camera Group</th><th>Global No.</th><th>⚡</th><th>⊘</th><th>⊘</th><th>⟳</th><th>👁</th></tr>
<tr><td>C01 (Outside 001)</td><td>GCore</td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>C02 (Test 002)</td><td>GCore</td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>C04 (Outside 004)</td><td>GCore</td><td></td><td>4</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>C05 (Alarm channel)</td><td>GCore</td><td></td><td>5</td><td>⚡</td><td></td><td></td><td></td><td></td></tr>
<tr><td>C06 (Test 006)</td><td>GCore</td><td></td><td>6</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>C07 (Outside 007)</td><td>GCore</td><td></td><td>7</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>C08 (Outside 008)</td><td>GCore</td><td></td><td>8</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>C09 (Outside 009)</td><td>GCore</td><td></td><td>9</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>C10 (Outside 010)</td><td>GCore</td><td></td><td>10</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<ul>
<li>When the <b>VideoSyncDetected</b> action is detected, it means that the connection to the camera is re-established. The Camera Sync State icon is not displayed.</li>
</ul>
</td></tr>
</table>

Though most of it is obvious, the following is highlighted:

Activity and Status The last column in the list shows the current status of the camera e.g. viewed or unavailable for viewing. See Camera Status Indicators later in this chapter for more detail.

Dock List This function allows the Camera List to be duplicated in any viewer. After clicking it the available viewer windows will be highlighted with the corresponding short-cut key that may be pressed to dock the list in the designated viewer (see **Main Interface**).

Unblock all Cameras Blocked by Me All blocked cameras of the user will be unblocked, not only the blocked cameras visible in the Camera List. See **Camera Detail**.

Filtering the Camera List

Filtering is as explained in **Filtering**.

Camera Status Indicators

Viewed The camera has one or more open connections. By selecting the camera you will be able to see which users are currently viewing this camera.

Viewed by me You (the logged in user) have one or more connections to this camera.

Viewed in Tour The camera is part of a Tour being viewed by someone. By selecting the camera you will be able to see which Tours containing this camera are viewed by whom.

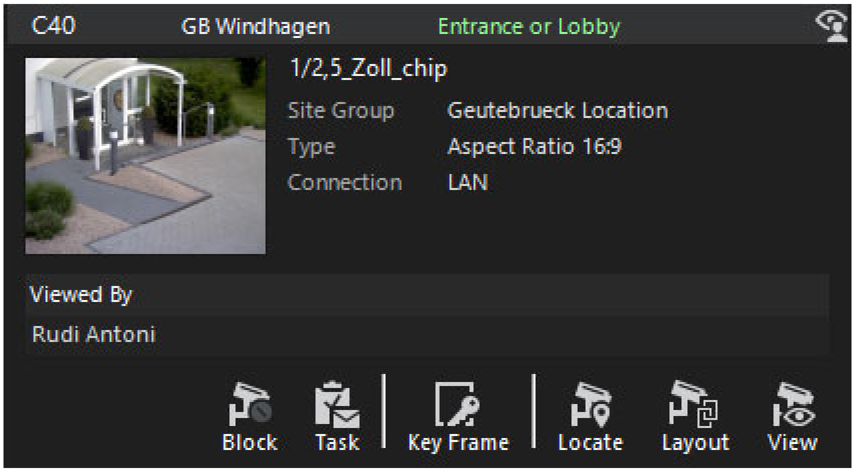
Viewed in Tour by me The camera is part of a Tour being viewed by me.

Blocked to me The camera is blocked by someone, and you (the logged in user) may not view it at this stage. If you were viewing the camera when the blocked was applied, the live feed will stop and a message will be displayed. The name of the user who applied the block is displayed on the Camera Detail Card.

Blocked by me You (the logged in user) blocked this camera.

Disabled The camera is not available for viewing. This might typically be when a camera was removed by maintenance personnel for reparation.

Camera Detail



C40 GB Windhagen Entrance or Lobby

1/2,5_Zoll_chip

Site Group	Geutebrueck Location
Type	Aspect Ratio 16:9
Connection	LAN

Viewed By

Rudi Antoni

A Camera Detail Card will be displayed if you select a camera item in the Camera List (by clicking the item) or by right clicking on any viewer displaying camera footage. The detail card displays general camera info and a list of all users viewing the camera and all playing Tours which contains the selected camera. It also shows the camera reference image if one has been configured by the administrator.

The following two areas needs further explanation.

Camera Usage Summary The two tables show a summary of how the camera is currently being used; i.e. Viewed/Reviewed, as part of one or more Tour. If the camera is not currently used in either of these methods, the corresponding table will not appear.

The user names and the Tour names in these two lists may be dragged to any other screen component that can drop-accept a user or Tour. (You may e.g. drag the user name of a user viewing the camera to the Messages Tab to send a message to the user, or you may drop the Tour on a viewer to view the same Tour another user is viewing etc.

Camera Actions

The following action buttons are available on the Camera Detail Card:

Button	Description
Block	With this function, you can block access to these cameras for any users or user groups. This is described below.
Enable camera	This button only appears when the camera has been

Button	Description
	blocked by the logged on user. (It replaces the "Block camera" button.) More information can be found **here**.
Task (delegate camera)	Create a new task to delegate the display/control of this camera to a selected user. See Create new tasks.
Key Frame (display camera reference image)	Click this button to open the functions for camera status images and create new reference images.
Locate (show on map)	This button allows you to highlight the position of a camera on the map in the selected Viewer. If you select a viewer that already contains other content, the initial content will be replaced by the (first) map with camera. If in the corresponding viewer a map of the site is already displayed, the map is shifted so that the sought camera is displayed in the center. The camera label is highlighted with the color "Map Highlighted Camera Outline" (see mapping in G-SIM).
Layout (show linked layout)	Show linked layouts (Template Walker Mode)
View (live video)	With this button you can display the live video images of a camera in a selected viewer. If you select a viewer that already contains other content, the initial content will be replaced.
Add camera to tour	If you create a new tour or edit an existing tour, click this button to add the selected camera to the tour. However, it is easier to simply drag cameras onto the tab of the tour with the mouse.

Blocking and Unblocking Cameras

Blocking and unblocking of cameras is a privilege which allows a user to prevent any other user or group of users to access a camera or group of cameras. This may be required to ensure fast and dedicated access to the camera footage (especially if there are bandwidth limitations to the site) or to isolate a site or part thereof in the case of an emergency. If a blocked user was viewing a camera before the block was applied, a message will be displayed in the viewer indicating that the live video stream was blocked by another user.

After the Block Camera button was clicked, either on a Camera Detail Card or on the toolbar at the top of the Camera List, a pop-up window will be displayed from where you may select the user or group of users you wish to block. This is done in exactly the same way as filters are defined. Multiple users or user groups may be selected before the Block button is click on the Block pop-up. The name of the user who blocked a camera will be visible to the blocked users on the Detail Card of the corresponding camera.

It is possible to block all cameras on a site by using the corresponding button on the Detail Card of the specific site (see **Site Detail**). You may also apply a filter to the Camera List and block all the cameras in the list by clicking the Block All Cameras in Current List button on the toolbar at the top of the Camera List (see **The Camera List**).

It is the responsibility of the user who applied the block to remove it again. You may remove the block on a single camera by clicking the Unblock Camera button on the Detail Card of the corresponding camera. You may also remove all camera blocks that you have applied by clicking the Unblock all Cameras Blocked by Me button at the top of the Camera List (see **The Camera List**).

To unblock all cameras on a specific site, use the Unblock All Cameras on Site button (see **Site Detail**).

Reference Frame Update

It is possible to check the Camera reference frame from a camera detail card by clicking the Check Camera reference frame button . The Reference Frame dialogue box will be displayed, allowing you to extract a current frame from the NVR (Refresh button), compare it with the current reference frame, and update (Update button) the reference frame if needed.

The reference frame is used for the thumbnail image on the camera detail card.

Viewing Camera Footage

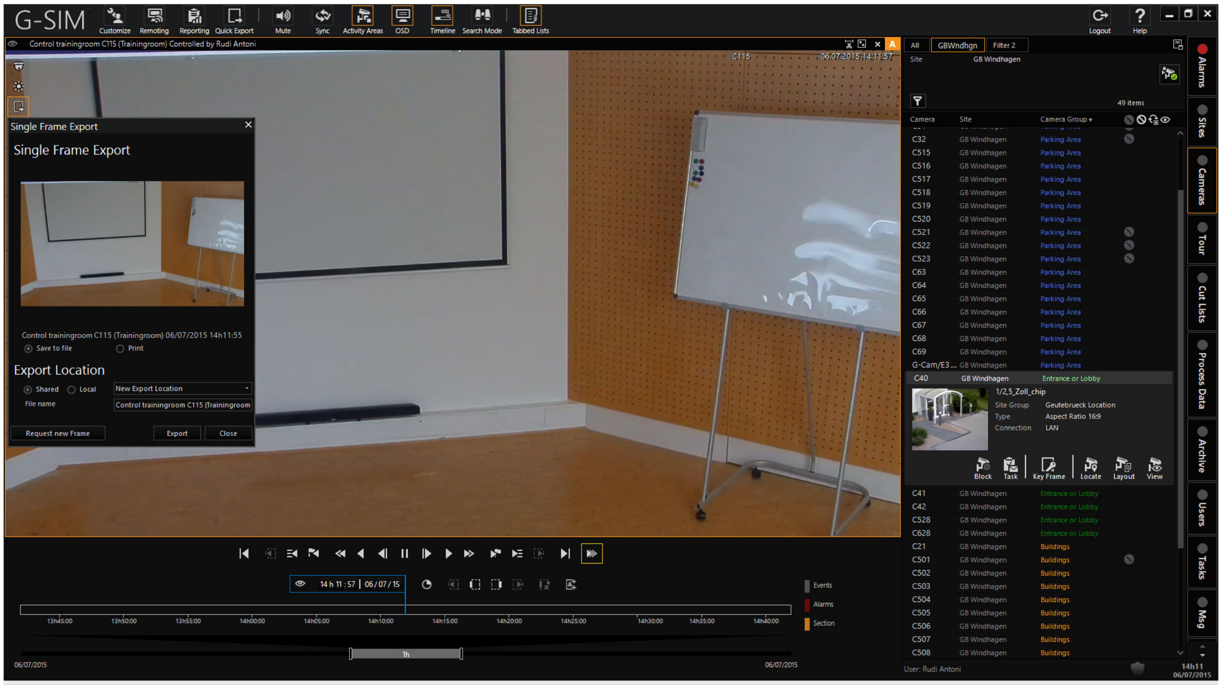
There are several ways to connect a Camera to a viewer for either a live view or for the reviewing of recorded footage:

- Drag a camera from the Camera List to another viewer.
- Drag a camera from a Map to another viewer.
- While a Tour is playing, drag the video content (do not start the drag on the window header) to another viewer. The Tour will continue to play and the

new viewer will contain the camera which was playing in the Tour when the drag was initiated.

- Several Detail Cards contain a View Live button, e.g. Camera Detail, Alarm Detail if the alarm is linked to a camera, and Task Detail if the Task is linked to a camera. If any of these Cards is dragged to a viewer, the linked camera's video stream will be displayed. Instead of dragging the Card, the button could also be clicked and a viewer selected. See **Main Interface.**

Viewer Control



Control trainingroom C115 (Trainingroom) Controlled by Rudi Antoni

Single Frame Export

Control trainingroom C115 (Trainingroom) 06/07/2015 14h11:55

● Save to file ○ Print

Export Location

● Shared ○ Local New Export Location

File name Control trainingroom C115 (Trainingroom

Request new Frame | Export | Close

All | GBWndhgn | Filter 2

Site GB Windhagen

49 items

Camera	Site	Camera Group
C32	GB Windhagen	Parking Area
C515	GB Windhagen	Parking Area
C516	GB Windhagen	Parking Area
C517	GB Windhagen	Parking Area
C518	GB Windhagen	Parking Area
C519	GB Windhagen	Parking Area
C520	GB Windhagen	Parking Area
C521	GB Windhagen	Parking Area
C522	GB Windhagen	Parking Area
C523	GB Windhagen	Parking Area
C63	GB Windhagen	Parking Area
C64	GB Windhagen	Parking Area
C65	GB Windhagen	Parking Area
C66	GB Windhagen	Parking Area
C67	GB Windhagen	Parking Area
C68	GB Windhagen	Parking Area
C69	GB Windhagen	Parking Area
G-Cam/E3 ...	GB Windhagen	Parking Area
C40	GB Windhagen	Entrance or Lobby
C41	GB Windhagen	Entrance or Lobby
C42	GB Windhagen	Entrance or Lobby
C528	GB Windhagen	Entrance or Lobby
C628	GB Windhagen	Entrance or Lobby
C21	GB Windhagen	Buildings
C501	GB Windhagen	Buildings
C502	GB Windhagen	Buildings
C503	GB Windhagen	Buildings
C504	GB Windhagen	Buildings
C505	GB Windhagen	Buildings
C506	GB Windhagen	Buildings
C507	GB Windhagen	Buildings
C508	GB Windhagen	Buildings

1/2,5_Zoll_chip
Site Group Geutebrueck Location
Type Aspect Ratio 16:9
Connection LAN

User: Rudi Antoni
14h11 06/07/2015

The current viewer (click on it to make a viewer active) is indicated by highlighting its border. When the mouse is in the active viewer, its control icons become visible.

- You can zoom the image with the mouse button, and pan it by dragging it around. If it is not a PTZ (or you don't have rights to control it), then it is simply a panning and zooming of the image itself.
- If you double-click the viewer, its image will take up the whole of the display area, which is useful if you need to see something larger quickly.

- Double-clicking again restores it. You can also use the buttons in the viewer's header.

The icon in the top left indicates live, playback, or pause state, while the rest of the buttons in the images are used for the following control purposes. While many of the buttons have obvious functions, we need to highlight some which are less obvious or which have some subtleties about them.

☼ Allows you to change the brightness, contrast, and saturation of the image. Clicking on each icon in the pop-up window resets that control to its default.

Creates a video event from one of the pre-defined possibilities The result is the same as when you click the New Event button in the Events List and this video is inserted as the new event.

This will only appear if a PTZ camera is displayed in the viewer. If you have the necessary rights, click here to take control of the PTZ camera. To pan and tilt, drag the image with the left mouse button. To zoom, rotate the mouse wheel. You can also select or define preset points.

The pop-up window is displayed for searching according to time/date. Click the plus sign to add the currently selected frame to a jump list, which allows you to jump to specific interesting events. There is no way to delete elements from the jump list, but the entire list is deleted once the viewer is closed or another camera is shown in the viewer; it is only a short-term aid.

Specifying the video section: Enter the start and end of the section. To do so, you can use a combination of an exact time (date and time) and delta. The current frame can be used as a start or end point.

Select "Jump type": The event type is thus specified for the execution of jump instructions. The default value is "move". The "Events" here are not G-SIM video events, but instead events marked by the DVRDigital video recorder itself.

When browsing video records, the direction of the search (forward or reverse) and speed are indicated in the playback display. If no speed is displayed, the playback for the search is performed at the speed of the video recording (1x).

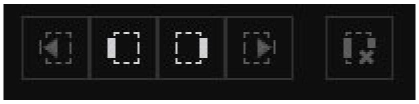
Starting from the middle button ("pause"), the next seven buttons of the controls are used for video playback in both directions (forward and rewind): "Single step", "Playback", "Fast playback", "Next Event", "Next movement", "Next selection", "Start/end of the video".

Switches back to the live video image from the camera.

Switching the controls: The first time you click this button, a timeline is shown that you can use to select the desired recording position by dragging with the mouse. The second time you click on it, a slider appears that you can use to change the playback speed from "Pause" to "100x" (forward and rewind) if you need to perform fast searches. On the third click, the normal controls appear again.

The status symbol "Tour" indicates that a tour is currently being displayed in the viewer, meaning that all cameras allocated to this tour are shown in a loop.

All selected cameras can be synchronized with this button. The active video is used as a reference. If the "Synchronize" button appears light blue, the camera is part of a synchronous group (see Working with synchronous groups).



Start and end marks can be defined with these buttons. In addition, the buttons can be used to identify whether section markers are present in a viewer (see below).

All/Selected viewers can als be sent to the cut list.

With this icon on the top right side of the viewer it is possible to jump directly to the start of the current selection.

If these symbols are displayed white, a start and/or end marker has been set for the corresponding viewer.

Start/end markers are highlighted in green when the current frame is the selected frame.

The zoom symbol is highlighted in yellow when the image in a viewer is displayed with a zoom factor. Click on the symbol to switch to the original size.

Clearing All Viewers

As this is quite a drastic action, it requires a bit more work to get to (so you cannot accidentally clear them all). You will find it under Customize | Templates.

Multi-Selection in Viewer

Selecting multiple camera viewers allows the user to control all the selected items at once, e.g. to navigate simultaneously through the selected footage using the Video Controls functionality by adding all selected cameras to a Sync Group.

To select more than one item, the standard Windows method may be used by holding the Ctrl key while clicking the desired items with the mouse. Note: the block selection method (i.e. using the Shift key) does not work with the Viewers.

All the cameras in the selection will be marked with a light blue viewer identifier and border. The camera that is selected last will be the Active Video, and is indicated by a blue viewer identifier but with the standard active border colour.

The Active Video will be the master viewer when controlling the others.

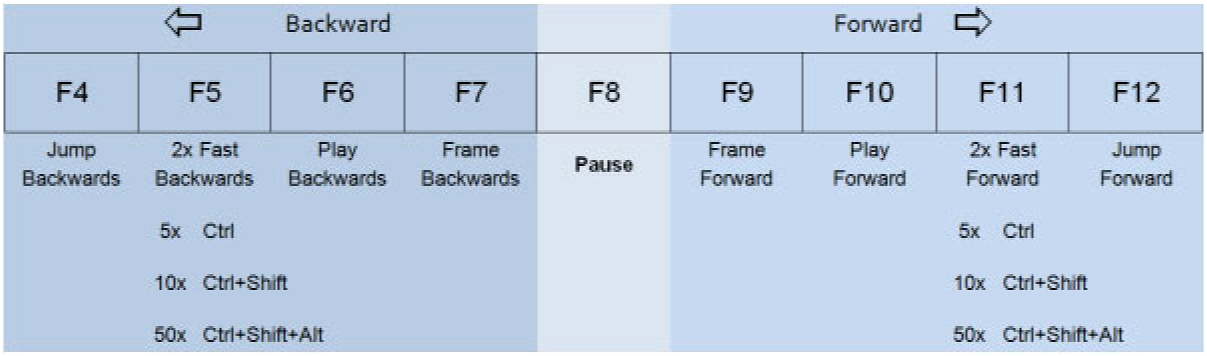
Video Playback Control

Using Keyboard

Users with the **Playback Control** privilege may pause a live video stream to navigate forward and backwards through the recorded footage. The function keys F4 through F12, are used for video control.

Note that fast playback (forward or backwards) is possible by using the Ctrl (5x), Ctrl+Shift (10x) or Ctrl+Shift+Alt (50x) keys together with the function keys F5 (for double speed backward play) or F11 (double speed forward play).

The following table summarizes the above.



	⇦	Backward				Forward	⇨	
F4	F5	F6	F7	F8	F9	F10	F11	F12
Jump Backwards	2x Fast Backwards	Play Backwards	Frame Backwards	**Pause**	Frame Forward	Play Forward	2x Fast Forward	Jump Forward
	5x Ctrl						5x Ctrl	
	10x Ctrl+Shift						10x Ctrl+Shift	
	50x Ctrl+Shift+Alt						50x Ctrl+Shift+Alt	

Other shortcut keys are:

- F2: Stop playback of recordings and switch to live video image.
- Ctrl + F2: Switch PTZ control on/off.
- Shift + F3: Enter the time and date of the position to which you want to jump.
- Ctrl + F3: Export current frame as JPEG or BMP file (much larger!).

Using MBeg Controller

When in MV-mode, use the Up and Down arrow keys on the unit to select the Playback Softkey Menu.

The Softkeys beneath the MBeg menu give you access to the following Playback control functions:

- Full-screen switching: switch between viewing the selected camera full-screen or multiple viewers.

- Variable reverse (reverse speed can be varied)
- Synchronous reverse (reverse speed is the same as the speed of the recording)
- Stop
- Synchronous replay (speed of replay is the same as the speed of the recording)
- Variable forward (forward speed can be varied)
- Live

If a non-PTZ camera is "controlled" by the MBeg, the digital pan & zoomwill be used, much like with the mouse wheel and dragging. The Operating keys (e.g. the "Camera", "Viewer" or "Event" keys) allow preset functionality. See **Using an MBeg Controller**.

PTZ Control

PTZ Control During Viewing

Pan, Tilt & Zoom cameras must be configured as such in the G-SIM Management Console. They are then clearly marked on the Camera Detail Card (e.g. in the Camera List) and in the Viewer when the camera is being viewed.

These cameras may be controlled by users with the correct privileges. Camera control is prioritised, allowing users of a higher level to take control away from users of a lower level. This hierarchy is configured in the Management Console by ordering the User Groups so that the top User Group has the highest level. Thus, a user from a lower level cannot take control away from a higher level user.

Direct PTZ Control

The direct PTZ control option enables you to start controlling a PTZ camera only by selecting the camera for a viewer. As soon as the viewer is selected, there is an indication in the upper row saying **Controlled by** followed by the name of the respective user.

This functionality only works if the system setting Activate PTZ Control on Viewer Selection is enabled in the ManCon (see Operator Console).

1. To start direct PTZ control, open a PTZ camera in a viewer. You are now controlling the PTZ camera.

2. Move the PTZ camera around by mouse clicking.
3. To revoke the PTZ control, deselect the viewer. You are no longer controlling the PTZ camera.

If multiple PTZ cameras are in use in different viewers, the PTZ control will only work with the focused viewer.

Take Control of a PTZ Camera

1. Open the PTZ camera in a Viewer, making sure it is selected (i.e. the Active Camera).
2. To take control, you can:
    - Press Ctrl+F2 to enter PTZ control mode, or
    - Click on the PTZ Control button in the Viewer.

You will retain control until:

- You relinquish control (press Ctrl+F2 again or click the Relinquish Control button).
- Another user with the same or higher user level takes over the control.
- Another viewer is selected.
- A Timeout occurs (default timeout occurs after 1 minute, but this can be configured).
- You log out or lose connection with the server.

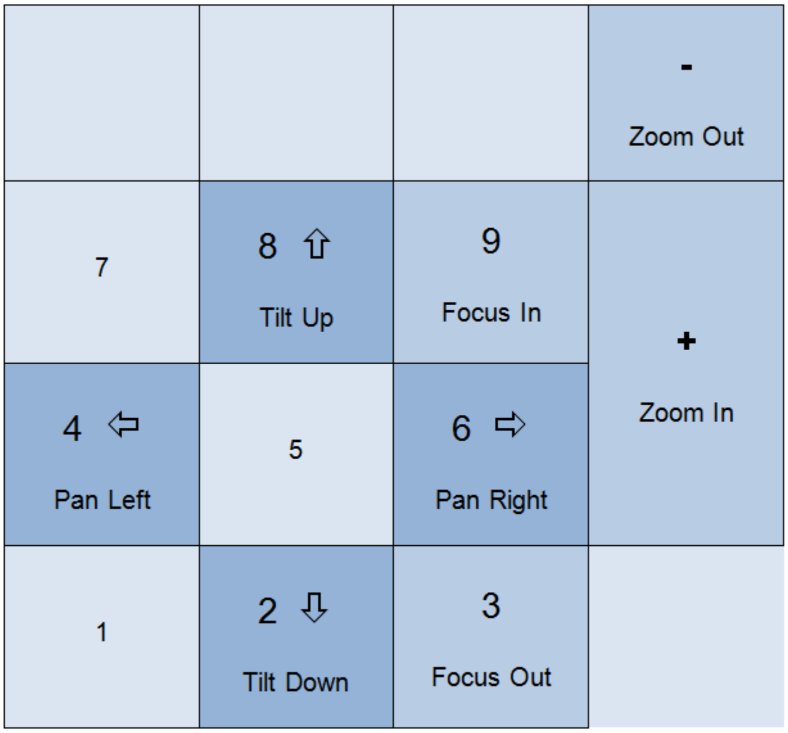
When you are controlling a PTZ camera, "Controlled by" and your name will be in the viewer header as well as in the camera detail card. If you are viewing a PTZ camera that is being controlled by another user of the same or a lower level than you, you can press the Take Control button to take control of the camera.

Once you have control, you can control the camera's viewing direction, focus and zoom in one of three ways: via the keyboard, the mouse, or an MBeg controller. The MBeg controller has additional functionality not available when using the other methods.

i **Note that there may be a considerable lag in the reaction of the camera view and responsiveness, depending on your network and the type of camera being controlled.**

Controlling PTZ Cameras Using Keyboard

Keyboard control is using done by the numeric keypad as shown in the diagram below.



			- Zoom Out
7	8 ⇧ Tilt Up	9 Focus In	+ Zoom In
4 ⇦ Pan Left	5	6 ⇨ Pan Right	
1	2 ⇩ Tilt Down	3 Focus Out	

Other shortcut keys are:

- Ctrl + F2: Switch PTZ control on/off.
- 0...9: Use positions 0...9

The keyboard shortcuts for PTZ actions are only activated when the "PTZ Control" mode is active and the Controlled by %currentuser% indicator appears in the Viewer header. If the PTZ control is not active, it will be activated with the first execution of the key combination. You must then press the key combination a second time to perform the desired PTZ action. If the PTZ control is already active, the execution of the key combination will work from the first time.

Controlling PTZ Cameras Using Mouse

Click and drag the mouse in the direction you wish the camera to move (this is the opposite to what you do when you drag an image) and it will do the necessary tilting and panning to do so. The further you move the mouse from your starting click point, the faster the movement will be. There is a "dead zone" around the point you click where camera movement will not take place. This is so that you do not inadvertently cause camera jitter.

If your mouse cannot move far enough because you are at the edge of the screen, press either Shift or Control to increase the speed. Pressing both makes it go even faster. Letting go of the mouse stops the movement.

There are two ways to zoom: the mouse wheel and the keyboard (the + and - keys on the numeric keypad to zoom in and out, respectively). We have found that the keyboard is easiest if you need to zoom whilst moving, and that the mouse wheel is easiest when you are only zooming, and not moving at the same time.

Controlling PTZ Cameras Using MBeg Controller

MBeg control for PTZ cameras is fully supported in G-SIM — just remember that you will only be able to control the functions which are supported by your PTZ camera.

You can take control of a PTZ camera (if the user privileges and control-priority allow it) by pressing the F2 button on the MBeg when the PTZ camera is the Active Viewer. Now you can start controlling video playback with the MBeg (see below). Pressing the F2 button again will relinquish control.

Make sure you understand the implications of the user level hierarchy on PTZ Controlling (described above).

Using PTZ Presets

Most PTZ cameras can save a number of preset positions, which can be recalled to move the camera to a specific position. This is useful when certain positions need to be viewed often, e.g. an outside door. Such presets can also be used to define points on a Tour.

Presets are defined and may be selected and edited from the PTZ Control pop-up when you have control of it. Preset positions are also shown in the Camera Detail card. To move the camera to a Preset position, you can either double-click on it in the Camera Detail card (which will implicitly take control of the PTZ), or from the Preset list. You can also use drag & drop to display it in a particular viewer.

You can move the PTZ to a Preset by double-clicking on it or by pressing ENTER on a highlighted position.

To create or edit Presets, click on the Edit Presets button (pencil icon). This will change the interface to look as follows:

To create a Preset, move and zoom the PTZ camera into the position you want the Preset to. Then click in the Description text box and enter the description, and either press ENTER, or click on the Add button. This adds the Preset to the bottom of the list.

To move a Preset to a different position, click on it once to select it, then move it up or down with the arrow buttons. This updates the short-cut keys as well.

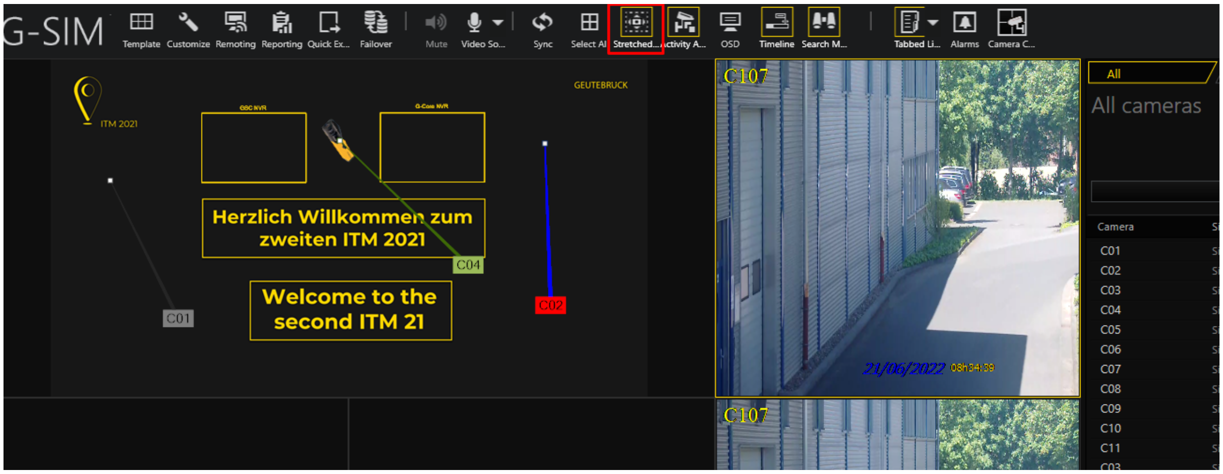
To rename a Preset, click on its description and type in the new text. To save it either press ENTER or click on the Edit Presets button.

To delete a Preset, select it, and then press the Remove Item button (the red minus sign).

Stretched View Mode

Operator Console

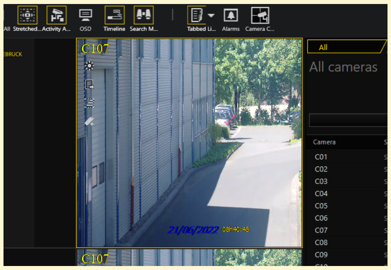
The **Stretched View** mode of the viewer can be activated/deactivated using the **Stretched View** button in the toolbar of the OpCon.



The Stretched View mode is saved and restored the next time the Operator Console is started.

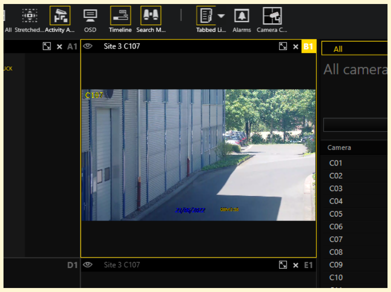
When the Stretched View mode is activated:

- The header of the viewer is hidden.
- The video image of the camera is stretched to the size of the viewer.



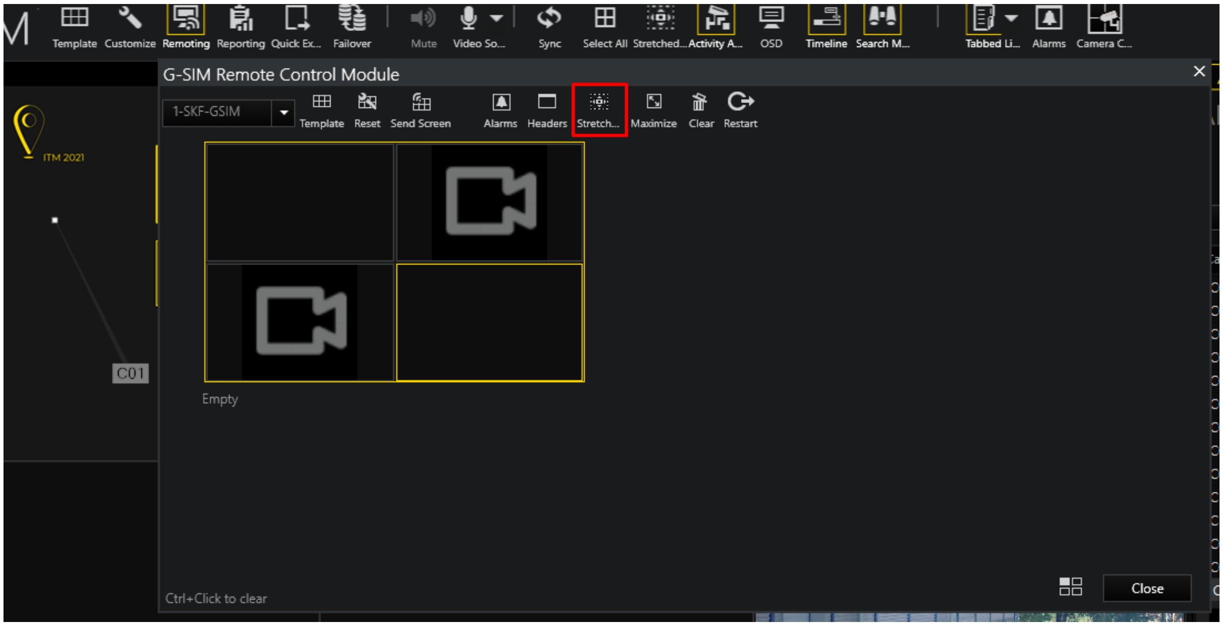
When the Stretched View mode is disabled:

- The Viewer header is displayed.
- The video frame of the camera is stretched according to the aspect ratio of the camera type.



Remote Console

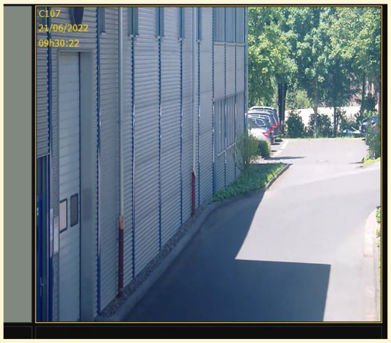
The **Stretched View** mode can be activated/deactivated using the **Stretched View** button in the toolbar of the G-SIM Remote Control Module.



The Stretched View mode is saved and restored the next time the Operator Console is started.

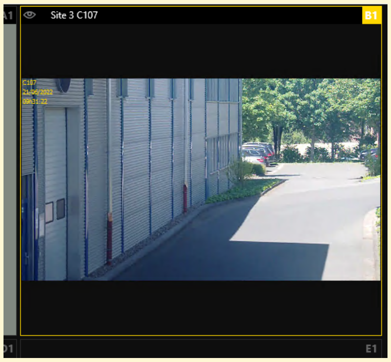
When the Stretched View mode is activated:

- The header of the viewer is hidden.
- The video image of the camera is stretched to the size of the viewer.

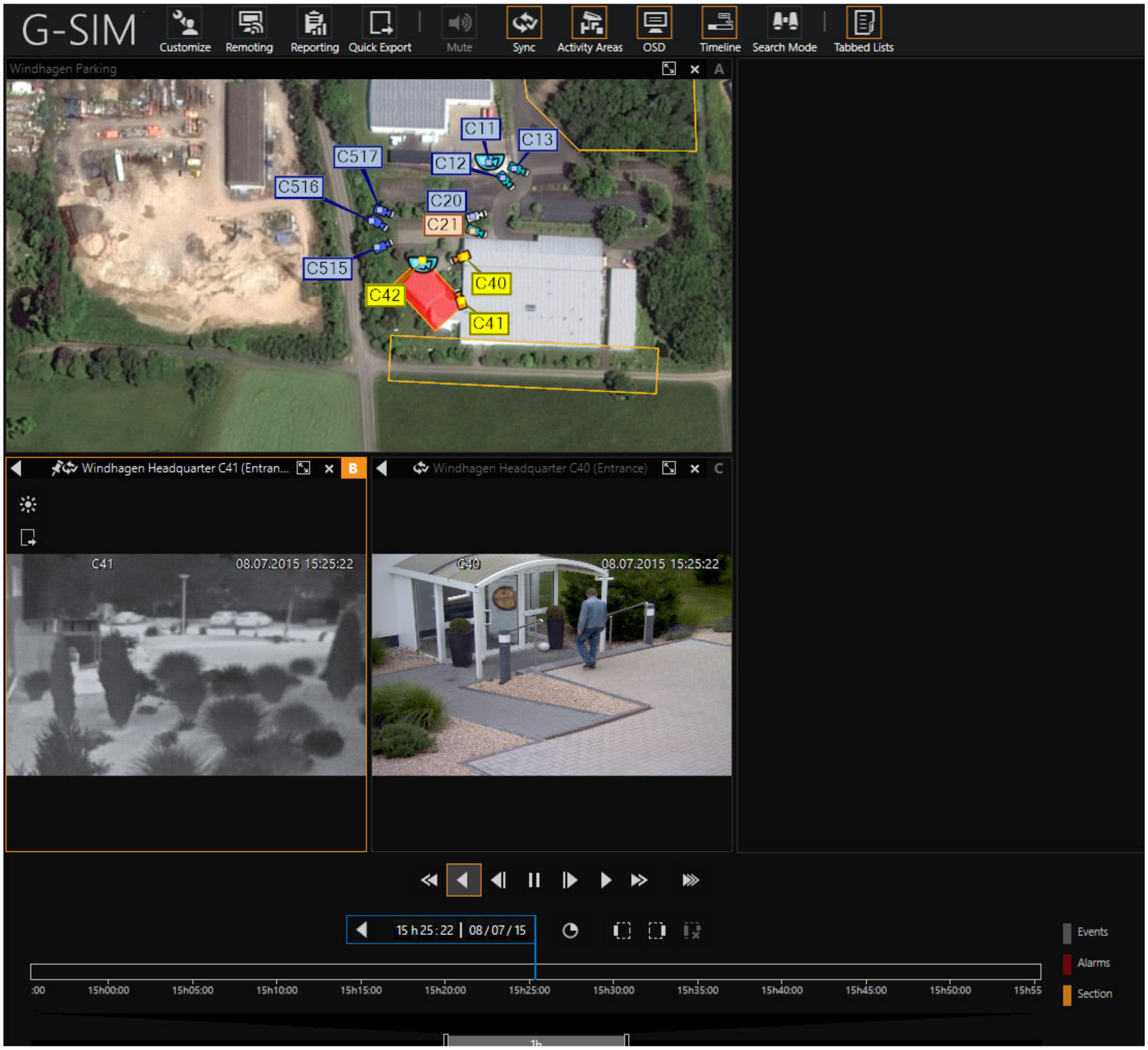


When the Stretched View mode is disabled:

- The Viewer header is displayed.
- The video frame of the camera is stretched according to the aspect ratio of the camera type.



Working With Sync Groups



You can group of cameras into ad hoc Sync Group, which means that their playback is synchronised, and that you then control all those viewer together. This is extremely useful (actually, necessary) when you want to export video for evidentiary purposes and you require footage from different cameras.

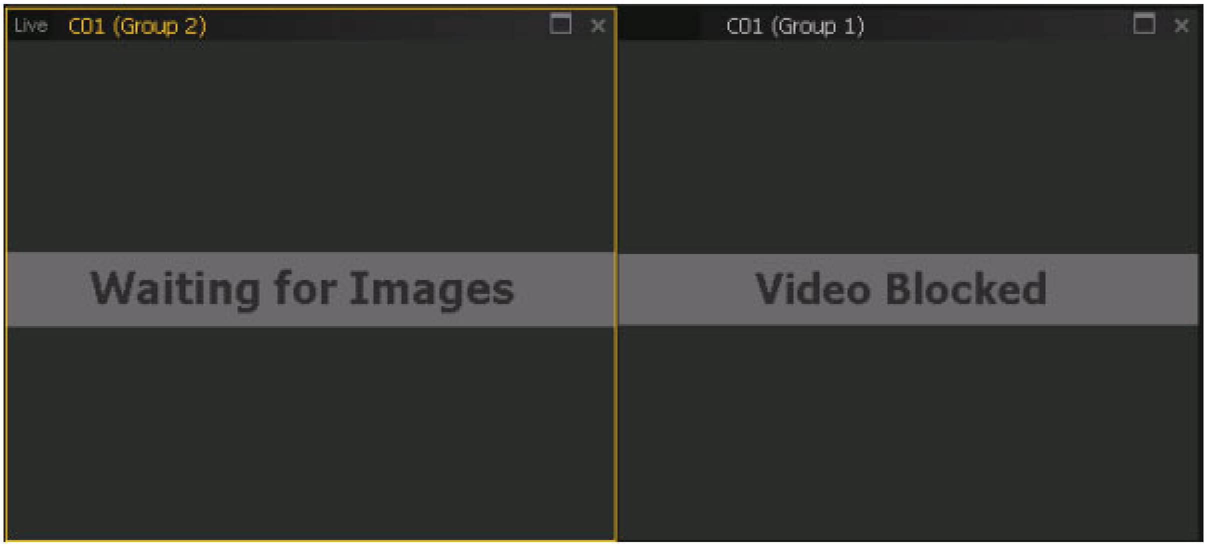
Sync Groups are created on-the-fly by choosing the first one (it will be the one the others sync to), then clicking on the others you want in the group while holding down the Ctrl key on the keyboard. If you accidentally added a viewer, simply click on it again (while holding down Ctrl). The viewer borders will change to cyan to indicate that they are part of a sync group, while the most recently chosen one will have only its shortcut character highlighted in cyan.

Once you have created the group, you sync the cameras by clicking on the sync button on any of the viewers.

If the master viewer was recorded at a lower frame rate than others and you step forward one frame, the others will jump to the time that is displayed in the master.

Feedback Messages During Viewing

Several feedback messages may be displayed in a viewer before video streaming starts or during viewing. A message is displayed as a text band on grey background in a viewer, such as in the following example.



Message	Description
Connecting...	The viewer waits for the connection to the digital video recorder (DVR) via the image server and the start of live streaming. For ISDN this may take some time, as it may be necessary to first establish the ISDN connection.
Images are being retrieved...	A connection to the DVR was established and the viewer waits for the first images from the recorder. On slow connections, this may take a while.
Access denied	You do not have the required permission level to display the selected camera.
Site not avail-	A connection could not be made to the DVR that hosts the

Message	Description
able	selected camera. This may be due to a fault with the DVR or with the network.
Camera not available	The camera was removed in the management console, and you are attempting to access a previously generated tour or a previously generated alarm.
Site in use	For each connection type, a maximum number of connections to the site is supported. For connections with limited bandwidth, such as ISDN, the maximum number of connections is very small, typically 2 to 4. If two cameras at an ISDN site are already being observed by another user (or you) and the connection limit is 2, the following message appears. Close other viewers for cameras at this site, or ask other users to terminate their connections.
Video blocked	The camera has been locked by another user. In the detail view for the camera you can see who blocked the camera. For more information, see Site details.
No data available	This message appears when you want to play video recordings that have already been overwritten or were never saved.
Overloaded network	This message is displayed for ISDN connections when the maximum number of connections configured in the management console (MaxOutgoingISDNLinesToUse) is reached.
Network error	When connecting to a DVR, a network error occurred.
Connection error	This message is displayed when the server has allowed the connection to a DVR, but the Operator Console cannot establish a connection.
Audit log of observed cameras	All camera display and playback actions are stored in the audit log of G-SIM. Users with the necessary permission levels can not only see what other users have seen, they can also playback the same video recordings in the exact same order.

Audit Logging of Cameras Viewed

All camera view and review actions are stored in the G-SIM Audit Log. Not only is possible for a user with the necessary privileges to see what other users have viewed, but also to review the same video footage in the exact same sequence afterwards.

Exporting Video Footage

You can export a single frame as a JPEG or BMP (Bitmap) image. To export a frame, press Ctrl+F3. Pause the video prior to exporting a frame to make sure the correct frame is exported.

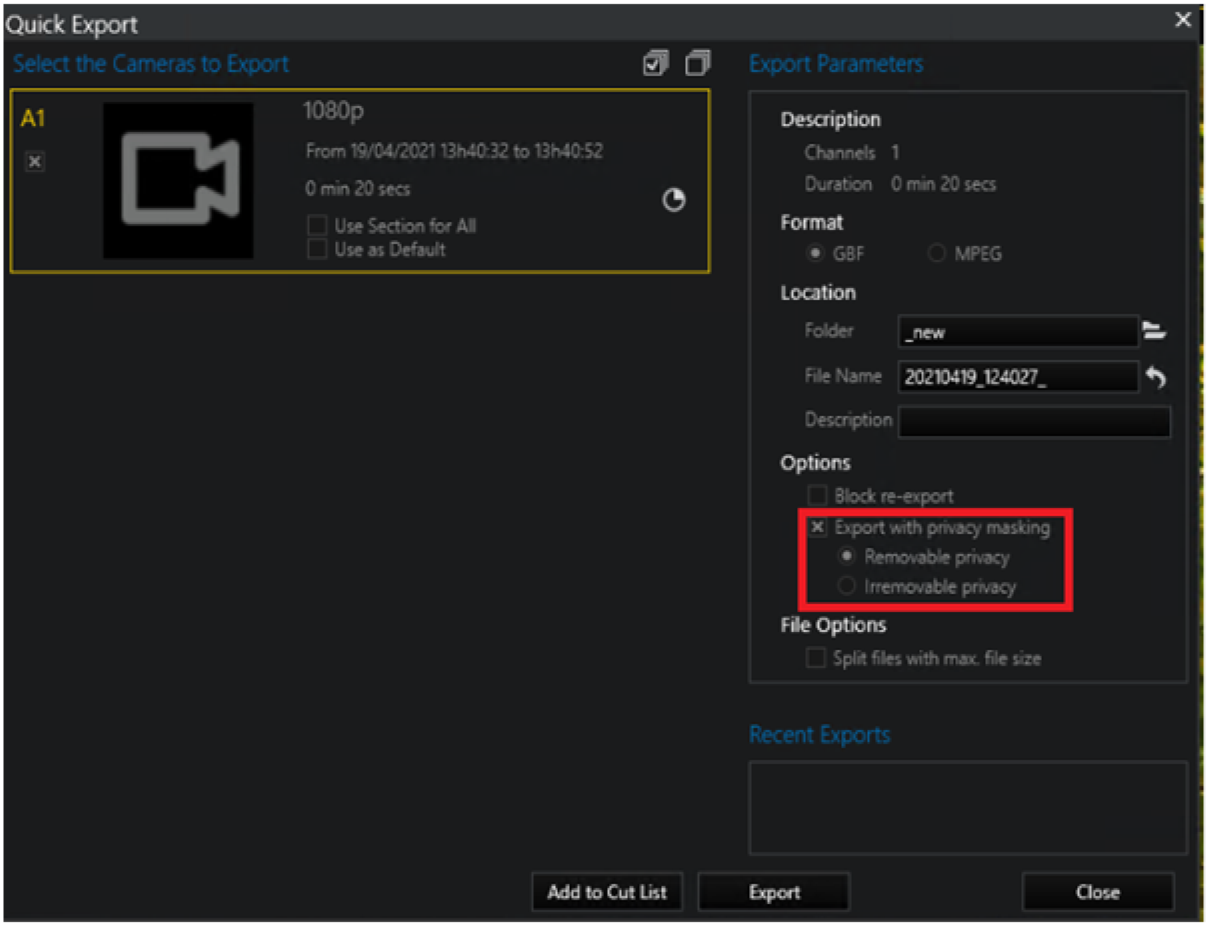
You can also export a sequence of frames from a single camera or multiple cameras using the "Export and Print" option on the Tools Tab. See Tools.

Privacy Export

Removable privacy describes an export which allows, depending on the users permission to see or not see masking in the viewer with the corresponding camera.

If the user is not in possession of the permission Overrride Montion Privacy and Client Privacy and makes an Removable privacy export there will be masking so that the image is not fully visible by the user. If the user is possessing the permission no masking will be seen in the image.

ⓘ **In case of watching the export in G-View " gbf" is an export with and "gcl" without masking.**



With the permission **May disable protection for another user** it is possible to control which user can export removable. By possessing these permission the user is able to decide if he wants to make a Removable privacy export . Depending on the assigned permission of the **Override Montion Privacy and Client Privacy** masking is either visible or not. It is also possible to continue exporting Irremovable privacy so that no one can see the full image in the viewer. If the user is not possessing **May disable protection for another user**permission the export will always be irremovable and the red marked menu is not accessible.

In a Removable privacy export the masking can not be switched on and off by pressing a button. The masking depends on the assigned permission of the user.

The Irremovable privacy export is separately from the permission Override Montion Privacy and Client Privacy. The masking is visible for everyone.

Dragging and Dropping Cameras

Dragging a Camera Item

A camera drag may be initiated from the following places (remember that you make a copy if you drag the content, but you move if you drag the viewer header):

- A camera item in the Camera List.
- A viewer showing a camera — start the drag from the body of the viewer and not from the header.
- A viewer playing a Tour.
- The camera name of a camera listed in the "Cameras Viewed by User" list on a User Detail Card (in a User List).
- A camera in a Site detail card's list of viewed cameras (in a Site List).
- A camera in a Tour detail card's camera list — start the drag on the camera name of a camera entry.
- A Task with a camera attached (Task detail card or task item in the Task List).
- An alarm with a camera attached (Alarm Detail Card or alarm item in the Alarm List)

Dropping a Camera Item

A Camera item may be dropped onto:

- An empty viewer to show the live camera feed.
- A viewer already containing a camera to replace it with the dropped camera.
- A Map to highlight the position of the camera on the map. If the map does not contain the camera, the relevant map will be loaded and the camera selected. The map will automatically pan to centre the highlighted camera. If the current map does not contain the camera, the correct map will be loaded.

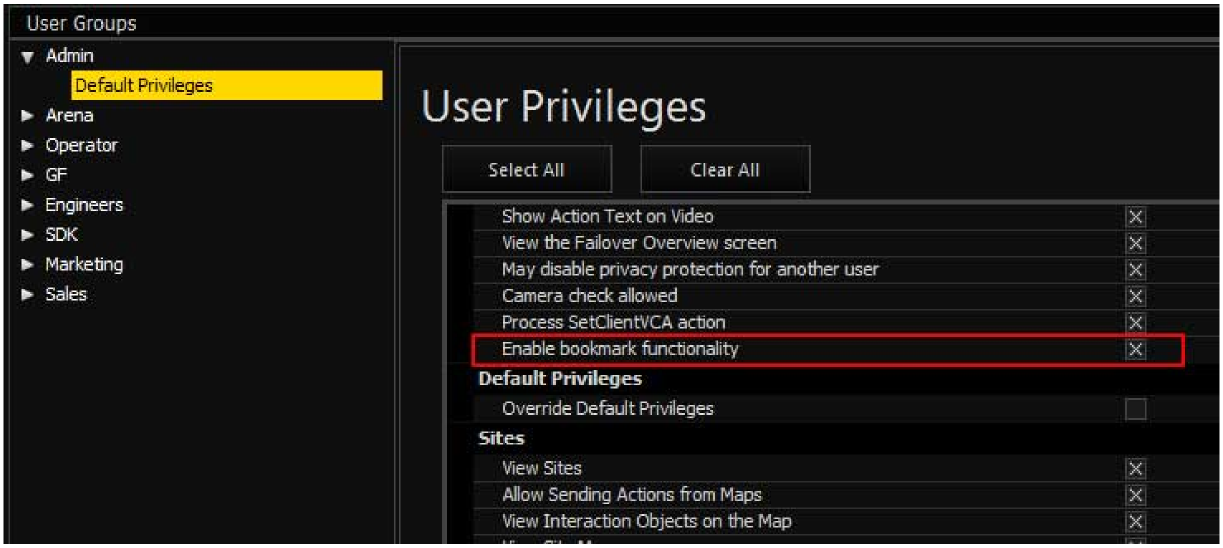
- A Camera List to select the camera and show its detail (if the list contains the camera, i.e. it was not filtered to exclude the camera), otherwise "All Cameras" will be selected.
- A Tour Card which is in edit mode to add the camera to the Tour.
- The Tasks Tab to switch to the Task List, creating a new task and linking it to the camera.
- A new Task Card in the Task List to link the camera to the task.

In the case of a list, if the list contains the dropped camera (i.e. the list was not filtered to exclude the camera) the camera will be selected and the card expanded to show the camera’s detail. Otherwise the List will automatically switch to the "All" tab and the selected camera.

Bookmark Functionality

Prerequisites

- Software version GSIM-Server and -Client > Build 8.2.1
- The user / user group / console must have the **Enable bookmark functionality** permission .



Show Action Text on Video ☒
View the Failover Overview screen ☒
May disable privacy protection for another user ☒
Camera check allowed ☒
Process SetClientVCA action ☒
Enable bookmark functionality ☒

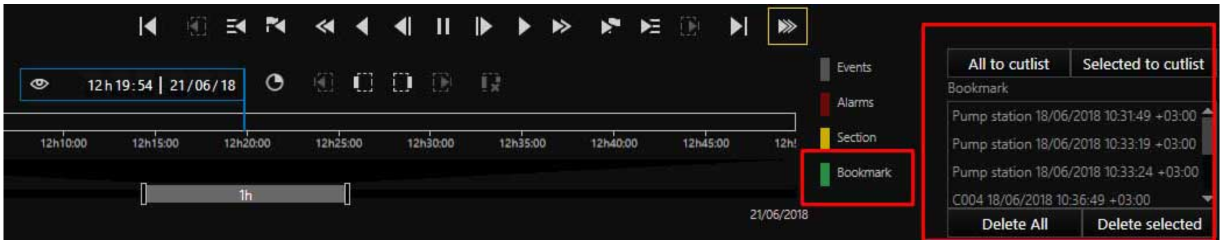
Default Privileges

Override Default Privileges □

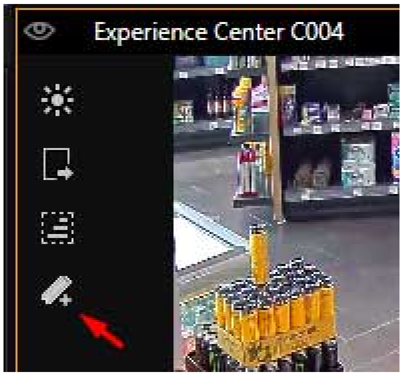
Sites

View Sites ☒
Allow Sending Actions from Maps ☒
View Interaction Objects on the Map ☒

When permission is enabled, the user can see the bookmark list to the right of the timeline:



Pump station 18/06/2018 10:31:49 +03:00
Pump station 18/06/2018 10:33:19 +03:00
Pump station 18/06/2018 10:33:24 +03:00
C004 18/06/2018 10:36:49 +03:00

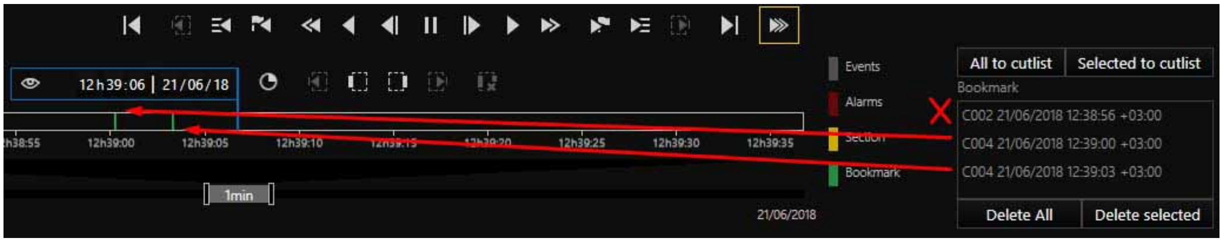


The user can add a new bookmark by clicking on the symbol in the viewer or by pressing Ctrl+B.

All bookmarks are displayed to the user in the bookmark list. Each bookmark contains the camera name and time of the bookmark. The user can jump to the bookmark by double-clicking on an entry in the bookmark list.

To delete a bookmark, select the bookmark and click the **Delete all** or **Delete selected** buttons at the bottom of the bookmark list.

The bookmark list displays bookmarks of all cameras to the user. On the timeline, however, the user can only see bookmarks that refer to the camera currently being viewed:



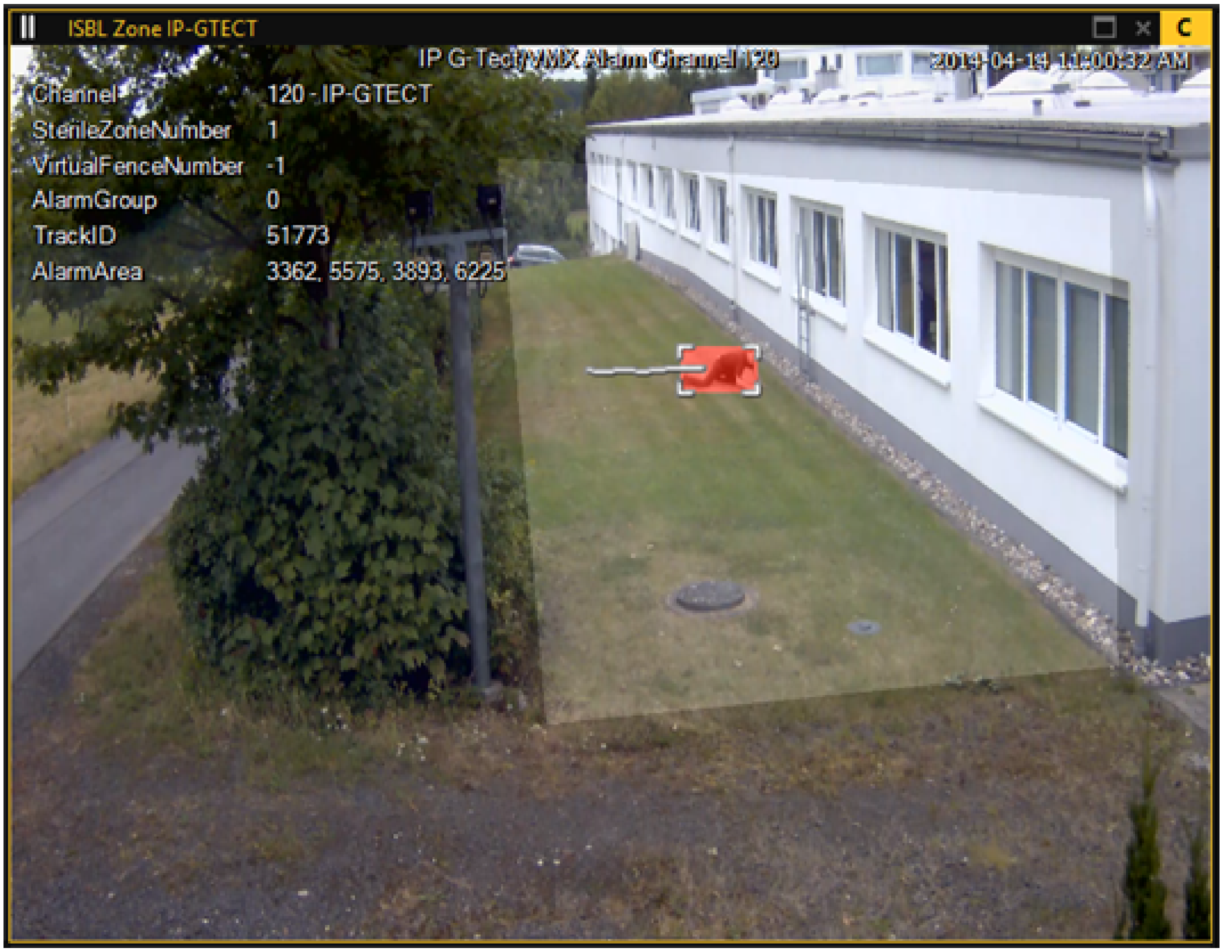
C002 21/06/2018 12:38:56 +03:00
C004 21/06/2018 12:39:00 +03:00
C004 21/06/2018 12:39:03 +03:00

Export to the Cutting List

Bookmarks can be exported to a cut list. This is done using the **All to cutlist** or **Selected to cutlist** buttons in the bookmark list. If no cutting list is currently in edit mode, a new one is created.

OSD for GeViScope Events

This feature is mainly in the Operator Console. With this feature you are able to show the text detail of the current GeViScope Event on the video. While the video is playing (live or recorded footage) the events are cached locally and displayed based on the timestamp of the current frame.



Channel	120 - IP-GTECT
SterileZoneNumber	1
VirtualFenceNumber	-1
AlarmGroup	0
TrackID	51773
AlarmArea	3362, 5575, 3893, 6225

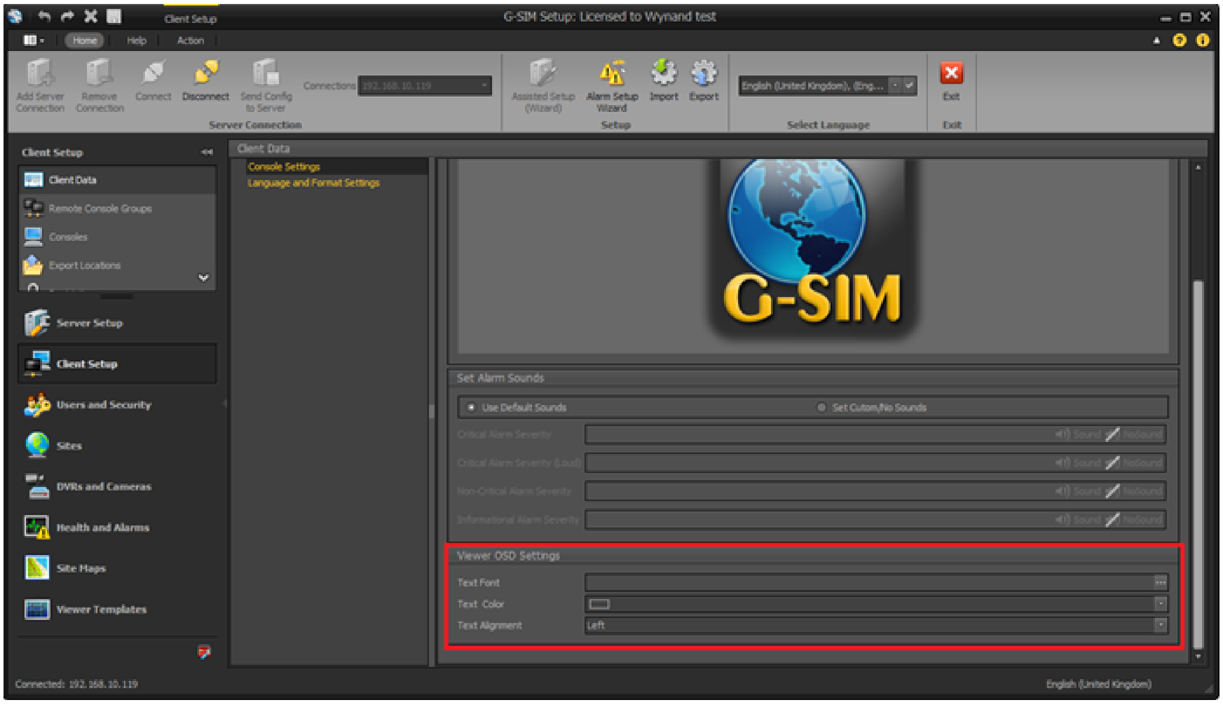
The user can turn this on/off globally by clicking the **Activity Areas** button on the main toolbar in the Operator Console. These button will turn on/off all overlay text and drawing of activity areas and movement lines.

The appearance configuration is found in the Management Console is under **Client Setup** > Client Data. There you can change the Text Font, Font color and Text Alignment.

For the event overlay to work the Agent must be configured to record these events in a central SQL Server.

The settings can be found in the Management Console under **Health and Alarms** > **Health Agents** > **Event Storage** Tab. When you select a NVR from the list the Management Console will retrieve all the configured GeViScope Events so that you can select the ones that need to be saved.
After a change has been made to the selected events, the Agent will subscribe to those selected and the recording of it will start. The Agent saves the events in the

SQL database where the Operator Console can retrieve them when needed. If the events have been retrieved once from the NVR you can force a refresh by clicking on the **Retrieve Events** button.



Connections 192.168.10.119

English (United Kingdom), (Eng...

Set Alarm Sounds

● Use Default Sounds ○ Set Cutom/No Sounds

Critical Alarm Severity

Critical Alarm Severity (Loud)

Non-Critical Alarm Severity

Informational Alarm Severity

Viewer OSD Settings

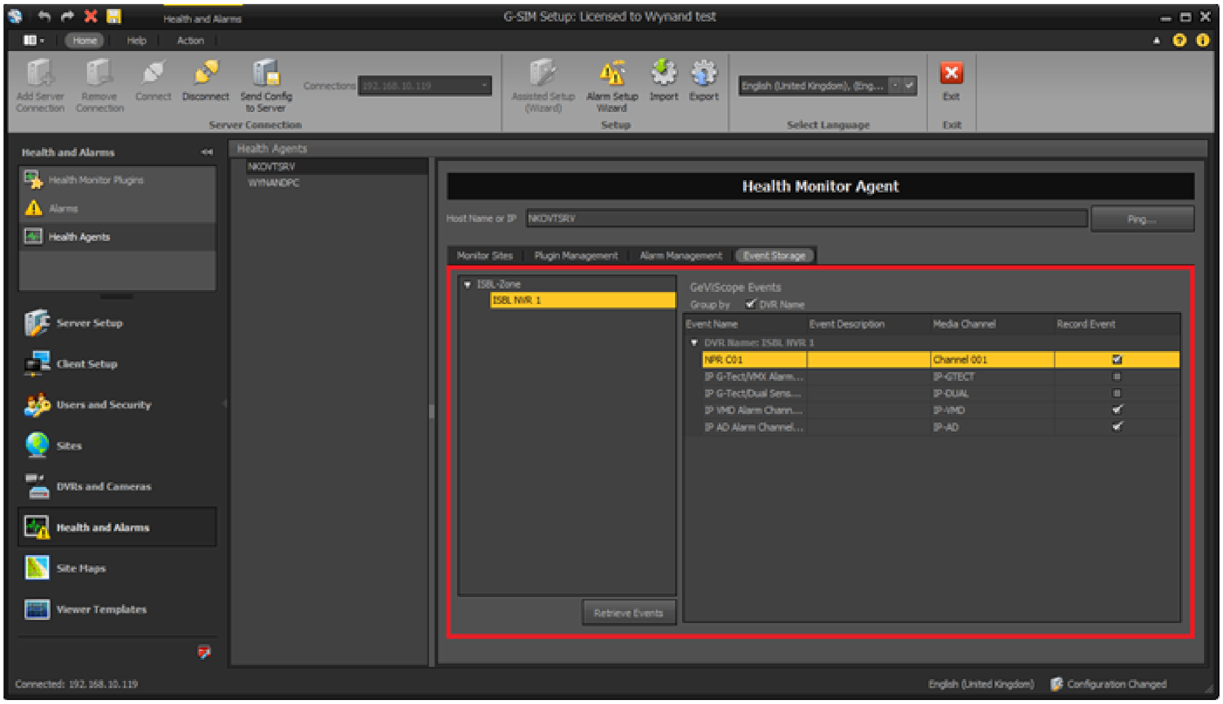
Text Font

Text Color

Text Alignment: Left

Connected: 192.168.10.119

English (United Kingdom)



Connections 192.168.10.119

English (United Kingdom), (Eng...

Health Agents

NKOVTSRV

WYNANDPC

Health Monitor Agent

Host Name or IP: NKOVTSRV

ISBL-Zone

ISBL NVR 1

GeViScope Events

Group by ☑ DVR Name

Event Name	Event Description	Media Channel	Record Event
DVR Name: ISBL NVR 1			
NPR C01		Channel 001	☑
IP G-Tect/VMX Alarm...		IP-GTECT	□
IP G-Tect/Dual Sens...		IP-DUAL	□
IP VMD Alarm Chann...		IP-VMD	☑
IP AD Alarm Channel...		IP-AD	☑

Connected: 192.168.10.119

English (United Kingdom)

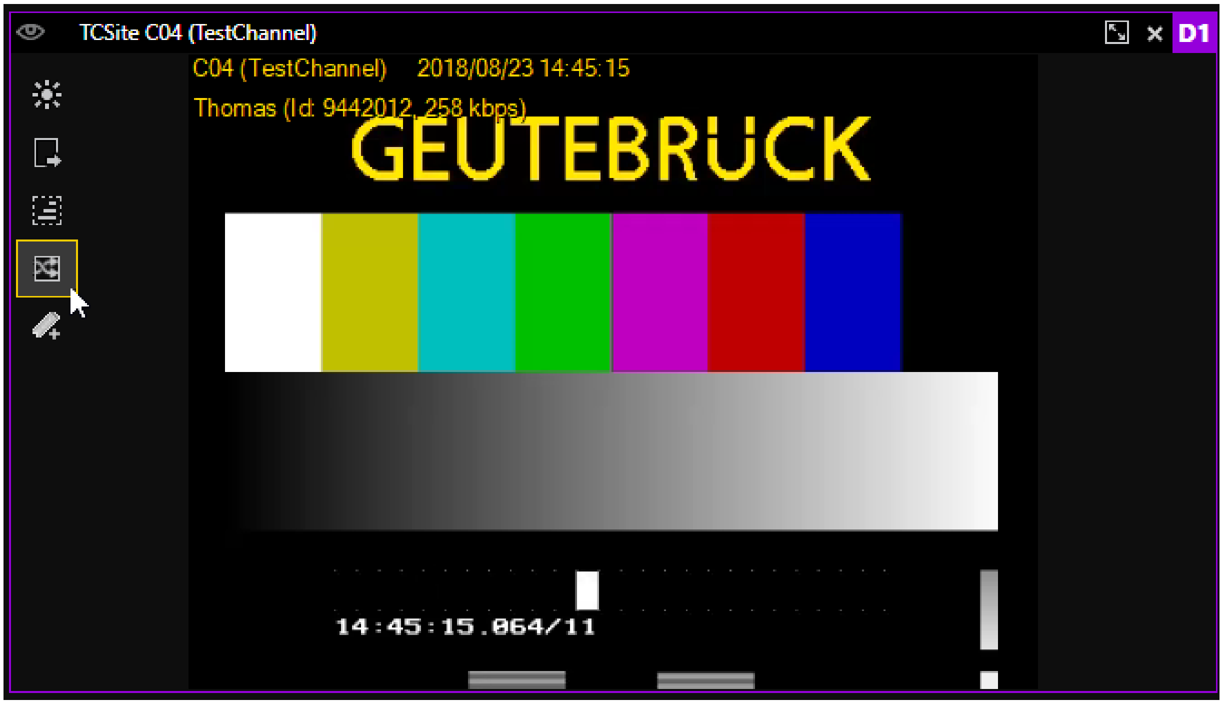
Configuration Changed

TC Viewer Host

Allow Transcoding Viewers (Not required for Dual channels)

There is an ability to display transcoded streams in the Operator Console.

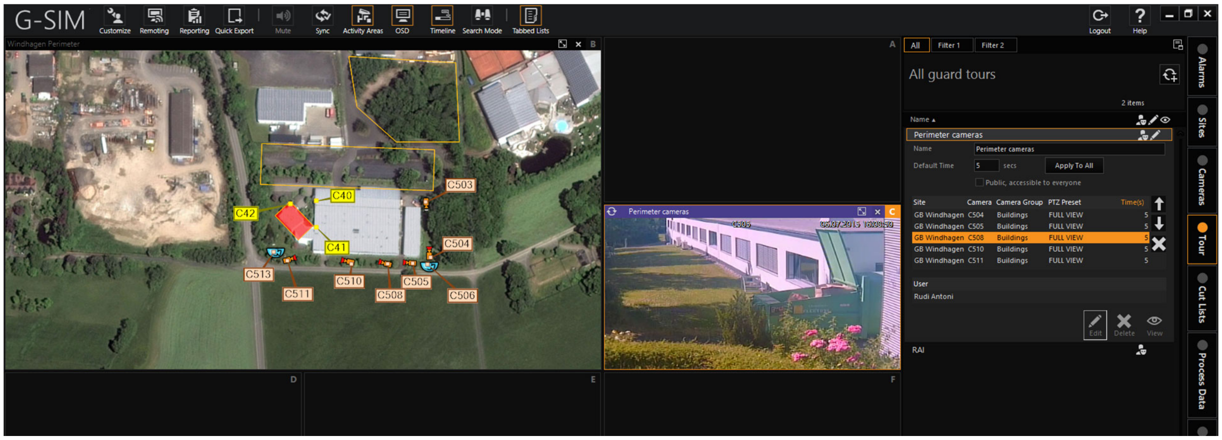
The user can view any camera that was set-up with **Use Transcoding** in the Management Console. If no restrictions were applied, the user will see a button in the Operator Console that can be used to switch the camera between normal and transcoding view.


TCSite C04 (TestChannel)
D1
C04 (TestChannel) 2018/08/23 14:45:15
Thomas (Id: 9442012, 258 kbps)
GEUTEBRUCK
14:45:15.064/11

If a secondary channel was set up and the **Use Transcoding** option was not selected, the user can switch the camera between primary and secondary channel using the button. When a secondary channel exists, the viewer will be displayed using the **Low Resolution** channel by default.

A remote site will always display the remote channel if available.

Guard Tours



All guard tours

2 items

Name ▲

Perimeter cameras

Name: Perimeter cameras

Default Time: 5 secs Apply To All

□ Public, accessible to everyone

Site	Camera	Camera Group	PTZ Preset	Time(s)
GB Windhagen	C504	Buildings	FULL VIEW	5
GB Windhagen	C505	Buildings	FULL VIEW	5
GB Windhagen	C508	Buildings	FULL VIEW	5
GB Windhagen	C510	Buildings	FULL VIEW	5
GB Windhagen	C511	Buildings	FULL VIEW	5

User

Rudi Antoni

RAI

A Guard Tour is a pre-defined sequence of cameras, each of which will be viewed for a defined time in the same viewer. Think of it as a guard walking from point to point. Guard Tours assist a user in general surveillance because a relatively large number of cameras may be monitored easily.

Some examples are: all entrance view cameras for a number of different sites, or a logical sequence of all cameras on a single site to simulate a virtual guard walking through the site.

A GuardTour is either private or public. Private Guard Tours are visible only to their owner whilst public tours are visible to all users who have the privilege to view Guard Tours. Users with the privilege to create Guard Tours may very easily create a list of cameras to view in sequence.

A Guard Tour may be viewed just like a camera by dropping it on a viewer. A Guard Tour may be suspended, which will stop it from looping through the camera list with the last viewed camera in live mode, or the tour may be paused, freezing the last video frame.

The currently viewed camera of a Guard Tour may be dragged to a viewer of its own — the Guard Tour will continue to play in its own viewer.

It is easy to jump to another camera in a Guard Tour's camera list by double clicking on it. The Guard Tour cycle will continue from the newly selected camera.

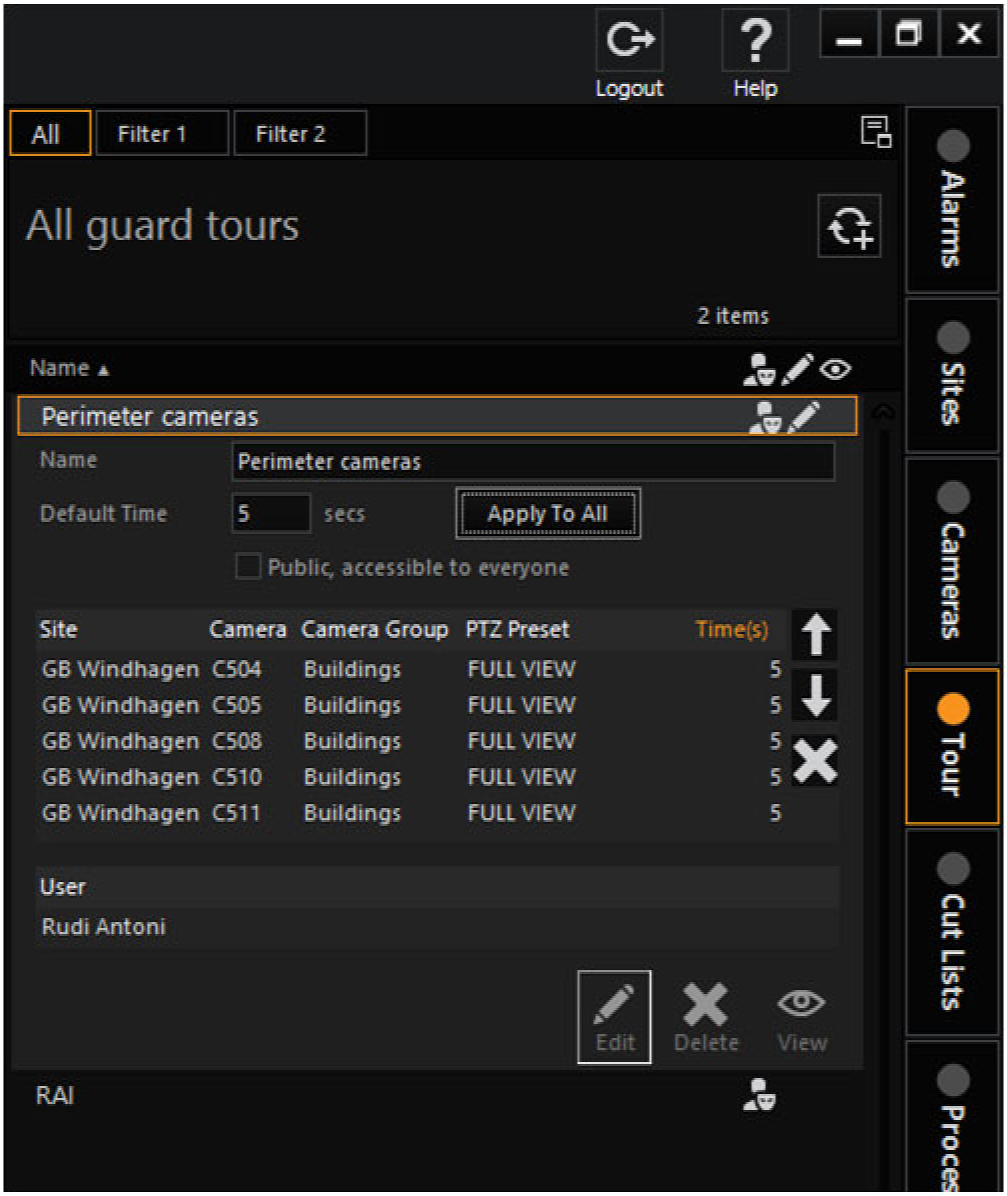
All cameras included in a Guard Tour will be indicated with the Tour status icon in the Camera Lists the moment the Guard Tour is played.

Two important points still need to be mentioned:

1. PTZ preset positions can be used as virtual cameras in Guard Tours — even different presets form the same PTZ in the same Tour.
2. Tours are independent of each other. Thus if two separate users are both viewing the same public Guard Tour, the first could be at camera position 3 while the other is at camera position 7. The only time one Tour would influence another is if they accessed different presets of the same PTZ camera at the same time.

Guard Tour List

The Guard Tour List gives you quick access to all the available tours. Each row in the list represents one tour, with the Guard Tour name as identifier and sorting field. State icons indicate whether a tour is private (for use by the current user only) and which tours are currently being viewed.



All guard tours

2 items

Name ▲

Perimeter cameras

Name: Perimeter cameras

Default Time: 5 secs

□ Public, accessible to everyone

Site	Camera	Camera Group	PTZ Preset	Time(s)
GB Windhagen	C504	Buildings	FULL VIEW	5
GB Windhagen	C505	Buildings	FULL VIEW	5
GB Windhagen	C508	Buildings	FULL VIEW	5
GB Windhagen	C510	Buildings	FULL VIEW	5
GB Windhagen	C511	Buildings	FULL VIEW	5

User

Rudi Antoni

RAI

List Layout And Buttons

List Filter The Guard Tour filter is very powerful in what it allows you to filter on. It is simple, for example, to search for Guard Tours which contain a specific camera. See **Filtering** for more on how to filter.

Dock List This function allows the Guard Tour List to be duplicated in any viewer. After clicking it the available viewer windows will be highlighted with the corresponding short-cut key that may be pressed to dock the list in the designated viewer (See **Main Interface**).

Guard Tour Status Indicators

The following status icons may be displayed as part of a tour item in the Guard Tour List:

Icon	Description
👤	Private tour
👁	Observed
👁	Observed by me
✎	Edit mode

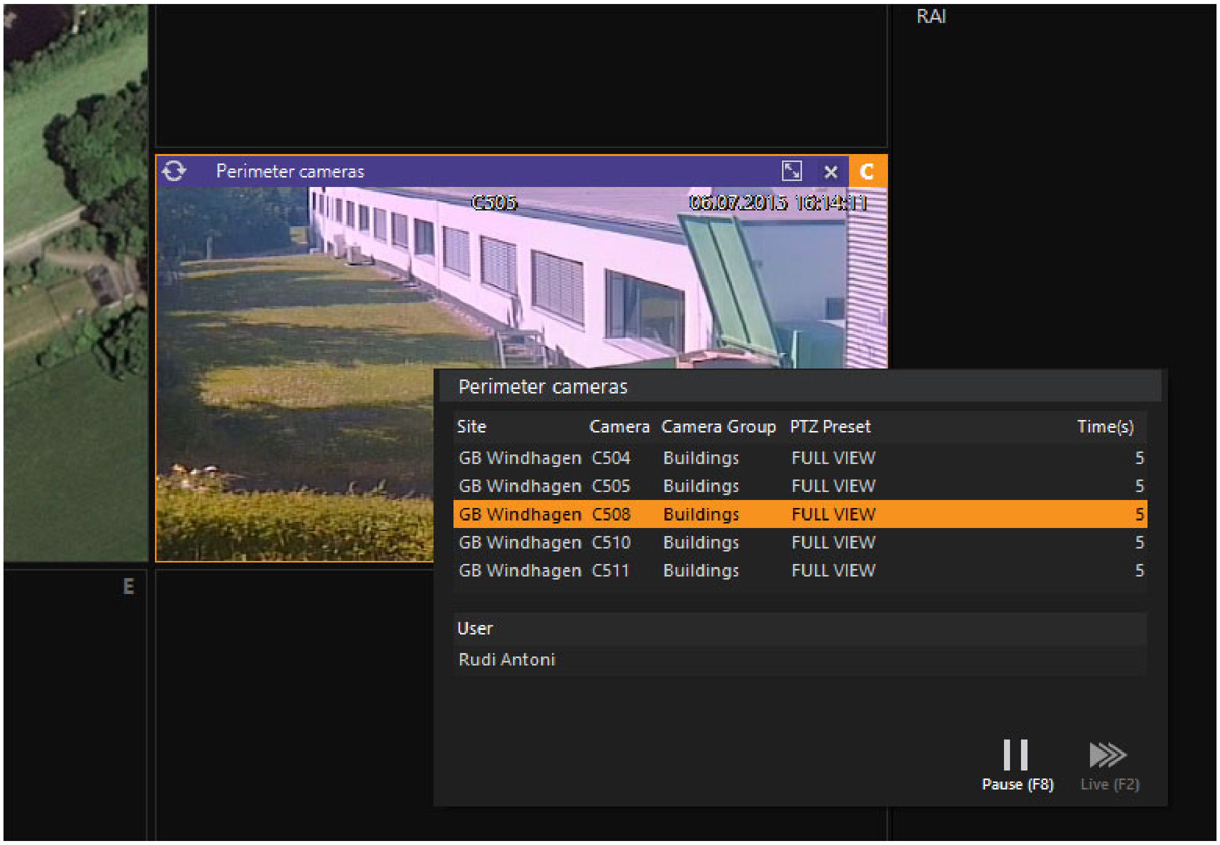
Private Tour The Guard Tour is private, meaning it is only visible to you (who created it).

Viewed The Guard Tour is currently being viewed by at least one other person. By selecting the tour you will be able to see which users are currently viewing this tour.

Viewed by me You (the logged in user) are viewing this Guard Tour.

Edit mode The Guard Tour is in edit mode and may be modified. All cameras dropped on the Guard Tour tab will be added to this Guard Tour. This is the easiest way of adding cameras to a Guard Tour — you can drag a camera from the camera list or even a viewer onto the Guard Tour tab, and it gets added automatically.

Guard Tour Detail



Perimeter cameras

Site	Camera	Camera Group	PTZ Preset	Time(s)
GB Windhagen	C504	Buildings	FULL VIEW	5
GB Windhagen	C505	Buildings	FULL VIEW	5
GB Windhagen	C508	Buildings	FULL VIEW	5
GB Windhagen	C510	Buildings	FULL VIEW	5
GB Windhagen	C511	Buildings	FULL VIEW	5

User
Rudi Antoni

The detail of a tour will be displayed when an item is selected in the Guard Tour List, or if a user right clicks on a playing tour in a viewer. When a tour is not in edit mode, its detail card consists mainly of a list of cameras with their timings. If the tour is playing, the current camera will be highlighted in the list. You can jump to any other position in the tour by double clicking on another camera in the list.

Camera Organiser The camera organizer is only visible if the tour is in edit mode. These buttons allow you change a camera's position in the list or to remove it from the tour.

"Viewed By" List If the tour is viewed by one or more users, this list will show all the users currently viewing the tour.

Users need the "Edit Public Guard Tours" privilege to be able to create public tours.

Guard Tour Actions

The following actions are highlighted.

Pause Tour This is available when you right-click on the tour. It will suspend the tour when clicked the first time, showing the current camera live but not proceeding to the next camera. When clicked a second time the actual live streaming will be paused, freezing the current frame. (See **Controlling Guard Tours**.) Click the Guard Tour Live button to commence the tour.

Tour Live This button will become visible after a guard was suspended or paused. When clicked, the tour will continue with normal playing, usually skipping directly to the next camera.

Creating and Modifying Guard Tours

To avoid frustration and confusion, remember that a Tour can only be edited or deleted if it is not currently being viewed.

Settings	Description
⟳+	Creating a new tour
↑ ↓	Changing the order of cameras
✕	Removing a camera
✎ Edit	Editing a tour
✕ Delete	Deleting a tour
👁 View	Displaying a tour in the viewer

Creating a New Guard Tour

To create a new Guard Tour, click the New Guard Tour button in the toolbar at the top of the Guard Tour List. The detail card of the tour will expand and the Guard Tour will be automatically in Edit Mode, allowing the user to enter a name for the tour and to mark it as public (if other users may use it as well). Cameras may now be added to the tour as explained below. Note that PTZ pre-set positions can be use as virtual cameras in Guard Tours.

Note that the Edit button is a toggle — you press it both to enter and to leave edit mode.

Adding Cameras to a Guard Tour

Cameras may be added to a Guard Tour which is in edit state as follows:

- Drag a camera from a viewer, the Camera List or a map and drop it on the Guard Tour, or on the Guard Tour Tab. It is thus possible to put the Guard Tour in edit mode, go to the Camera List and drag cameras from the list to the Guard Tour Tab.
- All Camera Detail Cards (e.g. in the Camera List) will contain an Add to Guard Tour button if a Guard Tour is in edit mode. For example you may put a Guard Tour in edit mode, right click on a map camera and add it to the Tour by clicking the Add to Guard Tour button. (Cameras may also be dragged from a map to a Tour which is in edit mode.)
- PTZ cameras can have Presets added to Guard Tours. This is done by taking control of the PTZ, clicking on its Preset drop-down button, and dragging a Preset onto the Tour. Important: see the note below on using PTZ Presets in Guard Tours.
- You need not use a PTZ preset if you don't care which position the PTZ is in when the Guard Tour reaches it (e.g. if all the Tour does is to show whether the camera is active or not). In such a case simply drag the PTZ viewer onto the Guard Tour, which will display "- current pos - " in the PTZ Preset column. You do not need to be in control of the PTZ to do this.

Note on Using PTZ Presets in Guard Tours

Please note that while use of Presets will greatly ease the use of PTZs in Tours, this also implies careful consideration: what to do if different Guard Tours use different Presets on the same PTZ?

The solution we have implemented is that whichever Guard Tour currently has control of the camera keeps that control for as long as that Guard Tour is viewing a preset. Once that Guard Tour has moved on, other Guard Tours can use the camera. Not doing so would mean that the camera could end up spinning around as different Guard Tours try to take control of it in quick succession.

By the same token, a Guard Tour will not move a PTZ if someone is currently controlling the PTZ.

Camera Timings

Camera timings are in seconds, and be changed for any camera in a Guard Tour. Put the Guard Tour in edit mode and enter new timings directly in the appropriate field in the list of cameras. The default timing is 30 seconds per camera. You can also set all cameras to the same timing in one step. Some people may refer to this as the dwell time or camera cycle time.

Ordering Cameras in a Guard Tour

If a Guard Tour is in edit mode, the cameras may be ordered by moving the selected camera up or down in the list, using the two buttons on the right of the list. Click the Remove Camera button to remove a camera from the Guard Tour.

Editing an Existing Guard Tour

A Guard Tour must be in Edit Mode to be able to modify it — click the Edit Guard Tour button to activate this mode. Only one Guard Tour can be in edit mode at any time and it will be indicated by the "edit" icon in the Guard Tour header. Putting a Guard Tour in Edit Mode will take any other editable tour out of this mode. Whilst in edit mode, all the options apply as described above for a new Guard Tour: Cameras may be added, removed, ordered or the name or visibility (public or private) of the Guard Tour may be changed.

Taking a Guard Tour out of Edit Mode

A Guard Tour will be taken out of edit mode if:

- The Edit Guard Tour button is clicked again (released)
- Any other tour is selected in the Guard Tour List
- Edit Mode is activated for another Guard Tour — only one tour may be edited at a time.

Deleting a Guard Tour

In the case of a public Guard Tour (which may be in use by another user), the Guard Tour will be deleted from the server and will not be available to any users who log in after the deletion. Current logged in users who have the Guard Tour in their lists will be able to use it until they log out.

Controlling Guard Tours

Suspending and Pausing a Playing Guard Tour

A playing Guard Tour may be paused in two stages: The first pause (called suspending the Guard Tour) will stop the Guard Tour cycle, but the current camera will still be Live. A label in the left corner of the viewer header will clearly mark the Guard Tour as "Suspended". A second pause will pause the live streaming of camera footage, showing only the static frame from when the pause occurred. This will be indicated as "Paused" in the viewer header.

Guard tours may be paused by clicking the Pause Guard Tour button on the pop-up detail card you get when you right-click on the viewer, or by using the F8 hot-key. A Guard Tour must have the input focus (orange frame around the viewer) to accept the hot-key.

To continue normal viewing of a suspended or paused Guard Tour, click the Guard Tour Live button on the detail card, or press the F2 (play) hot-key.

Skipping Cameras while Viewing a Guard Tour

The current camera may be skipped by pressing the F2 (play) hot-key during normal Guard Tour playing. If the Guard Tour is suspended or paused, pressing F2 will continue the Guard Tour loop.

Jumping Backwards or Forwards in the Guard Tour Sequence

You may jump to any camera in the Guard Tour List by double-clicking the camera. Open the Guard Tour Detail Card by right-clicking in the viewer where it is playing. The current camera will be highlighted — double-click on any other camera to continue viewing from there. This is only the case with the list attached to the viewer, and not the tab list on the side of the screen.

Viewing a Guard Tour Camera in its own Viewer

To continue viewing the current Guard Tour camera in its own viewer, simply drag the video footage (viewer body) to another viewer. The Guard Tour will continue playing and the dragged camera will be cloned in the other viewer.

The cameras listed in a Guard Tour Detail Card are items that may be dragged, so even if it is not the current camera displayed, you may drag it from the Guard Tour's camera list to another viewer. Make sure you drag the camera and not the site of the camera, in which case you will end up with a map of the camera location! This last point is quite important, and easy to get wrong.

Audit Logging of Guard Tour Actions

All Guard Tour actions are stored in the G-SIM Audit Log. It is possible for a user with the necessary privileges to see which Guard Tours were viewed by other users.

Dragging and Dropping Guard Tours

Dragging a Guard Tour Item

A Guard Tour may be dragged from:

- A Guard Tour item in the Guard Tour List.
- A viewer playing a Guard Tour — start the drag from the header of the viewer and not from the body, in which case the current camera will be selected and not the Guard Tour itself.
- The Guard Tour name of a tour listed in the "Viewed Guard Tours" list on a Camera Detail Card (in a Camera List).
- The Guard Tour name of a tour listed in the "Guard Tours Viewed by User" list on a User Detail Card (in a User List).

Dropping a Guard Tour Item

A Guard Tour item may be dropped onto:

- An empty viewer to play the tour in this viewer.
- A viewer containing another Guard Tour, a camera (video stream) or a map to replace the viewer content with the Guard Tour.
- A Guard Tour List to select the dragged tour and show its detail (if the list contains the Guard Tour, i.e. the list is not filtered).
- A viewer linked to a camera
- A viewer displaying a map

Starting a drag operation from the header of a Guard Tour viewer will drag the tour itself, i.e. move it to a different viewer). Starting a drag in the body (video area) of a Guard Tour will drag the current camera. This is very useful if a user wants to continue viewing a certain camera — just drag the camera to a new viewer, and the Guard Tour will continue playing in the original viewer, while you can work with the footage of one particular camera.

Cut Lists

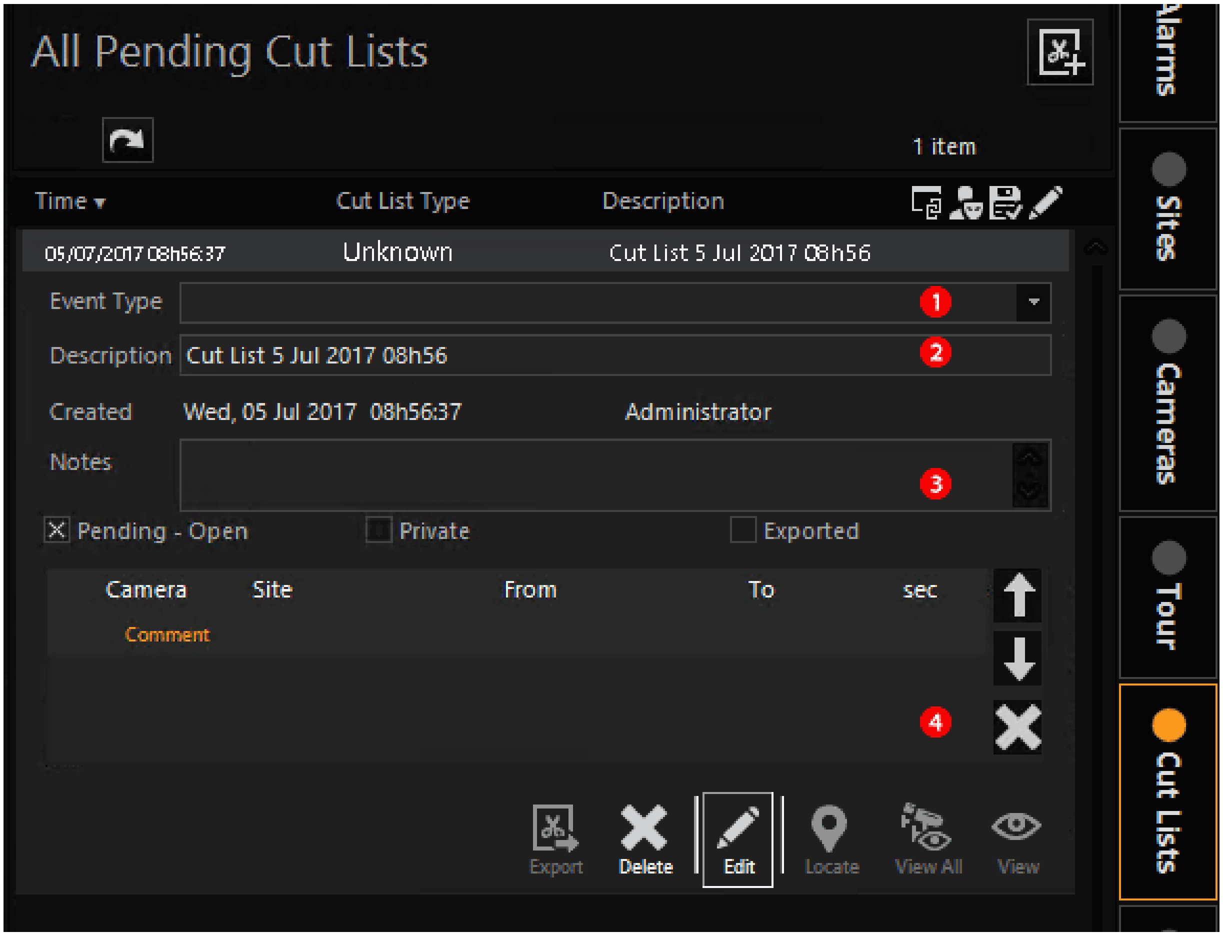
G-SIM offers you the following functions for cut lists:

- Creation
- Export
- Editing
- Replay

It is also possible to let G-SIM generate auto cut lists for MOS.

Creating Cut Lists

In G-SIM, cut lists can be created and exported with ease. Clicking on the ✂ icon opens the dialog for creating a cut list.


All Pending Cut Lists

1 item

Time ▾	Cut List Type	Description
05/07/2017 08h56:37	Unknown	Cut List 5 Jul 2017 08h56

Event Type

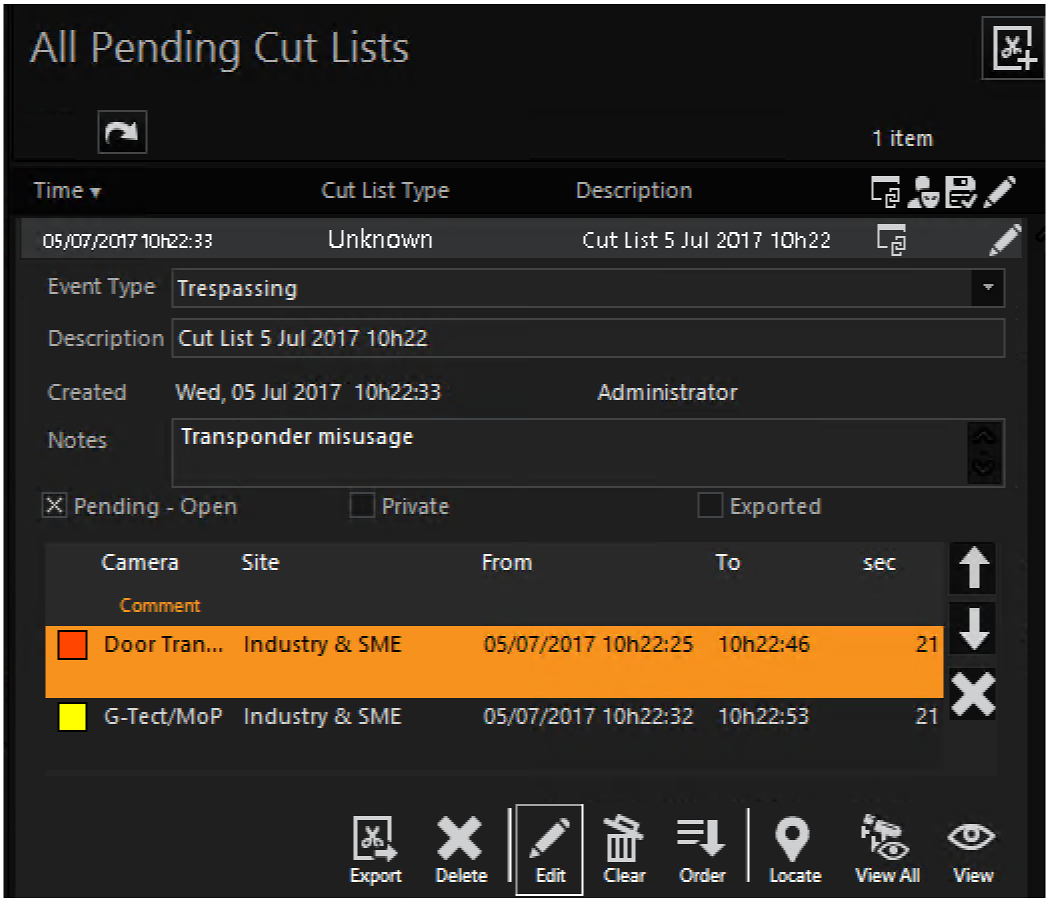
Description: Cut List 5 Jul 2017 08h56

Created: Wed, 05 Jul 2017 08h56:37 Administrator

Notes

☒ Pending - Open ☐ Private ☐ Exported

Settings		Description
1	Event type	Open the selection and select one of the event types defined in Management Console.
2	Description	A general name with counter, date and time of creation is created by default as description. You can edit this information.
3	Notes	Add explanatory notes (optional).



All Pending Cut Lists

1 item

Time ▾	Cut List Type	Description
05/07/2017 10h22:33	Unknown	Cut List 5 Jul 2017 10h22

Event Type: Trespassing

Description: Cut List 5 Jul 2017 10h22

Created: Wed, 05 Jul 2017 10h22:33 Administrator

Notes: Transponder misusage

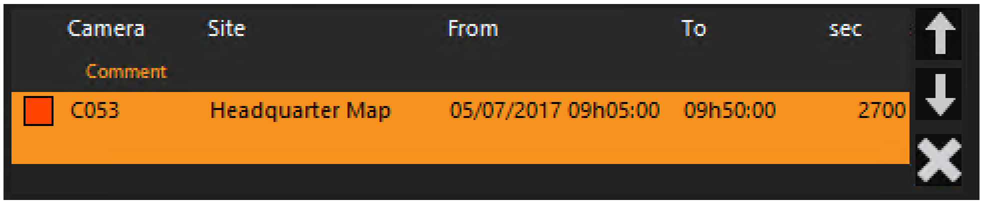
☒ Pending - Open ☐ Private ☐ Exported

	Camera	Site	From	To	sec
	Comment				
🟥	Door Tran...	Industry & SME	05/07/2017 10h22:25	10h22:46	21
🟨	G-Tect/MoP	Industry & SME	05/07/2017 10h22:32	10h22:53	21

Now drag one or more viewers into the field 4. The order can be changed using the arrows, affect playback and export. An accidentally created entry can be deleted with x.

New entries always have the current time as begin time and an end time of 20 seconds later. The first column of the entry contains the camera name. This is followed by the name of the location. The next two columns contain the begin time and the end time and the last column contains the length of the recording. All media channels are color-coded so they can be found quickly in the viewer.

The media channels that should be added to the cut list can be edited using the time line so that the correct point in time and length are used. A corresponding entry could be as follows:



	Camera	Site	From	To	sec
	Comment				
🟥	C053	Headquarter Map	05/07/2017 09h05:00	09h50:00	2700

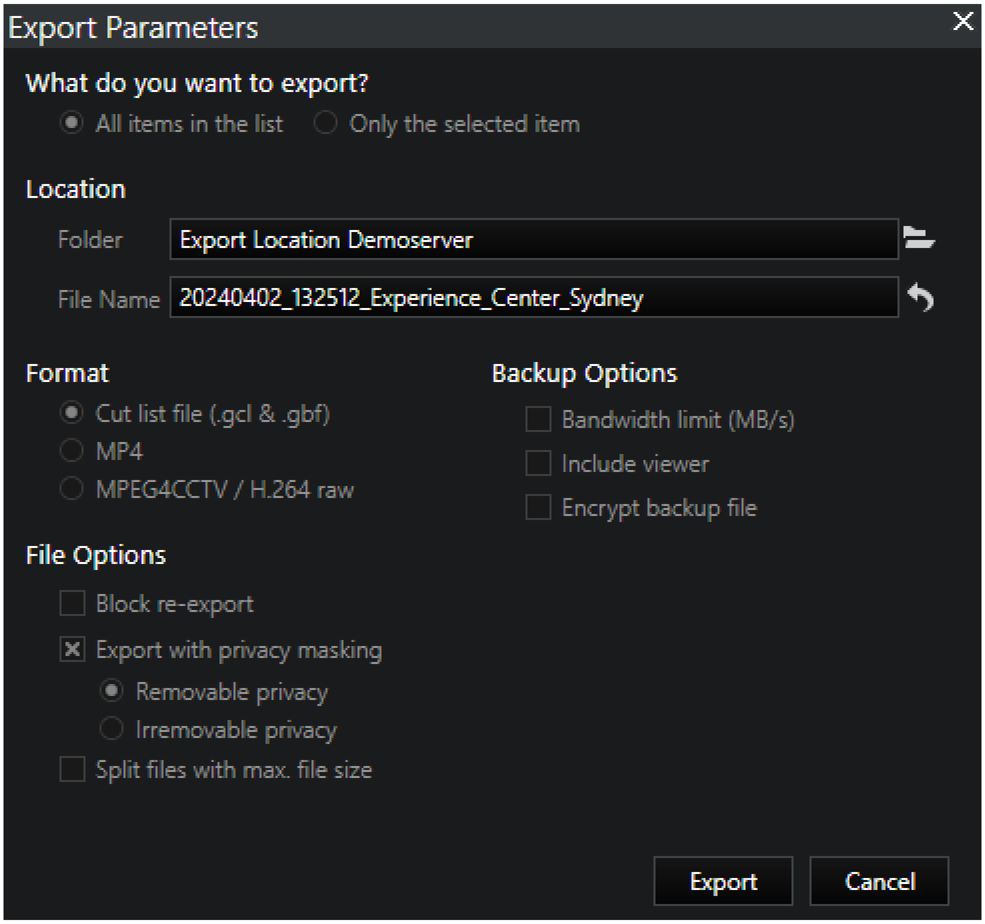
In the cut list dialog, you will find a row of buttons:

Buttons	Description
Export	Opens the dialog for the **cut list export**
Delete	Deletes the entire cut list
Edit	Edits the cut list data
Clear	Deletes all entries in the cut list
Order	Orders the entries chronologically
Locate	Shows the active camera on the map
View all	Shows all entries in the selected viewer
View	Shows the marked entry in the selected viewer

Cut List Export

How to Export a Cut List

1. Click on the **Cut Lists** tab. The cut lists appear.
2. Click on the wished cut list item and then on the ✂ button. The **Export Parameters** dialog window opens.



Export Parameters

What do you want to export?

● All items in the list ○ Only the selected item

Location

Folder: Export Location Demoserver

File Name: 20240402_132512_Experience_Center_Sydney

Format

● Cut list file (.gcl & .gbf)

○ MP4

○ MPEG4CCTV / H.264 raw

Backup Options

□ Bandwidth limit (MB/s)

□ Include viewer

□ Encrypt backup file

File Options

□ Block re-export

☒ Export with privacy masking

● Removable privacy

○ Irremovable privacy

□ Split files with max. file size

3. Enter the necessary **Export Parameters** (for detailed information on the different parameters see **Parameters**).
4. Click on **Export**.

Parameters

What do you want to export?

Parameter	Description
All items in the list	All entries will be exported to the list.
Only the selected item	Only the selected item is exported to the list.

Location:

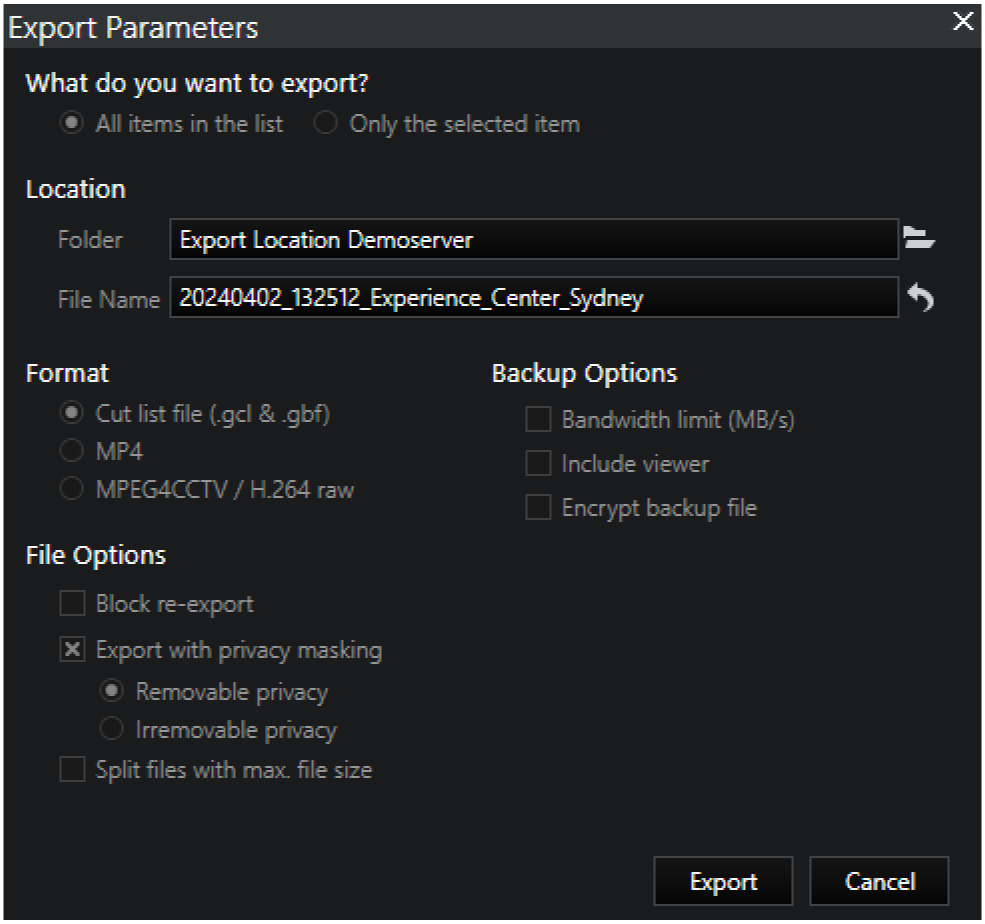
Parameter	Description
Folder	Here the folder must be specified where the export will be saved.
File name	Name of the export file.

Format:

Parameter	Description
Cut list file	Export as cut list file.
MP4	Export as a file in MP4 format.
MPEG4CCTV / H.264 raw	Export as a file in MPEG4CCTV format.

The following parameters vary depending on the selected format.

Cut list file



Export Parameters

What do you want to export?

● All items in the list ○ Only the selected item

Location

Folder: Export Location Demoserver

File Name: 20240402_132512_Experience_Center_Sydney

Format

● Cut list file (.gcl & .gbf)

○ MP4

○ MPEG4CCTV / H.264 raw

Backup Options

□ Bandwidth limit (MB/s)

□ Include viewer

□ Encrypt backup file

File Options

□ Block re-export

☒ Export with privacy masking

● Removable privacy

○ Irremovable privacy

□ Split files with max. file size

File Options:

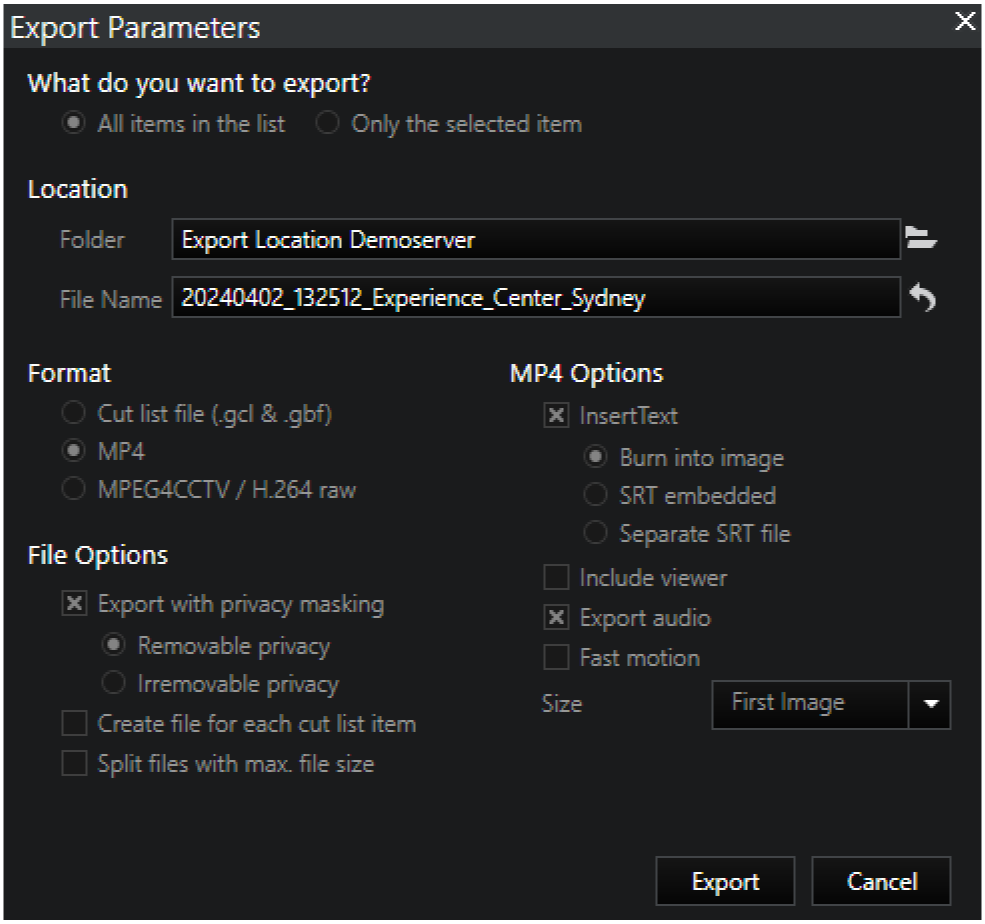
Parameter	Description
Block re-export	Prevents re-exporting.
Export with privacy masking	Exports the file with privacy masking. You have two options: • **Removable privacy**: Active privacy masking which can be removed later. • **Irremovable privacy**: Active privacy masking which cannot be removed later.

Parameter	Description
Split files with max. file size	Splits files with a maximum size for the export. To split files for export, enable the **Split files with max. file size** checkbox and enter a **Max. file size [MB]**. For detailed information see **Export Video Event**.

Backup Options:

Parameter	Description
Bandwidth limit (MB/s)	Limits the bandwidth.
Include viewer	Export includes G-View in viewer mode and VLC player.
Encrypt backup file	The back up file is encrypted.

MP4



Export Parameters

What do you want to export?

● All items in the list ○ Only the selected item

Location

Folder: Export Location Demoserver

File Name: 20240402_132512_Experience_Center_Sydney

Format

○ Cut list file (.gcl & .gbf)
● MP4
○ MPEG4CCTV / H.264 raw

File Options

☒ Export with privacy masking
● Removable privacy
○ Irremovable privacy
□ Create file for each cut list item
□ Split files with max. file size

MP4 Options

☒ InsertText
● Burn into image
○ SRT embedded
○ Separate SRT file
□ Include viewer
☒ Export audio
□ Fast motion

Size: First Image

File Options:

Parameter	Description
Export with privacy masking	Exports the file with privacy masking. You have two options: • **Removable privacy**: Active privacy masking which can be removed later. • **Irremovable privacy**: Active privacy masking which cannot be removed later.
Create file for each cut list item	Instead of writing all entries to a file, when this option is selected,

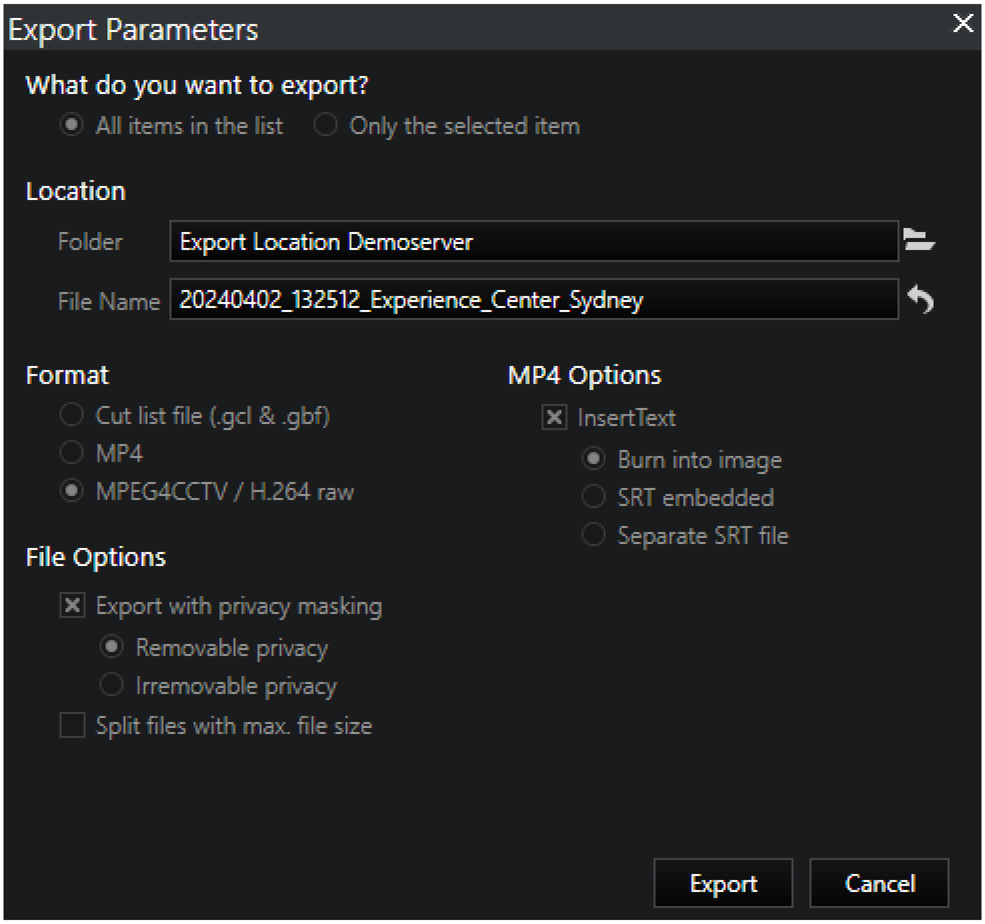
Parameter	Description
	a file is created for each entry.
Split files with max. file size	Splits files with a maximum size for the export. To split files for export, enable the **Split files with max. file size** checkbox and enter a **Max. file size [MB]**. For detailed information see **Export Video Event**.

MP4 Options:

Parameter	Description
InsertText	Inserts text into file. You have three options here: • **Burn into image**: Text is firmly integrated in the image. • **SRT embedded**: Subtitles are embedded in the file. • **Separate SRT file**: Subtitles are stored in a separate file.
Include viewer	Export includes G-View in viewer mode and VLC player.
Export audio	Export file includes audio.
Fast motion	Exports file in fast motion to reduce file size.
Size	You have several options regarding the size: • **First Image** (Resolution of the first image): The resolution of the first image determines the resolution of the backup file. • **Split**: The resolution of the first

Parameter	Description
	image determines the resolution of the backup file. If the resolution changes in the selected time frame, for example due to an event recording with higher resolution, the backup file is split each time the resolution is changed. • **UHD** • **Full HD** • **HD** • **4CIF** • **CIF**

MPEG4CCTV / H.264 raw



Export Parameters

What do you want to export?

● All items in the list ○ Only the selected item

Location

Folder: Export Location Demoserver

File Name: 20240402_132512_Experience_Center_Sydney

Format

○ Cut list file (.gcl & .gbf)
○ MP4
● MPEG4CCTV / H.264 raw

MP4 Options

☒ InsertText
● Burn into image
○ SRT embedded
○ Separate SRT file

File Options

☒ Export with privacy masking
● Removable privacy
○ Irremovable privacy
□ Split files with max. file size

File Options:

Parameter	Description
Export with privacy masking	Exports the file with privacy masking. You have two options: • **Removable privacy**: Active privacy masking which can be removed later. • **Irremovable privacy**: Active privacy masking which cannot be removed later.
Split files with max. file size	Splits files with a maximum size for the export.

Parameter	Description
	To split files for export, enable the **Split files with max. file size** checkbox and enter a **Max. file size [MB]**. For detailed information see **Export Video Event**.

MP4 Options:

Parameter	Description
InsertText	Inserts text into file. You have three options here: • **Burn into image**: Text is firmly integrated in the image. • **SRT embedded**: Subtitles are embedded in the file. • **Separate SRT file**: Subtitles are stored in a separate file.

i **MPEG files can be authenticated easily (see** Authentication of Exported Files **for detailed information).**

Replay a Cut List

After a cutlist was created, several methods exist to play the list.

1) Dragging the whole list to a viewer (typically from the card header):

The first item in the list will start to play, and this item will be marked in the list with 'n coloured circle (typically a red circle if it is the first item that is viewed). The circle indicates that the whole list will be played - when the end of the first item is reached the circle will move to the next row. The background colour of the viewer panel name (e.g. "A") will also change to the same colour as the indicator circle in the list. These matching colours indicate that the list item is synced with the viewer. The header colour of the viewer will change to green to indicate that it is playing a whole list - it may switch to a different camera when the item changes.

It is the same as playing a guard tour, except it is not live data. After the last item in the list is played, the play loop will restart from the first item.

A green link status symbol in the tabbed list of all cut lists will indicate that this specific cut list contains items linked to viewers.

Right-clicking with the mouse on the viewer will show the cut list card, and just as in the case of a guard tour being played a user may click on an item to jump to it - the loop will continue from here.

2) Dragging an item in the list to a viewer:

Here two scenarios exist:

- If it is the first item in the list to be displayed in a viewer, the whole list will be looped as described above, but starting from the dragged item. When the end of the item is reached it will move to the next item. When the end of the list is reached it will restart from the first item. A green viewer header and a circle indicator in the list will indicate that a whole list is being played.
- If it is not the first item in the list to be linked to a viewer, the viewers will no longer loop through all items in the list - the previous linked viewer will stay linked to the item it is currently playing, and the newly dragged item will be linked to the viewer where it was dropped. The two viewers will now have different background colours for the panel names (e.g. "A" & "B"). The first panel's header will also not be green anymore because it does not loop through a list. The circle indicators in the list will change to squares to show it is not looping anymore.

3) Viewing all items in a cut list:

The "Show all items" button on the cut list card will automatically drop all items in the cut list on viewers - if the list contains 3 items, 3 viewers will be used. After clicking the button the user is presented with an overlay showing all the panel names.

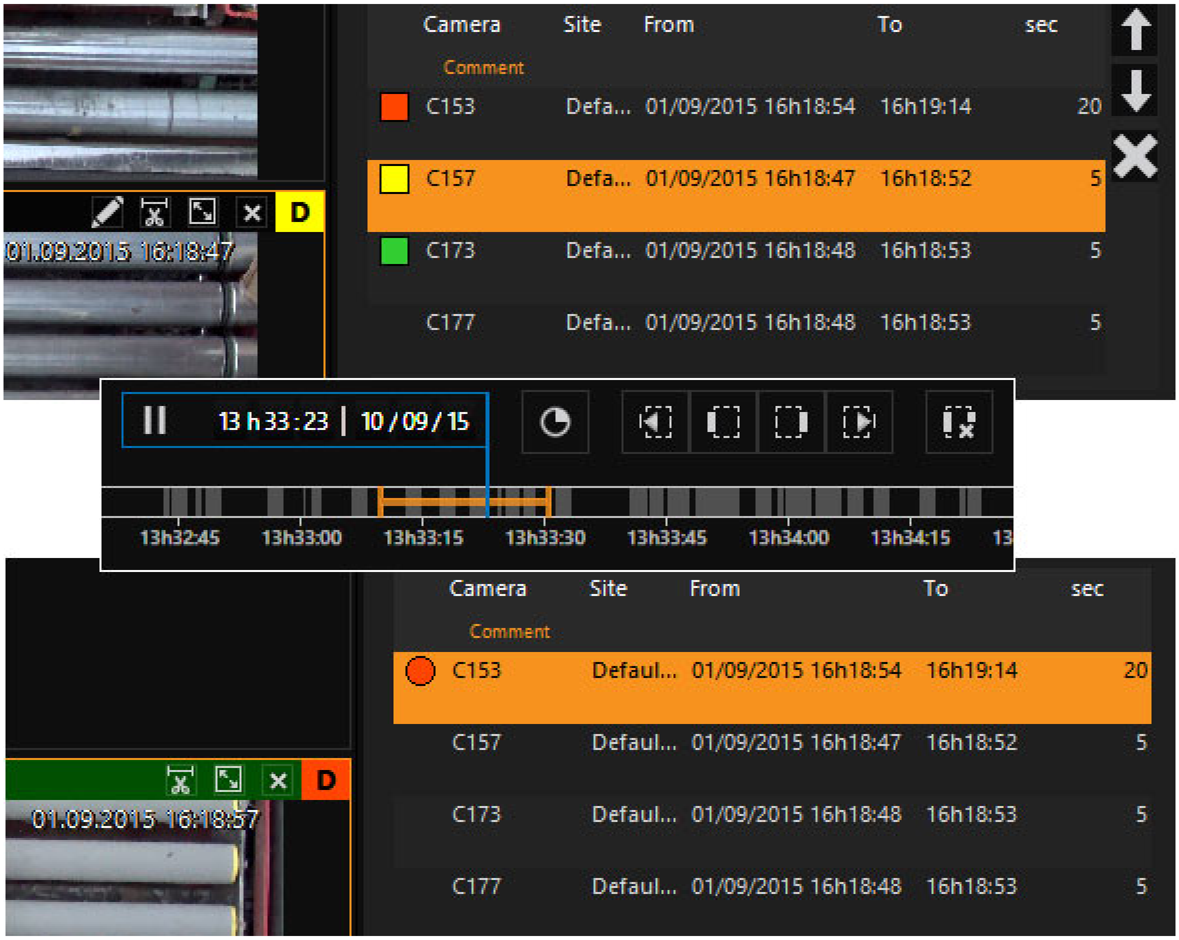
Clicking on a name will start to the process to drop the items, starting from the selected viewer. If the list has 3 items and the user click on panel "C", the items will be linked to panels "C", "D" and "E". All existing content on these viewers will be removed. Clicking the Order Chronologically button will sort all items according to their start times, giving you a chronological order of events when all items are dropped on viewers.

Editing a Cut List

A number of actions are available for editing a cut list.

Action	Description
	Create cut list
Clear	Empty list
Order	Order chronologically
✎	Edit cut list
✖ Delete	Delete cut list
Export	Video export
Locate	Show the active camera on the map
View	Activate the camera in the viewer

An entry to be processed is simply dragged onto a viewer. The color coding shows the linking.



	Camera	Site	From	To	sec
	Comment				
🟥	C153	Defa...	01/09/2015 16h18:54	16h19:14	20
🟨	C157	Defa...	01/09/2015 16h18:47	16h18:52	5
🟩	C173	Defa...	01/09/2015 16h18:48	16h18:53	5
	C177	Defa...	01/09/2015 16h18:48	16h18:53	5

	Camera	Site	From	To	sec
	Comment				
●	C153	Defaul...	01/09/2015 16h18:54	16h19:14	20
	C157	Defaul...	01/09/2015 16h18:47	16h18:52	5
	C173	Defaul...	01/09/2015 16h18:48	16h18:53	5
	C177	Defaul...	01/09/2015 16h18:48	16h18:53	5

The selection can then be edited using the **Timeline**.

The duration of the cut list entries can be adapted manually. The following criteria must be observed:

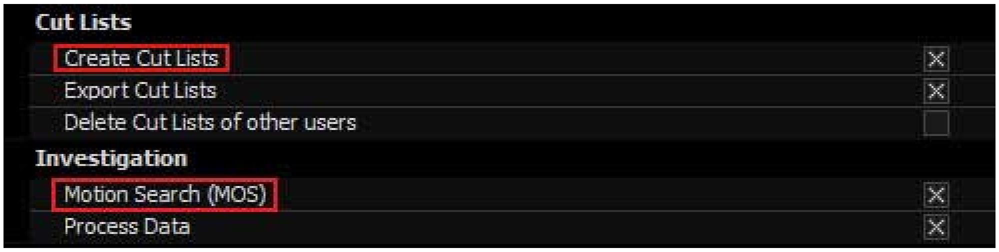
- The minimum value is 1 second.
- Changes to the duration values are only possible in edit mode.
- The start time of the cut list snippet stays the same independent of the changed duration values.
- The end time of the cutting list snippet automatically adapts to the changed duration values.

MOS Live

Requirements

MOS in live images requires two rights: the Motion Search MOS right and the right to create cut lists.

You can find the settings under **Users and Security** > **User groups** > **[Name of the user group]** > **Default privileges**.



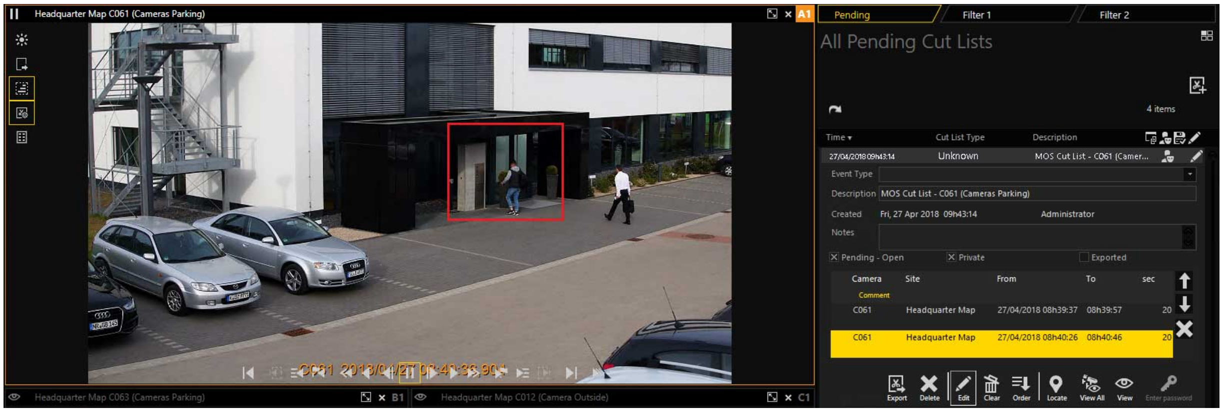
Cut Lists

- Create Cut Lists ☒
- Export Cut Lists ☒
- Delete Cut Lists of other users □

Investigation

- Motion Search (MOS) ☒
- Process Data ☒

Operator Console


Headquarter Map C061 (Cameras Parking)
A1
Headquarter Map C063 (Cameras Parking)
B1
Headquarter Map C012 (Camera Outside)
C1
Export
Delete
Edit
Clear
Order
Locate
View All
View
Enter password

Pending | Filter 1 | Filter 2

All Pending Cut Lists

4 items

Time ▾	Cut List Type	Description
27/04/2018 09h43:14	Unknown	MOS Cut List - C061 (Camer...

Event Type

Description MOS Cut List - C061 (Cameras Parking)

Created Fri, 27 Apr 2018 09h43:14 Administrator

Notes

☒ Pending - Open ☒ Private □ Exported

Camera Comment	Site	From	To	sec
C061	Headquarter Map	27/04/2018 08h39:37	08h39:57	20
C061	Headquarter Map	27/04/2018 08h40:26	08h40:46	20

In the Operator Console, you select the viewer in which you want to activate MOS for live images.

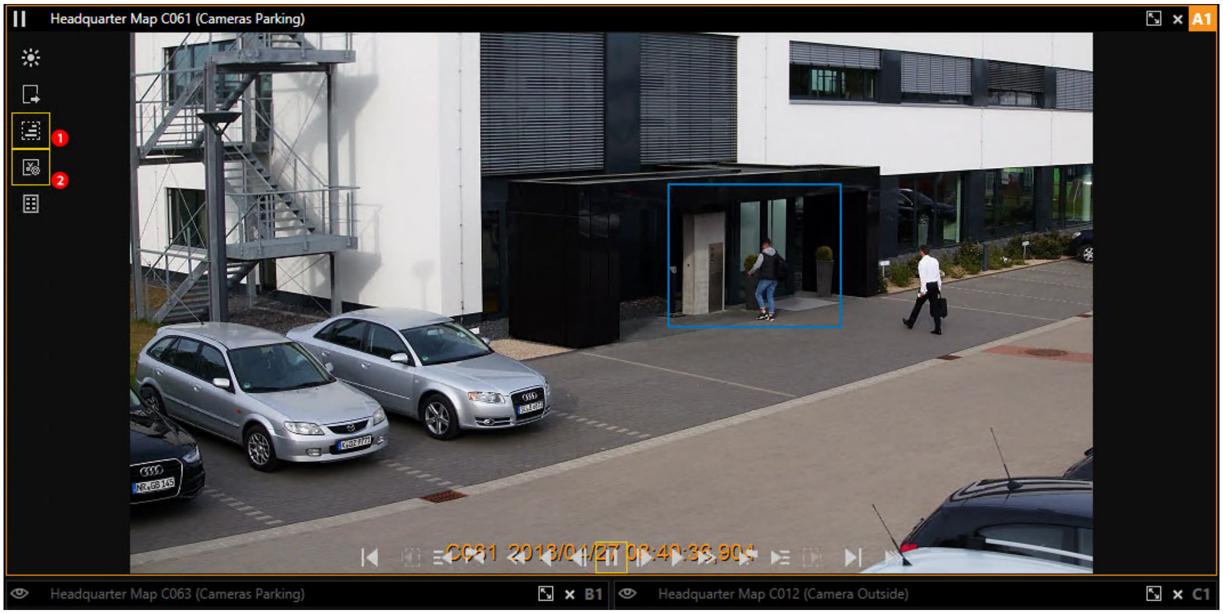
Search Mode	Then click **Search Mode**. As a result, an additional button appears in the overlay.
	This is the **MOS** button. If you select this button, in the viewer you can draw a rectangle to restrict the MOS function.
	The **Auto Cut List** button is displayed when the **MOS** button has been selected and the user has the necessary privileges.

MOS for Live Images

Select the MOS button in the overlay 1. Draw a rectangle (from the top left to the bottom right) onto the viewer.

The movement inspection is activated immediately and the rectangle switches to the status of motion detection when an activity has been started.

The colors of the motion rectangles can be set in the Management Console (normal colors, colors for motion detection and rectangle colors when removing).


Headquarter Map C061 (Cameras Parking)
A1
1
2
C061 2018/04/27 08:40:36,904
Headquarter Map C063 (Cameras Parking)
B1
Headquarter Map C012 (Camera Outside)
C1

If the rectangle is smaller than 10x10 pixels and is released at this size, the rectangle is not drawn; instead a previously drawn MOS rectangle is removed.
The same functionality can be realized by drawing a rectangle from the bottom right to the top left.

The standard window sound is also played. The sound can be activated/deactivated by right-clicking and using the context menu.

Auto Cut List

If the **Auto Cut List** button is selected 2, a new cut list is generated when an activity is detected for the first time. The default duration results from the default cut-list time set in the Management Console.

If a new movement is detected and the recorded time falls into the current section of the cut list, nothing happens. If the recorded time is outside the current section time, a new section is added to the cut list.

If you want to change something on the camera, such as zooming, pausing, etc., the current auto-cut list is ended and the button is deactivated.

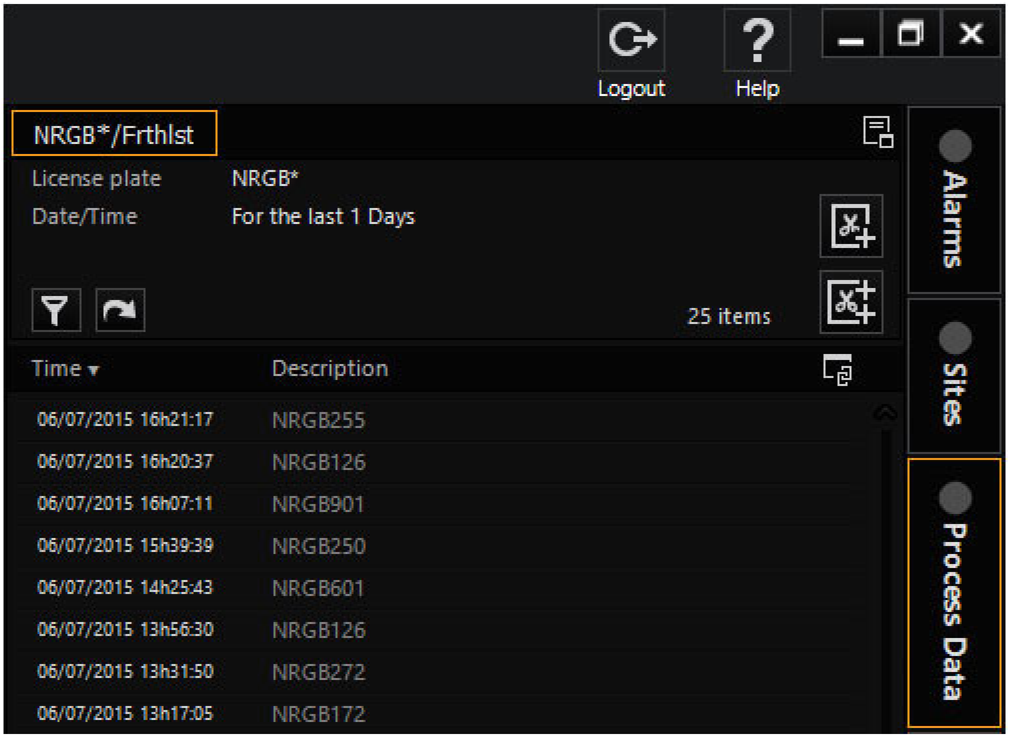
Process Data

G-SIM offers you the following main functions for process data:

- Export
- Search
- Display

Process Data Search and Display

Search for Process Data



NRGB*/Frthlst

License plate NRGB*

Date/Time For the last 1 Days

25 items

Time ▾	Description
06/07/2015 16h21:17	NRGB255
06/07/2015 16h20:37	NRGB126
06/07/2015 16h07:11	NRGB901
06/07/2015 15h39:39	NRGB250
06/07/2015 14h25:43	NRGB601
06/07/2015 13h56:30	NRGB126
06/07/2015 13h31:50	NRGB272
06/07/2015 13h17:05	NRGB172

Under the **Process Data** tab you find a list of process data. This data includes, for example, vehicle license plates, scanned barcodes, transactions in a retail store, ATM transactions, etc. Which process data is available depends on the structure of the system. By default, no process data is available.

You configure the information that is displayed on the individual process data cards in the Management Console (see Process Data Filters**).**

Start search

To make the process data available, start a relevant search. Process data is displayed only when a relevant search is started. This can be an individual number plate or an individual barcode or also comprehensive data on transactions in a shop with multiple fields and table entries.

Search queries usually contain a date range and/or time period as well as a fully or partially entered registration number, transaction number, etc., to search for.

Only the first 1000 matches are shown for each search operation. When 1000 matches are displayed, refine your search further.

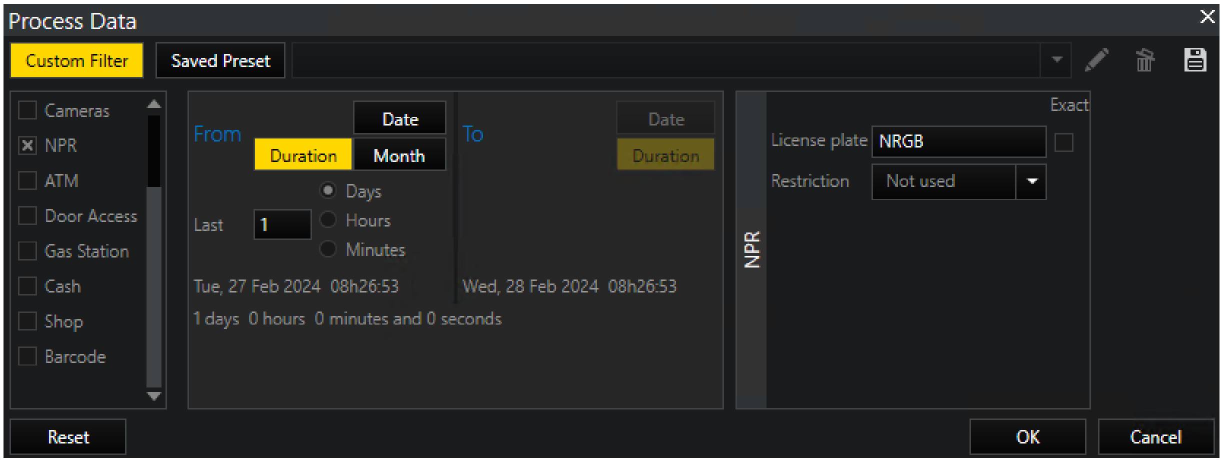
Export process data

Working with process data follows the same principles as working with cut lists.

To export process data, drag process data elements and entire process data events onto a cut list.

Open filter dialog

To open the filter dialog, click on the ▼ icon. You can now specify which process data is shown. The figure below shows some of the process data you can search for. In the example below, license plates with the identifier NR GB from yesterday are searched for.



Process Data

☐ Cameras
☒ NPR
☐ ATM
☐ Door Access
☐ Gas Station
☐ Cash
☐ Shop
☐ Barcode

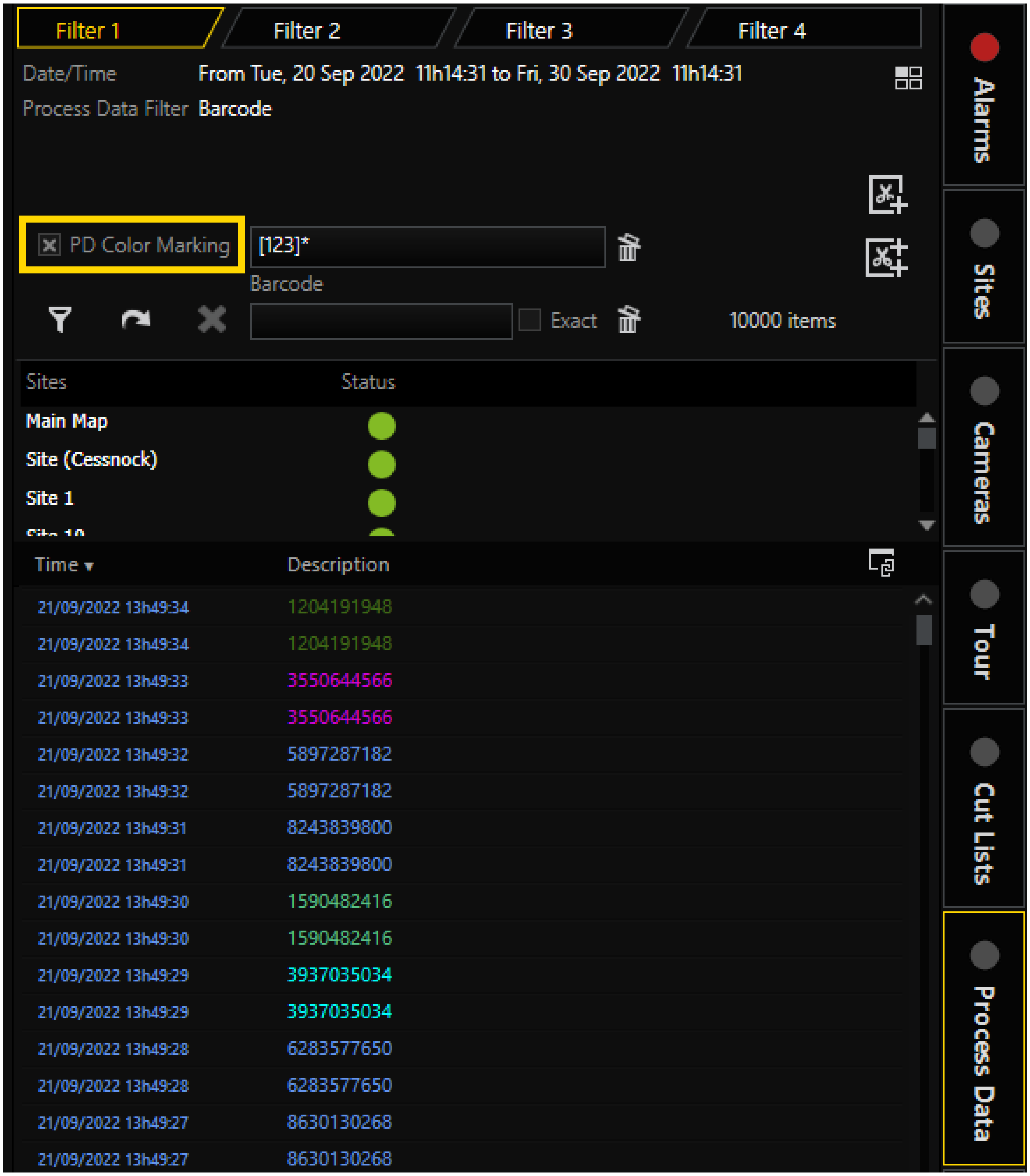
From: Duration, Month
Last 1 ● Days ○ Hours ○ Minutes
Tue, 27 Feb 2024 08h26:53
To: Duration
Wed, 28 Feb 2024 08h26:53
1 days 0 hours 0 minutes and 0 seconds

NPR
License plate NRGB ☐ Exact
Restriction Not used

ⓘ **The setting section on the right side opens after selecting a custom filter in the list on the left and varies depending on the selection. In the example above the NPR setting section where you can enter a License plate and select a Restriction opens after selecting NPR as custom filter.**

Color Marking of Process Data

The PD Color Marking filter function will expand the search for process data by marking all data that matches the search in color. Duplicates will be marked in the same color.



Date/Time From Tue, 20 Sep 2022 11h14:31 to Fri, 30 Sep 2022 11h14:31

Process Data Filter Barcode

☒ PD Color Marking [123]*

Barcode

□ Exact

10000 items

Sites	Status
Main Map	●
Site (Cessnock)	●
Site 1	●
Site 10	●

Time ▾	Description
21/09/2022 13h49:34	1204191948
21/09/2022 13h49:34	1204191948
21/09/2022 13h49:33	3550644566
21/09/2022 13h49:33	3550644566
21/09/2022 13h49:32	5897287182
21/09/2022 13h49:32	5897287182
21/09/2022 13h49:31	8243839800
21/09/2022 13h49:31	8243839800
21/09/2022 13h49:30	1590482416
21/09/2022 13h49:30	1590482416
21/09/2022 13h49:29	3937035034
21/09/2022 13h49:29	3937035034
21/09/2022 13h49:28	6283577650
21/09/2022 13h49:28	6283577650
21/09/2022 13h49:27	8630130268
21/09/2022 13h49:27	8630130268

1. To enable color marking of the process data search results, select the **PD Color Marking** checkbox.
2. Specify the template phrase in the text box. The process data descriptions that match this template phrase are selected in color.

A maximum of 30 colors can be displayed at once. The first group of process data items with the same descriptions corresponding to the template phrase is selected with the first color, the second group with the second color and so on.

Template phrases are case sensitive. A template phrase can contain the following wild cards:

Symbol	Description	Example
*	Represents zero or more characters.	bl* finds bl, black, blue, and blob
?	Represents a single character.	h?t finds hot, hat, and hit
[]	Represents any single character within the brackets.	h[oa]t finds hot and hat, but not hit
!	Represents any single character outside the brackets.	h[!oa]t finds hit, but not hot and hat
-	Represents any single character within the specified range.	c[a-b]t finds cat and cbt
#	Represents any single numeric character.	2#5 finds 205, 215, 225, 235, 245, 255, 265, 275, 285, and 295

To receive results, you must enter a valid template phrase:

Example NPR search (all letters are in upper case).

- Entering a range in lowercase letters, e.g. [a-b]*, will return no results.

- Entering a range in upper case letters, e.g. [A-B]*, will produce results.

Example NPR search (all letters are in upper case, followed by numbers "AN2384").

- Entering the range [A-B] will return no results.

- Entering the range plus additional wild cards, i.e. [A-B]?#*, will return results.

Delete template phrase:

To delete the template phase, click on the 🗑 button.

Display of Process Data

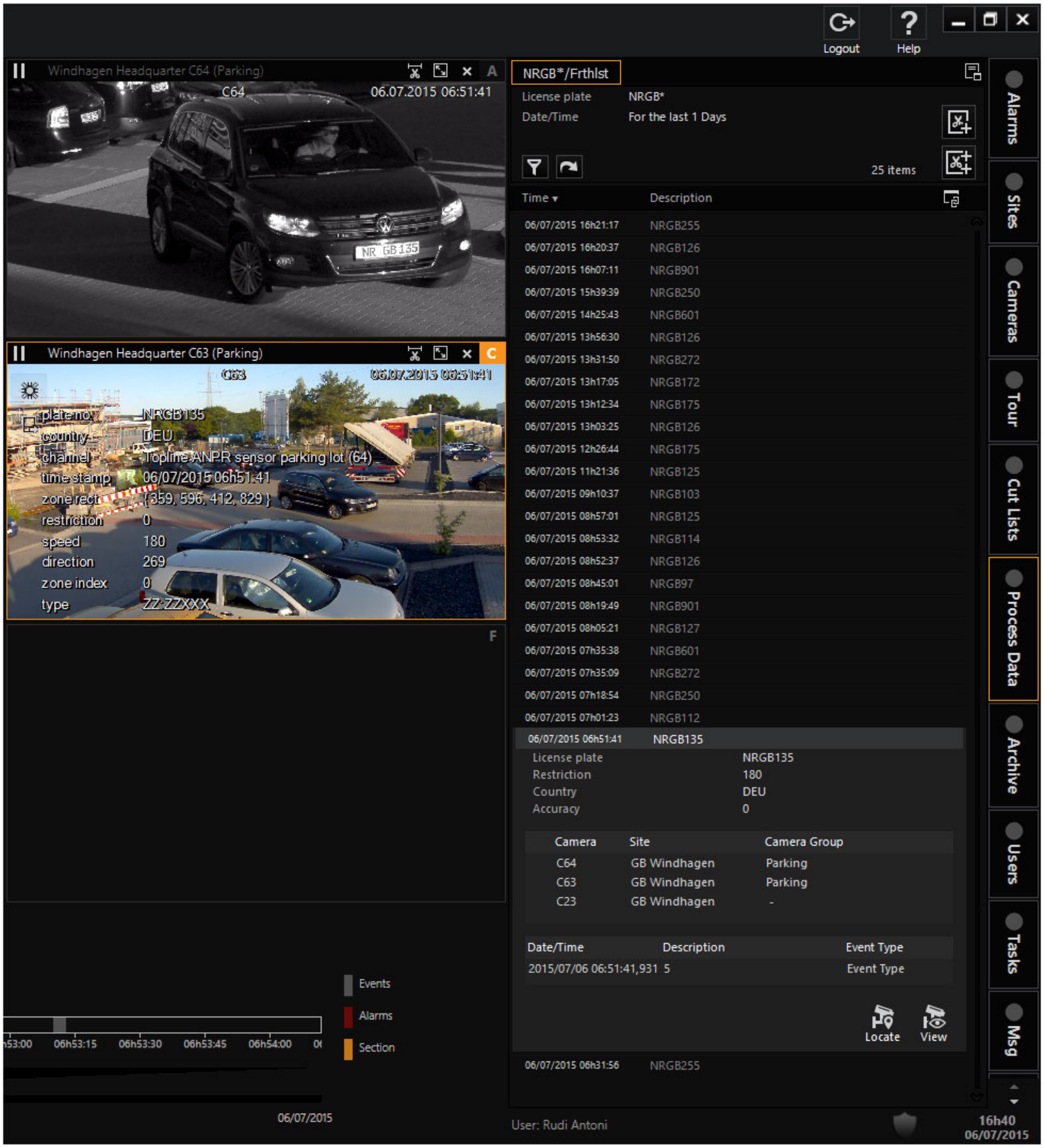


plate no	NRGB135
country	DEU
channel	Topline ANPR sensor parking lot (64)
time stamp	06/07/2015 06h51:41
zone rect	{359, 596, 412, 829 }
restriction	0
speed	180
direction	269
zone index	0
type	ZZ-ZZXXX

NRGB*/Frthlst

License plate NRGB*

Date/Time For the last 1 Days

25 items

Time ▾	Description
06/07/2015 16h21:17	NRGB255
06/07/2015 16h20:37	NRGB126
06/07/2015 16h07:11	NRGB901
06/07/2015 15h39:39	NRGB250
06/07/2015 14h25:43	NRGB601
06/07/2015 13h56:30	NRGB126
06/07/2015 13h31:50	NRGB272
06/07/2015 13h17:05	NRGB172
06/07/2015 13h12:34	NRGB175
06/07/2015 13h03:25	NRGB126
06/07/2015 12h26:44	NRGB175
06/07/2015 11h21:36	NRGB125
06/07/2015 09h10:37	NRGB103
06/07/2015 08h57:01	NRGB125
06/07/2015 08h53:32	NRGB114
06/07/2015 08h52:37	NRGB126
06/07/2015 08h45:01	NRGB97
06/07/2015 08h19:49	NRGB901
06/07/2015 08h05:21	NRGB127
06/07/2015 07h35:38	NRGB601
06/07/2015 07h35:09	NRGB272
06/07/2015 07h18:54	NRGB250
06/07/2015 07h01:23	NRGB112
06/07/2015 06h51:41	NRGB135

License plate	NRGB135
Restriction	180
Country	DEU
Accuracy	0

Camera	Site	Camera Group
C64	GB Windhagen	Parking
C63	GB Windhagen	Parking
C23	GB Windhagen	-

Date/Time	Description	Event Type
2015/07/06 06:51:41,931	5	Event Type

06/07/2015 06h31:56	NRGB255

User: Rudi Antoni

The figure shows the process data for the filter described above. Each list entry can now be viewed in the viewer.

Example To show the process data for NR-GB 135, select the entry and drag and drop it onto a viewer.

To show the selected view, you can also click on the Locate button.

To show the camera on the map, click on the View button.

Freeflow Mode

ⓘ **The View further than Event Runtime for Process Data privilege in the ManCon must be activated.**

1. To play back an event in freeflow mode, select the desired event under the Process Data tab.
2. Play the event back by using the View button in the viewer. If the process data event has several cameras, the different cameras can be displayed in the viewer by clicking on the View All button.

Display of Customer User Actions

To display customer user actions properly in the Operator Console (both in the OSD and in process data search), you must copy the XML file into the Operator Console directory (`C:\Program Files\Geutebrueck\GSim\Operator Console`).

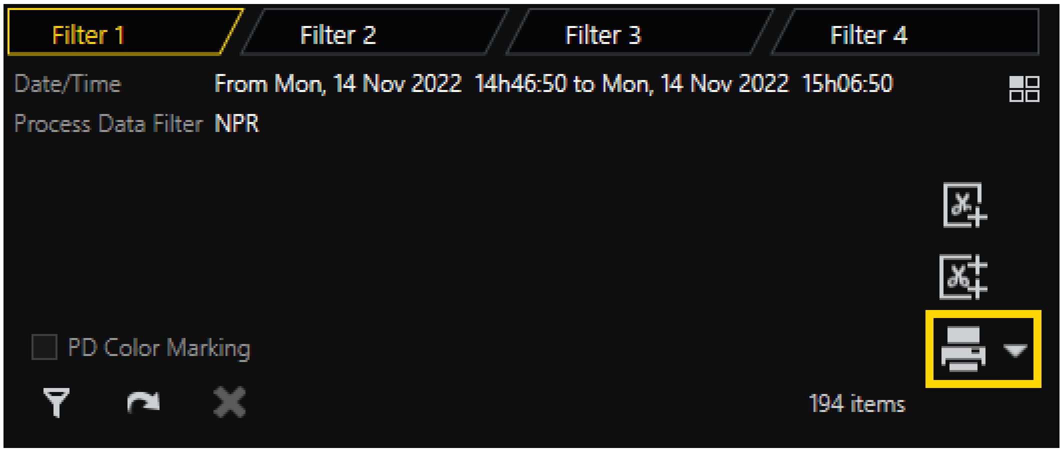
For information on how you can use your own defined customer actions in the G-SIM process data filters, see **Customer User Actions**.

ⓘ **The action code must be unique or else there is the possibility that actions will be overwritten.**

Export Process Data

1. Click on the Print list icon to export the searched process data.

   ⓘ **This function is only available if the Export Process Data privilege is enabled for the respective user (see** Privileges**).**



Filter 1 | Filter 2 | Filter 3 | Filter 4

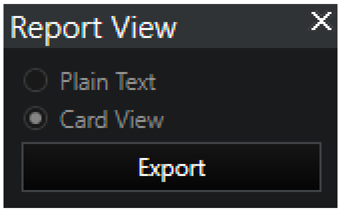
Date/Time From Mon, 14 Nov 2022 14h46:50 to Mon, 14 Nov 2022 15h06:50

Process Data Filter NPR

□ PD Color Marking

194 items

2. The **Report View** dialog window opens.



Report View

○ Plain Text

● Card View

Export

3. You can choose between two export options:
   - **Plain Text** - A simple table that contains the data in plain text form.
   - **Card View** - A detailed table whose structure is based on the view in the process data tab.
4. Click Export.
5. You can choose the following export formats: PDF, RTF, XLSX, CSV.

Alarms

Alarms are an important part of the G-SIM system, and are notifications that may be generated by hardware or software as a result of some kind of user interaction or equipment failure across the video network. Samples of alarms are: Duress Alarms where somebody pressed a panic button, a Security Breach Alarm if a user tries unsuccessfully for a number of times to get access to one of the G-SIM consoles, or Camera/Hard Drive Failure Alarms where physical equipment failed.

Depending on its definition, an alarm might have an item attached to it, e.g. a camera may be attached to a camera-related alarm. Dragging the alarm item would then actually drag the attached camera, thus a camera failure alarm may be dropped on a viewer to view the camera. Buttons on the alarm detail card also allow a user to view cameras or maps directly from the alarm card.

Alarms may be critical or non-critical (there are three alarm levels), and not all users will receive all alarms. While certain equipment failure alarms may only be of interest to support personnel, they may not be able to handle a duress alarm, for example. The basic idea is that a user must acknowledge an alarm as soon as possible after it was generated. After acknowledging an alarm it is the user's responsibility to handle and complete it.

As soon as a new alarm is generated by the system, it will be broadcast to all users who may handle the specific type of alarm. A red indicator light on the Alarm Tab will inform a user that there are new alarms in his alarm list and it will appear in the Alarm View for immediate access. An audible alarm sound will also be generated by the Operator Console if audible alarm sounds were not disabled in the Management Console by the system administrator. Different alarm sounds will be played depending on the importance of the alarm. New (unhandled) alarms are displayed in a separate list accessible via the first tab at the top of the Alarms list. These alarms cannot be filtered and will remain visible until they are acknowledged by any user with the necessary rights.

If a user acknowledges an alarm, the alarm level colour will darken to indicate this. It will stay in the list until you switch to another tab. Once tabs have been switched, acknowledged alarms are moved to the "Mine" tab list. They will be removed from there once they have been completed. If you have the privilege, then you can click on the tab "Others" to see alarms acknowledged by other users.

Acknowledged alarms are the user's responsibility and s/he must go through the whole process of handling and completing the alarm. Every type of alarm may have a unique list of handling procedures that must be completed (these procedures are specified in the Management Console).

An important feature that the administrator can configure is that certain alarms may be set to auto-expire. This is necessary in the case of equipment malfunction or misconfiguration which causes a flood of alarms. It is never a fix for a problem — merely a work-around until the problem itself is fixed.

Uncompleted alarms may be transferred from one user to another if the responsible user is unable to complete the alarm for whatever reason. The other user must accept the transferred alarm, and it will remain the responsibility of the original user until the other user has accepted it. Alarms which are not completed within 24 hours will be flagged by a status indicator.

An important feature of the alarm lists is multi-selection and simultaneous handling. This allows a user to select multiple alarms of the same type for acknowledgement or handling, easing the management of large volumes of similar alarms that may be generated under extreme fault conditions.

Alarms List

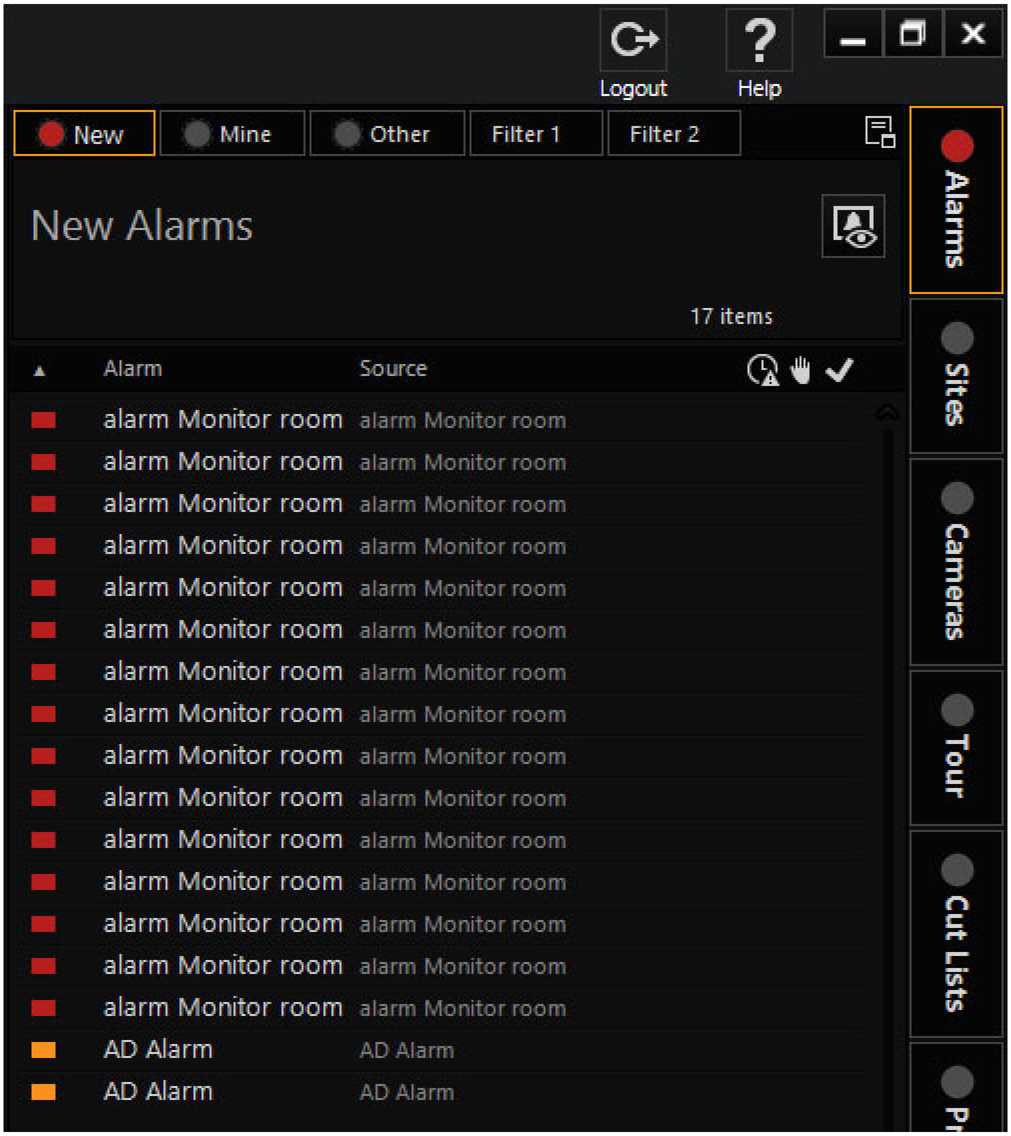
The Alarms List is split into three parts which are accessible via tabs at the top of the list:

New: Alarms which have not been acknowledged yet. This includes alarms transferred to you from another user, but which you have not yet accepted. Note that until you move to another list, this list will include alarms you have accepted . Their color will be darker to indicate this, though. This is so that you can see which you have accepted while still viewing new alarms. Once you change lists , the acknowledged alarms are move to the "Mine" list.

Mine: Those alarms which you have acknowledged (taken ownership of), but have not yet completed.

Other: Alarms which other users have acknowledged. You will need special privilege to see these.

In addition, you can define further filters as per **Filtering**.



New Alarms

17 items

▲	Alarm	Source
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟧	AD Alarm	AD Alarm
🟧	AD Alarm	AD Alarm

The first field of an alarm item is a colored block which indicates the severity level. Further states are indicated by state icons: if an alarm was acknowledged by the current user, was transferred to the user, is not completed, pending for more than 24 hours, or has auto-expired.

List Layout, Buttons, and Status Indicators

Dock alarm list: If an alarm display should be permanently visible for new alarms, you can use the "Dock" button to dock this list to a sufficiently large viewer.

Status: Various status symbols signal that an alarm has been pending for more than 24 hours, whether the alarm is public or private and whether the alarm has been completed.

The following status symbols require further explanation:

Meaning of the symbols	
✋	My alarm – I am responsible for this alarm
☑	Alarm is closed
✉	The alarm has been delegated to another user
24 ⚠	The alarm has been pending for more than 24 hours
🕒⚠	The alarm has expired (exceeded lifetime)

My alarm: (List of accepted alarms) The current user has accepted the alarm (and is responsible for completing the alarm if the alarm has not yet been completed).

Completed: (List of accepted alarms) The alarm has been completed.

Delegated: The meaning of this status symbol depends on the list in which it is displayed. In the alarm list "Mine" it means that you have delegated the alarm to another user who has not yet accepted this alarm (meaning you are still responsible for the alarm). In the alarm list "New", it means that another user has delegated the alarm to you and is waiting on your response.

Expired: Alarms that exceed their lifetime expire automatically.

Alarm Levels and Colors

Alarm items are marked with one of three colors in the alarm lists, depending on how critical the alarm is. The three alarm levels are:

Level 1	Critical	Red
Level 2	Noncritical	Yellow
Level 3	Informative	Blue

Sounds Associated with Alarms

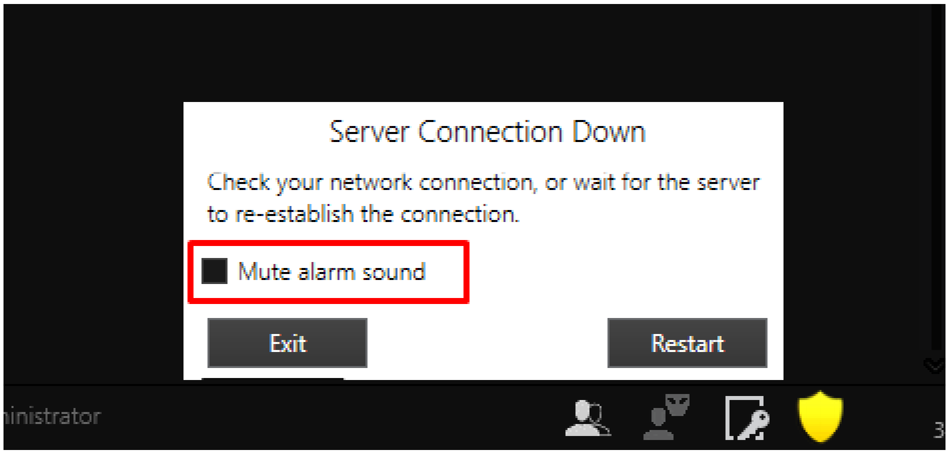
For new (unacknowledged) critical and non-critical alarms an audible alarm sound will be played (depending on the level of the most critical alarm in the list).

These sounds are .WAV files and may differ from installation to installation. Alarm sounds will not be played if the "Play Audio for Unhandled Alarms" privilege is not selected for the logged-in user (in the Management Console).

You can mute the sounds by pressing the mute button in the toolbar, but it will be unmuted the moment any new (non)critical alarm arrives.

Alarm Sound for Connection Loss

If in Management Console a sound was set for **G-SIM Server connection loss** and the connection to the G-SIM server in the Operator Console gets lost, the selected sound will be played. At the same time, a form called **Server Connection Down** will appear.



Server Connection Down

Check your network connection, or wait for the server to re-establish the connection.

If the connection to the G-SIM server is restored, the **G-SIM Server connection loss** sound stops playing.

If the connection to the G-SIM Server is not restored, the sound keeps playing.

- To mute the alarm sound, check **Mute alarm sound**.
- To unmute the alarm sound, uncheck **Mute alarm sound**.

The state of the **Mute alarm sound** checkbox is saved while the Operator Console is working.

The Mute alarm sound checkbox is visible only if a sound was set for the G-SIM Server connection loss setting in the Management Console.

Alarm Detail

The detail displayed when an alarm is selected depends on if the alarm is already acknowledged or not. In the case of a new alarm only the alarm description will be displayed. Once you acknowledge the alarm, however, the whole list of alarm handling procedures will also be displayed. These handling procedures are definable per alarm type in the Management Console.

The following needs further explanation:

Alarm State: Contains detail about the state and responsible user. In the case of a transferred alarm the transfer status will be displayed here.

Handling Procedure: Items must be completed in sequence. If you find that you cannot proceed, then either you forgot to complete one of the steps, or the defined steps are insufficient, in which case put the relevant detail in the comments field.

Comments: Additional comments regarding the alarm may be entered here. This is not a compulsory field to complete an alarm. It makes sense to enter relevant information here before an alarm is transferred to another user.

Alarm Actions

The following action buttons are available on the Alarm Detail Card:

View Live: This button will only be active if a camera was linked to the alarm and allows you to view the recorded footage of the attached camera at the time of the alarm. See below for more on this.

Complete This and Similar Alarms: In addition to completing the selected alarm, this will find similar alarms (e.g. other “Intrusion” or “Camera Failure” alarms) and complete them also. This is very useful in the case of malfunctioning equipment creating spurious alarms. Your administrator should than also take steps to deal with these automatically until the necessary repairs have been made.

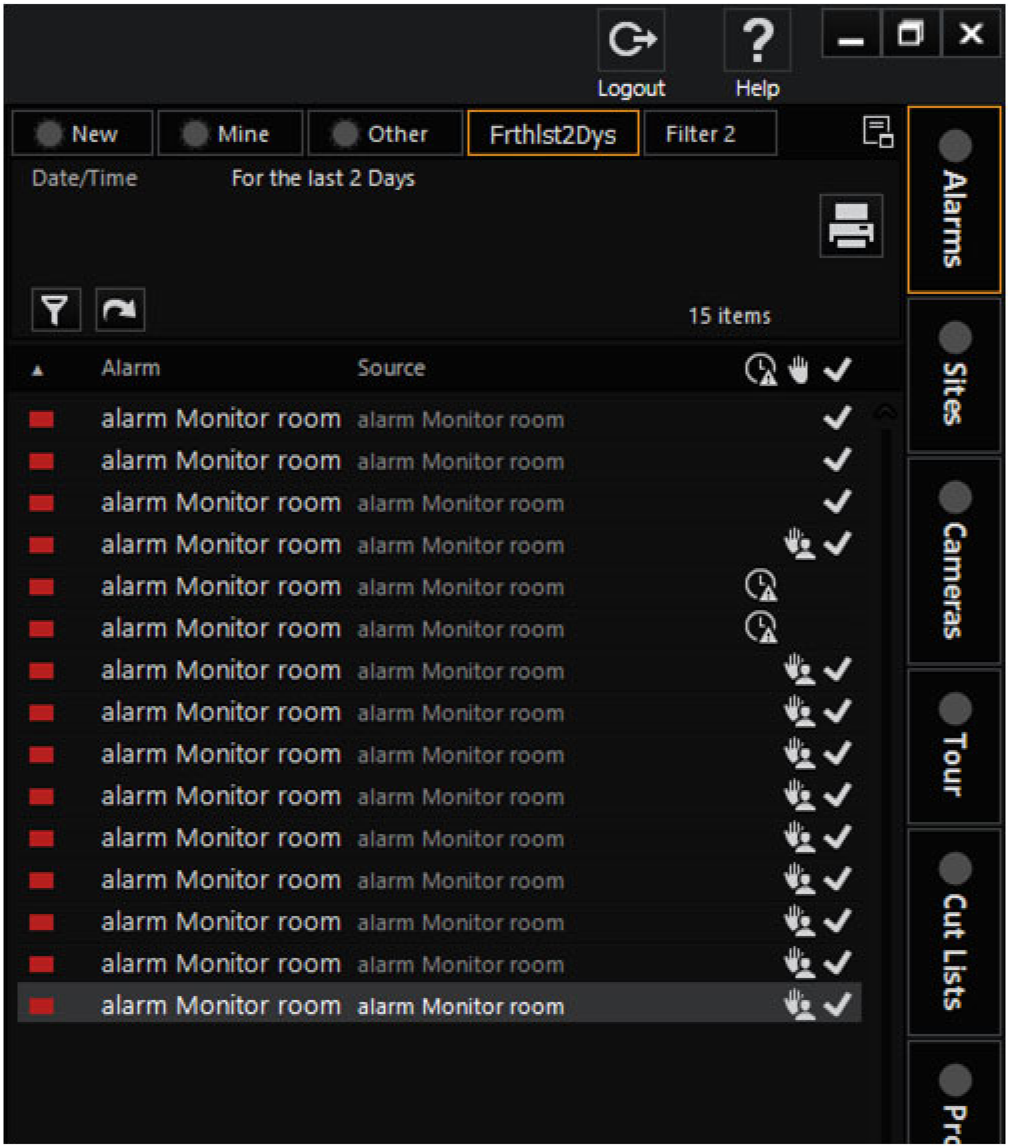
Note Regarding Live View

Once you have closed an Auto View alarm and you open it again, its cameras defined as live view will no longer be live. Instead they will show footage as at the time of the incident, starting at the pre-roll defined for this alarm.

You will notice the **Live** and **Replay** buttons. **Live** will make the cameras marked as live display what is happening right now, while **Replay** will replay them as if you had just re-opened the alarm.

Alarm Query Builder

Querying alarms is exactly the same as executing any other quer. See **Filtering** for how to use the query builder.

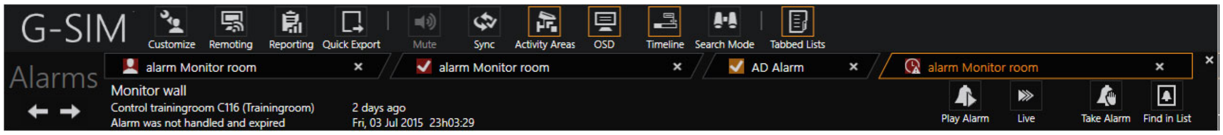


Date/Time For the last 2 Days

15 items

▲	Alarm	Source			
🟥	alarm Monitor room	alarm Monitor room			✓
🟥	alarm Monitor room	alarm Monitor room			✓
🟥	alarm Monitor room	alarm Monitor room			✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room	⏲		
🟥	alarm Monitor room	alarm Monitor room	⏲		
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓
🟥	alarm Monitor room	alarm Monitor room		✋	✓

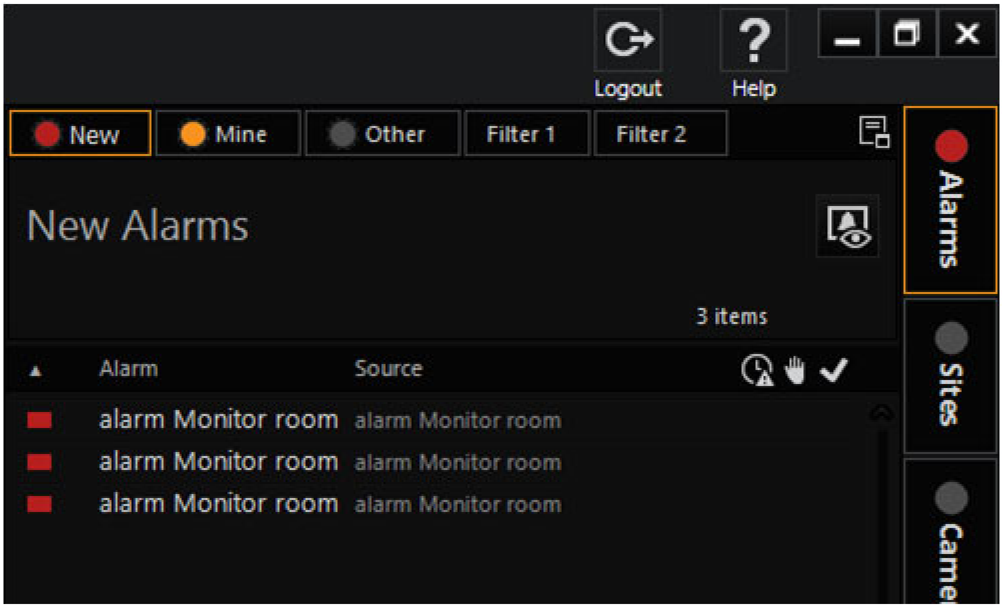
Alarm View



Monitor wall
Control trainingroom C116 (Trainingroom)
Alarm was not handled and expired

2 days ago
Fri, 03 Jul 2015 23h03:29

The Alarm View is basically a popup screen that is used to view Alarms easily that have cameras attached to them. Each Alarm is displayed on its own tabbed page which allows you to work with multiple alarms at once.



New Alarms

3 items

▲	Alarm	Source
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room
🟥	alarm Monitor room	alarm Monitor room

All physical aspects of the Alarm View screen are centrally configured, such as the Viewer layout and the screen on which it should be displayed. Also, Auto View Alarms can be set up from the Maintenance side to display associated content in specific Viewers on the Alarm View screen. For example, multiple live camera views of the triggered Alarm area, a reference map, and paused video of the time the alarm occurred.

You can show or hide the Alarm View screen at any time using the **Alarm View** toggle button on the list header (if it is disabled, there are no Alarms open for viewing). Hiding the Alarm View does not close any open alarm tabs.

Using the Alarm View

To open an alarm in the Alarm View, click on the **View Alarm** button on any pending/completed Alarm Detail Card. If the button is disabled, the alarm does not have any cameras associated with it and thus cannot be viewed.

Alarm View Toggle Button: Click to show or hide the Alarm View.

Alarm View Tabs: Each opened Alarm has its own page that can be accessed by clicking on its Tab. The Tab displays the Alarm's type (e.g. Duress), and once completed it also displays a "completed" status icon. The Tab and Header's background color shows the Alarm's level (See **The Alarm List**).

Alarm View Header: The Header displays all relevant information from the Alarm's Detail Card (like the alarm description, state, and date and time), and gives quick access to some basic Alarm Actions and video navigation buttons. The Header's background color shows the Alarm's level.

Video Navigation and Alarm Action Buttons

Button	Description
👁	Hide/show alarm display
Play Alarm	Repeat alarm
Live	Play live
Find in List	Search in the list
Take Alarm	Accept
×	Close

Repeat/live: If you select a viewer in which video recordings from a camera are being displayed, you can view the video recordings from the point in time when the alarm was triggered by clicking "Repeat" or you can display the live video from this camera.

Search in list: The alarm is opened in the alarm list (required to close an alarm after you have accepted it). See Alarm processing.

Accept: With this option you can assume responsibility for a new alarm (i.e. accept the alarm). This is a requirement for being able to close it. This button appears only for alarms that have not yet been accepted.

Close: The alarm display tab is closed, but the alarm is not completed. The alarm continues to be available in the alarm list and can be shown again in the alarm display. To do so, select it in the list and click Show alarm.

Auto View Alarms

Alarms that are configured as AutoView alarms are automatically displayed on the screen of the corresponding user the moment that the alarm is triggered. This function is useful for critical alarms that must be processed immediately. Otherwise AutoView alarms are the same as normal alarms. It will quickly become apparent if your administrator was too generous when assigning AutoView alarms.

AutoView alarms are displayed on the AlarmView screen. If more than one AutoView alarm was triggered and no user reaction has been detected on the AlarmView screen, all pending AutoView alarms are displayed in a continuous loop at a configurable speed (normally set to 6 seconds).

If you close an AutoView alarm and open it again later, live images are no longer shown for the live cameras. Instead, the recorded video images are displayed from the alarm period, starting from the specified point in time before the alarm-triggering event.

Note the buttons Live and Repeat. Click Live to display the live image from the live cameras. Click Repeat to repeat the video sequence from the alarm timeframe, as it would be shown when opening the alarm again later.

IMPORTANT: When AutoView should not be set
The use of AutoView alarms is not recommended when systems are connected to the corresponding cameras over slow network connections, as just a few successfully triggered AutoView alarms will cause an overload in slow networks. In addition, AutoView alarms result in a significant disruption to normal operations and should only be used for rare, extremely critical alarms.

Alarm Presentation

An alarm may be set up in the Management Console to be an Auto View alarm. Auto View alarms will automatically be displayed in the Operator Console when they are triggered. There are two different display mechanisms to choose from:

- A Tab View, which is a completely new template laid over an existing Operator Console screen (a new alarm will be displayed in a new tab on this overlay screen).
- A Viewer Group View, which will display the alarm in a group of predefined viewers in a template already visible on one of the screens.

Differences between Tab Auto View and Viewer Group View:

Tab View	Viewer Group View
Tab Views are always on one screen.	A **Viewer Group** may stretch over multiple screens.
Only one alarm will be visible on the selected tab of a **Tab View**.	Multiple alarms may be visible at once in different **Viewer Groups** (different types of alarms may also be displayed on one template, but in different **Viewer Groups**).
A **Tab View** is overlaid on a full screen – all viewers behind it are hidden.	A **Viewer Group** may take any number of viewers on a template and will usually occupy a whole row. All other viewers may be used for normal viewing of cameras or maps.
Alarms cannot be dragged to an **Auto View Tab**.	Alarms may be dragged from the **Alarms List** to a **Viewer Group**.

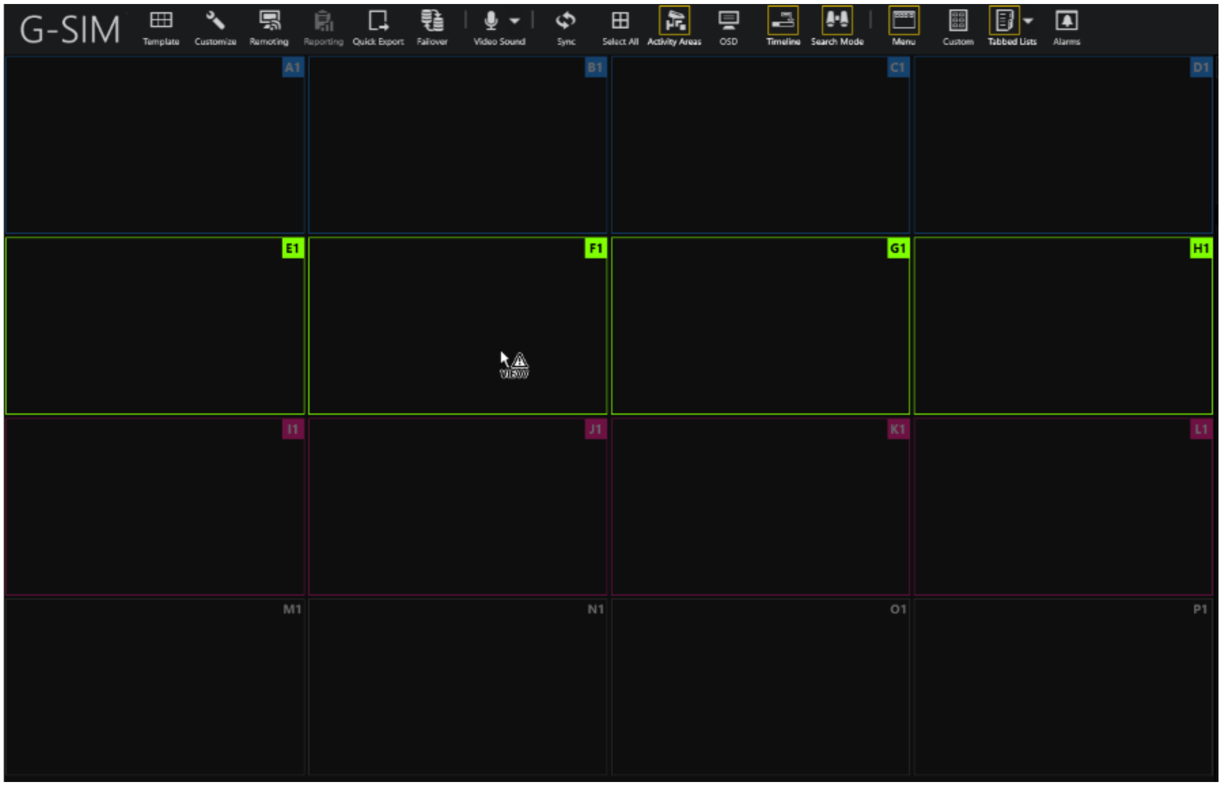
Viewer Groups View

Selecting a Template Containing Viewer Groups

Any screen may be set up to contain a template of Viewer Groups. Templates containing Viewer Groups are listed under Populated Templates. Viewer Groups are indicated on the preview images in the Template Selector by their colors defined in the Management Console. A Viewer Group may stretch over two or more templates. In such a case it makes sense to select both templates on different screens.

Display of Viewer Groups in the Operator Console

Viewers belonging to a Viewer Group are indicated by colored frames. The color defined in the Management Console is used as highlighting color while the frame uses a darker version of this color.



The image shows three **Viewer Groups**. One of them is highlighted before an alarm is dropped. A typical setup would be that a new alarm is displayed at the top row. It will move down to the second row when another alarm comes in. On yet another alarm, it will move to the third row where all active alarms will cycle.

Auto Viewing Alarms in Viewer Groups

If an Operator Console receives a new **Auto View** alarm to be displayed in a **Viewer Group**, a check will be performed to determine if the **Populated Template(s)** containing the **Viewer Group** is/are already applied:

- If the **Viewer Group** exists, it will be populated with the new alarm.
- If the screen templates for the multi-template **Viewer Group** were applied in a different order, it will be used as it is.
- If only some of the templates for a multi-template **Viewer Group** are already applied, the Operator Console will try to apply the missing templates (if enough screens are attached).

- If none of the **Populated Templates** containing the alarm's **Viewer Group** is applied on any screen, all necessary **Populated Templates** will be applied in order.

If any **Populated Template** is automatically applied to a screen, the **Monitor Settings** for the specific Operator Console (as defined in the **Client Setup**) will be taken into account. Any specific configured layout for a monitor will be used by preference.

> Example If a template must be automatically applied to a screen and the template is specifically included in Monitor 2's settings, it will be applied to Monitor 2 rather than Monitor 1 (with no customized settings).

When a new alarm that is linked to a **Viewer Group** is received, the current alarm in the **Viewer Group** may be

- dropped,
- moved to another **Viewer Group** or
- put in a buffer and cycled through (together with the newly added alarm).

Viewer Groups may be defined to stretch over several templates. If not all **Populated Templates** containing viewers for a specific **Viewer Group** are applied and the missing templates cannot be applied for some reason, an alarm will still use the viewers available.

i **If more viewers than available are needed, the rest of the alarm content will not be displayed. The user will only see some of the cameras/maps linked to the alarm.**

Viewing a Past Alarm

To view past alarms from the **Alarms List**,

- drag the alarm to a **Viewer Group** or
- click **Alarm** > **View Alarm**.

View Alarm will always open the alarm in a tabbed alarm window. The user may drag and view alarms configured to be auto viewed in the tabbed alarm window in a **Viewer Group**.

Clearing an Alarm from a Viewer Group

It is possible to configure an alarm to be cleared from a **Viewer Group** when this alarm is either acknowledged or completed by another user.

To clear an alarm manually from a **Viewer Group**, close any one of its viewers.

→ A pop-up window will appear informing the user that all viewers are going to be cleared when one viewer is closed.

Viewer Group Response After It Got Cleared

The response or state of **Viewer Group** after it got cleared will depend on the setup. If it is set up to **Move alarm back if original Viewer Group becomes free**, it will keep all previous alarms in a stack and move the top (last) one back to the viewers as alarms are closed (either manually closed or as a result of being acknowledged or completed by another user).

Saving of Viewer Group Content When the Operator Console is Closed

Viewer content of viewers belonging to a **Viewer Group** is **not** saved when the application is closed. This means that **Viewer Group** viewers will always be empty on start-up. A **Viewer Group** may however have a whole stack of alarms behind used to fill in again when an alarm is cleared, or to cycle through if that option was selected. This alarm stack will typically consist of the latest open alarms.

Dragging and Dropping Content to and from a Viewer Group

Dropping an Alarm from the Alarms List on a Viewer Group

Any alarm with cameras linked to it may be dropped on a **Viewer Group** (even alarms configured to be auto displayed in a **Tab View**). All attached alarms and maps will be displayed in sequence to fill all available viewers of the **Viewer Group**. If the **Viewer Group** contains extra viewers, these will be cleared. Regarding an alarm, it does not matter on which viewer the alarm is dropped – the **Viewer Group** will be populated starting from the first viewer in any case. The user may thus drop an alarm on the viewer closest to the **Alarms List**.

Dragging an alarm over a **Viewer Group** will highlight all viewers belonging to the **Viewer Group** to indicate which viewers will be affected.

Dropping Other Content on Viewer Group Viewers

Viewers belonging to a **Viewer Group** accept any content just like a normal viewer. This content will be replaced when a new alarm populates the **Viewer Group**. This content will also **not** be saved when the application is closed.

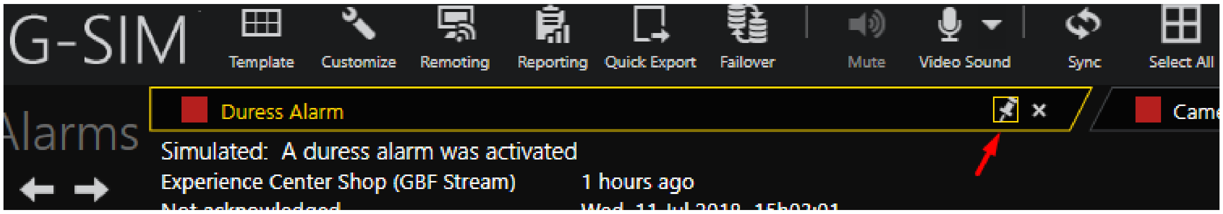
Dragging a camera or map over a **Viewer Group** will only highlight the one viewer the cursor is placed on. Only the content of this one viewer will be changed if the content is dropped.

Dragging an Alarm from a Viewer Group to the Alarm List

Dragging any viewer content from a populated **Viewer Group** to the **Alarms List** will select the specific alarm in the list.

Auto View Cycle Time

On the **Alarm** tab of the Operator Console, there is a button with a pin. The pinned Alarm tab means that the alarm is being processed by the operator.



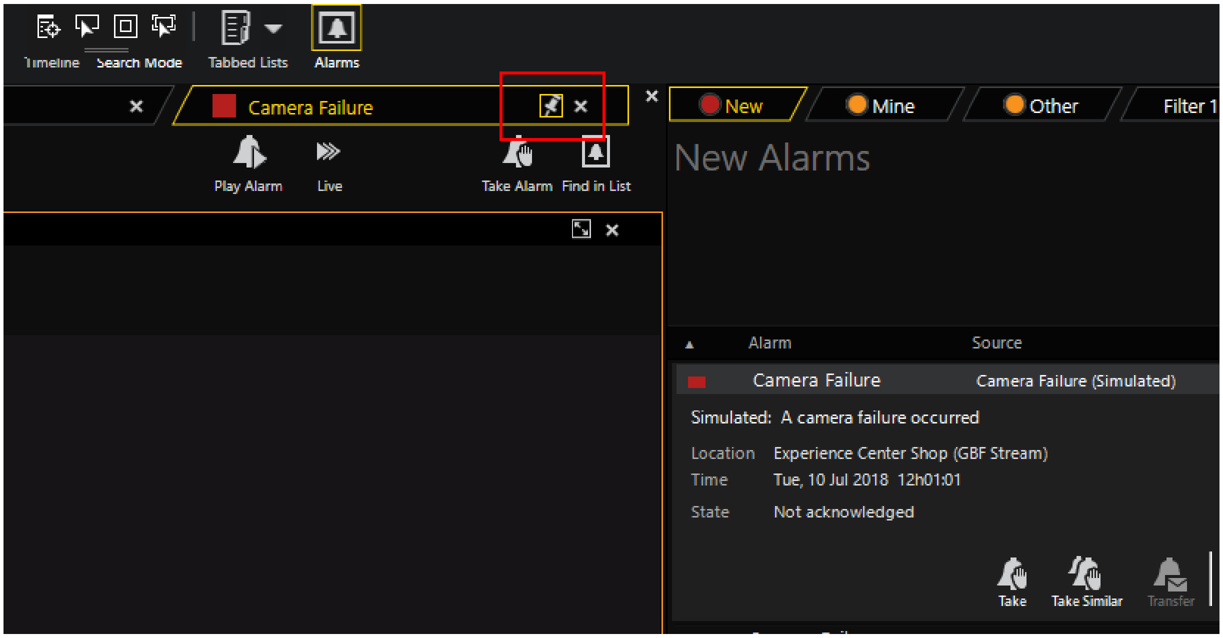
Simulated: A duress alarm was activated

Experience Center Shop (GBF Stream) 1 hours ago

Not acknowledged Wed, 11 Jul 2018 15h03:01

Only one alarm can be pinned at a time. If the user selects another alarm, the previous alarm is enabled. The newly selected alarm is also enabled until the operator manually pins it.

When the user views an alarm from the **Alarms** tab, this alarm is automatically pinned.



Camera Failure Camera Failure (Simulated)

Simulated: A camera failure occurred

Location Experience Center Shop (GBF Stream)

Time Tue, 10 Jul 2018 12h01:01

State Not acknowledged

There is NO pin functionality in the remote console!

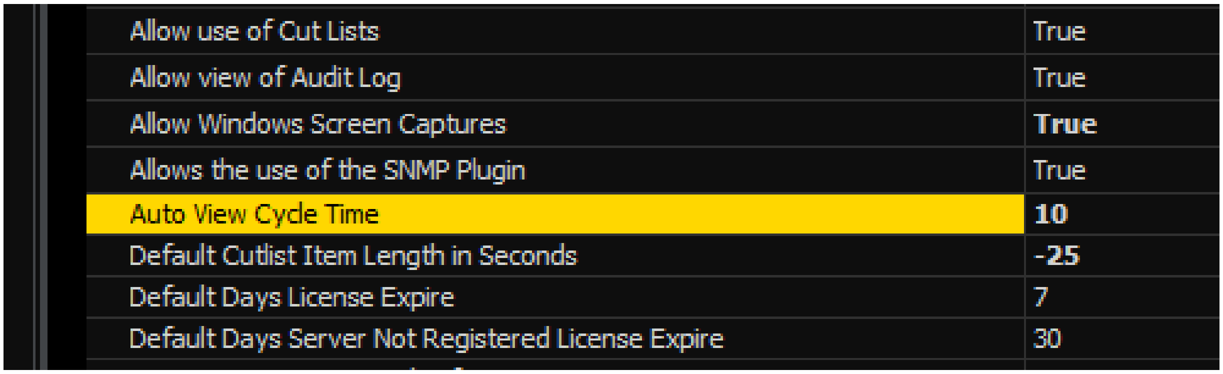
Deactivating the Automatic View of the Alarm Cycle

There are two mechanisms to disable the automatic display of the alarm cycle based on the value of the **Auto View Cycle Time** in the Management Console:

- If the cycle time of the automatic display is greater than zero
- If the cycle time of the automatic display is zero.

If the Cycle Time of the Automatic Display is Greater Than Zero

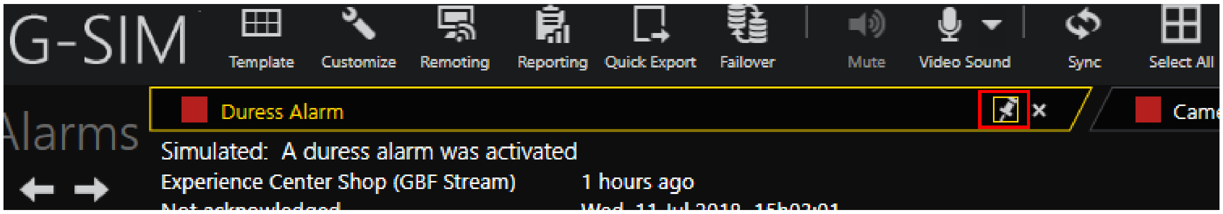
If the automatic display cycle time is greater than zero, alarms will be automatically set according to the setting in **Auto View Cycle Time**.



Allow use of Cut Lists	True
Allow view of Audit Log	True
Allow Windows Screen Captures	**True**
Allows the use of the SNMP Plugin	True
Auto View Cycle Time	**10**
Default Cutlist Item Length in Seconds	**-25**
Default Days License Expire	7
Default Days Server Not Registered License Expire	30

When the alarm is pinned, the automatic display cycle is disabled until the user cancels the alarm.

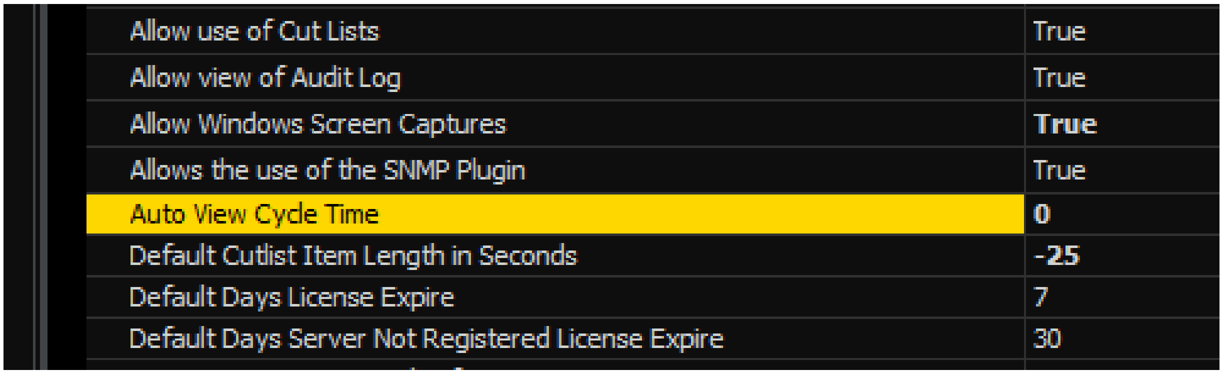
When the alarm is pinned and a new alarm arrives, the new alarm appears on the control panel, but the pinned alarm is still selected.



Simulated: A duress alarm was activated
Experience Center Shop (GBF Stream) 1 hours ago
Not acknowledged Wed, 11 Jul 2018, 15h03:01

If the Cycle Time of the Automatic Display is Zero

If the cycle time of the automatic display is zero, the automatic display cycle is deactivated.



Allow use of Cut Lists	True
Allow view of Audit Log	True
Allow Windows Screen Captures	**True**
Allows the use of the SNMP Plugin	True
Auto View Cycle Time	**0**
Default Cutlist Item Length in Seconds	**-25**
Default Days License Expire	7
Default Days Server Not Registered License Expire	30

If no alarm is pinned and a new alarm is received, the new alarm appears on the control panel and is selected.

When the alarm is pinned and a new alarm arrives, the new alarm appears on the control panel, but the pinned alarm is still selected.

Instance Alarms, GeViSoft Alarms & Events

This section is for reference/interest only, and may safely be skipped.

Instance Alarms

The term Instance Alarm or Alarm Instance is used to denote Alarms that are specifically created by the administrator to make use of predefined criteria (as opposed to generic Alarms that are inherent to G-SIM, such as Sync Loss).

Instance alarms are configured to fulfil specific needs, such as linking multiple cameras to a single Alarm, setting up the Alarm View to display additional information for an Alarm, such as additional maps and paused video. More technically, Alarm Instances are specific alarms triggered by one-to-one relationships with defined trigger events.

Note that Instance Alarms can be very beneficial, but they require special configuration by the administrator.

The Difference Between Generic Alarms and Alarm Instances

Although there is a difference between generic Alarms (those inherent to G-SIM, e.g. Sync Loss) and Alarm Instances (user-defined criteria), this difference is only apparent to the administrator because it deals with how an Alarm is triggered. Once an Alarm is triggered and appears in the Alarm List, there is no difference between generic Alarms and Alarm Instances, and therefore these are all simply called Alarms.

GeViSoft Alarms and Events

GeViSoft alarms and events may be used to create G-SIM Alarms. When configured correctly, GeViSoft can extend the functionality of Alarms in G-SIM immensely by using virtually any alarm source. Furthermore, it will allow the system administrator to add complex Alarm logic, for example to combine multiple Alarms to create new Alarm triggers.

Any GeViSoft alarm or event configured in G-SIM will automatically be an Instance Alarms, making it possible to link multiple cameras to such an alarm.

How it works

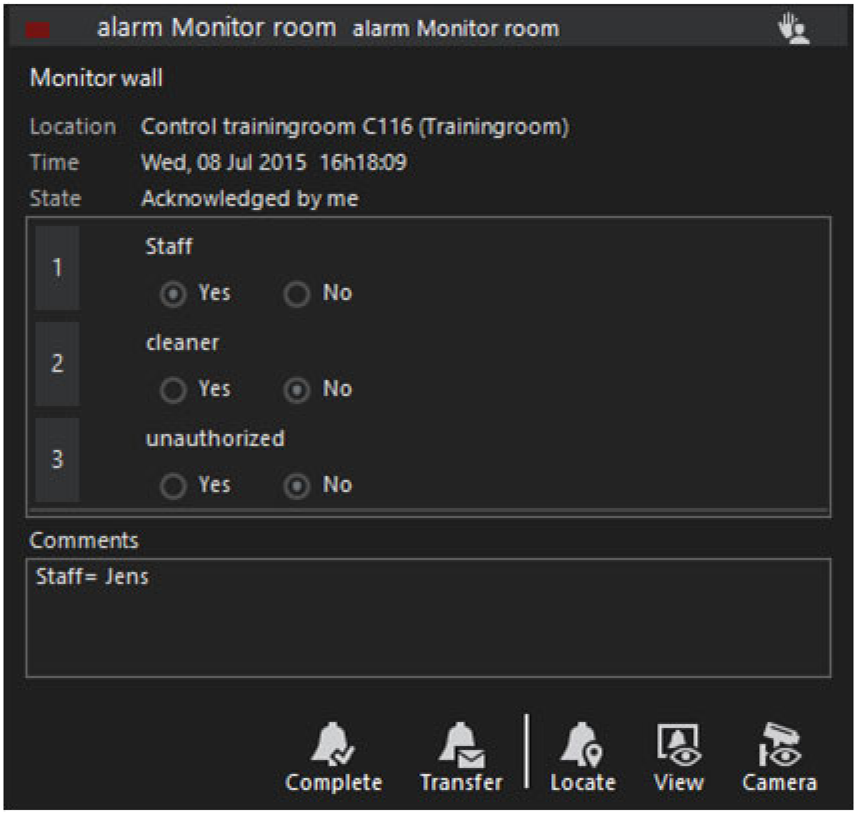
Internally, G-SIM will create a new Alarm when triggered by a GeViSoft alarm or event. This Alarm can then be acknowledged by a user, which will automatically Acknowledge the alarm within GeViSoft as well. While the Alarm is being handled in G-SIM, the GeViSoft state will remain Acknowledged until it is completed, after which its GeViSoft state will be set to Quit.

The reverse has also been implemented, so that when an alarm is set to Quit within GeViSoft, it will be completed within G-SIM (by the "System User"). This is particularly useful if you want to add Alarm completion logic to GeViSoft.

Technical Note Regarding GeViSoft Alarms

Owing to the alarm structure of GeViSoft, G-SIM Alarms generated from GeViSoft alarms can only exist once at any given time, which means that a GeViSoft alarm cannot be triggered again until it is completed. If this is not what you want to do, use GeViSoft events instead.

Handling Alarms



alarm Monitor room alarm Monitor room

Monitor wall

Location Control trainingroom C116 (Trainingroom)
Time Wed, 08 Jul 2015 16h18:09
State Acknowledged by me

1 Staff
● Yes ○ No

2 cleaner
○ Yes ● No

3 unauthorized
○ Yes ● No

Comments
Staff= Jens

The alarm handling process consists of three steps:

1. Taking responsibility for (acknowledging) an alarm.
2. Filling in the alarm response.
3. Completing the alarm.

Taking Responsibility for an Alarm

Accepting an alarm is the first step you must take in the alarm handling process. Doing so will remove the alarm from other users' New Alarms Lists, and make you responsible for its completion.

There is more than one way to take responsibility of an alarm, the most obvious being to click the Acknowledge Alarm button . Indirect ways of acknowledging an alarm are to view the attached camera in a viewer, or by displaying the attached camera or site on a map. This may be done by dragging and dropping the alarm item onto a viewer or a map, or by using one of the "view" buttons on the alarm card.

Filling in the Alarm Response

Each type of alarm can have its own specific alarm response procedure. You must complete each of the alarm responses in sequence before you can complete the alarm.

The comments field is not required, but users are encouraged to enter any relevant or additional information here.

Completing an Alarm

Once all the alarm handling procedures are completed you will be able to complete the alarm. To complete the alarm, click on the Complete Alarm button. If any of the alarm responses are not filled in, G-SIM will display an error in the comments field.

Alarms not completed within 24 hours of generation will be flagged with a status indicator (See **Alarms List**).

ⓘ **As much as some people may like believe otherwise, life is not completely predictable. Thus the alarm handling procedure may not always reflect reality. In such cases you might not be able to complete the procedure (and thus the alarm) because there is a missing option at one of the steps.**
If that happens, simply choose one of the incorrect options, explain it in the comments section (possibly all in capital letters), and let the administrator know that the procedure must be amended. This last step is critical.

Transferring an Uncompleted Alarm

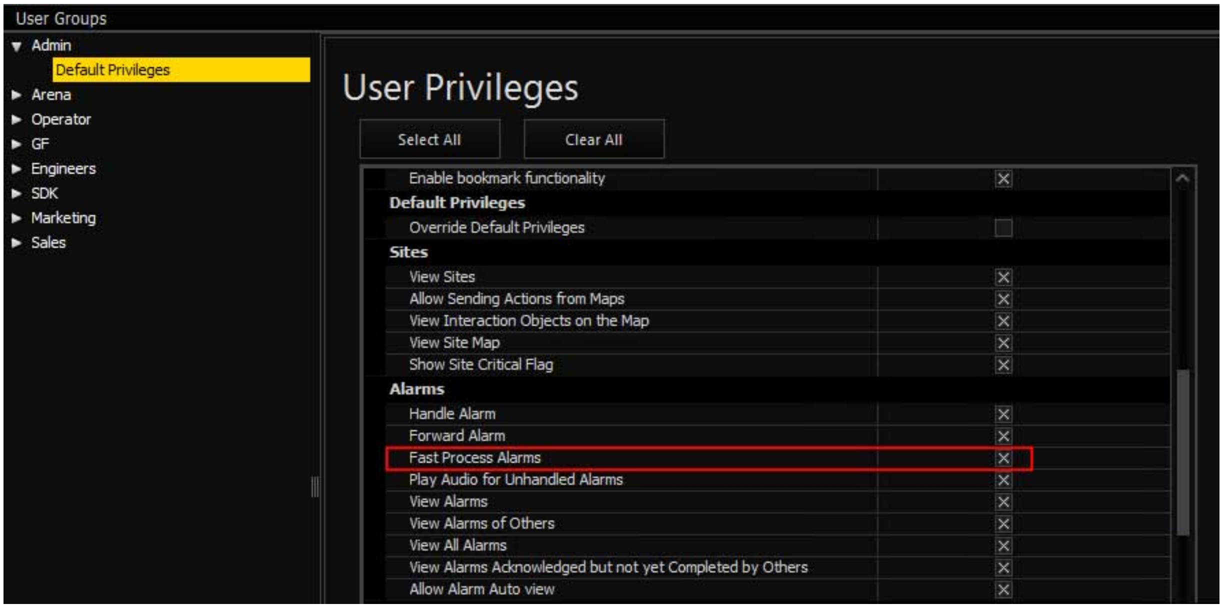
Sometimes you acknowledge an alarm which you cannot complete (end of shift, insufficient knowledge, etc.). This is done by clicking the Transfer Alarm button and then selecting a user to transfer it to. After a user was selected, the alarm will be moved from the list of acknowledged alarms to the list of new alarms. It will, however, stay visible to you until the other user accepts it, or you take it back (by pressing the Acknowledge button). The alarm will remain your responsibility until it is accepted by the transferred user.

ⓘ **Alarms may be transferred more than once between the same or different users.**

Fast Processing

Alarms can be quickly accepted and closed using the **Fast Process** button. Only two settings are necessary: firstly, the user must have the right to do this and secondly, the alarm must be enabled for fast processing.

The user is granted the right under **Users and Security** > **Users** > **Default Privileges** > **Alarms** > **Fast Process Alarms**. This can also be granted for a user group.



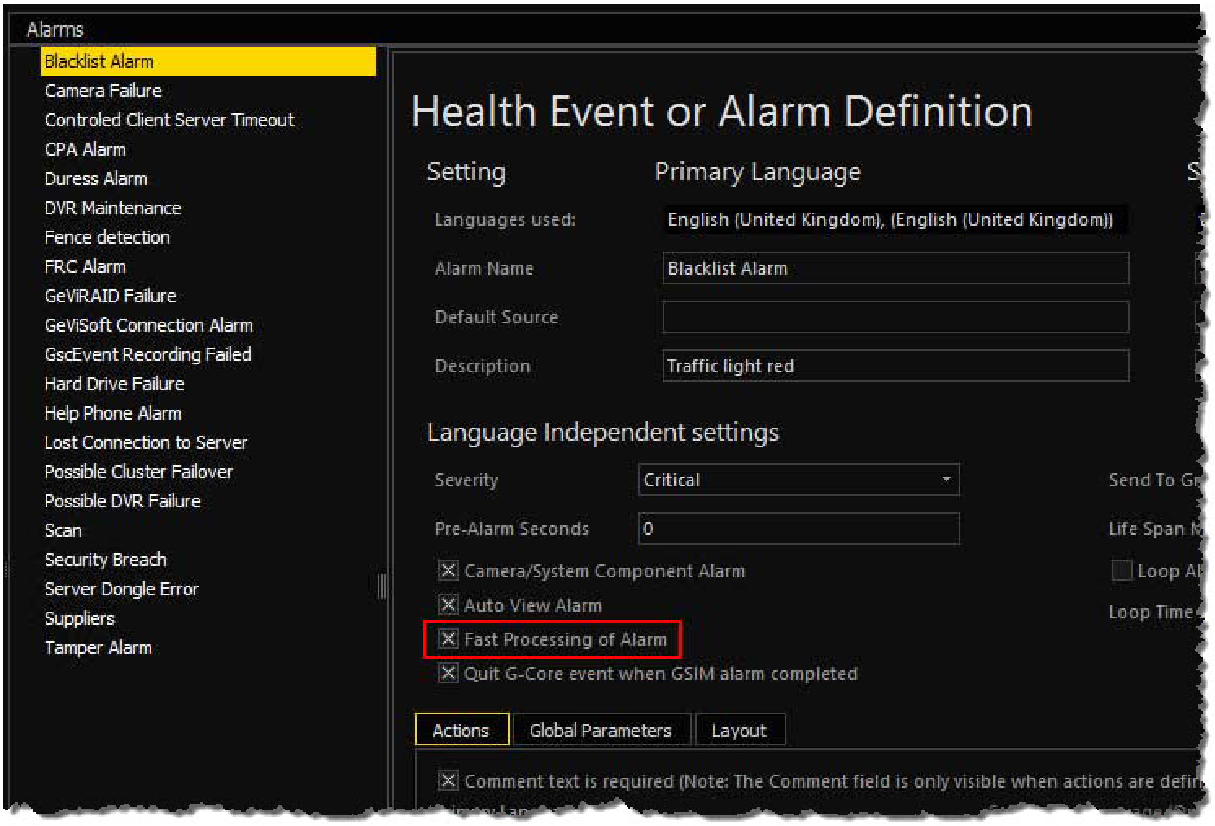
User Groups

- ▼ Admin
  - Default Privileges
- ▶ Arena
- ▶ Operator
- ▶ GF
- ▶ Engineers
- ▶ SDK
- ▶ Marketing
- ▶ Sales

User Privileges

Enable bookmark functionality	☒
Default Privileges	
Override Default Privileges	□
Sites	
View Sites	☒
Allow Sending Actions from Maps	☒
View Interaction Objects on the Map	☒
View Site Map	☒
Show Site Critical Flag	☒
Alarms	
Handle Alarm	☒
Forward Alarm	☒
Fast Process Alarms	☒
Play Audio for Unhandled Alarms	☒
View Alarms	☒
View Alarms of Others	☒
View All Alarms	☒
View Alarms Acknowledged but not yet Completed by Others	☒
Allow Alarm Auto view	☒

For our example, we allow quick editing for the **Blacklist Alarm** under **Health and Alarms** > **Alarms**.



Alarms

- Blacklist Alarm
- Camera Failure
- Controled Client Server Timeout
- CPA Alarm
- Duress Alarm
- DVR Maintenance
- Fence detection
- FRC Alarm
- GeViRAID Failure
- GeViSoft Connection Alarm
- GscEvent Recording Failed
- Hard Drive Failure
- Help Phone Alarm
- Lost Connection to Server
- Possible Cluster Failover
- Possible DVR Failure
- Scan
- Security Breach
- Server Dongle Error
- Suppliers
- Tamper Alarm

Health Event or Alarm Definition

Setting	Primary Language
Languages used:	English (United Kingdom), (English (United Kingdom))
Alarm Name	Blacklist Alarm
Default Source	
Description	Traffic light red

Language Independent settings

Severity	Critical
Pre-Alarm Seconds	0

☒ Camera/System Component Alarm

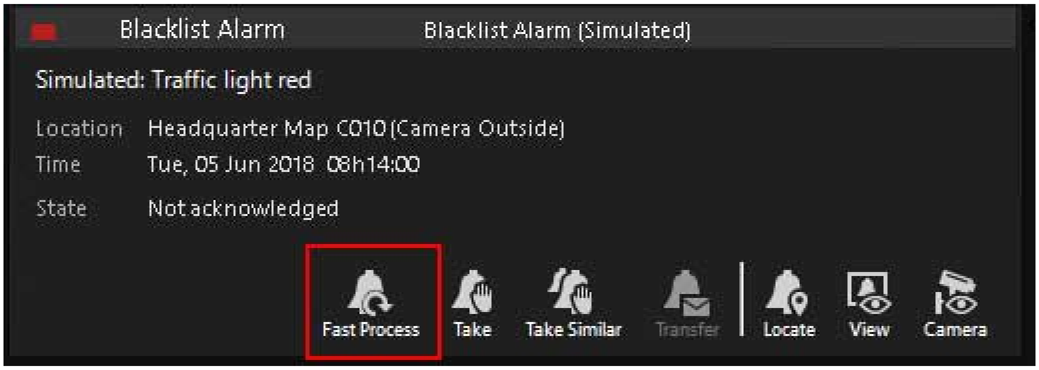
☒ Auto View Alarm

☒ Fast Processing of Alarm

☒ Quit G-Core event when GSIM alarm completed

☒ Comment text is required (Note: The Comment field is only visible when actions are defi

If both conditions are met, the **Fast Process** button appears in addition to the known buttons of the alarm display.



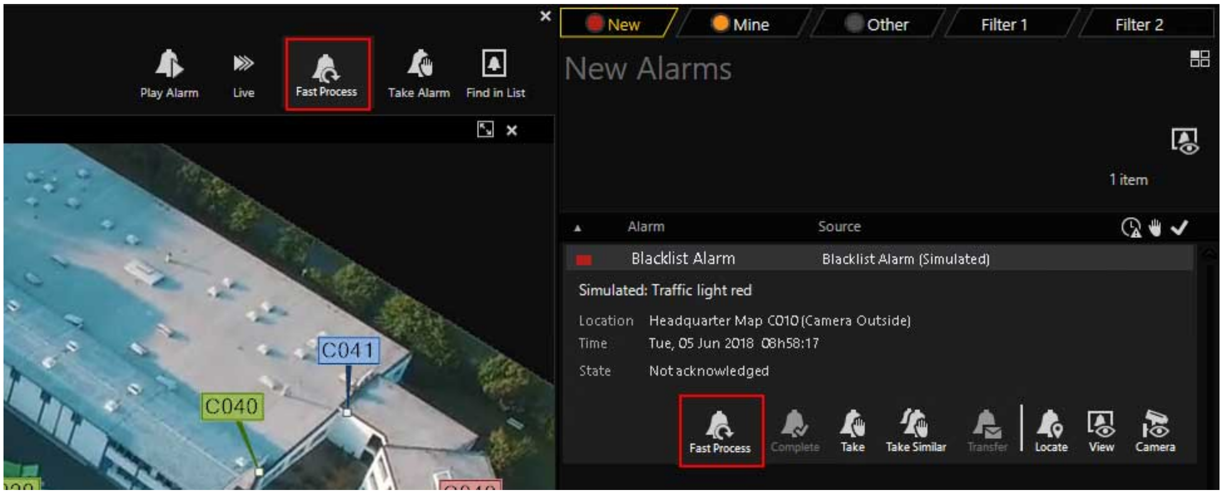
Blacklist Alarm — Blacklist Alarm (Simulated)

Simulated: Traffic light red

Location	Headquarter Map C010 (Camera Outside)
Time	Tue, 05 Jun 2018 08h14:00
State	Not acknowledged

With a click on the **Fast Process** button, the alarm is accepted and completed.

The button also appears also in the alarm view:



Alarm	Source
Blacklist Alarm	Blacklist Alarm (Simulated)

Simulated: Traffic light red

Location Headquarter Map C010 (Camera Outside)
Time Tue, 05 Jun 2018 08h58:17
State Not acknowledged

Dragging and Dropping Alarms

Dragging an Alarm Item

Drag-and-drop operations where Alarm Lists are the drop sites is the only time an actual alarm is dragged and dropped. This would happen when an alarm is dropped on a list to select and open that alarm in the list. In all other cases the dragged item is actually the object attached to the alarm, e.g. a camera or a site. The type of object attached (if any) will determine the drop action. An alarm drag may be initiated from an Alarm List.

Dropping an Alarm Item

As mentioned above the drop-action of an alarm usually depends on the type of object attached to the alarm:

- If a camera is attached to the alarm, it may be dropped anywhere a camera could be dropped.
- If a site is attached to the alarm, it may be dropped anywhere a site could be dropped.
- If it is dropped onto a list and the list contains the dropped alarm (i.e. the list was not filtered to exclude the alarm), then the alarm will be selected and the card expanded to show the alarm detail.
- If it is dropped onto a viewer, the recorded camera footage at the time of the alarm will be displayed. The viewer will be placed in pause mode and the

user may then review it from that point or step through it forwards or backwards.

- If it is dropped onto a map, the map will pan to show the camera in middle of the map, marked with a bright green border. If the current map does not contain the camera, the correct map will be loaded.

Alarm Reports

We have a powerful Alarm Reporting tool, accessed via clicking on the Reports button at the top of the home screen. Though it is similar to the query builder, it has extended functionality to allow both grid-based and graphical output.

The top half of its screen works in exactly the same way as the Alarm filtering interface. See **Filtering** for more on how to use it. The top half is used to define the query, while the bottom half is used to define how to present the results.

Sorting: Click on the header to sort (click again to toggle the sort order).

Grouping: Drag a column header such as "Site" to the bar directly above the headers. If you want a secondary sort order, drag the next header onto the same bar. In fact, you can continue to refine the presentation of the data in this way. The number of matching items is displayed in each header.

Filtering: Filters may be applied to data by clicking on the small filter icon in the top right position of headers. An edit filter section will appear at the bottom of the grid.

Graphing: Since some data are best viewed graphically, we have the option to display the returned data in a graphical format — simply click on the Graph tab. You are able to change what is used for the x-axis as well as the time interval.

Once you are happy with the report, you can print, mail, or export it to PDF. This output functionality is all accessed via the printer icon at the top right of the results pane. At the top of the output screen are a number of icons you can use to change the presentation and other options. They are all self-explanatory, and have tool-tips if you are unsure what any of them may do.

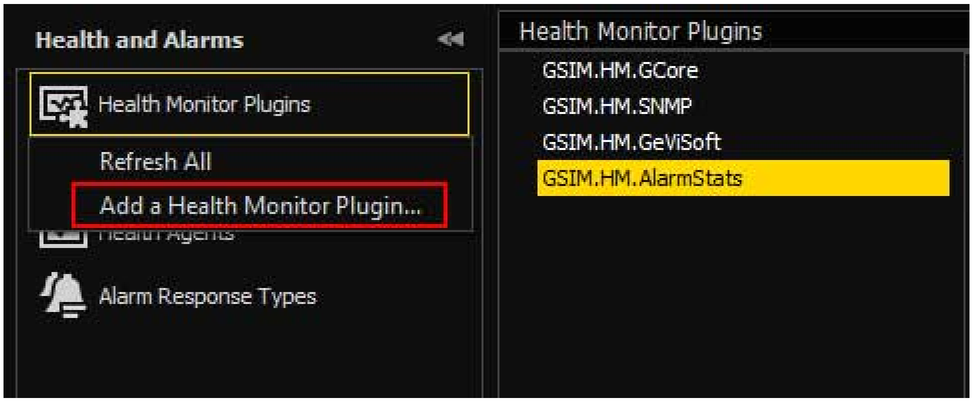
Export Alarm Information In Separate Database

This function stores alarm information in a database of your choice.

Management Console

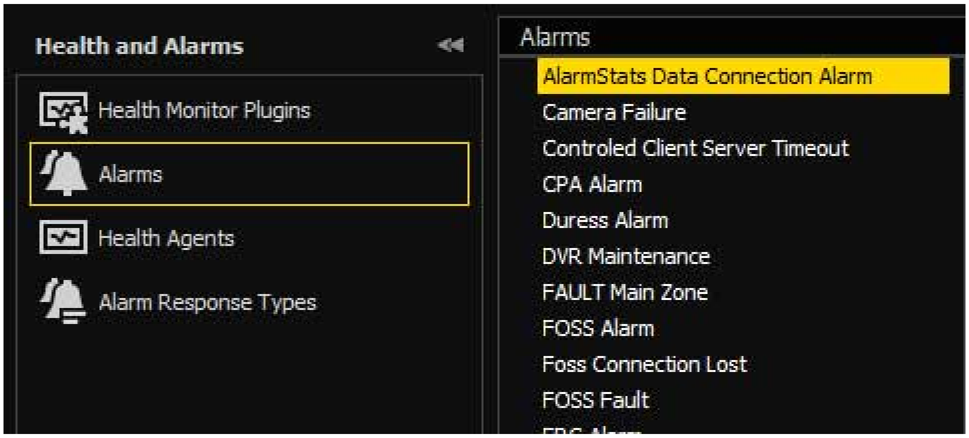
i **Make sure you are working in expert mode.**

To **Health and Alarms** right click **Health Monitor Plugins** and then **Add Health Monitor Plugin**.

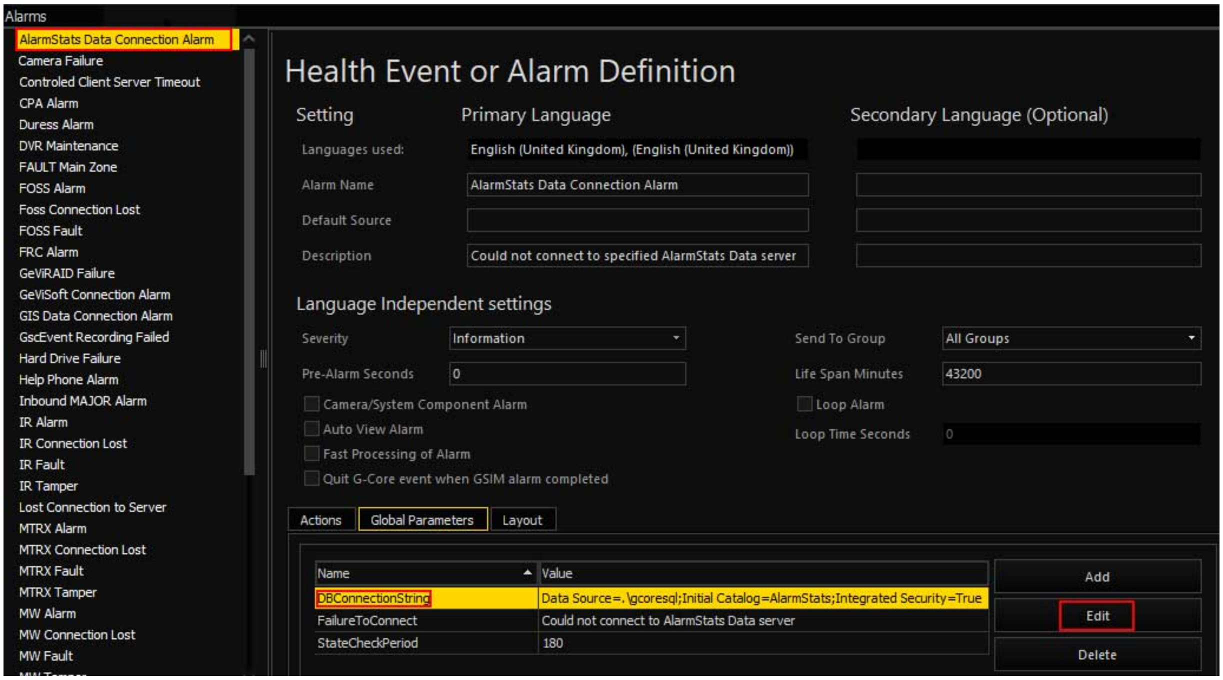


Navigate to the installation folder of the Health Agent `c:\Program Files\Geutebrueck\GSim\Health Agent` and select the file `GSIM.HM.AlarmStats.dll`.

Right-click **Health Monitor Plugins** and then **Refresh All**, click **OK**. This will add a new alarm type, which is listed under Alarms.



This alarm allows you to configure the database connection string under the global parameters.



Alarms

- AlarmStats Data Connection Alarm
- Camera Failure
- Controled Client Server Timeout
- CPA Alarm
- Duress Alarm
- DVR Maintenance
- FAULT Main Zone
- FOSS Alarm
- Foss Connection Lost
- FOSS Fault
- FRC Alarm
- GeViRAID Failure
- GeViSoft Connection Alarm
- GIS Data Connection Alarm
- GscEvent Recording Failed
- Hard Drive Failure
- Help Phone Alarm
- Inbound MAJOR Alarm
- IR Alarm
- IR Connection Lost
- IR Fault
- IR Tamper
- Lost Connection to Server
- MTRX Alarm
- MTRX Connection Lost
- MTRX Fault
- MTRX Tamper
- MW Alarm
- MW Connection Lost
- MW Fault

Health Event or Alarm Definition

Setting	Primary Language	Secondary Language (Optional)
Languages used:	English (United Kingdom), (English (United Kingdom))	
Alarm Name	AlarmStats Data Connection Alarm	
Default Source		
Description	Could not connect to specified AlarmStats Data server	

Language Independent settings

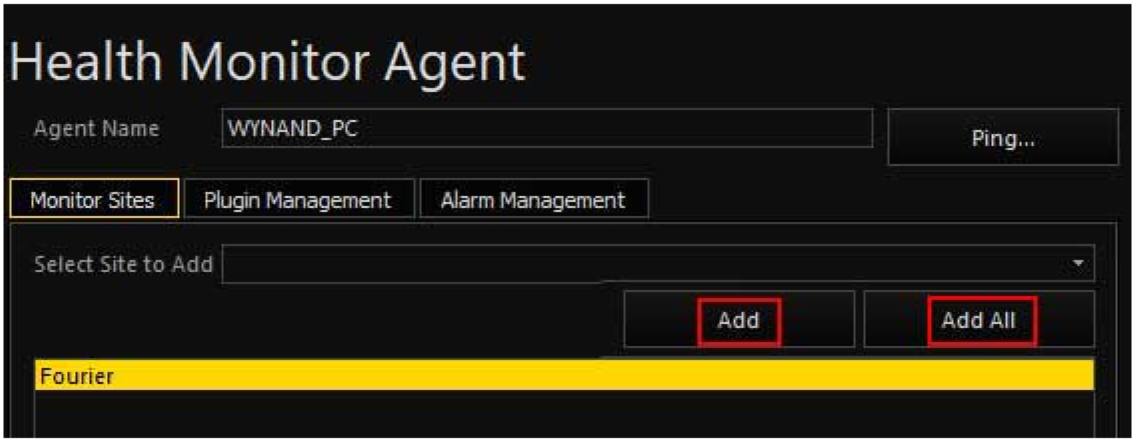
Severity: Information
Send To Group: All Groups
Pre-Alarm Seconds: 0
Life Span Minutes: 43200
□ Camera/System Component Alarm
□ Loop Alarm
□ Auto View Alarm
Loop Time Seconds: 0
□ Fast Processing of Alarm
□ Quit G-Core event when GSIM alarm completed

Name	Value
DBConnectionString	Data Source=.\gcoresql;Initial Catalog=AlarmStats;Integrated Security=True
FailureToConnect	Could not connect to AlarmStats Data server
StateCheckPeriod	180

Click the **Edit** button, change the connection string, and save the data.

Add an agent if you do not already have one.

Also, assign at least one **site** to let the agent know what to monitor. In the case of the **Alarm Stats plugin**, sites are not used, so you can add all sites.



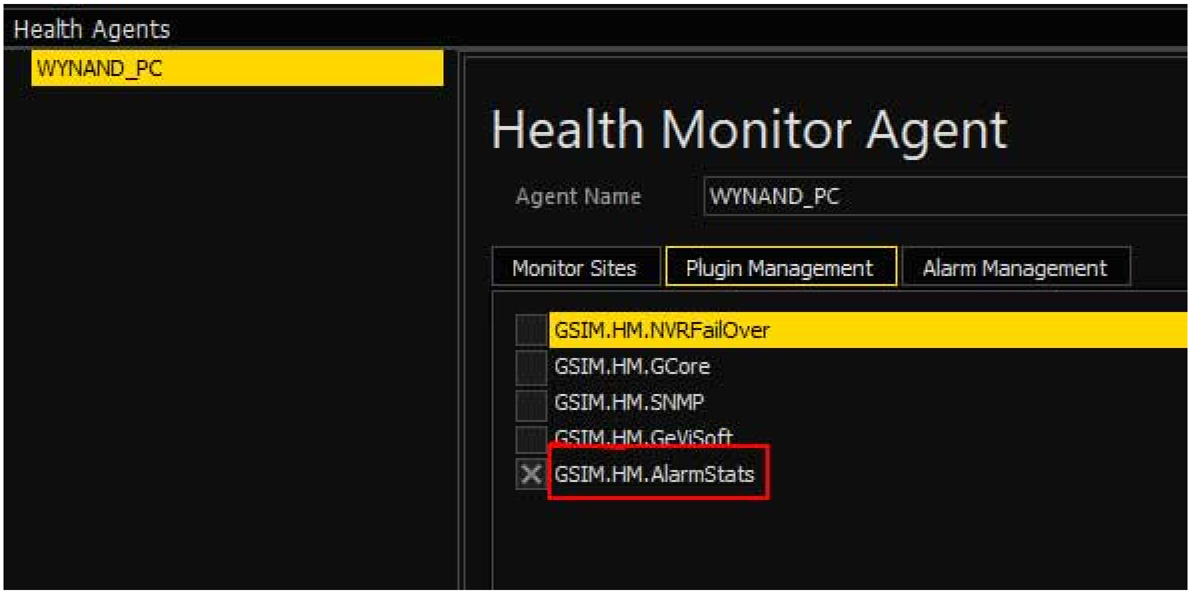
Health Monitor Agent

Agent Name: WYNAND_PC

Select Site to Add

Fourier

Now you can assign the plugin to an agent or health agent.



Health Monitor Agent

Agent Name: WYNAND_PC

- ☐ GSIM.HM.NVRFailOver
- ☐ GSIM.HM.GCore
- ☐ GSIM.HM.SNMP
- ☐ GSIM.HM.GeViSoft
- ☒ GSIM.HM.AlarmStats

Send the settings to the server and start the agent.

To check if everything works as expected, close an alarm in Operator Console and then check the table named: GSIM_Alarms for the alarm entry.

Video Events

Video Events are a convenient and powerful way to mark sections of video footage for future review. It allows a user that is watching video footage (live or not) to log any suspect behaviour or events as they are seen. These marked sections of video are called Video Events. While logging such events or adding detail to them, the system will keep track of them and give the user easy access to the stored events.

Creating Events can be as simple as clicking on the New Video Event button which will automatically save a 20 second clip (video section) of the Active Video starting from the current frame, and fill in all Event detail with default values. You can then edit the relevant event details, such as the event type, description, extra notes, status detail, video section length.

A powerful feature is the ability to add more video clips to the Event. This is typically done during the audit or evidence preparation phases, and allows you to add relevant footage. Adding footage from another camera is as simple as dragging it onto the event in the event list.

As with most other functionality, access is granted with Privileges on a per-user basis.

Event List

The Events List gives you quick access to all Events, pending and historical. Each row in the list represents an event, showing the type and camera identifier, and is sorted according to date with the newest at the top. Status indicators show whether an Event is private (visible to the current user only) and if an Event is in edit mode.

List Layout and Buttons

The following points stand out:

Pending Events: You will not see Private events that are assigned to someone else.

Refresh: Some filters could include dynamic items (e.g. events of the past hour) in which case you would need to refresh the list from time-to-time.

Event Detail: An Event's Detail will be displayed if you select a camera item in the Events List. See Event Detail, below, for detail.

Dock List: This function allows the Events List to be duplicated in any viewer. After clicking it, the available Viewer windows will be highlighted with the corresponding shortcut key that may be pressed to dock the list in the designated viewer.

New Video Event: Creates a new Video Event and adds a 20 second clip from the Active Video to the list of Event Instances.

Filtering the Events List

You may filter the events list as per usual (See **Filtering**). There is a built-in filter which shows only the pending (open) events — those which still need to be completely defined. Filtering events is extremely powerful: think of how useful it is to be able to create a list of specific events for a particular time period for specific cameras — without having to do any searching of your own.

Event Status Indicators

The following status icons may be displayed for an event in the Events Lists:

Private Event: This event is private, meaning it is only visible to you (who created it). Events that does not display this icon are public events and visible to all users.

Edit mode: The event is in edit mode and may be modified. All cameras dropped on the Events tab will be added to this event. This is a toggle button, so press it again to leave edit mode.

Event Detail

An Event Detail Card will be displayed if you select an item in the Events List. The Detail Card displays the Event's information, status and a list that contains one or more Event Instances (i.e. sections of video added to the Event Instances List).

Status Detail

When an Event is created, it will automatically be marked as both "Pending – Open", and "Private – Visible to me only" in the Status Detail.

To close an Event, clear the checkbox next to "Pending – Open". This will expose the event to your filters.

A Private Event is only visible to its owner (you), whilst a Public Events is visible to all users that have the necessary privilege. All Private Events are marked with the Private status icon in their Event headers. To make an Event Public, simply clear the checkbox next to "Private – Visible to me only".

Event Type

The Event Type is a drop-down combo box that gives you a list of Event Types to choose from. When you create a new event, the default value will be "Other" until you change it.

The following Event Types are currently available:

- Alcohol/Drugs
- Assault
- Harassment
- Illegal Conduct
- Loitering
- Suspect Behaviour
- Theft
- Trespassing
- Vandalism
- Other

Each Event Type has a shortcut key assigned to it, making it easy to create a specific Event quickly from anywhere in G-SIM (see Shortcut Keys, below). You can also do it directly from the viewer. See **Viewing Camera Footage** for more.

Adding Video Sections to an Event

Video sections may be added to an Event which is in Edit Mode by:

- Dragging a camera from a viewer, the Camera List or a map and either dropping it on the Event Instances List, or on the Events Tab. It is thus possible to put the event in Edit Mode, go to the Camera List and drag cameras from the list to the Events Tab.
- Pressing a Shortcut Key (See **Shortcut Keys**).

Ordering Cameras in an Event Instances List

If an Event is in Edit Mode, the video sections may be ordered by selecting a camera and moving it up or down in the list with the two buttons on the right of the list. Click the Remove From Event button to remove a video section from the Event.

Date and Start Time

When Live video is added to an Event, a 20 second video section is added to the Event Instances List that shows its creation time as the Date and Start Time (i.e. the moment you dragged-and-dropped it or clicked the button).

If you are reviewing footage (thus it’s not Live) and add it to the list, a 20 second video section, starting from the date and time of the video, is added to the Event Instances List, with a Date and Start Time that indicates the timestamp on the first frame of the video section.

There is one exception: if a video event was defined before you dragged the camera from a viewer to the video event and it is within 10 seconds of the previously-defined section, then the section's start and length will be used.

All these video sections can be viewed the same way as cameras throughout G-SIM, i.e. drag-and-drop on viewer or using the action buttons (see Event Actions below).

Video Section Lengths

The default length for a video section is 20 seconds, but this can always be changed after the video section has been added. Just click on the seconds and type the new length you want it to be. In the case of viewers with pre-defined video sections, these parameters will be used as described above.

Event Actions

The following action buttons need some explanation:

Export Video Event This button lets you export the Event as a Geutebrück cut-list, which can be archived and reviewed without the system at a later stage. See Back-up Events, below.

Edit Video Event This is a toggle button. It will remain selected as long as the Event is in Edit Mode. Note that it will stay in edit mode even if you switch to another tab. This is to allow you to drag cameras from the camera tab, for example. Dropping them onto the Events tab will then add them to the event in edit mode.

Creating and Modifying Video Events

Creating a New Event

You can create an empty Event (without selecting any video sections) by clicking the New Video Event button in the toolbar at the top of the Events List. Alternatively, you can use Live video to create an Event by clicking on the Create New Video Event button on the left hand side of the video control bar while viewing video. The Detail Card of the Event will expand in the Events List and will automatically be in Edit Mode, allowing you to select a type of event, enter a description and to mark it as private. Video sections may now be added to the Event (See **Event Detail** for how to add and sort video sections).

Editing an Event

An Event must be in Edit Mode to be able to modify it. Click the Edit Video Event button to activate this Mode.

Only one Event can be in Edit Mode at any time and it will be indicated by the “edit” icon in the Event header. Whilst in Edit Mode, the Edit Video Event button will remain selected, and the LED on the Events Tab will light up yellow (much like editing a Tour). All the same options apply as for a new Event: video sections may be added, removed, ordered or the type, description or visibility (public or private) of the Event may be changed.

Saving an Event / Taking It Out of Edit Mode

An Event will be taken out of Edit Mode (and subsequently saved) if:

- The Edit Video Event button is clicked again (released).
- Any other Event is selected in the Events List

Remember that the yellow LED is the quickest way to see if there is an event open in Edit Mode.

Shortcut Keys

While viewing any video, you can instantly create an Event by using the appropriate shortcut key. This will switch to the Events Tab and open a new Event in Edit Mode, using the Active Viewer as the Event Instance.

Shortcut	
Other	Ctrl + Shift + 0
Vandalism	Ctrl + Shift + 1
Theft	Ctrl + Shift + 2
Assault	Ctrl + Shift + 3
Suspect Behaviour	Ctrl + Shift + 4
Trespassing	Ctrl + Shift + 5
Loitering	Ctrl + Shift + 6
Harassment	Ctrl + Shift + 7
Alcohol/Drugs	Ctrl + Shift + 8
Illegal Conduct	Ctrl + Shift + 9

ℹ **If an Event is open in Edit Mode, using any shortcut key will simply add the Active camera to the open Event's Instance list, even if the shortcut key is for a different event type than the open Event. To create a new Event or a different type of Event using a shortcut key, you must first close the Event being edited.**

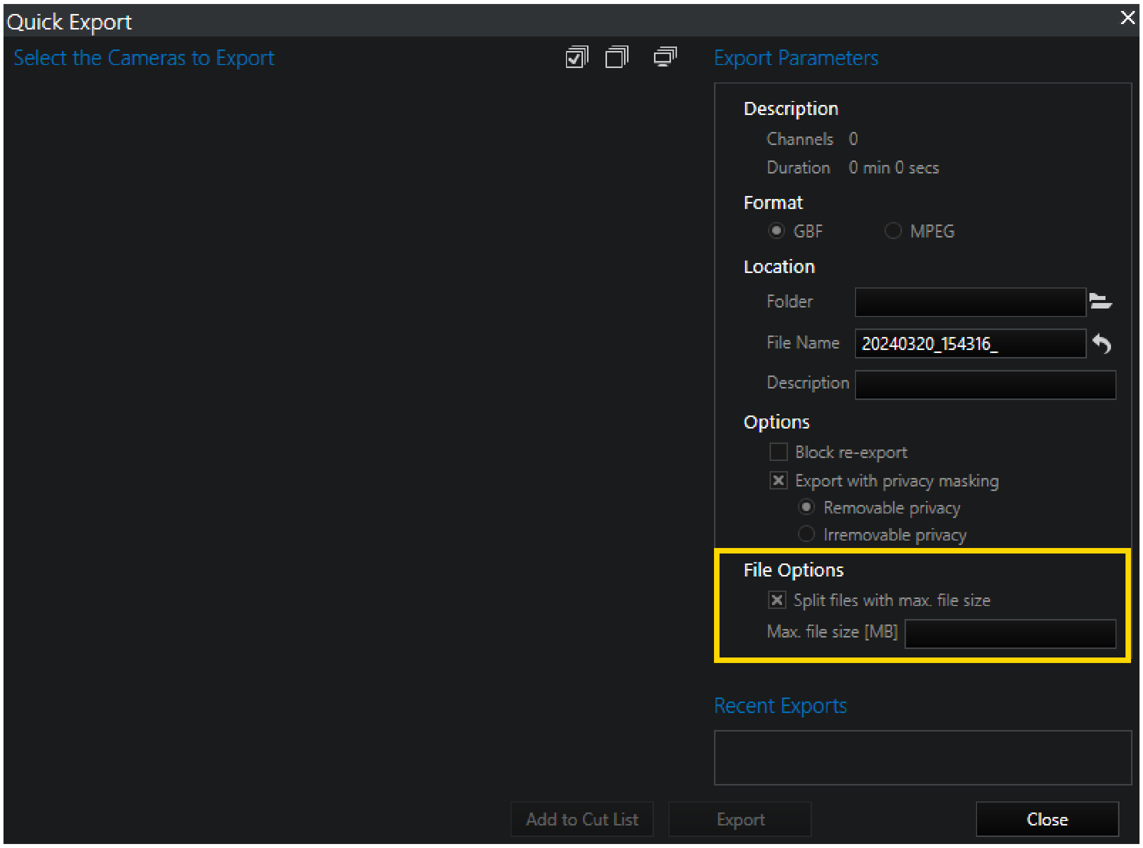
Export Video Event

Pressing ⇥ will export the event in question in any one of a number of different formats. Which you choose depends on the purpose of the export. The tabs and available options for export depend on the format chosen. For example, you can encrypt an export if it is to a Geutebrück cut list, but not if it to MPEG.

How to split export files:

1. In the toolbar, click on the button. The **Quick Export** dialog window opens.
2. Make the wished configurations in the **Export Parameters** section.
3. Under **File Options**, select the checkbox **Split files with max. file size** and enter a **Max. file size [MB]**.

   i The minimum file size must be 30 MB.



Description
Channels 0
Duration 0 min 0 secs

Format
● GBF ○ MPEG

Location
Folder
File Name 20240320_154316_
Description

Options
□ Block re-export
☒ Export with privacy masking
● Removable privacy
○ Irremovable privacy

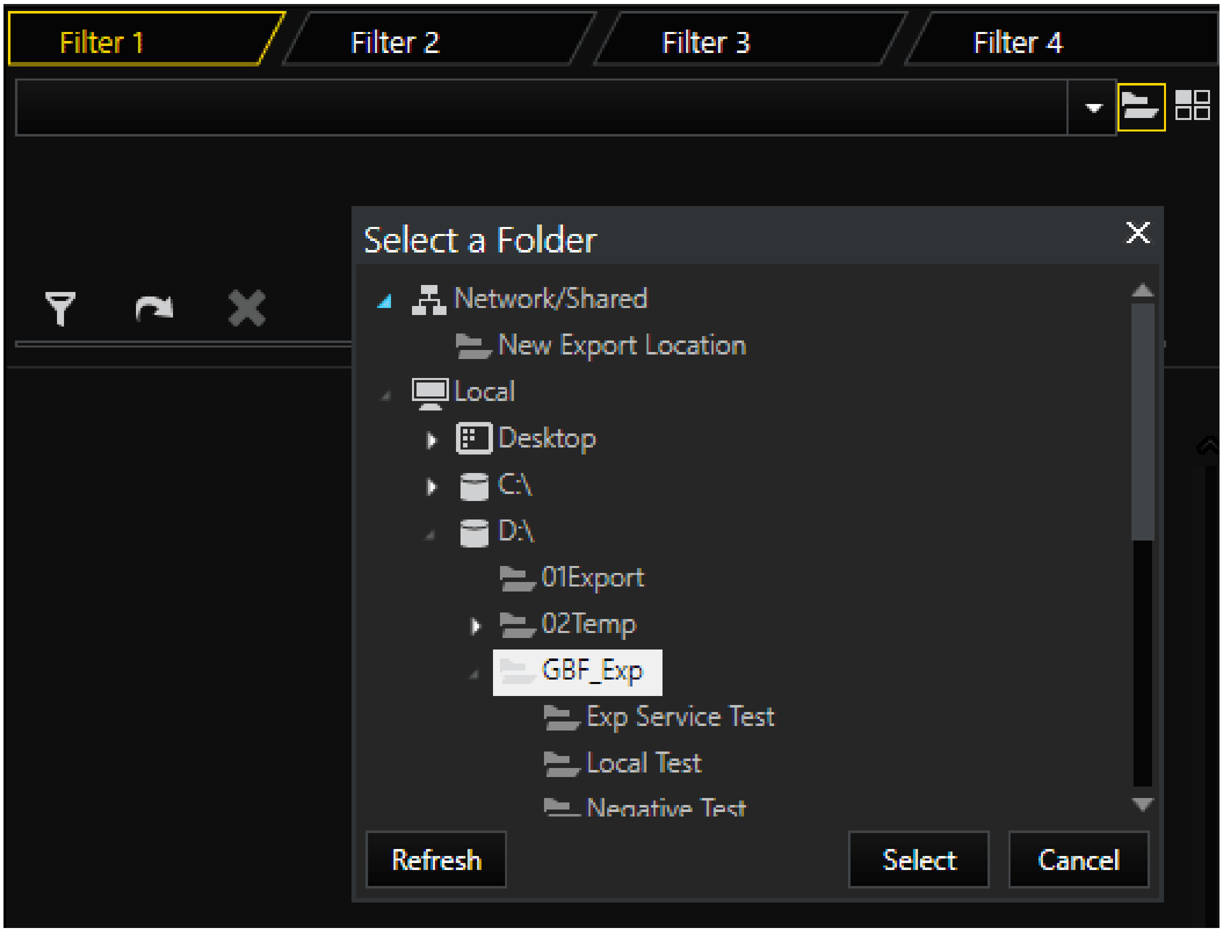
File Options
☒ Split files with max. file size
Max. file size [MB]

4. Click on **Export**.

Authentication of Exported Files

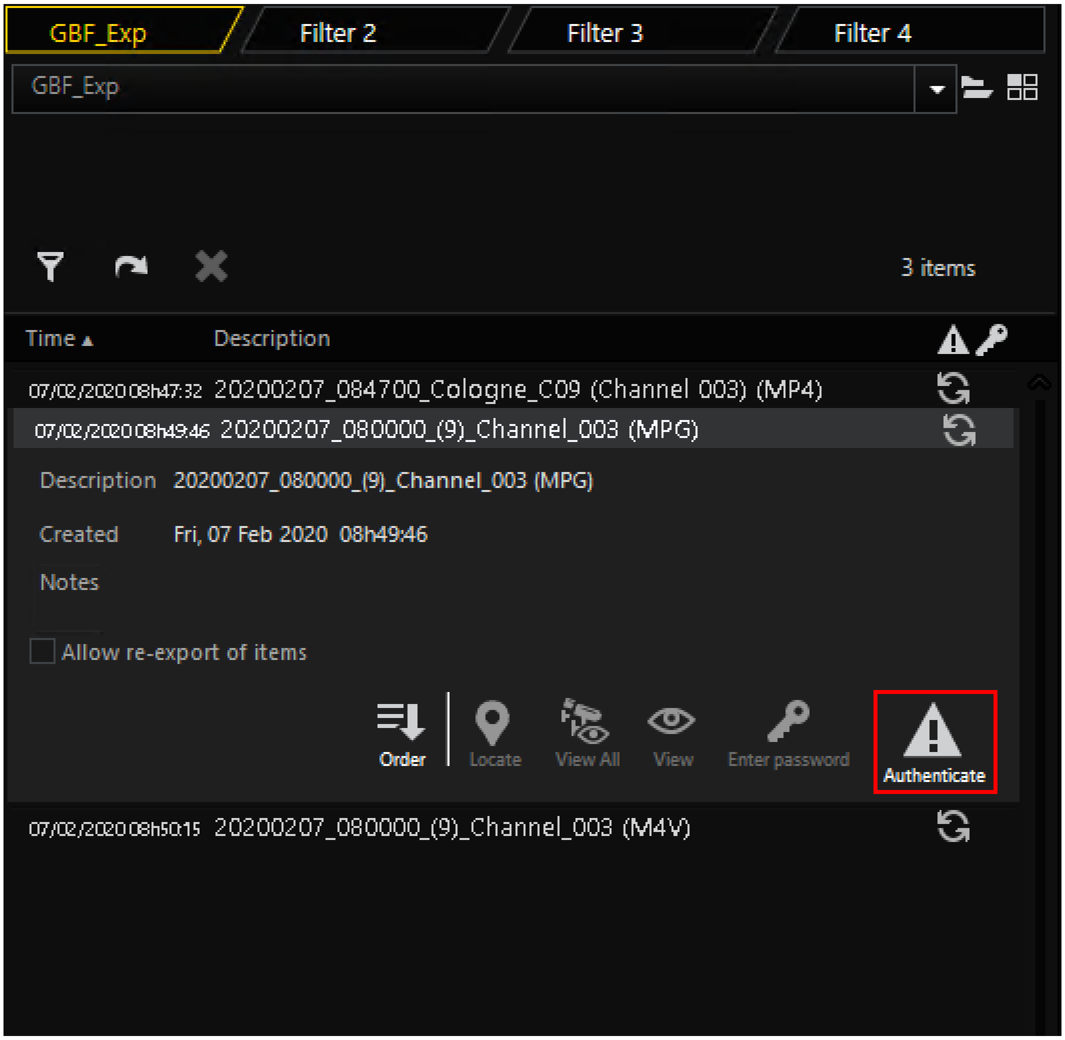
MPEG files are easy to authenticate.

Choose a folder in the Operator Console on the **Archive** tab which contains the exported files to be authenticated:



All the files that are stored in this directory (GBF and MPEG) are now listed. Files that can be authenticated are labeled with the 🔄 icon.

To authenticate a file, click on the file in the list to display the expanded view. Then click on the **Authenticate** button.



GBF_Exp

Time ▲	Description
07/02/2020 08h47:32	20200207_084700_Cologne_C09 (Channel 003) (MP4)
07/02/2020 08h49:46	20200207_080000_(9)_Channel_003 (MPG)
07/02/2020 08h50:15	20200207_080000_(9)_Channel_003 (M4V)

Description 20200207_080000_(9)_Channel_003 (MPG)

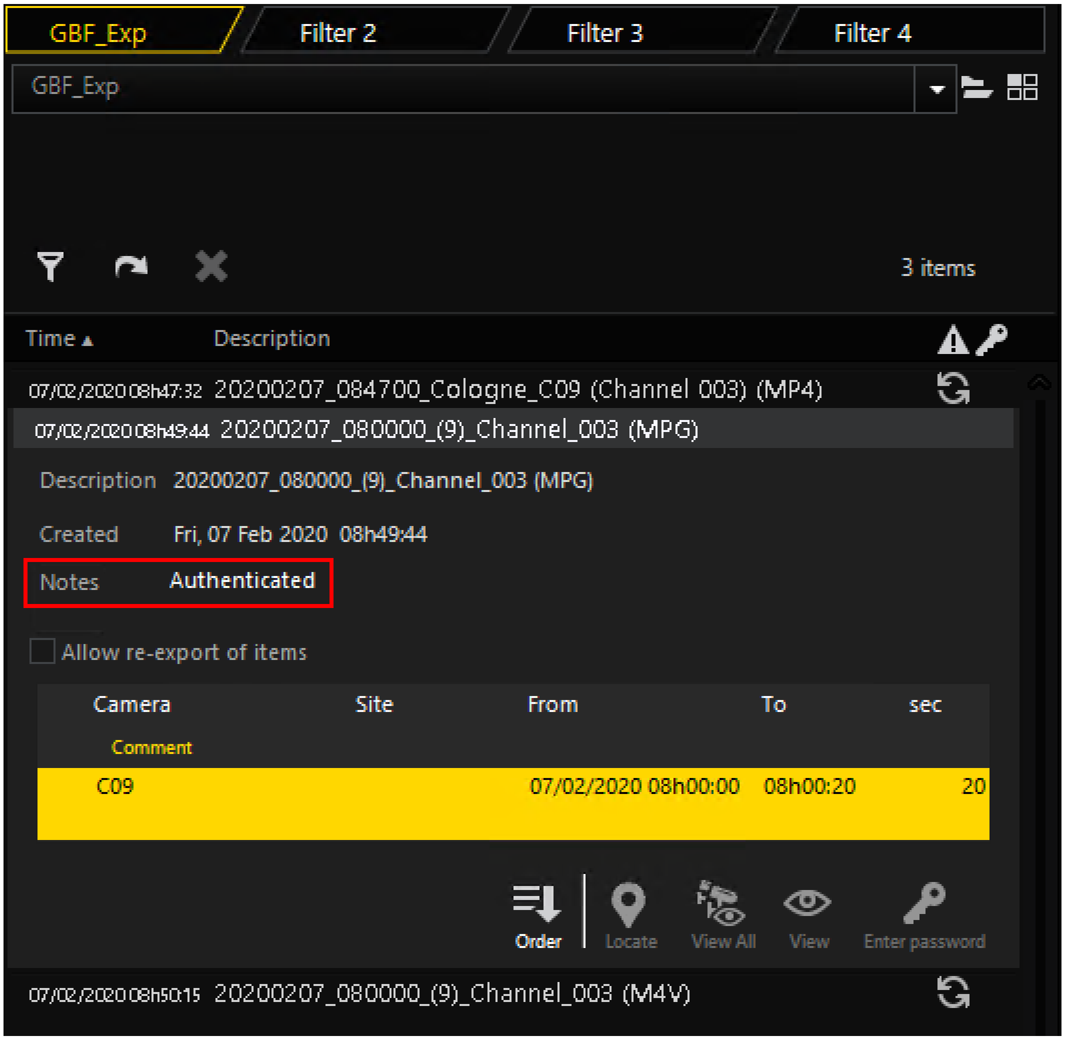
Created Fri, 07 Feb 2020 08h49:46

Notes

□ Allow re-export of items

In the expanded view under **Notes** the result of the authentication is displayed.

You can see the successful authentication of the selected file here:



Time ▲	Description
07/02/2020 08h47:32	20200207_084700_Cologne_C09 (Channel 003) (MP4)
07/02/2020 08h49:44	20200207_080000_(9)_Channel_003 (MPG)

Description 20200207_080000_(9)_Channel_003 (MPG)

Created Fri, 07 Feb 2020 08h49:44

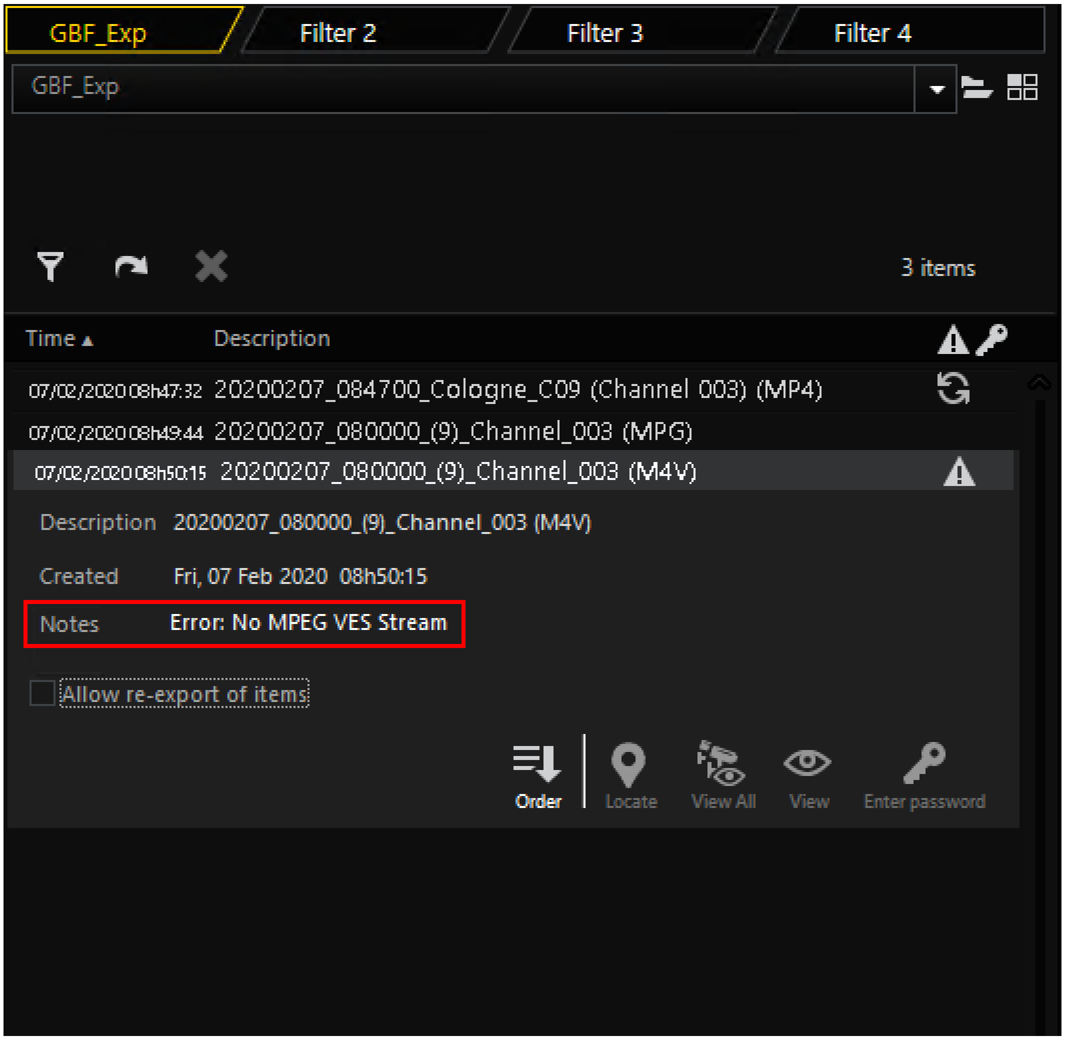
Notes Authenticated

□ Allow re-export of items

Camera Comment	Site	From	To	sec
C09		07/02/2020 08h00:00	08h00:20	20

Time	Description
07/02/2020 08h50:15	20200207_080000_(9)_Channel_003 (M4V)

If the authentication fails, a comment will be displayed under **Notes** and is labeled with the ⚠ icon:



Time	Description
07/02/2020 08h47:32	20200207_084700_Cologne_C09 (Channel 003) (MP4)
07/02/2020 08h49:44	20200207_080000_(9)_Channel_003 (MPG)
07/02/2020 08h50:15	20200207_080000_(9)_Channel_003 (M4V)

Description 20200207_080000_(9)_Channel_003 (M4V)

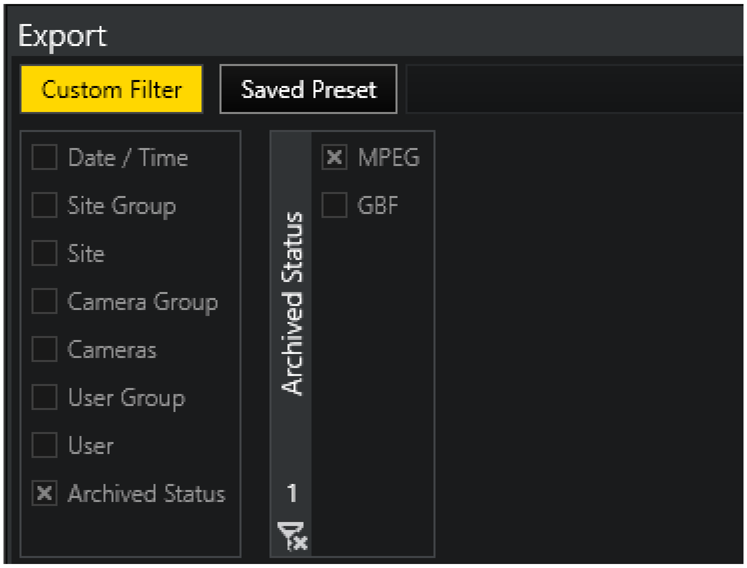
Created Fri, 07 Feb 2020 08h50:15

Notes Error: No MPEG VES Stream

□ Allow re-export of items

A filter can also be applied to the selected folder. To do this, click on the filter icon.
There is a new user-defined filter for the Archived Status specifically

for the archive tab. It allows the user to only display GBF or MPEG files.



☐ Date / Time
☐ Site Group
☐ Site
☐ Camera Group
☐ Cameras
☐ User Group
☐ User
☒ Archived Status

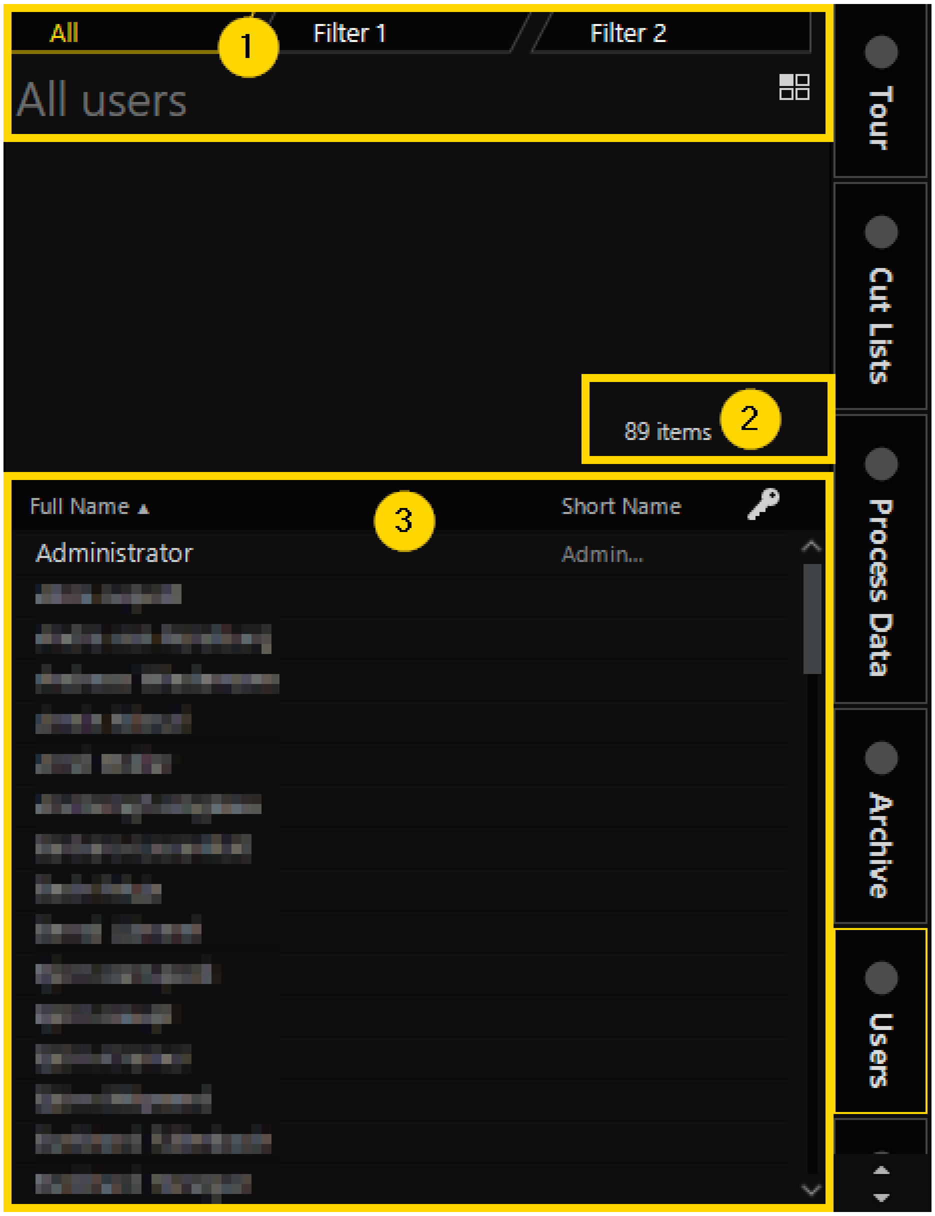
☒ MPEG
☐ GBF

Users

Under the **Users** tab you find a user list from which you can retrieve user data. You can apply filters to the list to find a user quicker and you can assign tasks or send messages to a user.

Overview

After opening the **Users** tab, the tabbed list **All users** appears:



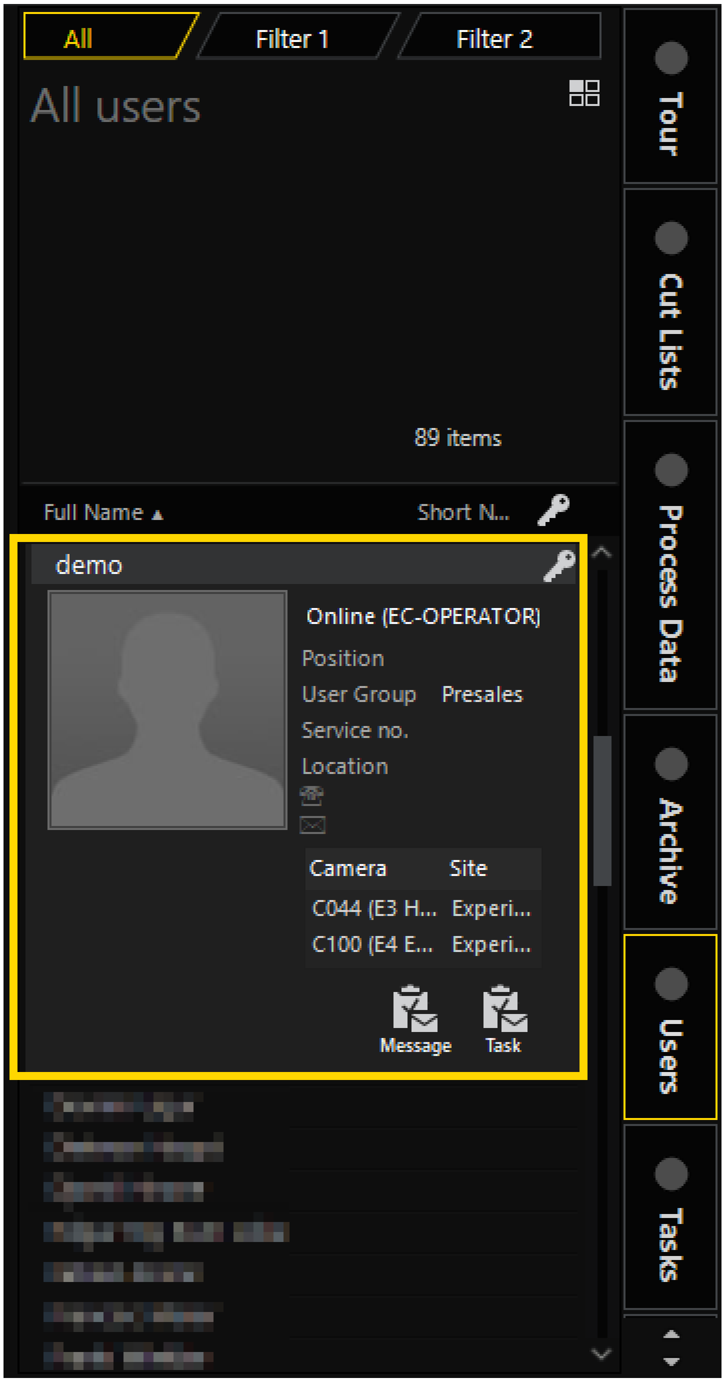
Full Name ▲	Short Name
Administrator	Admin...
[redacted]	

	Area	Description
1	Tabs	Displays the tabs which are available for you.
2	Items	Displays the number of users in the system.
3	User list	Displays a list of the users in the system which

	Area	Description
		contains: • Full name • Short name: alias which is used in messages, etc. • Log on status which is indicated by the key symbol. ⓘ **You can sort the list by using the arrow next to the Full Name column and** Apply Filters or Presets.

User Details

To see the details of a specific user, click on the respective name in the user list. The detail view opens:



demo

Online (EC-OPERATOR)

Position

User Group Presales

Service no.

Location

☎

✉

Camera	Site
C044 (E3 H...	Experi...
C100 (E4 E...	Experi...

[redacted]

The detail view shows you the following information if available for this user:

- Full name
- Short name

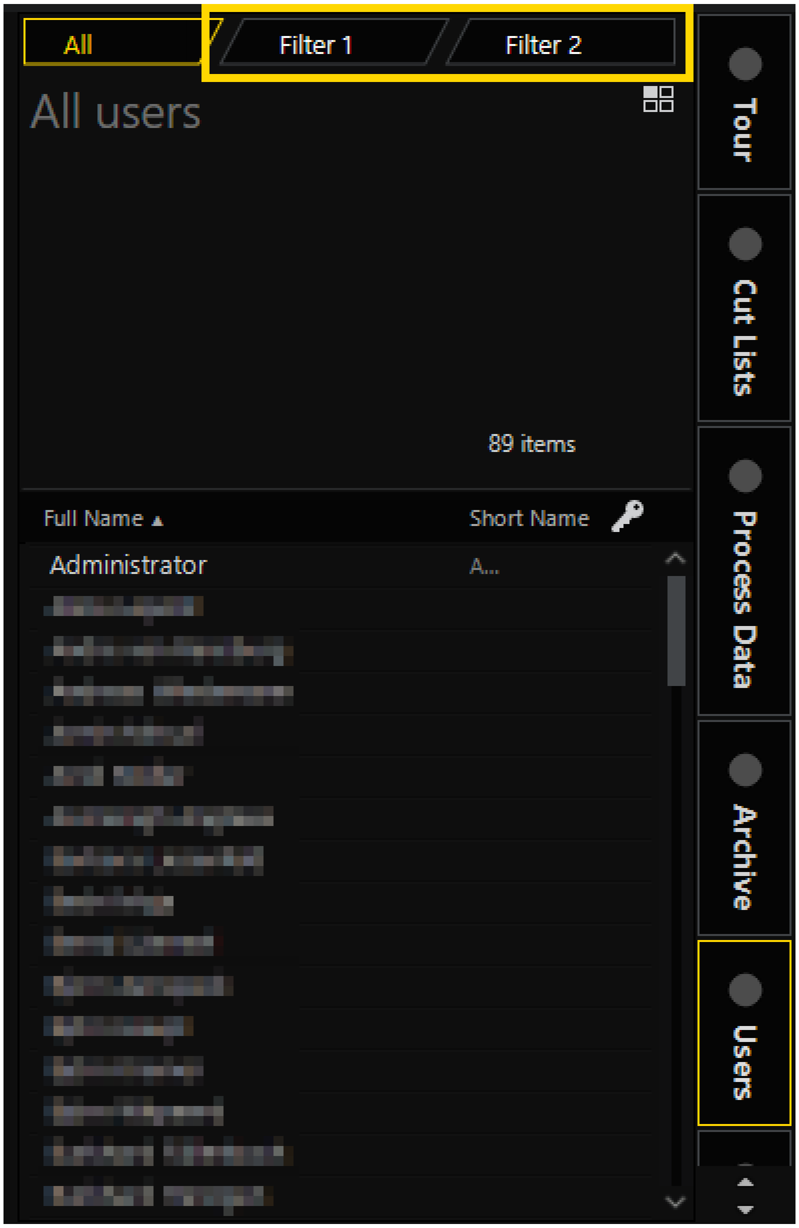
- Photo
- Login Status
- Position
- User Group
- Service no.
- Location
- Phone number
- E-Mail address

If the user is currently observing cameras or tours, the respective information is displayed here as well.

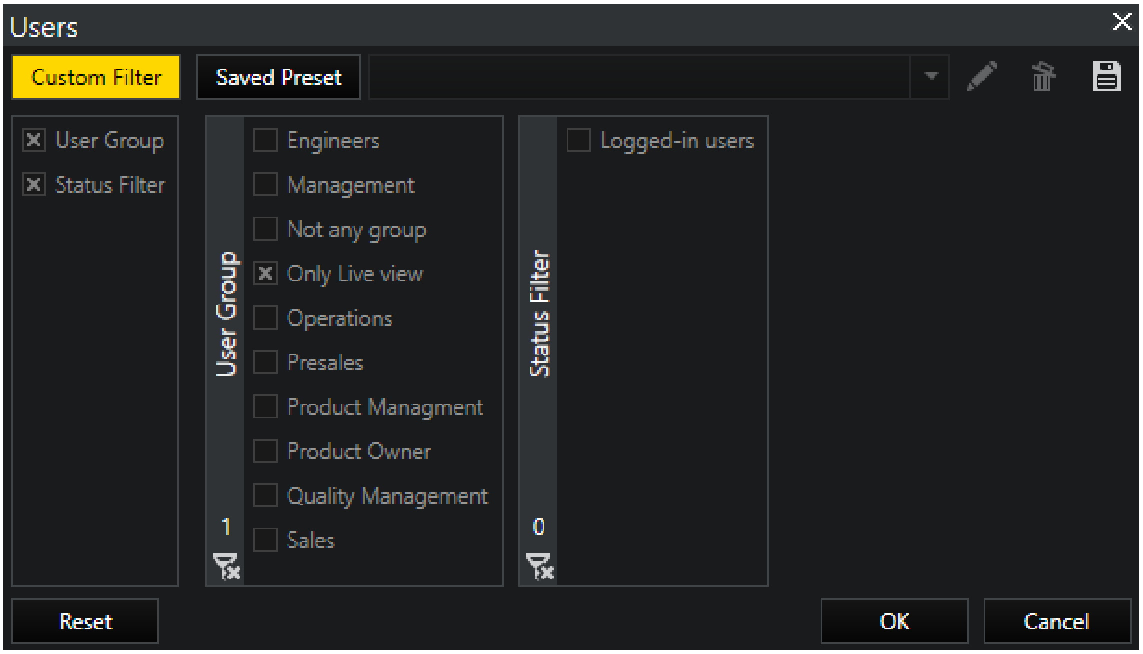
Additionally, the **Task** button is displayed with which you can assign a task to a user. The **Message** button with which you can send messages to a user is only displayed if the user is currently logged in. For detailed information see **User Actions**.

Apply Filters or Presets

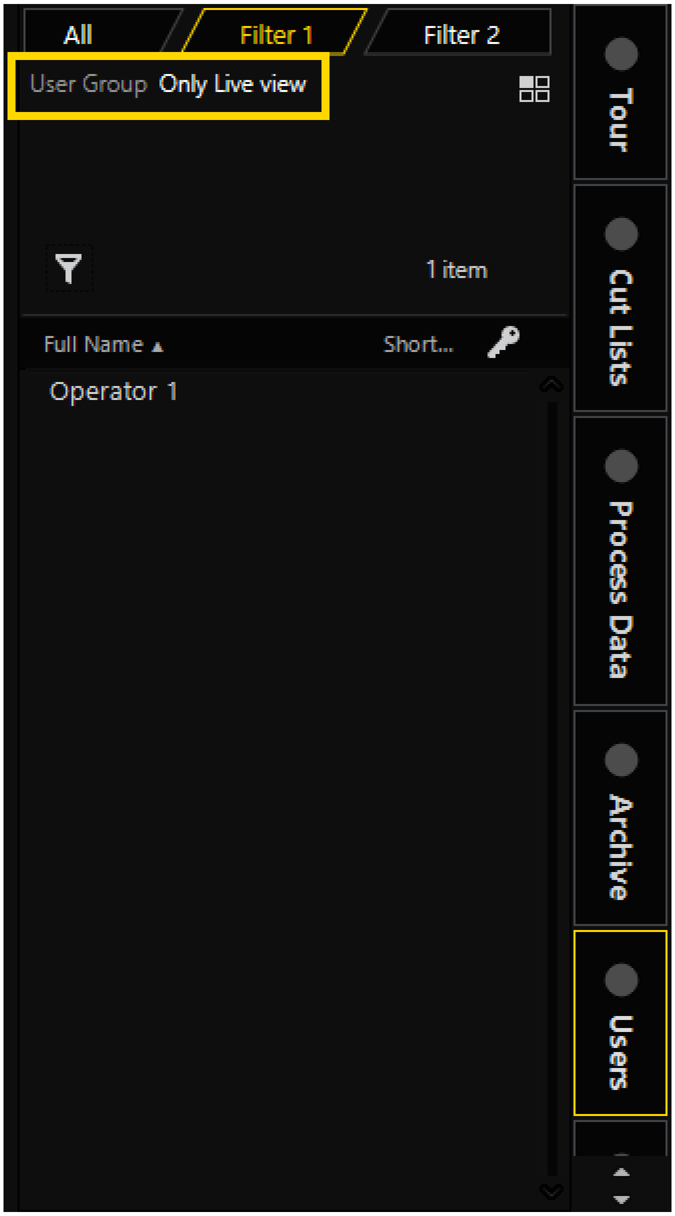
1. Click on a filter tab.



2. Click on the ▼ button in the respective filter tab. The **Users** dialog window opens.



3. Enable the respective checkboxes under **Custom Filter** or choose a preset from the drop-down menu under **Saved Preset**.
4. Click on **OK**. The applied filter is displayed in the upper area.

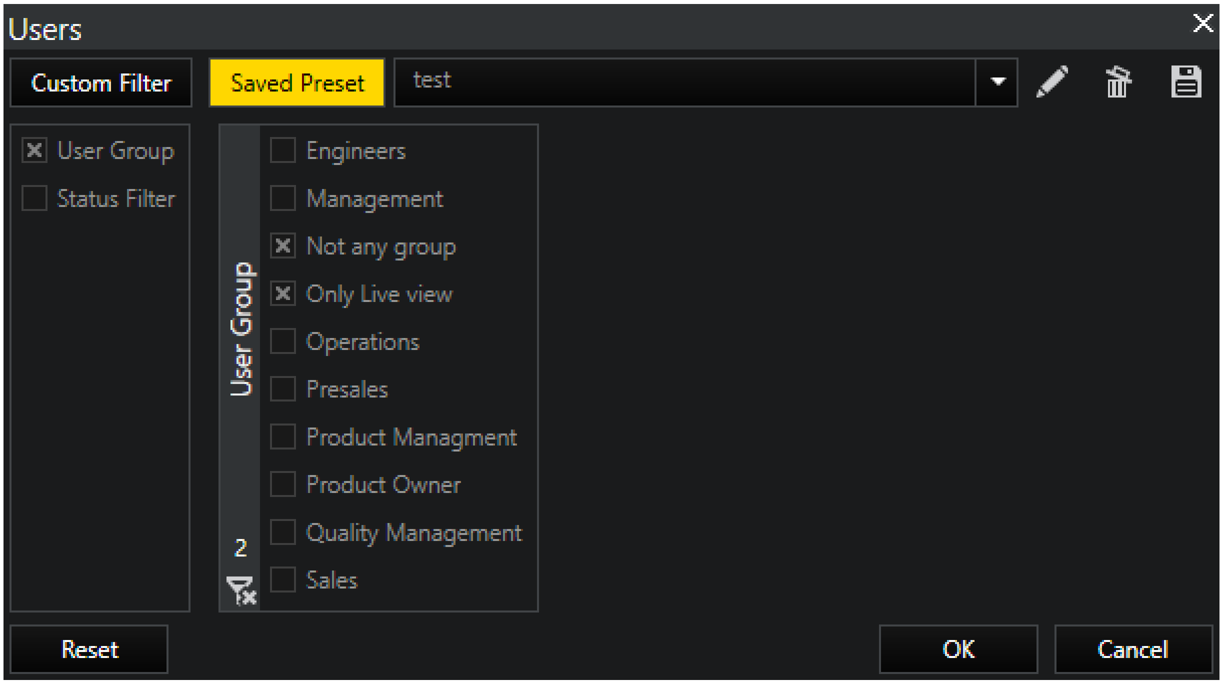


Operator 1

You can use different filter tabs to apply different filters.

Presets:

In the **Users** dialog window under **Saved Preset** you can edit or delete presets. Under **Custom Filter** you can save set filters as presets.



Users

Custom Filter | Saved Preset | test

☒ User Group

□ Status Filter

User Group

2

□ Engineers

□ Management

☒ Not any group

☒ Only Live view

□ Operations

□ Presales

□ Product Managment

□ Product Owner

□ Quality Management

□ Sales

Button	Description
✎	Use this button to edit a preset.
🗑	Use this button to delete a preset.
💾	Use this button to save the under **Custom Filter** set filters as a preset. **After you have clicked on this button, the Filter Criteria Detail window opens where you must enter Name and Description.**

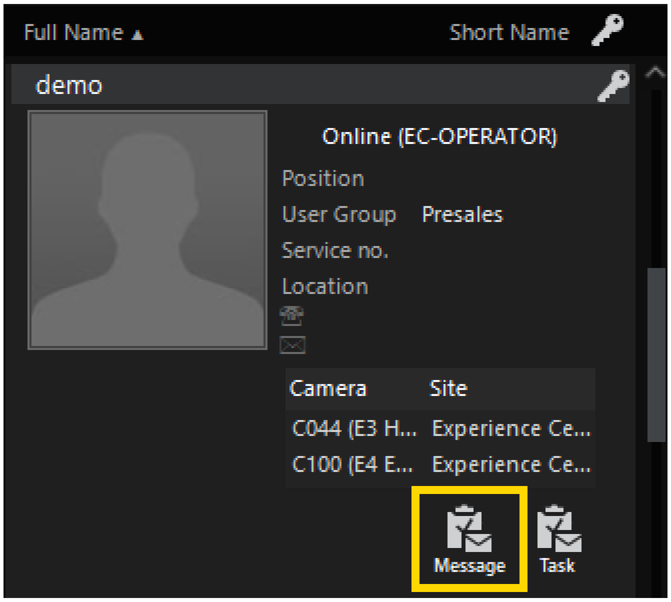
User Actions

The detail view of a user offers you two user actions: sending a message or assigning a task.

Send a Message

1. To send a message to a user, click on the name in the user list. The detail view of the user opens.

You can only send messages to users which are currently logged in. Otherwise, the Message button is not displayed.



Full Name ▲ Short Name

demo

Online (EC-OPERATOR)

Position

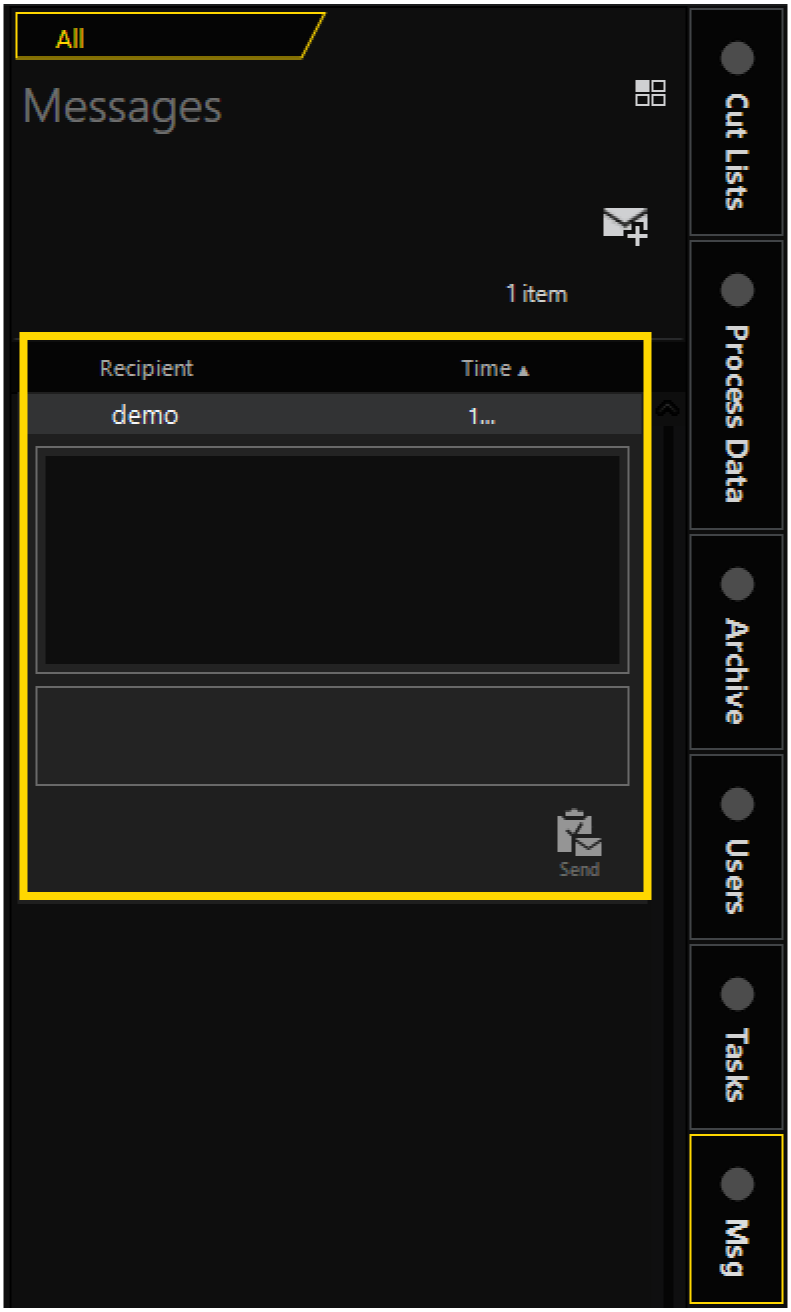
User Group Presales

Service no.

Location

Camera	Site
C044 (E3 H...	Experience Ce...
C100 (E4 E...	Experience Ce...

2. Click on the **Message** button. The **Msg** tab opens.



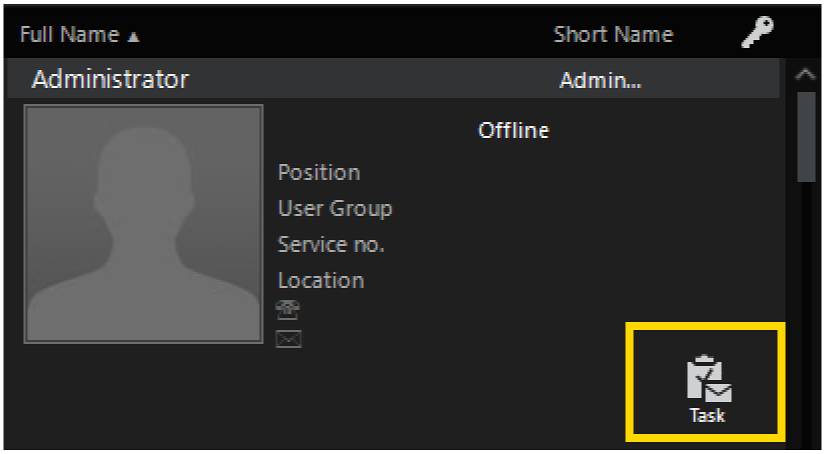
3. Enter a message in the text field. The **Send** button is now selectable.

4. To send your message, click on the **Send** button.

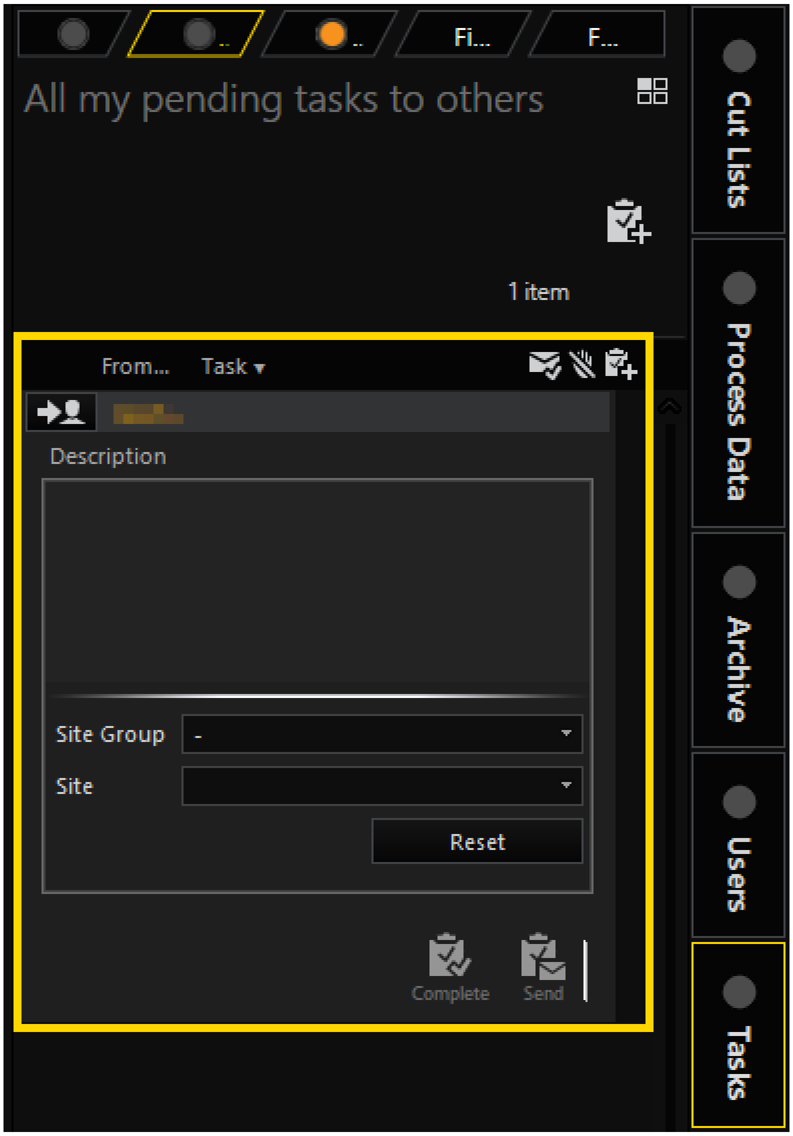
For detailed information on messages see **Messages**.

Assign a Task

1. To assign a task to a user, click on the name in the user list. The detail view of the user opens.



2. Click on the **Task** button. The **Tasks** tab opens.



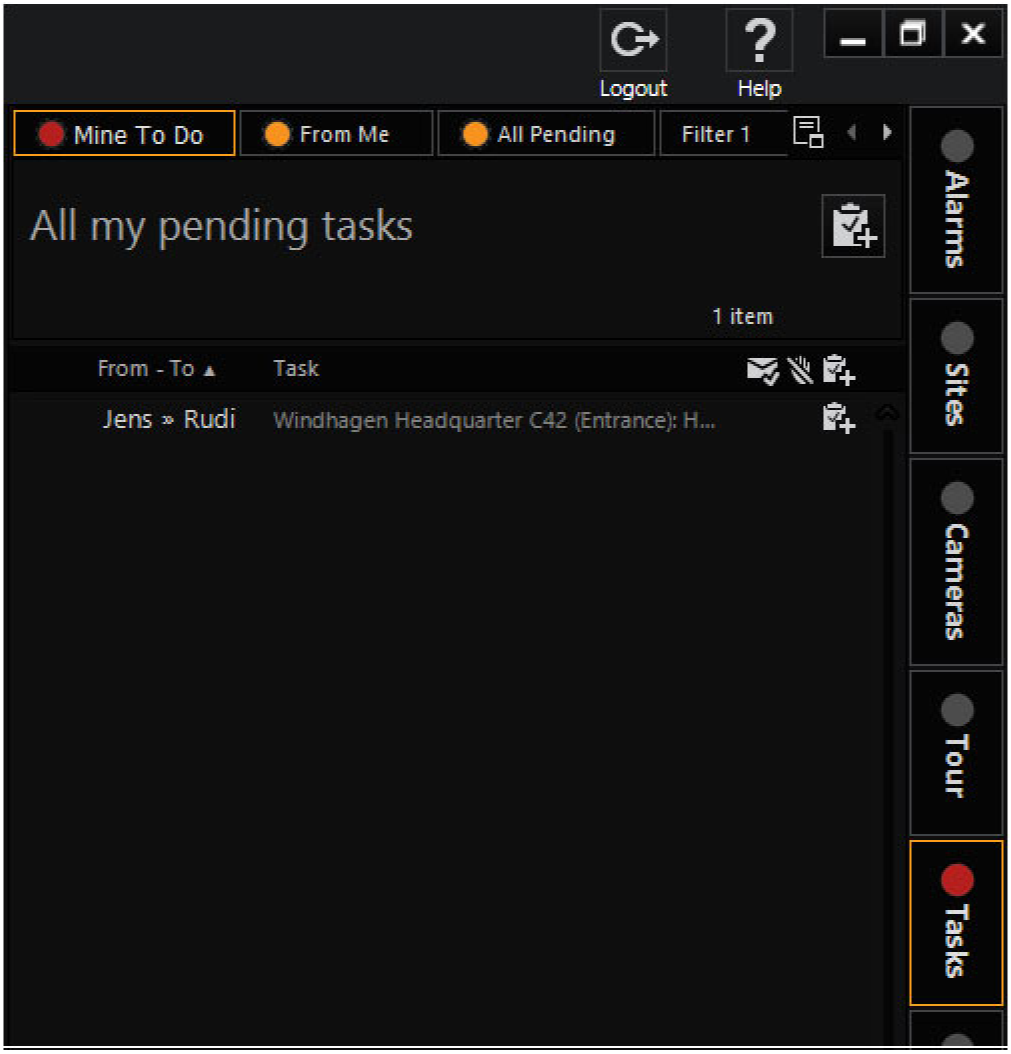
3. Enter a text in the **Description** field. The **Send** button is now selectable.

4. You can either click on the **Send** button to assign the task directly or add information to the fields under the **Description** field and click on the **Send** button afterwards.

   The fields under the Description field vary depending on your selection.

For detailed information on tasks see **Task Details And Actions**.

Tasks



All my pending tasks

1 item

From - To ▲	Task
Jens » Rudi	Windhagen Headquarter C42 (Entrance): H...

A user with the necessary privileges may assign a task to another user. A task is a simple instruction that must be accepted by the receiving party and then completed, or it may be rejected. On completion of a task a response will be sent back to the sender.

A site group, single site or camera may be attached to the task, making it easy for the receiver to get a task related map or a camera view. All task related actions are stored in the Audit Log (See **The Audit Log**). See **Differences between Messages and Tasks** for description of when messages may be used instead of tasks.

Dragging And Dropping Tasks

If a site or a camera is attached to a task, dragging the task will actually initiate a drag of the attached site or camera. It may be dropped anywhere a site or camera may be dropped, and the result will be the same. No drag-drop functionality is available for tasks without attached site or camera items.

Task List

Tasks are grouped into three lists: **My outstanding**, **From me** and **All outstanding**. The tasks are arranged chronologically. The oldest task is at the top. For the individual task elements, short names (aliases) are shown for the sender and recipient, and a part of the task description.

Task List Layout and Buttons

Sender >> recipient: The short names (aliases) of sender and recipient.

Dock list: With this function, a copy of the task list can be created in any viewer. Click this button to highlight the available viewer windows and display the related identifiers with which the list can be docked to the desired viewer.

New task: Click this button to create a new job. See Create new tasks.

Send task: This button only appears once you have entered sufficient data.

Filtering the Task List

Here the usual functions are available. See filter.

Task Status Indicators

📋	New task
✋	Task rejected
✉	Task completed

New task: A new task, which must be accepted or rejected by the recipient.

Task accepted: The recipient has accepted the task. The task must now be completed or transferred to another user.

Task rejected: The task was rejected by the recipient. The sender can then send the task to another user.

Task completed: The task was completed.

Transfer task: The task was transferred to another user. This user must now accept or reject the task.

The sender is responsible for the task until the other user has accepted it.

Task Details And Actions

Task Details

In the detail views of tasks, information on the sender, recipient, date, time, status and task description are displayed. When a site group, a site or a camera is linked with the task, this fact is indicated on the task description. When one of the specified elements is linked, in the detail display below, the buttons for displaying the element are shown on a map or in a viewer.

Site or camera details: This information is only shown when a corresponding element is linked with the task.

Comments: Comments of the recipient. The recipient can enter comments. This is also possible when rejecting tasks.

Task Actions

Complete task: Complete a task and send the entered comments to the original sender. Enter a comment before completing the task.

Transfer task: A task that was rejected by a user can be transferred by the sender to another user.

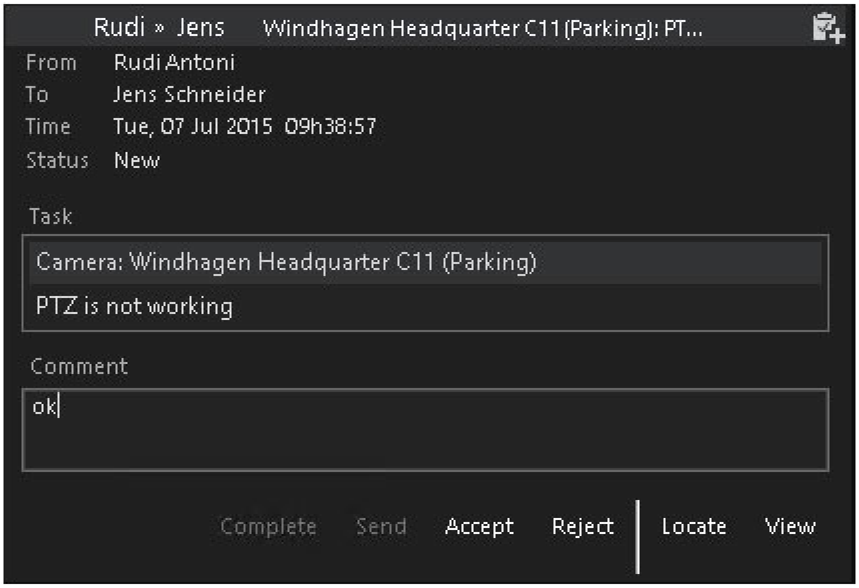
Send task: Enabled only for new tasks. With this function, the task is forwarded to the recipient. In order to send a task, a recipient must be selected and a task text entered.

Reject task: With this function, the recipient can reject a task. It is possible to enter a comment. However, this must be performed before the task is rejected.

Live video: This button is only active if the task is linked to a camera and it is possible to playback live video images in a viewer of choosing.

Check camera: This button is only active if a camera is linked with the task and there is access to the CPA function (reference image).

Creating a New Task



Rudi » Jens Windhagen Headquarter C11 (Parking): PT...

From Rudi Antoni

To Jens Schneider

Time Tue, 07 Jul 2015 09h38:57

Status New

Task

Camera: Windhagen Headquarter C11 (Parking)

PTZ is not working

Comment

ok

To create a new task, click the New task button in the Tasks tab. You must then select a recipient and, among other things, you can link a camera with the task. Whenever you create a new task, you must specify a recipient. You can make changes later.

However, it is easier to create a new task in the user list in the detail view of a user or to simply drag a user onto the Tasks tab. Users elements can be dragged from the list of users or any other lists in which user names are displayed (for example from the user list of a camera). If new (not yet sent) tasks are present in the task list, the saved user is specified as the new recipient. For this reason, when using this procedure it is important that you process the right task.

It is also just as easy to link up a camera: Simply drag a camera from any site onto the Tasks tab or onto a task that has not yet been sent. The aforementioned steps can be performed in any task: For example, you can drag a camera (or a site) onto the **Tasks** tab to create a new task and then select a recipient by dragging a user onto the task.

If an element (for example a camera) is linked with a task, the camera name should not be mentioned additionally in the task description. Simply select the camera and enter a task, like Please check focus. The complete camera description appears above the task text.

Transferring a Camera to a User

To create a task that is automatically linked with a camera, click on a map or, in the camera list in the detail display of the desired camera, on the Transfer camera button. This procedure is useful when it is necessary to assign a camera-related job to a user. To select the user, either click on … or drag a user element onto the newly created task.

Receiving a New Task

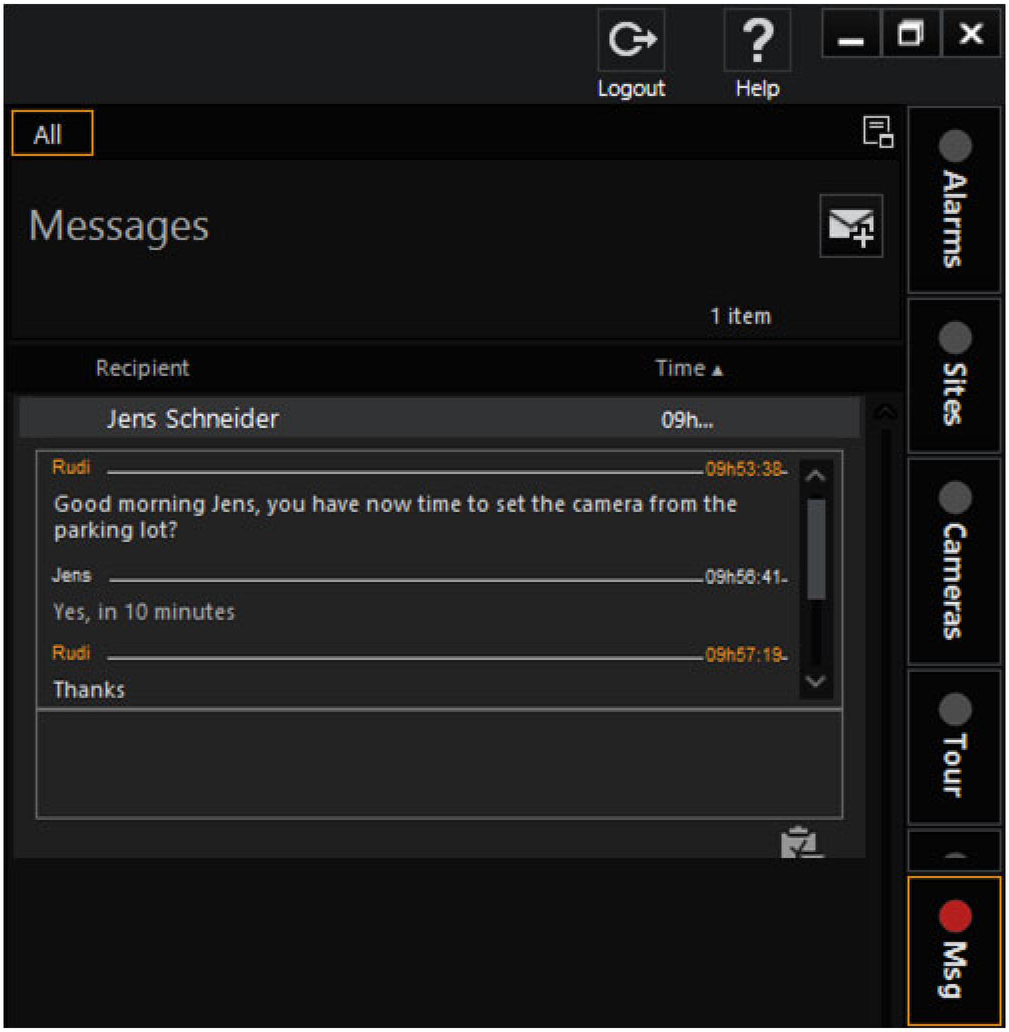
Once you have received a task, a red LED indicator lights up on the Tasks tab. In the task list, the new task is highlighted with the New task status symbol (see Status indicators for tasks). Click the corresponding buttons to accept or reject the task. Before rejecting a task, enter a comment to provide feedback to the sender.

Dragging and Dropping Tasks

When a site or a camera is linked to a task, dragging the task drags the linked element (site or camera). It can be placed at all positions at which placement is permissible. The same function is then triggered that would have been triggered by dragging from the camera list. Tasks with which no elements are liked cannot be dragged with the mouse.

Messages

G-SIM messaging is an easy, text based, communication method between logged-in users. Messages cannot be sent to users not currently logged in. While messages are not saved, they are recorded in the audit log. Because it is not stored, the message list will be cleared every time a user logs out. It is possible to send the same message to groups of users.



Jens Schneider 09h...

Rudi 09h53:38

Good morning Jens, you have now time to set the camera from the parking lot?

Jens 09h56:41

Yes, in 10 minutes

Rudi 09h57:19

Thanks

Message List

The message list displays all messages that have been received since logging on. They are grouped in the form of "conversations" with specific users or user groups. For the individual elements of the list, the name of the communication partner and time of the first message of the conversation are displayed.

Time: Time of the first message of this conversation.

Dock list: With this function, a copy of the message list can be created in any viewer. Click this button to highlight the available viewer windows and display the related identifiers with which the list can be docked to the desired viewer (see main user interface).

Status indicators for messages

Unread message: Indicates a new unread message in the conversation.

Message Details And Actions

Message Details

In the detail views of messages, all sent and received messages of a single user or user group are displayed. If you send a message to a user group and a member of the group responds, a new element is added to the message list, containing the communication with this user.

Name of the other party: If you send messages to a group of users, the description of the group is displayed here.

Correspondence: List of all messages that have been sent to the other party and have been received from the other party, as well as the time stamp of these messages. Sent messages are blue, received messages are black.

Input field: Enter your new message or your reply here. Press `Enter` to send the text to the other user. Hold down the `Shift` or `Ctrl` key and then press `Enter` to insert a line break in your message.

Message Actions

The following buttons are available in the detail views of messages:

Send message: This function is activated only when text has been entered into the input field. With this function, the text is sent to the other user just as it would be when you press the `Enter` key in the input field.

Create New Messages

Above the message list, click **New message** to send a message to a user or a user group. Then click , to select a recipient. You can also drag a user from the user list or another list with user names (for example from a list for using a camera) and drop the user onto the **Messages** tab. If no messages has previously been sent to this user, a new message is created and the dropped user is automatically entered as recipient.

Enter the desired message into the input field (see additional information above).

Receive New Messages

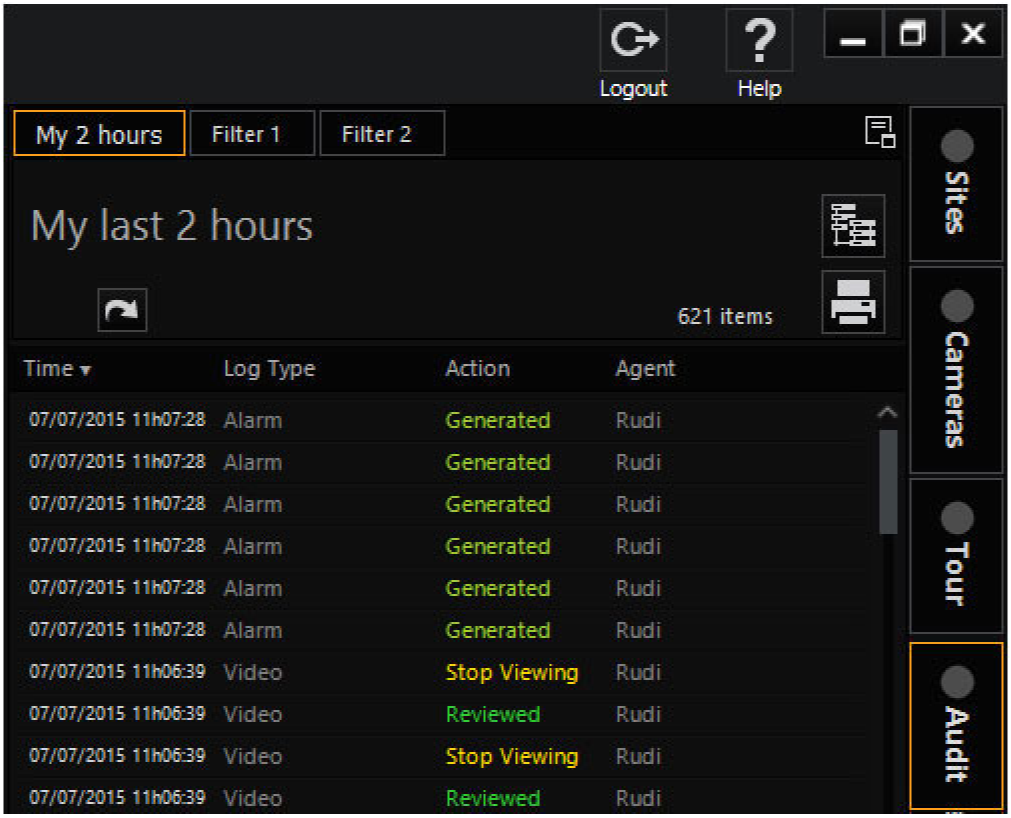
Once you have received a new message, a red LED indicator lights up on the **Messages** tab. When you switch to the message list, all conversation elements with unread messages are marked with the status symbol **Unread message**. Click on the individual elements to display the message details. If applicable, enter a response in the input field (see explanation above).

Differences between Messages and Tasks

There are three main differences between messages and tasks:

- Messages can only be sent to logged-in users.
- Messages are not saved. If you log out and back in again, your message list will be empty. Messages are recorded in the Audit Log.
- Cameras or Sites cannot be attached to a message.

Audit Log



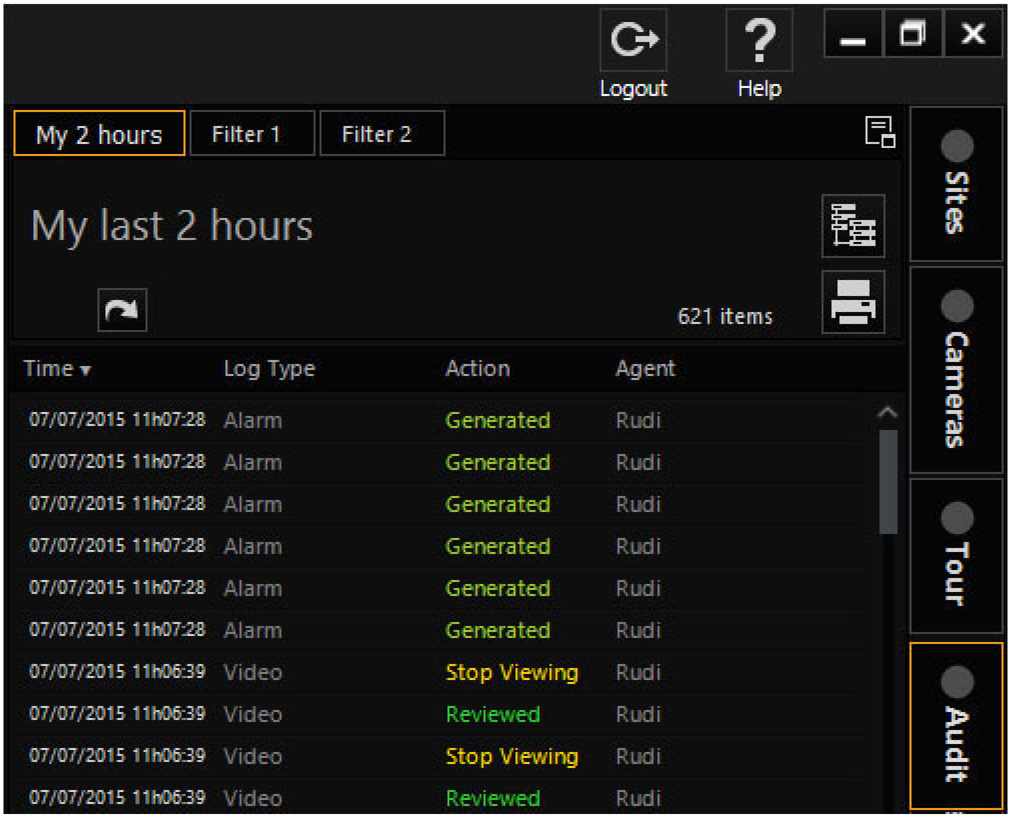
Time ▾	Log Type	Action	Agent
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h06:39	Video	Stop Viewing	Rudi
07/07/2015 11h06:39	Video	Reviewed	Rudi
07/07/2015 11h06:39	Video	Stop Viewing	Rudi
07/07/2015 11h06:39	Video	Reviewed	Rudi

The G-SIM Audit List is an audit trail of all server-related, system set-up changes, log-ins and log-outs, all viewing and reviewing of camera footage (including Tours), all alarm handling and task related actions, all messaging, and all export related events.

By default users can only view their own audit log, and can filter it for specific types of events over a specified time. Users with the necessary privilege may also view the audit logs of other users. In the case of cameras viewed or reviewed, the start and end time are stored, taking into account possible rewinds and jumps in the viewing sequence. This allows a user to see exactly which footage was viewed, and to even review it if necessary.

Reviewing here means seeing exactly what the other user saw. Simply drag an event onto the applicable viewer, and if it is a camera, what the user saw will be available as a video extract, starting in pause mode. From here you are able to create an "Other" event, allowing you to export it for evidentiary purposes, if required.

Audit List



My last 2 hours

621 items

Time ▾	Log Type	Action	Agent
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h07:28	Alarm	Generated	Rudi
07/07/2015 11h06:39	Video	Stop Viewing	Rudi
07/07/2015 11h06:39	Video	Reviewed	Rudi
07/07/2015 11h06:39	Video	Stop Viewing	Rudi
07/07/2015 11h06:39	Video	Reviewed	Rudi

The audit list contains all audit elements for one or more users within a specified period. Some elements are events that took place at a certain point in time, for example log-on operations onto the system. Other events (for example, displaying a camera) are assigned start and end times, and the time information of the played back video recording, which can be contiguous or in multiple fragments.

Layout and Buttons of the Audit List

The following is highlighted:

Time: Start time of the event. The times of events from today are displayed in black, all earlier events are blue.

User: Short name (alias) of the user who performed the activity.

Dock list: With this function, a copy of the audit log can be created in any viewer. Click this button to select the available viewer windows and display the associated keyboard shortcuts with which the individual lists can be docked to the desired viewers (see main user interface).

Print list: With this option, you can print or export the currently displayed audit log elements.

Query details: For certain audit elements, additional details are available (for example, if the video recordings of a camera were played back and the user played back a non-continuous video block). These details are not sent by the server by default, but if available they can be requested for the individual elements. Click this button to retrieve the available details for all items in the list.

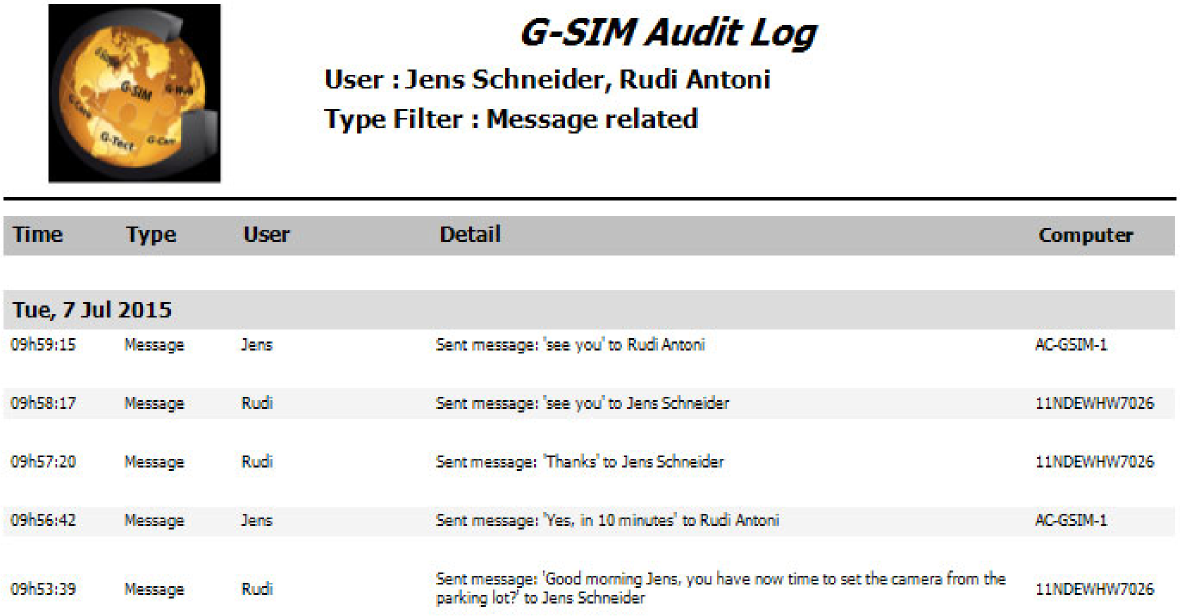
Filter Audit Log

Here the usual functions are available. For more information, see Filters. Pay particular attention to the information on the audit log.

Printing or Exporting the Audit List

See **Filtering** for special notes on this.

Audit Item Detail



G-SIM Audit Log

User : Jens Schneider, Rudi Antoni

Type Filter : Message related

Time	Type	User	Detail	Computer
Tue, 7 Jul 2015				
09h59:15	Message	Jens	Sent message: 'see you' to Rudi Antoni	AC-GSIM-1
09h58:17	Message	Rudi	Sent message: 'see you' to Jens Schneider	11NDEWHW7026
09h57:20	Message	Rudi	Sent message: 'Thanks' to Jens Schneider	11NDEWHW7026
09h56:42	Message	Jens	Sent message: 'Yes, in 10 minutes' to Rudi Antoni	AC-GSIM-1
09h53:39	Message	Rudi	Sent message: 'Good morning Jens, you have now time to set the camera from the parking lot?' to Jens Schneider	11NDEWHW7026

The appearance of the detail view for audit elements depends on the type of the displayed audit element. For most elements, time information, a description of the activity, the name of the acting user and the name of the computer used are displayed. Elements may also contain tables with activities, for example, if a user has played back a non-continuous video block.

The elements of the detail view are self-explanatory. Note that the computer is also specified from which a specific activity was initiated (Windows computer name).

Audit Item Actions

In the detail view for audit elements, the following activity buttons are available:

Display camera: This button is only active for the video events. The viewer is started in "Pause" mode. Playback is at the correct position.

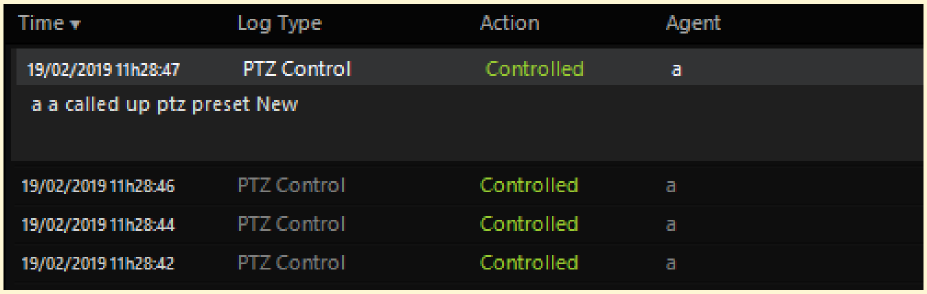
Show on map: This button is only active when a camera or a site is linked with the audit element. You can then display a map of the site or highlight the position of the camera on the map. The first map that contains the corresponding camera is shown. If in the corresponding viewer a map of the site is already displayed, the map is shifted so that the sought camera is displayed in the center. The camera label is highlighted with the color "Map Highlighted Camera Outline" (see mapping in G-SIM).

Query details: This option is only active for audit items for which details are available that have not yet been accessed. Click Query Details above the audit list to retrieve details of all list elements.

Automatically Logged Elements

Setting	Description
User	User has logged in or out.
Two Man Rule User	Two Man Rule User has logged in or out.
G-SIM Server Service	G-SIM server service was started or stopped.
Block/Unblock PTZ Control	Camera PTZ control was blocked or unblocked for user.
Block/Unblock Camera	Camera was blocked or unblocked for user.

Setting	Description
Text Message	Text message was sent to user.
Video Footage	Camera or site was viewed / Camera or site view was denied / Camera or site was viewed in time range (after viewing has stopped).
Guard Tours	Guard tour was viewed / Guard tour viewing was denied / Guard tour was deleted / Guard tour was watched in time range x.
Tasks	Task was sent to user / Task has changed status.
Set Reference Frame	Reference frame for camera was set by user.
Camera PTZ control	Start PTZ / Stop PTZ / PTZ was controlled in time range x.
Alarm	New alarm arrived / Alarm was acknowledged / Alarm was forwarded to User / Alarm was completed.
Dongle Error	Dongle error has occured.
User Password changed	User changes his password in Operator Console.
Export Video	Export of video material was done. To see more details, click on the **Detail** button.
Export Image	Export of image was done.
Map Interaction	Interaction on map has taken place.
Set Client VCA	Client VCA was disabled/enabled.
Camera Playback unlocked	Camera playback was unblocked.
Configuration changes	Configuration was changed.
Custom Button	Custom button was pressed.
Layout	Operator Console screen layout has been changed by user/action.

Setting	Description
PTZ Control	User has control over PTZ.
PTZ Preset Audit Log	Operator has control for PTZ and calls up a PTZ preset.  Time ▾ | Log Type | Action | Agent 19/02/2019 11h28:47 | PTZ Control | Controlled | a a a called up ptz preset New 19/02/2019 11h28:46 | PTZ Control | Controlled | a 19/02/2019 11h28:44 | PTZ Control | Controlled | a 19/02/2019 11h28:42 | PTZ Control | Controlled | a
Setup Import & Export	The import and export of a G-SIM setup in the ManCon is automatically logged in the audit.

Reviewing Viewed Video Footage

Video-related audit items may be viewed by dragging the item to a viewer or by using the View Camera button. In situations where detail exists (where a user jumped to different sections while reviewing footage) you may double-click on a detail line in the list to cue the current audit item viewer to that position.

Dragging and Dropping Audit Items

Drag-and-drop functionality is only implemented for video-related audit items. The video footage associated with the item will be displayed when dropped on a viewer, or the position of the camera indicated when dropped on a map. An audit item drag may be initiated from a list of audit items.

If dropped onto an alarm list containing the dragged audit item (i.e. the list was not filtered to exclude the item), then the audit item will be selected and its card expanded to show the associated details.

When dropped onto a viewer, the recorded camera footage associated with the audit item will be displayed. The viewer will be placed in pause mode and the user may then review it from that point or step through it forwards or backwards.

When dropped onto a map, the map will pan to show the highlighted camera in middle of the map. If the current map does not contain the camera, the correct map will be loaded. (See **Mapping in G-SIM**)

Remote Consoles

G-SIM allows you to share content with Remote Consoles by changing the Viewer content on their screens, sharing information, and even changing the screen layout in the case of an Unmanned Console. There are three types of Remote Consoles in G-SIM

- Remote Consoles
- Video Walls
- Manned Consoles

They are mostly similar, with the Remote Consoles (including Video Walls) giving you more control options, such as changing the screen layout. The reason for the difference is that the Manned Console has someone working at it, and the purpose of the remote control is usually to show the other operator something, not to re-do their screen for them. That is why you cannot change another user's screen layout remotely.

The content of a Remote Console’s screen(s) is determined by G-SIM users (operators or supervisors) who have the necessary privileges, as well as the system rules which may restrict some content, or set some default content views, etc.

Putting content onto a remote console is as simple as dragging it onto the viewer in the remote template view.

What You Can Do On a Remote Console

G-SIM gives you the ability to view quite a number of things on a Remote Console:

- Any combination of video signals (cameras), maps, and camera sequences (See **Guard Tours**) can be displayed.
- These combinations of cameras can be in any pre-defined screen layout for each DVI output (ranging from one camera to many cameras of various display sizes).
- The video (of any camera) can be viewed Live, Paused, or in Playback (See Video Tools).

- Camera sequences (Tours) can be viewed in any section of the screen, and any number of sequences could be viewed simultaneously.
- A reference map that shows the cameras and sensor equipment of a particular area can be displayed. These reference maps can be any digital image, like an overview map, aerial photo, GIS-generated bitmap, a sketch, a diagram, flow diagram, emergency procedure, etc.
- The Alarm Auto-view feature (See **Alarms**) could be enabled for one of the outputs, which will show new pending alarms of pre-configured types, with all the associated detail.
- Default (start-up or restored at request) layouts and favourite layouts with content can be stored at any time from a remote computer.
- The layout and content of any of a user's secondary screens can be sent to an Unmanned Console with the click of a button. In this way you could update a Video Wall with one of your secondary screens. Since primary screens contain the interactive UI constructs such as the tabs and the lists, primary screens cannot be sent to a remote console.
- To clear a remote viewer, simply Ctrl-click in it.

Before You Start

Before an Operator Console can be used as a Remote Console (Manned or Unmanned), it must be licensed and registered, and running G-SIM before it can be remotely controlled. If a new Unmanned Console logs in on the G-SIM server, it will automatically be added and licensed if there are licenses available.

Users must have the necessary privilege in order to share content with a Remote Console. All privileges are managed centrally.

i **As with all other aspects of the system configuration, this is configured in the Management Console, and we here assume that it has all been configured properly.**

Manned Consoles

Manned Consoles are Operator Consoles that are controlled by a user and have been configured centrally to receive content from other users via Remote Sharing. You can share any Viewer content with a Remote Console by sending it directly to its screen.

Remote Sharing

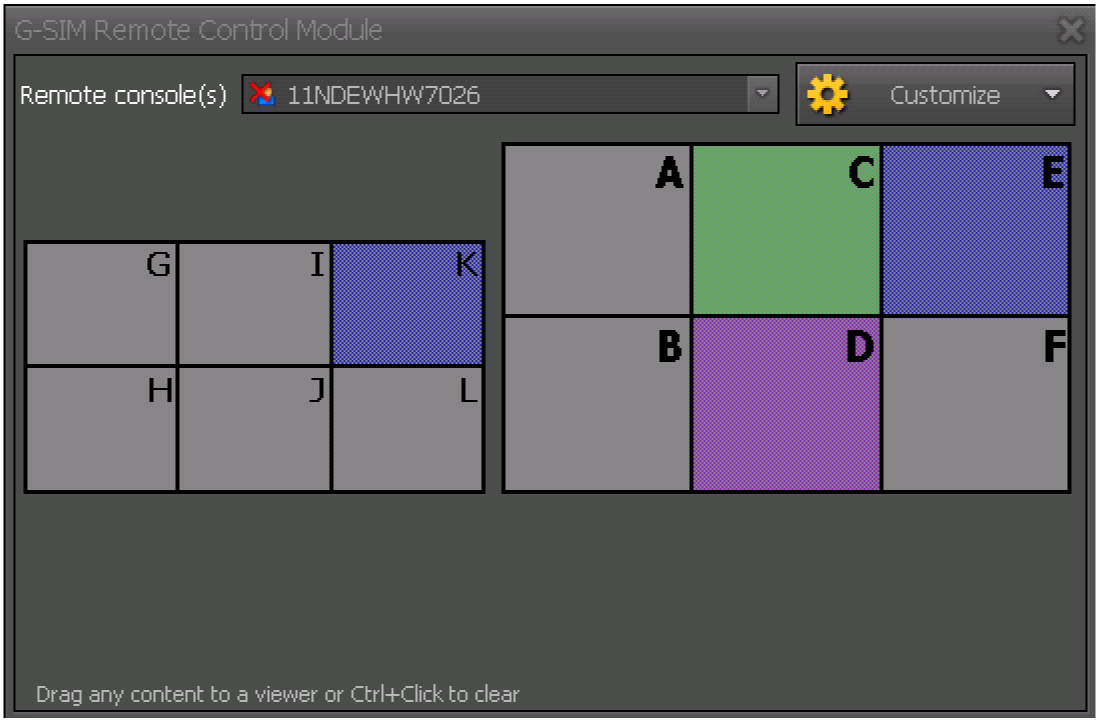
You can share all cameras (Camera List), Tours (Tour List) and Viewer content (except docked Lists) remotely. To do so, click on the Remote Control icon in the main toolbar. This opens up a resizable window which has a drop-down list of remote consoles which are available for remote sharing. Also in this window is a graphical representation in thumbnail form of the remote screen's layout.

When you choose one, the thumbnail updates to show the remote screen's layout as well as the thumbnail images of the cameras in view (if available). To share what is in one of your viewers, simply drag your viewer onto the place of the remote screen image where you want to display it — it's as simple as that.

This is definitely a case of "With power comes responsibility." It is very easy to share what is happening in your screen with another user, but understand that doing so may very well interrupt their work. In a security context that could endanger someone if not done correctly. Here correctly means that they are OK with part of their screen suddenly changing.

Recommendation: In light of the above, it would be best to have a site standard that, say, the bottom right viewer of a particular screen layout is always available for sharing. You can take it further by stipulating that only certain layouts may accept video. Of course, flexibility requires that such limitations can be overridden, which is why we implemented this the way we did — if you are in a crisis situation, you don't want the tool to constrain you by limiting what you can do. It is thus best for operators to work together.

Remote Screen Thumbnail


G-SIM Remote Control Module
Remote console(s)
11NDEWHW7026
Customize
G
I
K
H
J
L
A
C
E
B
D
F
Drag any content to a viewer or Ctrl+Click to clear

The Remote Screen thumbnail represents the Remote Consoles screen layout. Move the mouse over each block (i.e. Viewer) to see what type of content (Map, Camera or Tour) is being viewed, as well as its name. This is displayed underneath the thumbnail. If available, the reference frame for that camera will be shown.

Rules When Sharing Content

The same rules when viewing content locally also apply during Remote Sharing:

- Manned Consoles only: the Tabbed Lists are located on screen 1 and cannot be replaced by Remote Content.
- You can only clear the viewers of an Unmanned Console remotely.

Remote Consoles

An Unmanned Console is basically a computer that is running the G-SIM user-interface software, but is not manned by a user at its physical location. Instead, it is remotely controlled by one or many users from their own Operator Consoles. As such, it does not have any of the user interface components such as the toolbar or tabbed lists.

Remote Consoles are typically used for video walls, public displays, foyer displays, etc.

Grouping Remote Consoles

It is possible to add a number of Remote Consoles to a group. This will allow a user to send actions to more than one remote station, keeping their content synchronised.

These groups are set up in the Management Consoles.

Remote Console Enhancements

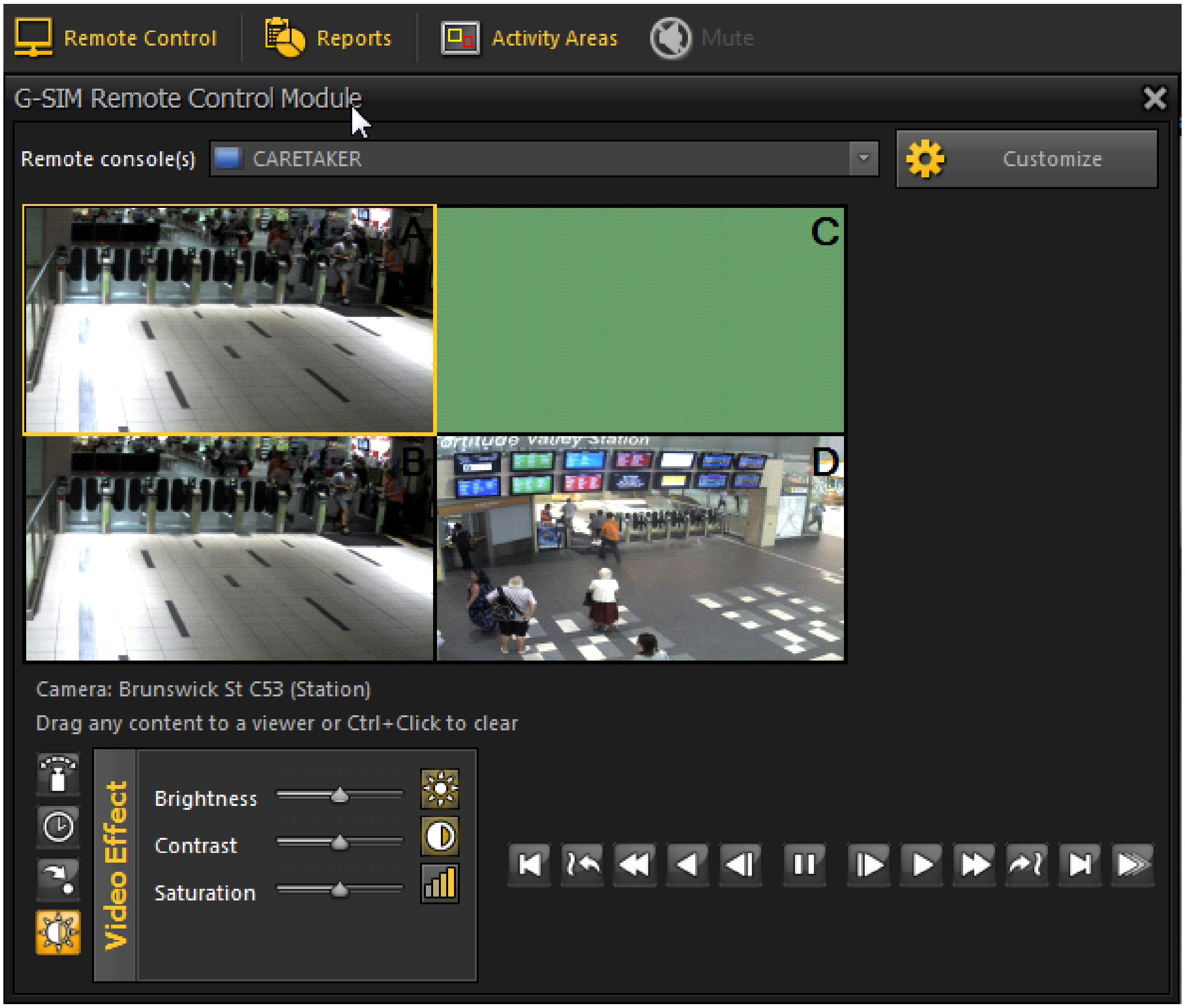
Previously (Build < 4.3.0.116) it was only possible to populate remote viewers with content by dragging e.g. a camera to a remote viewer. To this the user would open the Remote Control window and select a remote console to control. He would then be presented with a view of the remote console screens, and could change the content. It is now possible to do more control of remote viewers, e.g. Pause, Forward, Jump to Time, Jump to a PTZ pre-set, setting Brightness/Contrast etc.

Operation

Select a remote viewer containing video - the selected viewer will be marked with an orange frame as on the main interface. A control bar at the bottom gives users access to the normal Play Control Functions (Pause, Fast play etc.) A toolbar at the left of the control gives user access to PTZ pre-sets, Time Search (Jump to Time), Search options (Whether a Motion, Event or time-based search must be performed) as well as Brightness/Contrast/Saturation control for the remote viewer.

Other enhanced functionality:

- Viewer content may be dragged from one remote viewer to another remote viewer, and also from a remote viewer to a local viewer.
- Users may be restricted to use/access specific remote consoles – previously a user could access all remote console (e.g. post to all video walls) if he had the basic “Allow Remote Control” privilege – NB – see the next section for details on the Management Console setup.
- Basic MBEG control was implemented for remote viewers – if a remote viewer is selected (has an orange frame around it), MBEG actions will be routed to the remote viewer and not be executed locally.



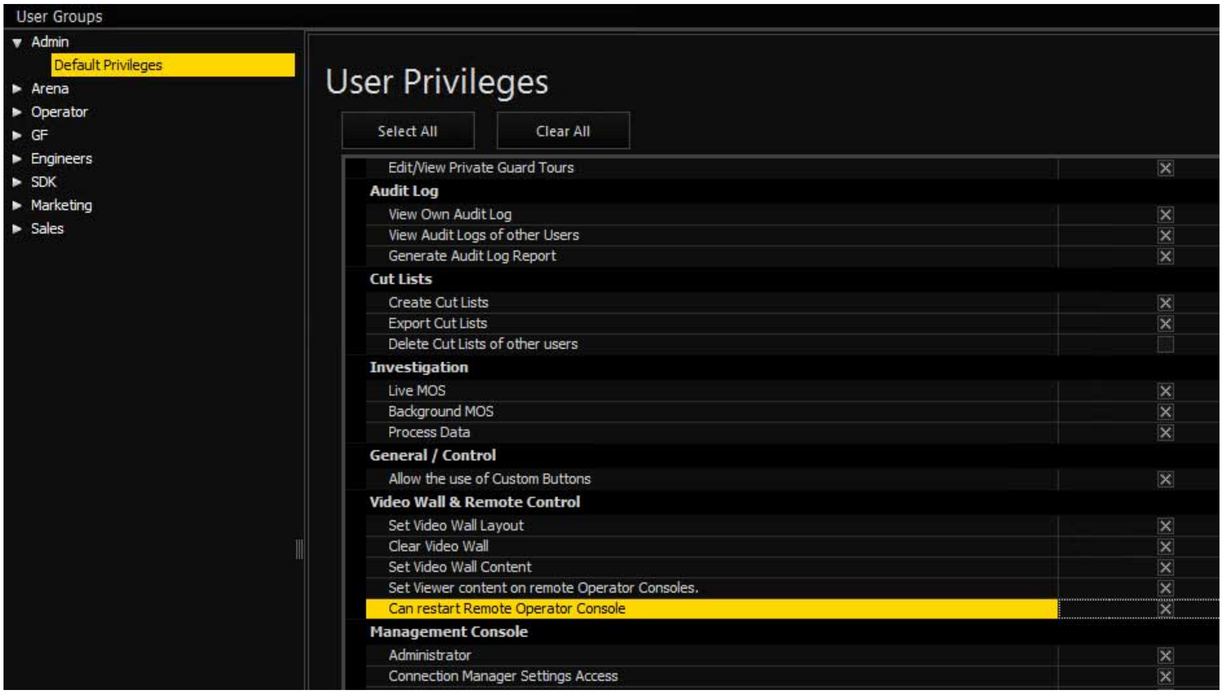
Remote console(s) CARETAKER

Camera: Brunswick St C53 (Station)

Drag any content to a viewer or Ctrl+Click to clear

Restarting Remote Console in the Operator Console

The right **Can restart Remote Operator Console** is in the area **Video wall & Remote Control** of the user rights. It is disabled by default.



User Groups

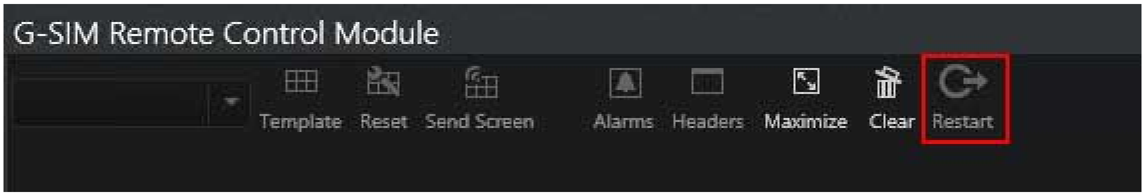
- Admin
  - Default Privileges
- Arena
- Operator
- GF
- Engineers
- SDK
- Marketing
- Sales

User Privileges

Select All | Clear All

Edit/View Private Guard Tours	☒
Audit Log	
View Own Audit Log	☒
View Audit Logs of other Users	☒
Generate Audit Log Report	☒
Cut Lists	
Create Cut Lists	☒
Export Cut Lists	☒
Delete Cut Lists of other users	□
Investigation	
Live MOS	☒
Background MOS	☒
Process Data	☒
General / Control	
Allow the use of Custom Buttons	☒
Video Wall & Remote Control	
Set Video Wall Layout	☒
Clear Video Wall	☒
Set Video Wall Content	☒
Set Viewer content on remote Operator Consoles.	☒
Can restart Remote Operator Console	☒
Management Console	
Administrator	☒
Connection Manager Settings Access	☒

If it is activated, the user can restart the respective remote console in the Operator Console in the **G-SIM Remote Control Module** by clicking **Restart**.



This function uses port 13210.

Camera Check Service

This is the old version of the Cam Check, which is located directly in G-core.
Information about the new version of the Cam Check is available here: Cam Check Documentation

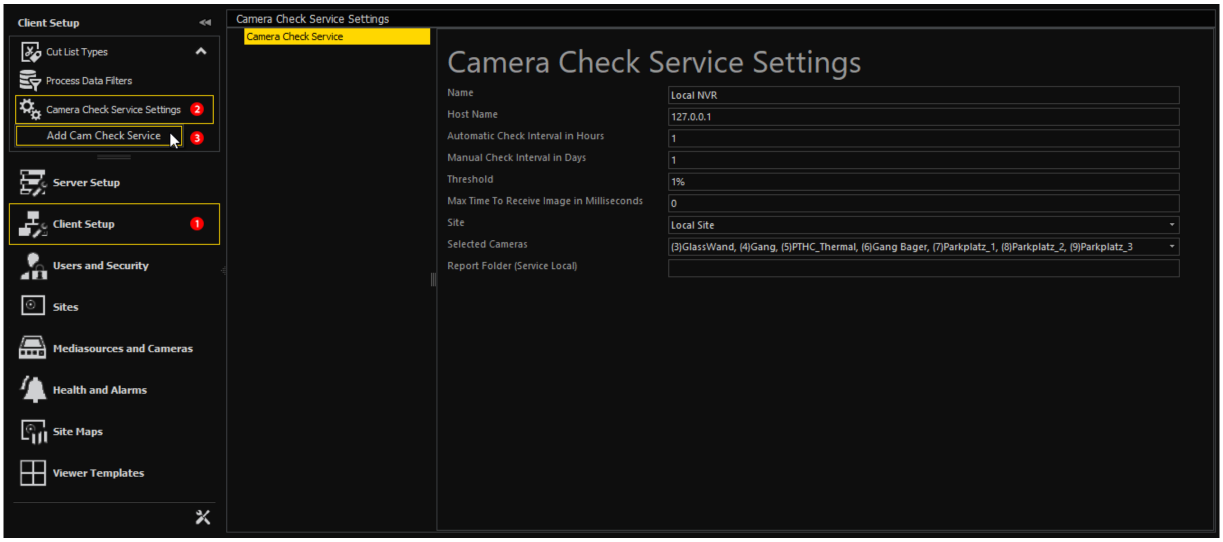
The Camera Check Service is licensed per channel. The license must be added in G-SIM under **Server Setup** > **Server Licenses** > **Dongles**.

Management Console

There is a configuration for the Camera Check Service under **Client Setup** > **Camera Check Service Settings**. Several services can be configured here so that it is possible to use one service per site or multiple sites for one service.

Creating New Service Settings

After opening the management console, right click **Client Setup** 1 > **Camera Check Service Settings** 2 and then on **Add Cam Check Service** 3 .



Camera Check Service Settings

Name	Local NVR
Host Name	127.0.0.1
Automatic Check Interval in Hours	1
Manual Check Interval in Days	1
Threshold	1%
Max Time To Receive Image in Milliseconds	0
Site	Local Site
Selected Cameras	(3)GlassWand, (4)Gang, (5)PTHC_Thermal, (6)Gang Bager, (7)Parkplatz_1, (8)Parkplatz_2, (9)Parkplatz_3
Report Folder (Service Local)	

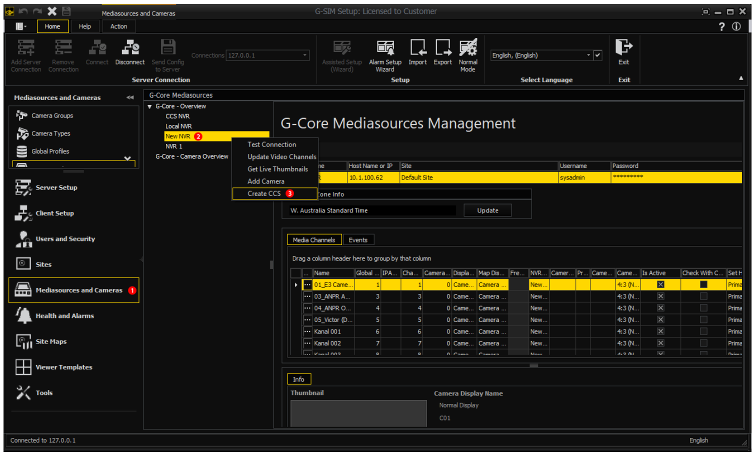
Setting	Description
Name	Service name to differentiate between multiple service instances (G-SIM-side only, no service connection itself), default: **CamCheck Service**
Hostname	Host name of the server running CamCheck
Automatic Check Interval in Hours	Amount of time after which the service automatically compares the reference image with the live image
Manual Check Interval in Days	Amount of time after which camera requires to be manually checked by an operator (open CCS window in Operator Console, compare reference image and camera live video and then accordingly click the green or red button)

Setting	Description
Threshold	Threshold for the CPA algorithm (between zero and one hundred percent)
Max Time To Receive Image	Maximum amount of time to receive an image from the camera (in milliseconds)
Site	Selection of sites to be checked by the service
Selected Cameras	Cameras at the selected sites to be checked by the service
Report Folder (Service Local)	Path to a.csv file where the service logs events

Inherit a CCS from a NVR

The feature **Create CCS** enables the user to add a new entry in the **Camera Check Service Settings**.

1. In the navigation bar on the left, click 1 **Mediasources and Cameras**.
2. Right-click 2 a mediasource.
   → The mediasource context menu appears.
3. Click 3 **Create CCS**.



...ne	Host Name or IP	Site	Username	Password
...R	10.1.100.62	Default Site	sysadmin	*********

W. Australia Standard Time

...	Name	Global ...	IPA...	Cha...	Camera...	Displa...	Map Dis...	Fre...	NVR...	Camer...	Pr...	Came...	Came...	Is Active	Check With C...	Set H
...	01_E3 Came...	1		1	0	Came...	Camera ...		New...				4:3 (N...	☒	■	Prima
...	03_ANPR A...	3		3	0	Came...	Camera ...		New...				4:3 (N...	☒	□	Prima
...	04_ANPR O...	4		4	0	Came...	Camera ...		New...				4:3 (N...	☒	□	Prima
...	05_Victor (D...	5		5	0	Came...	Camera ...		New...				4:3 (N...	☒	□	Prima
...	Kanal 001	6		6	0	Came...	Camera ...		New...				4:3 (N...	☒	□	Prima
...	Kanal 002	7		7	0	Came...	Camera ...		New...				4:3 (N...	☒	□	Prima

Normal Display

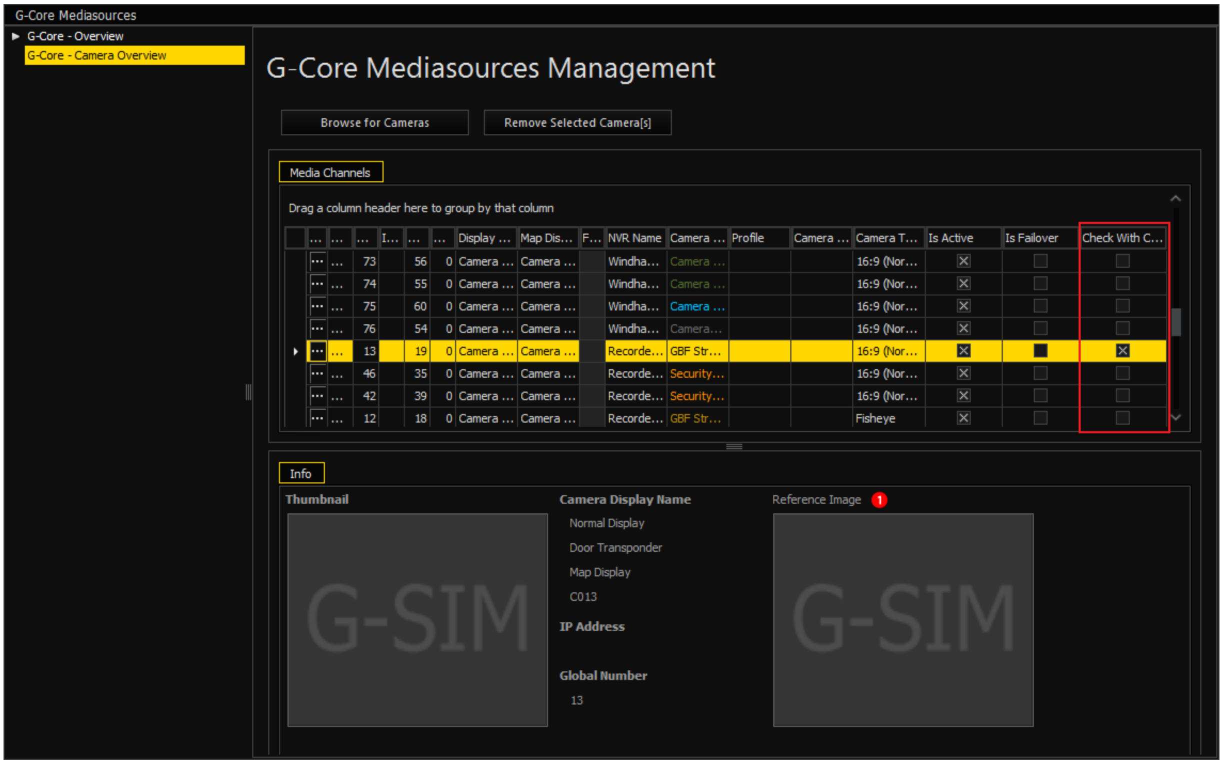
C01

If the user creates a new entry, the following occurs:

- the new item’s name is taken from the selected mediasource;
- the new item’s site is taken from the selected mediasource;
- all cameras from the selected mediasource are marked at **Check with CamCheck** and added to the new item’s cameras list
- if there is already a CCS item that is assigned to the selected mediasource's site, all cameras from the selected mediasource will be added as "checked by the existing CCS".

Select Cameras to Check in Recorder Settings

The admin can select cameras for monitoring from the recorder settings. This option is only available for selected sites. This works for G-Core and GeViScope recorders.



G-Core Mediasources

- G-Core - Overview
- G-Core - Camera Overview

G-Core Mediasources Management

Browse for Cameras
Remove Selected Camera[s]
Media Channels
Drag a column header here to group by that column

	...	...	...	I...	...	...	Display ...	Map Dis...	F...	NVR Name	Camera ...	Profile	Camera ...	Camera T...	Is Active	Is Failover	Check With C...
	⋯	...	73		56	0	Camera ...	Camera ...		Windha...	Camera ...			16:9 (Nor...	☒	□	□
	⋯	...	74		55	0	Camera ...	Camera ...		Windha...	Camera ...			16:9 (Nor...	☒	□	□
	⋯	...	75		60	0	Camera ...	Camera ...		Windha...	Camera ...			16:9 (Nor...	☒	□	□
	⋯	...	76		54	0	Camera ...	Camera ...		Windha...	Camera...			16:9 (Nor...	☒	□	□
▸	⋯	...	13		19	0	Camera ...	Camera ...		Recorde...	GBF Str...			16:9 (Nor...	☒	■	☒
	⋯	...	46		35	0	Camera ...	Camera ...		Recorde...	Security...			16:9 (Nor...	☒	□	□
	⋯	...	42		39	0	Camera ...	Camera ...		Recorde...	Security...			16:9 (Nor...	☒	□	□
	⋯	...	12		18	0	Camera ...	Camera ...		Recorde...	GBF Str...			Fisheye	☒	□	□

Info

Thumbnail

Camera Display Name
Normal Display
Door Transponder
Map Display
C013

IP Address

Global Number
13

Reference Image 1

The cameras marked under **Check with CamCheck** are checked by CCS. The reference image 1 is visible to the cameras selected for observation after saving the settings.

Save the Settings

To apply all settings, you must save them!

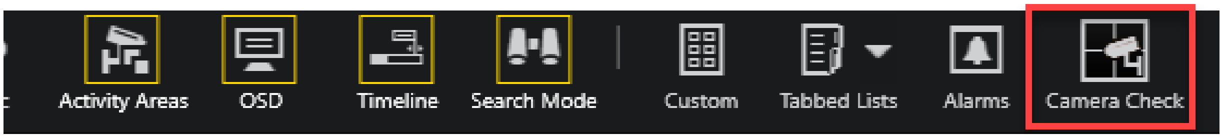
The settings of the CamCheck service (CCS) are stored in the database of G-SIM and the database of CCS.

After saving the settings, you will first receive the message that CCS is not available or that data is not stored in the DB of CCS.

In order to use CamCheck in Operator Console, the user right Camera check allowed must be granted (Users and Security > Users > Privileges).

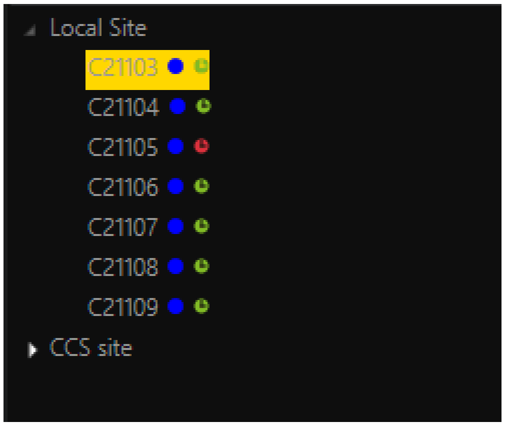
Operator Console

To open the Camera Check window, in the Operator Console toolbar, click the **Camera Check** button.



Camera Check Window

The **Camera Check** window contains a list of all sites and their cameras that are monitored by CamCheck.



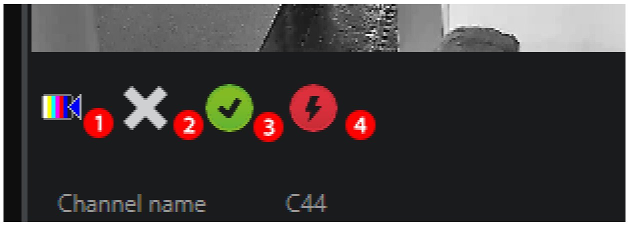
Local Site
C21103
C21104
C21105
C21106
C21107
C21108
C21109
CCS site

LEDs indicating the camera status:

- Green: camera status okay
- Red: camera status failed

- Grey: camera status unknown
- Blue: camera status offline

Furthermore, in the **Camera Check** window, the user can create or remove a reference image and set the manual status to "OK" or "Not OK".



Channel name C44

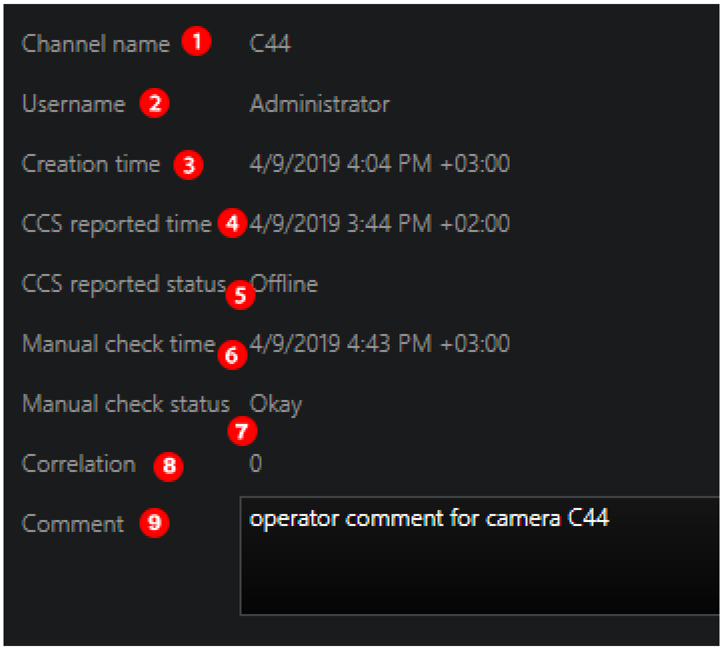
Prerequisites: CCS must be connected and live image must be available.

1 The user can create a reference image from the current live image by clicking this button.

2 The user can remove a reference image by clicking this button.

3 The user can set the manual status to "OK" by clicking this button.

4 The user can set the manual status to "Not OK" by clicking this button.



Channel name	C44
Username	Administrator
Creation time	4/9/2019 4:04 PM +03:00
CCS reported time	4/9/2019 3:44 PM +02:00
CCS reported status	Offline
Manual check time	4/9/2019 4:43 PM +03:00
Manual check status	Okay
Correlation	0
Comment	operator comment for camera C44

This field contains information on:

Explanation	
Channel name	The camera name
Username	The user that is working with the **Camera Check** window
Creation time	The reference image creation time
CCS reported time	The CCS reported date
CCS reported status	The CCS reported status
Manual check time	The manual date (set by the Operator)
Manual check status	The manual status (set by the Operator)
Correlation	Information on correlation
Comment	The Operator comment for the camera

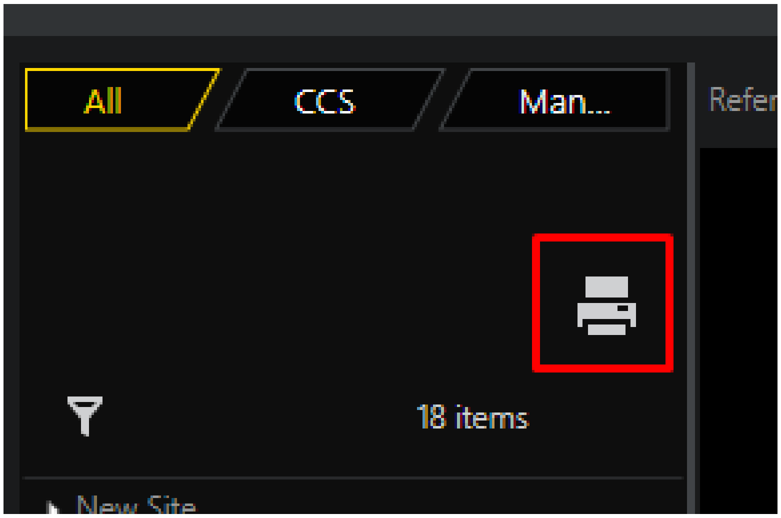
The Operator comment is only enabled for editing if the CCS is connected and a reference image is set.

Camera Check Report

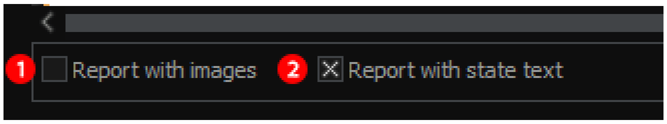
The feature **Camera Check Report** enables the user to create a report on the CCS state of the cameras.

The **Camera Check Report** obtains information from the cameras included in the currently active filter of the Camera Check window. This way the user can specifically check the cameras that appear in the report.

To create a **Camera Check Report**, click the **Print** icon on the right.

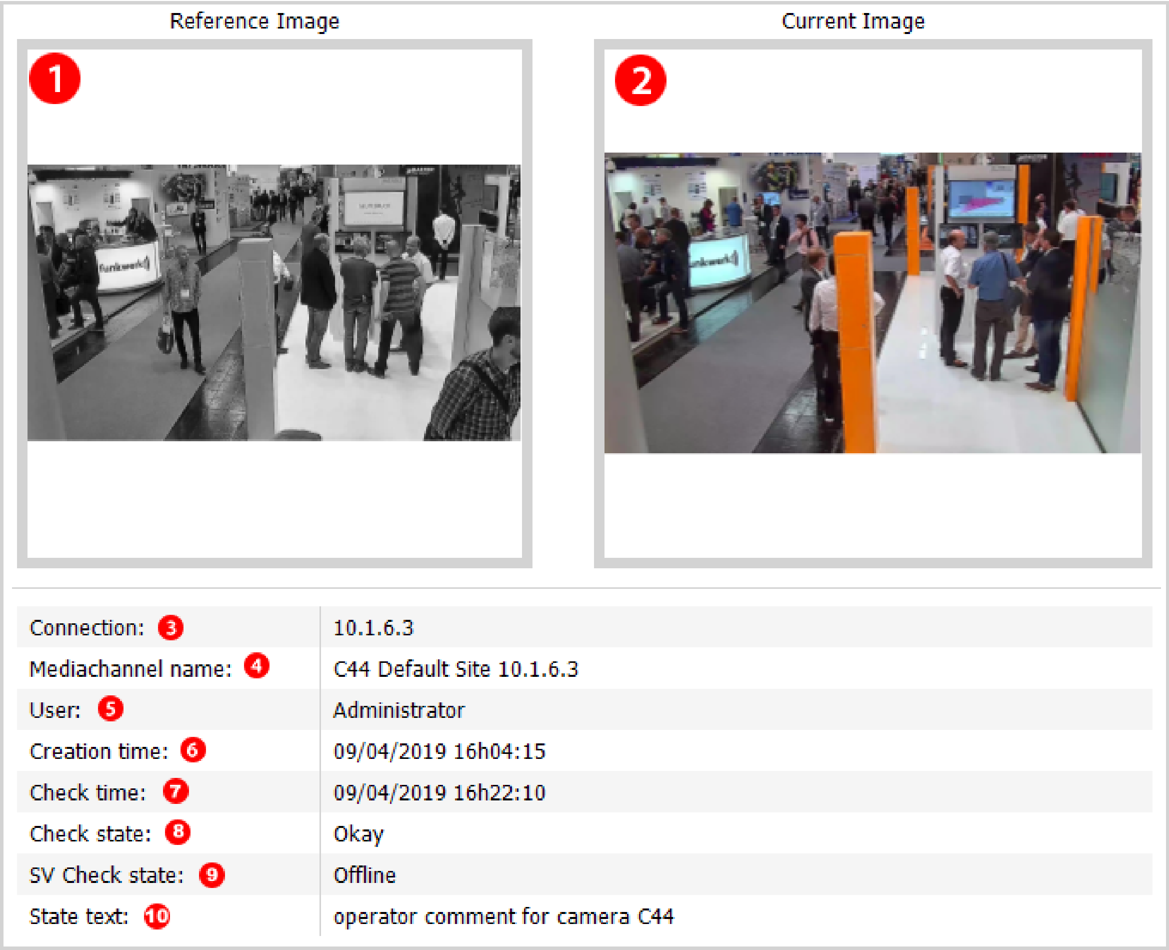


The user can 1 include or exclude reference and live images in the report . He can also 2 include or exclude the Operator comment (**state text**) for the camera.



□ Report with images ☒ Report with state text

The **Camera Check Report** contains the following information:



Connection:	10.1.6.3
Mediachannel name:	C44 Default Site 10.1.6.3
User:	Administrator
Creation time:	09/04/2019 16h04:15
Check time:	09/04/2019 16h22:10
Check state:	Okay
SV Check state:	Offline
State text:	operator comment for camera C44

The **Camera Check Report** displays 1 a reference image as well as 2 a live image.

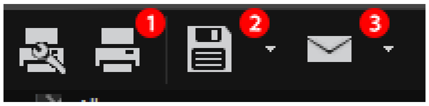
The visibility of those images depends on the **Report with images** settings.

Furthermore, the **Camera Check Report** contains information on:

Explanation	
Connection	The CSS name
Mediachannel name	The full camera name
User	The user working with the **Camera Check** window
Creation time	The reference image creation time

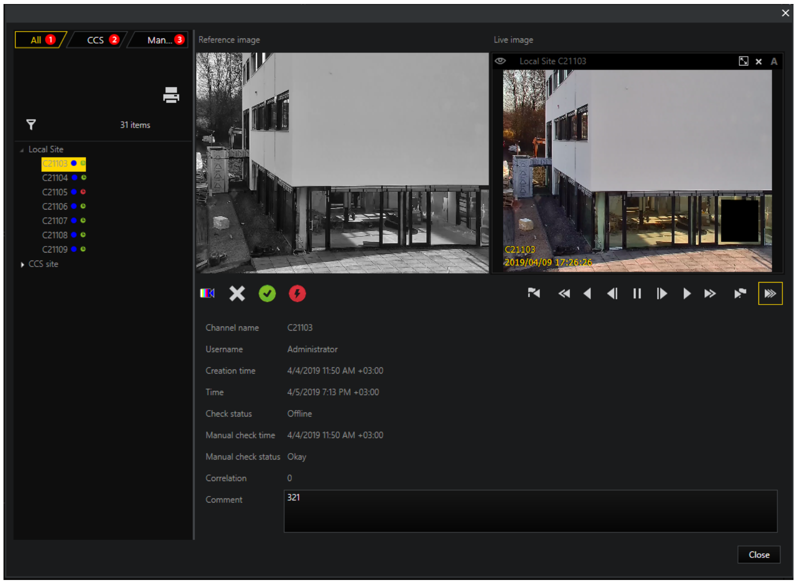
Explanation	
Check time	The manual time (set by the Operator)
Check state	The manual status (set by the Operator)
SV Check state	The CSS reported state
State text	Operator comment (**state text**)

i **The visibility of the Operator comment depends on the Report with state text settings.**



The user can 1 print the report, 2 export the report in different formats , or 3 send the report via email .

The **Camera Check** window contains three different filter tabs:



Channel name C21103
Username Administrator
Creation time 4/4/2019 11:50 AM +03:00
Time 4/5/2019 7:13 PM +03:00
Check status Offline
Manual check time 4/4/2019 11:50 AM +03:00
Manual check status Okay
Correlation 0
Comment 321

1 The **All** filter tab is the default tab and shows all cameras that are configured to be checked by CCS. Here, the user can also apply a custom filter.

2 The **CCS reported** filter tab shows all cameras having the CCS status “Failed”.

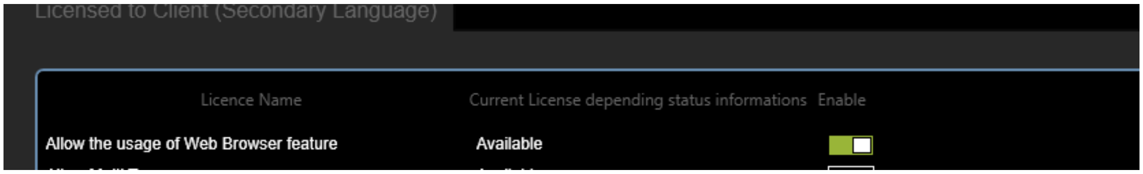
3 The **Manual check** filter tab shows all cameras that exceeded the configured time interval since the last manual check (See Management Console > **Manual Check Interval in Days**).

> **In the tree view, such a camera node features a clock sign. The clock sign can be filled with either a green color, indicating that the current manual check status is "OK", or with a red color, indicating that the current manual check status is "Not OK".**

Browser

The browser tab is visible when the following conditions are met:

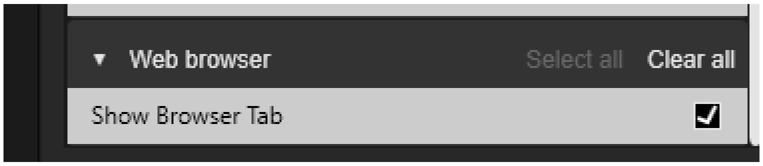
- G-SIM server supports the browser bookmarks functionality.
- The **Allow the usage of Web Browser feature** is available and enabled in the Server Licenses view of the Management Console.



Licensed to Client (Secondary Language)

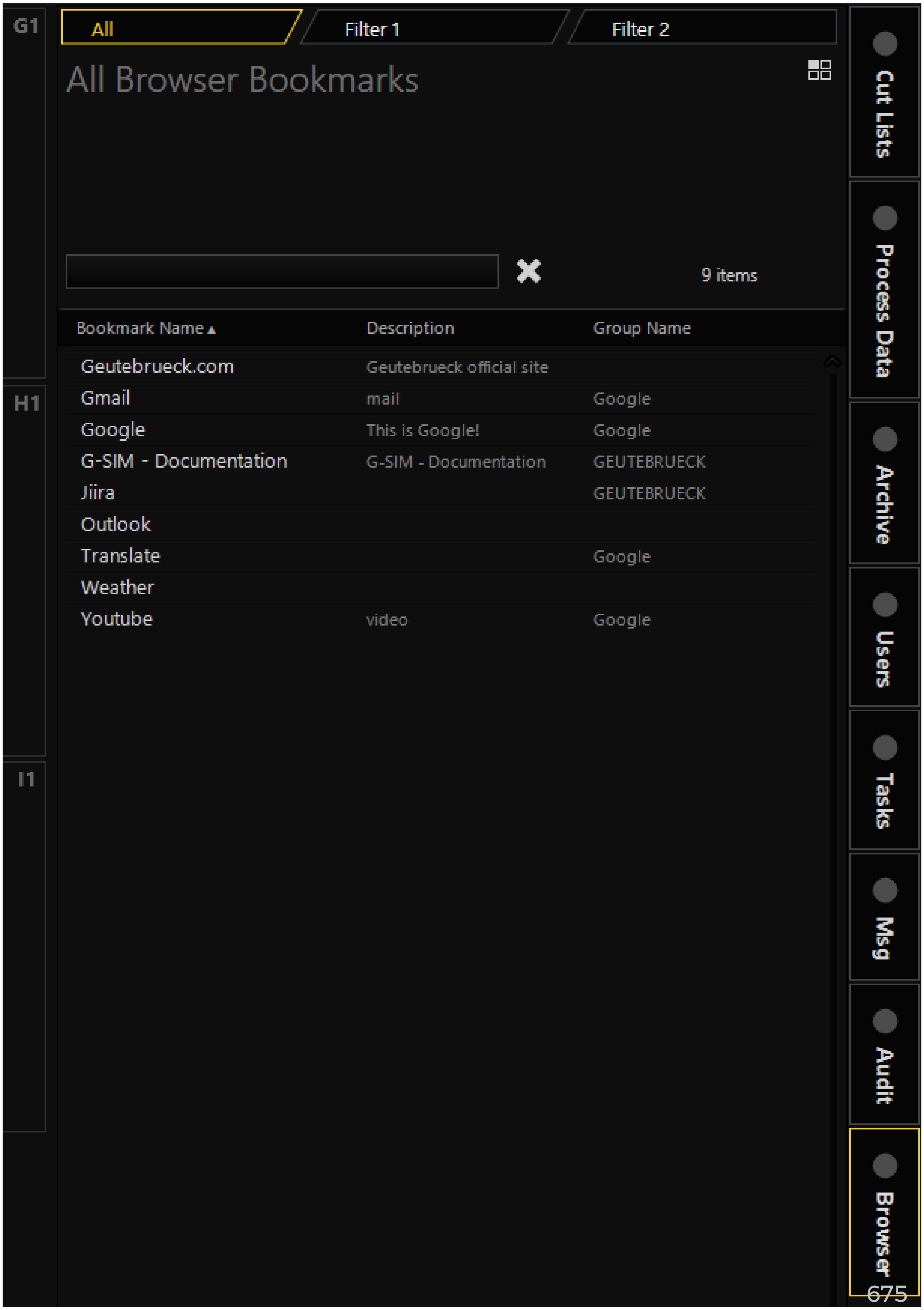
Licence Name	Current License depending status informations	Enable
Allow the usage of Web Browser feature	Available	🟩

- Logged user / Privilege group has the **Show Browser Tab** privilege.



Show Browser Tab ☑

The browser tab contains a list of the browser bookmarks that are accessible to the Logged user / Privilege group.

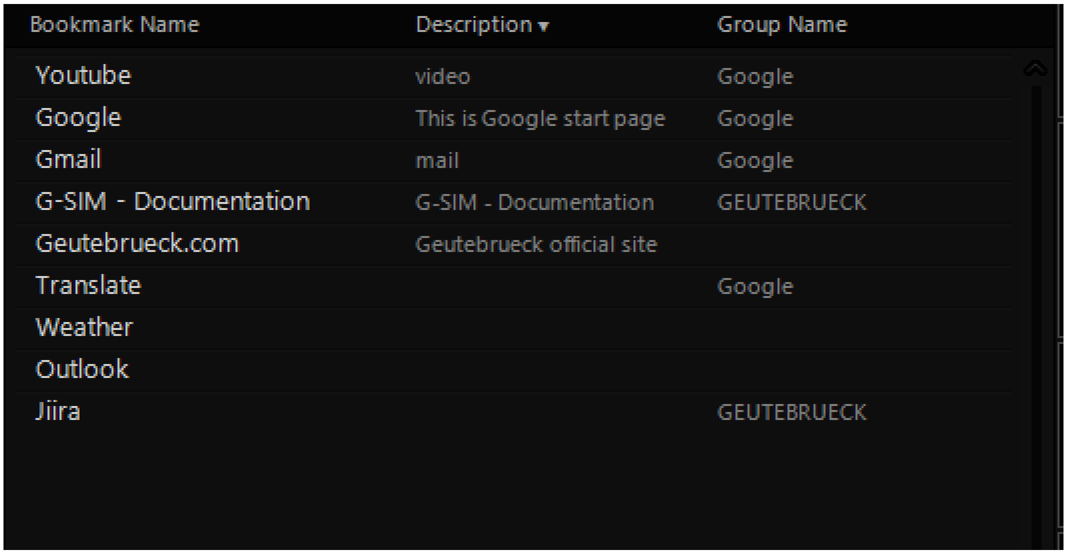


All Browser Bookmarks

9 items

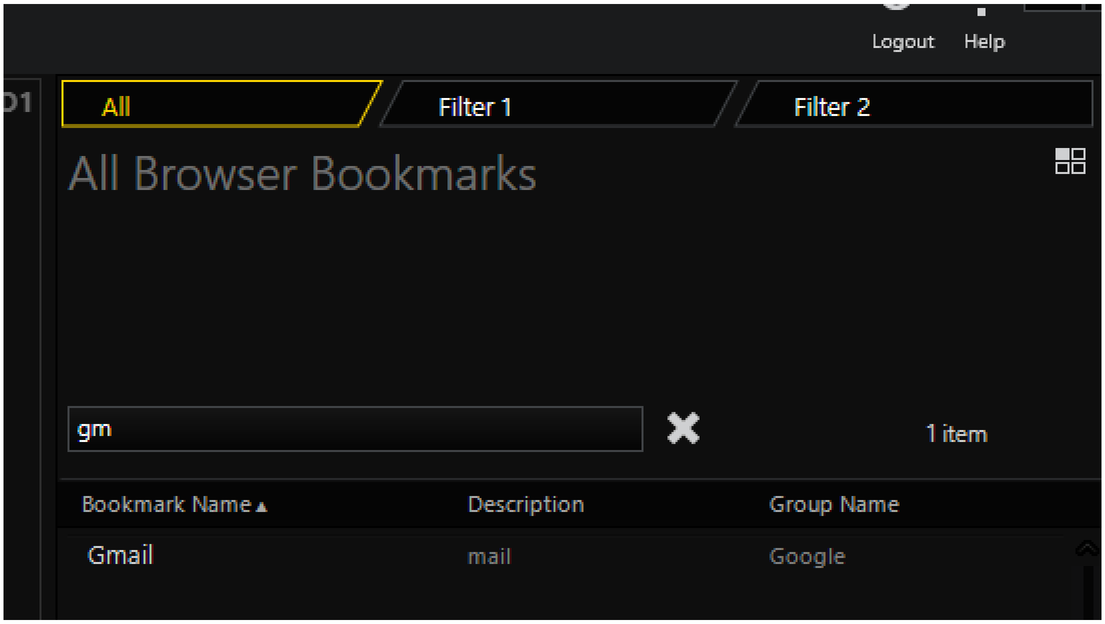
Bookmark Name ▴	Description	Group Name
Geutebrueck.com	Geutebrueck official site	
Gmail	mail	Google
Google	This is Google!	Google
G-SIM - Documentation	G-SIM - Documentation	GEUTEBRUECK
Jiira		GEUTEBRUECK
Outlook		
Translate		Google
Weather		
Youtube	video	Google

The user can sort the browser bookmarks by **Bookmark Name**, **Description** or **Group Name**.



Bookmark Name	Description ▾	Group Name
Youtube	video	Google
Google	This is Google start page	Google
Gmail	mail	Google
G-SIM - Documentation	G-SIM - Documentation	GEUTEBRUECK
Geutebrueck.com	Geutebrueck official site	
Translate		Google
Weather		
Outlook		
Jiira		GEUTEBRUECK

The user can use a quick filter to quickly find the desired bookmark.



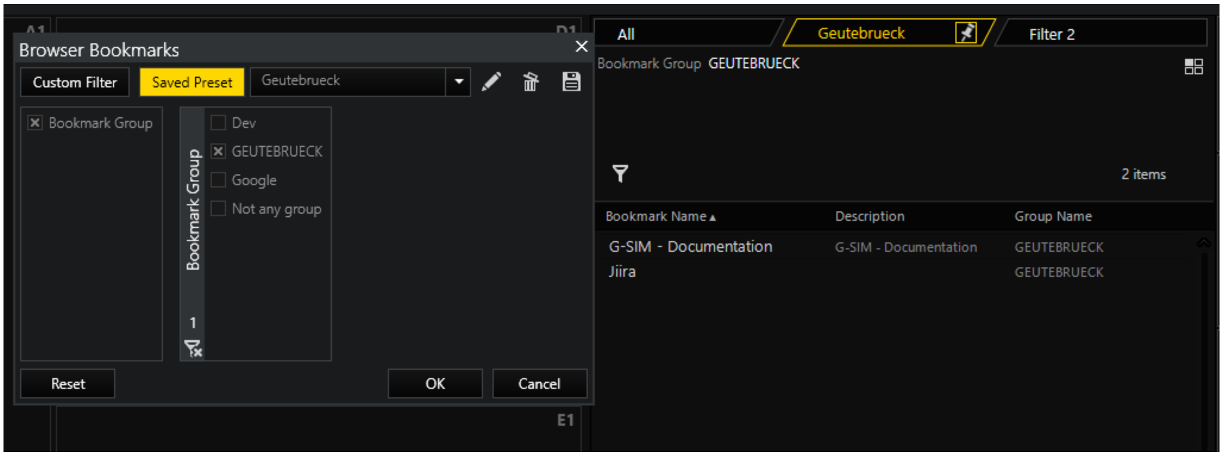
All Browser Bookmarks

gm

1 item

Bookmark Name ▴	Description	Group Name
Gmail	mail	Google

The user can use regular filters to filter bookmarks by Group Name (and servers in case of the global installation).



Saved Preset: Geutebrueck

☒ Bookmark Group

Bookmark Group:
- ☐ Dev
- ☒ GEUTEBRUECK
- ☐ Google
- ☐ Not any group

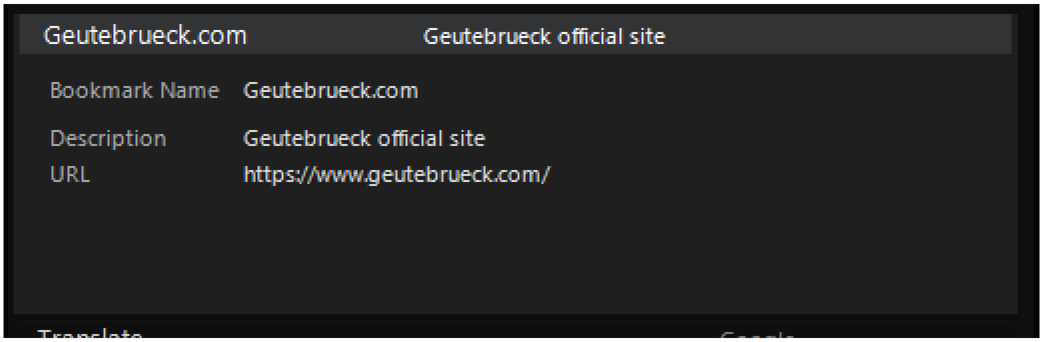
Bookmark Group GEUTEBRUECK

2 items

Bookmark Name ▴	Description	Group Name
G-SIM - Documentation	G-SIM - Documentation	GEUTEBRUECK
Jiira		GEUTEBRUECK

Browser Bookmark Card

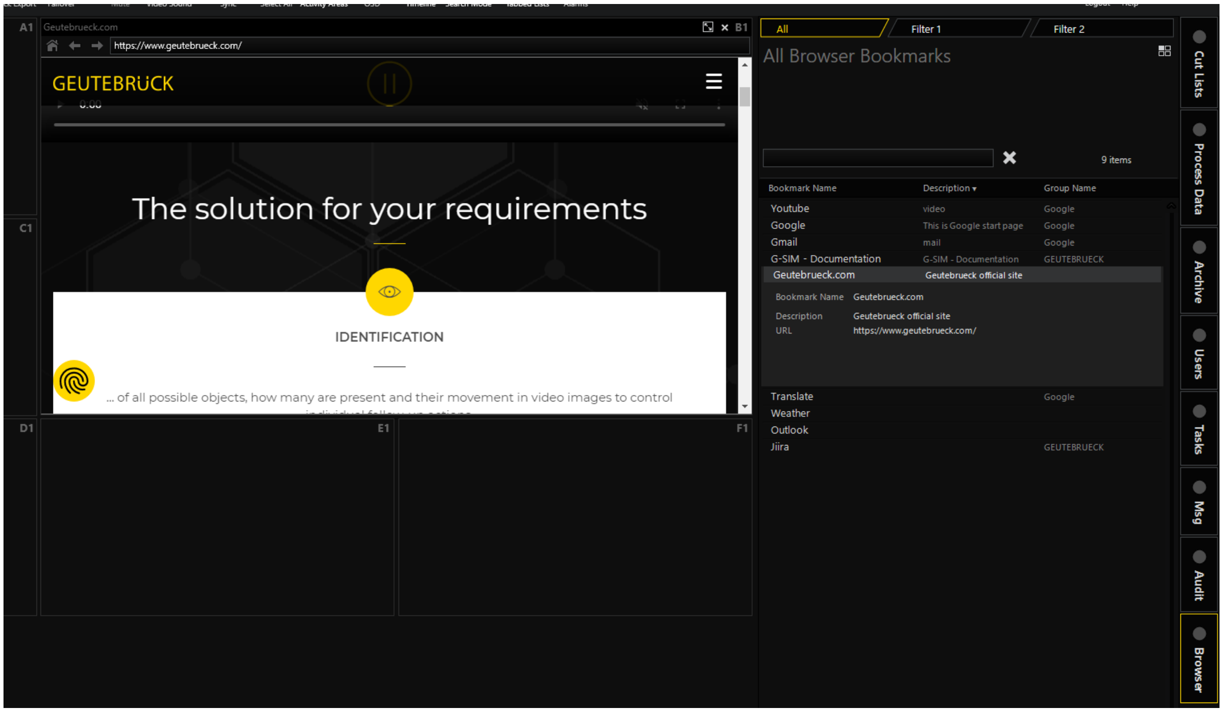
The browser bookmark card contains the **Bookmark Name**, **Description** and **URL** fields.



Geutebrueck.com Geutebrueck official site

Bookmark Name	Geutebrueck.com
Description	Geutebrueck official site
URL	https://www.geutebrueck.com/

If the viewer can accept browser bookmarks, the browser bookmark card can be opened in the viewer by using drag and drop. In this case, the web browser will be created in the viewer, and the appropriate URL (site) will be opened in the web browser.

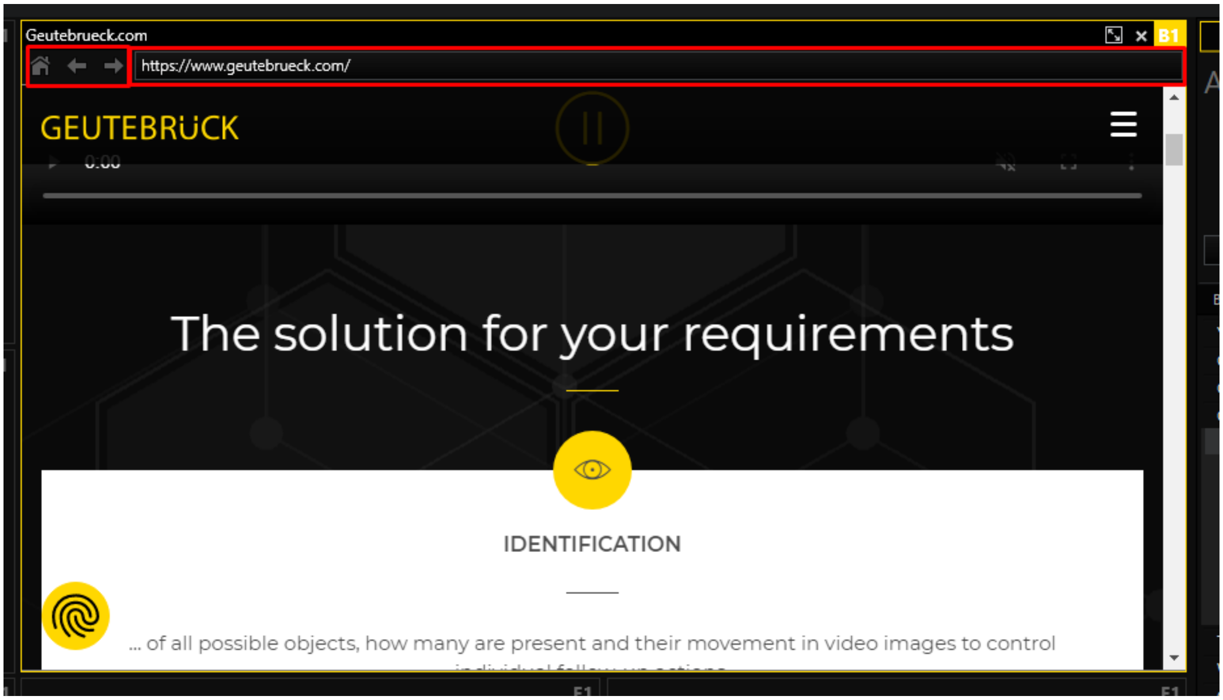

A1
Geutebrueck.com
B1
https://www.geutebrueck.com/
GEUTEBRÜCK
The solution for your requirements
IDENTIFICATION
... of all possible objects, how many are present and their movement in video images to control
C1
D1
E1
F1
All
Filter 1
Filter 2
All Browser Bookmarks
9 items
Cut Lists
Process Data
Archive
Users
Tasks
Msg
Audit
Browser

Bookmark Name	Description ▾	Group Name
Youtube	video	Google
Google	This is Google start page	Google
Gmail	mail	Google
G-SIM - Documentation	G-SIM - Documentation	GEUTEBRUECK
Geutebrueck.com	Geutebrueck official site	
Translate		Google
Weather		
Outlook		
Jiira		GEUTEBRUECK

Bookmark Name: Geutebrueck.com
Description: Geutebrueck official site
URL: https://www.geutebrueck.com/

Web Browser in Viewer

The web browser is configured according to the browser bookmarks and system settings in Management Console. For detailed information about the settings, see **Browser bookmarks** and **Web Browser Management**.


Geutebrueck.com
B1
https://www.geutebrueck.com/
GEUTEBRÜCK
0:00
The solution for your requirements
IDENTIFICATION
... of all possible objects, how many are present and their movement in video images to control
F1
F1

Web browser can be dragged onto the other viewer (if that viewer can accept browser bookmarks). When the web browser is dragged to the browser tab, the appropriate browser bookmark card will be automatically selected.

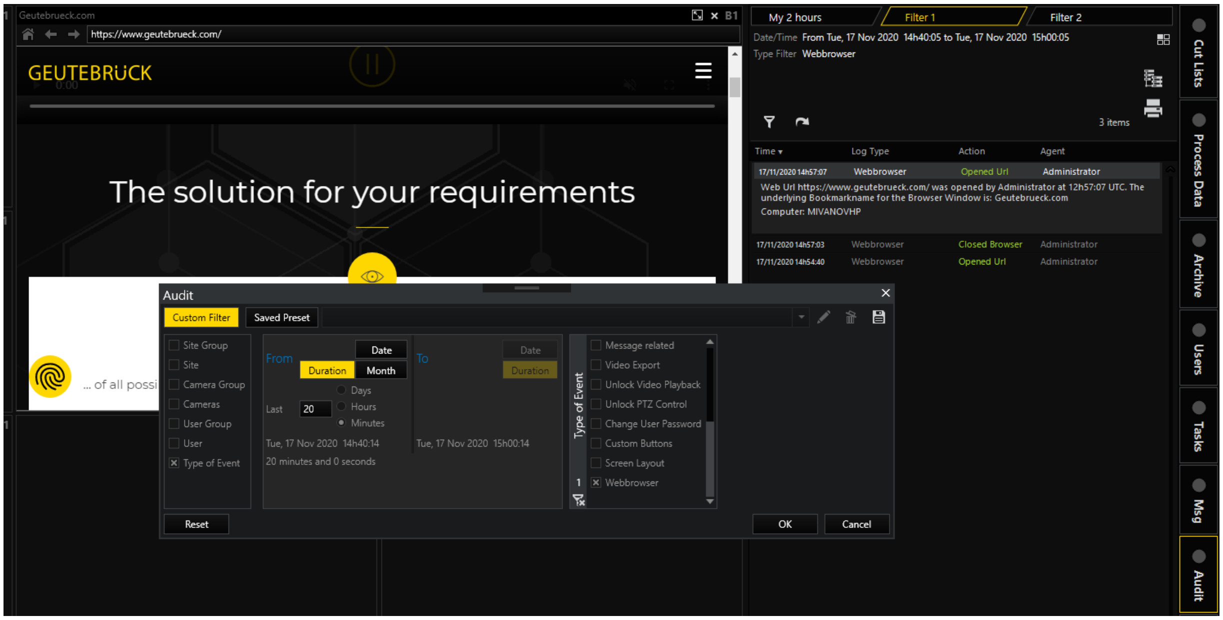
Viewers with browser bookmarks are restored when the Operator Console is opened again.

Audit

When the viewer is closed with the web browser in which the related browser bookmark **Create audit entries** (see **Browser bookmarks)** or the system setting **Create audit entries** (see **Web Browser Management**) is checked, the appropriate entry is stored in the audit log.

All sites that are navigated in the viewer with the web browser in which the related browser bookmark **Create audit entries** or the **Create audit entries** system setting is checked are stored in the audit log.

The user can filter audit for the web browser activity.



Date/Time From Tue, 17 Nov 2020 14h40:05 to Tue, 17 Nov 2020 15h00:05
Type Filter Webbrowser

Time ▾	Log Type	Action	Agent
17/11/2020 14h57:07	Webbrowser	Opened Url	Administrator
17/11/2020 14h57:03	Webbrowser	Closed Browser	Administrator
17/11/2020 14h54:40	Webbrowser	Opened Url	Administrator

Web Url https://www.geutebrueck.com/ was opened by Administrator at 12h57:07 UTC. The underlying Bookmarkname for the Browser Window is: Geutebrueck.com
Computer: MIVANOVHP

□ Site Group
□ Site
□ Camera Group
□ Cameras
□ User Group
□ User
☒ Type of Event

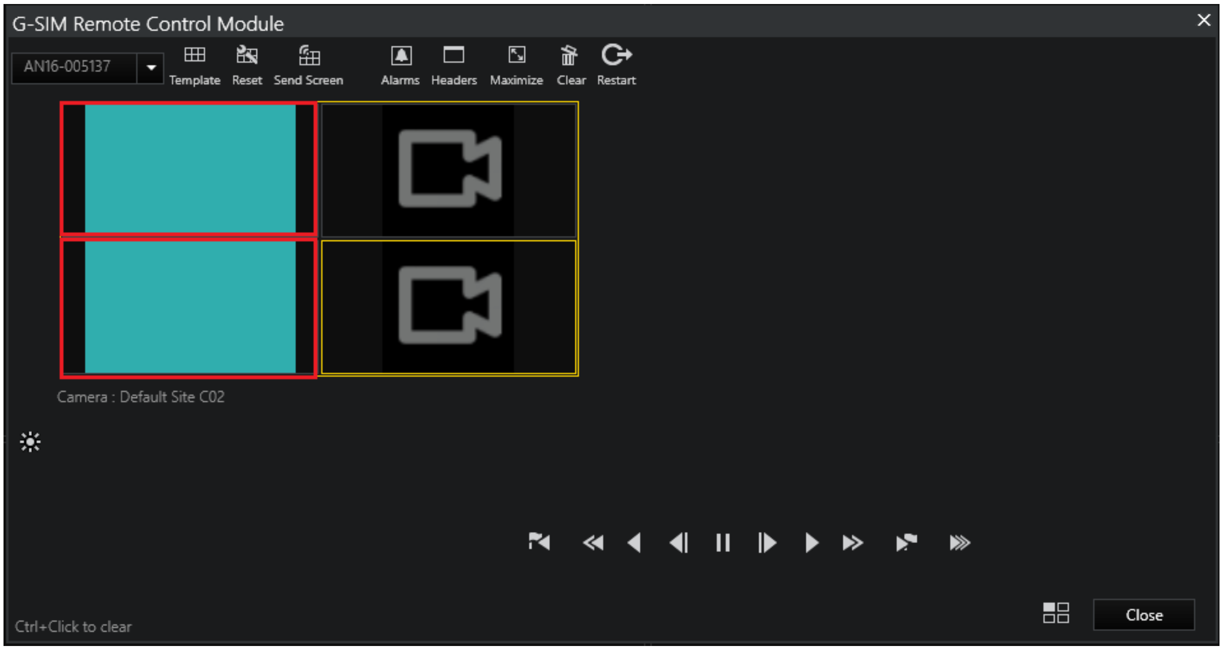
From: Date / Duration / Month
Last 20 ○ Days ○ Hours ● Minutes
Tue, 17 Nov 2020 14h40:14
20 minutes and 0 seconds

To: Date / Duration
Tue, 17 Nov 2020 15h00:14

Type of Event 1
□ Message related
□ Video Export
□ Unlock Video Playback
□ Unlock PTZ Control
□ Change User Password
□ Custom Buttons
□ Screen Layout
☒ Webbrowser

Remote Console

Browser bookmarks can be displayed in the remote console using the G-SIM remote control module. The remote viewer that displays the browser is filled with cyan color.



Camera : Default Site C02

Ctrl+Click to clear

Client Certificate Authentication

Some websites need Client Certificates for authentication. In case G-SIM Web Browser is not able to uniquely identify the Client Certificate in the current user certificates store,it needs an additional mechanism to provide the Client Certificate for authentication.

Therefore G-SIM uses a plugin-based approach for the Client Certificate provider implementation. This approach gives the opportunity to create custom Client Certificate provider plugins to fit the customers specific requests without changing any G-SIM modules.

A default G-SIM Client Certificate provider plugin is included in G-SIM and will be installed on the client computer during the G-SIM installation process.

Custom Client Certificate Provider Plugin

The `GSIM.OperatorUI.exe.Config` file contains the MEFPluginsPath setting. It specifies the path to the folder where the custom Client Certificate plugin is going to be searched.

Whenever G-SIM Web Browser needs Client Certificate to be provided, the Client Certificate plugin will be searched in this folder. If a plugin exists in this folder, it will be used.

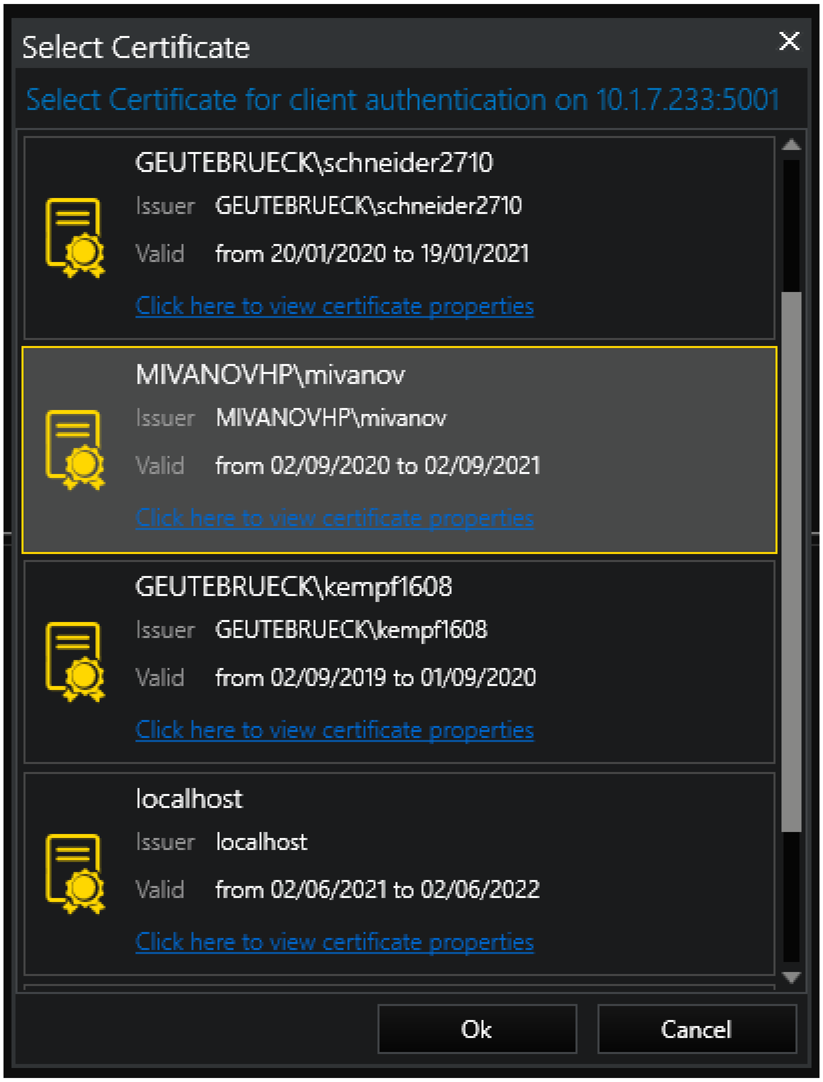
Otherwise the default G-SIM Client Certificate provider plugin will be used.

The default MEFPluginsPath setting refers to `<gsim_installation_path>\Geutebrueck\GSim\MEFPlugins`.

This folder is going to be created by the G-SIM installer.

Default Client Certificate Provider Plugin

Default Client Certificate provider plugin will be used if custom client certificate is absent. It opens a popup window like the following, with a list of all certificates in the current user certificates store which are issued for the client authentication.



Select Certificate

Select Certificate for client authentication on 10.1.7.233:5001

GEUTEBRUECK\schneider2710

Issuer GEUTEBRUECK\schneider2710

Valid from 20/01/2020 to 19/01/2021

Click here to view certificate properties

MIVANOVHP\mivanov

Issuer MIVANOVHP\mivanov

Valid from 02/09/2020 to 02/09/2021

Click here to view certificate properties

GEUTEBRUECK\kempf1608

Issuer GEUTEBRUECK\kempf1608

Valid from 02/09/2019 to 01/09/2020

Click here to view certificate properties

localhost

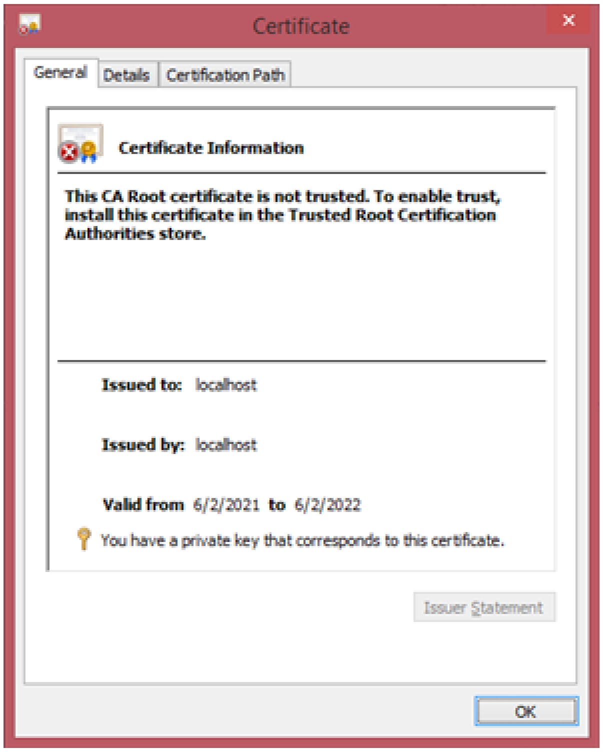
Issuer localhost

Valid from 02/06/2021 to 02/06/2022

Click here to view certificate properties

To use a certificate for client authentication select the desired certificate and click on the **Ok** button. Click on the **Cancel** button to close the popup window without providing a certificate to the G-SIM Web Browser.

To get additional certificate details, click on **Click here to view certificate properties** and a properties window is going to open.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: localhost

Issued by: localhost

Valid from 6/2/2021 to 6/2/2022

You have a private key that corresponds to this certificate.

Caching Client Certificate

The selected Client Certificate is cached per Website during operator console sessions.

Whenever operator console is restarted, Client Certificate should be provided again.

Technical Details

G-SIM uses the Microsoft Managed Extensibility Framework (MEF) for Client Certificate provider plugin usage.

To create a custom Client Certificate provider plugin, developers should build a .Net assembly with a class that implements the **GSIM.CertificateProvider.ICertificateProviderPlugin** interface from the `GSIM.CertificateProviderPluginInterface.dll` assembly.

The Class should be marked with **[Export(typeof(ICertificateProviderPlugin))]** attribute.

The Assembly should be copied to the folder from `GSIM.OperatorUI.exe.Config` file's MEFPluginsPath setting.

Global Operator Console

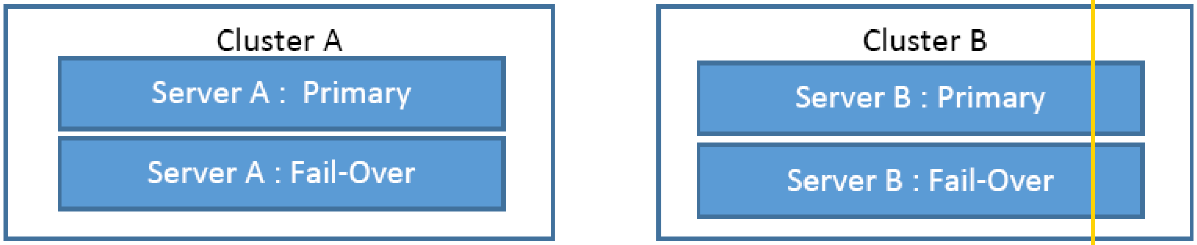
Login / Connection to Server

One advantage in a GSIM Global environment is that GSIM Operator Consoles may connect to another Global Server if the preferred (local) server is not available. This is called “auto-connect” and is in short a list of Global Servers in a user defined order to which a connect will be attempted. The first server in the list will be the user's preferred (usually local) server. A Global Server may be a single server or a cluster consisting of a Primary and a Failover server. A cluster is handled as a single server in the Global environment – only one of the cluster servers will be active and the other one on stand-by if both are up and running.

It is important to understand that the synchronization of data between two servers in a cluster is real-time: All data is immediately sent to the Failover server, and the data on these two servers is identical. It is not necessary for a user to know which one of the two he is connected to. These clustered servers may swap between each other (e.g. when failover occurs), and the user might not even realize the swap as it happens in the background.

Global Servers differ from each other, and a user may have limited usability if he logs in to another server instead of his preferred (local) server. A Global Server will have its own unique sites and cameras (called local sites/cameras), and may then also have access to other Global Servers’ sites, cameras etc. Even if the same camera is accessible from both Global Servers, it will belong to only one of the servers (will be a local camera for one server, and a remote camera for the other). For this reason a “hot swap” between two Global Servers is not possible. If the user's preferred server is down and he has to connect (log in) to another Global Server, the Operator Console will need to restart and reload all the resources from the “new” server.

Example Consider this case scenario:



If a Management Console is logged into **Server A Primary** and this machine is shut down or disconnected from the network, the **Server A Fail-Over** will immediately take over, and the user will continue as if nothing happened. If this **Server A Failover** machine is also shut down, the user will be informed that the preferred server is down, but that another Global Server is available. To log in to this server, the Operator Console must restart and reconnect to the new server. When the Operator Console restarts, it will attempt to connect to the preferred server A. After the connect process timed out, an attempt will be made to connect to the next Global Server (as defined in the Management Console) – in this case **Cluster B**. If anyone of the **Cluster B** servers is available, the user's credentials will be passed to this cluster and the user will be logged in. Depending on the setup, he might not have access to the same cameras and receive all the same alarms as to when he was logged in to Server A. If any of the Server A machines go online again, the user will be notified that his preferred server is available again, and he will have the option to log out from B and log in to A.

Setup for alternate auto-connect servers is done in the Management Console. The user can specify:

- which other Global Servers may be used and
- the sequence in which the connection will be attempted.

The preferred server is the one specified in the Operator Console's CONFIG file. After the first successful login, the sequence of Global Servers, which may be used for auto-connect, is stored locally in `C:\ProgramData\G-SIM\OpCon\Cluster`. All these files may be deleted if e.g. the preferred server is changed in the CONFIG file but the change is ignored – the files will be recreated after the first successful login. These files will also be updated when changes are made to the auto-connect options in the Management Console.

Currently Connected and Available Servers

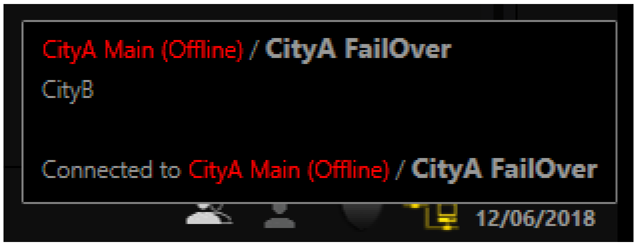
The state of the Global Server Network is indicated by the network icon in the right-hand corner of the main screen.

There are four states:

Explanation of states	
🖧	All Global Servers are available – everything OK
🖧	One or more remote servers are not available
🖧	The local cluster server is not fully functional (one server down)
🖧	Lost connection to the logged in server – Restart to connect to another server

Hovering with the mouse over the network icon will show a pop-up window with all the Global Servers as well as their current state. Clustered servers are displayed in a single line.

The following image shows a state in which the user is connected to the server of CityA, which is a cluster. However one of the cluster servers is down. CityB has a single server, which is available.



CityA Main (Offline) / **CityA FailOver**

CityB

Connected to CityA Main (Offline) / **CityA FailOver**

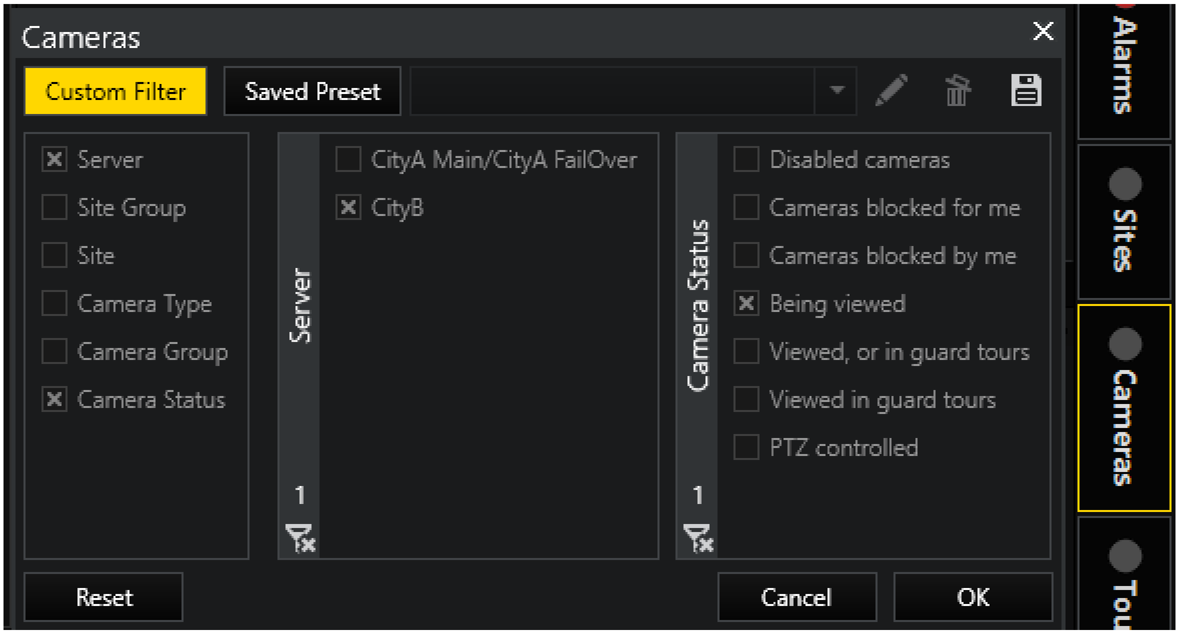
12/06/2018

Global Handling of Camera-, Site-, Guard Tour- and User-Lists

This "static" data is synced between all connected servers in a Global G-SIM network.

The syncing is not real-time (as it is for a cluster). Changes may take a few minutes to be propagated to all Global Servers.

The “All” **Cameras** and **Sites** lists will contain all cameras etc. over the whole Global network (all of which are accessible for the currently logged-in user). To filter for a specific Global Server, a new **Server** filter was added to all the list filters.



Cameras

☒ Server
☐ Site Group
☐ Site
☐ Camera Type
☐ Camera Group
☒ Camera Status

Server 1
☐ CityA Main/CityA FailOver
☒ CityB

Camera Status 1
☐ Disabled cameras
☐ Cameras blocked for me
☐ Cameras blocked by me
☒ Being viewed
☐ Viewed, or in guard tours
☐ Viewed in guard tours
☐ PTZ controlled

Clustered servers act as one server, but will be indicated by both of the server names e.g. “NY / NY-FailOver”.

Global Handling of Alarms

When logged into a specific server, the user will receive all Alarms which he has privilege to and which are generated on that server. Alarms from other Global Servers (remote servers) may be pushed from their server to other Global Servers and will then also appear in the user's **Alarm** list.

Which alarms are pushed to other servers is part of the Alarm setup in the Management Console.

What happens on login is:

- The **local** alarms are received from the server the user logged in to. Usually this will be the user's preferred server. If logged into another server because the preferred server was not available, the user will receive all the alarms generated in that server’s database. This **Alarm** list is very different from what the user would have received when logged into his preferred server.

- Then, a query is sent to all other available Global Servers to send their uncompleted alarms to the Operator Console. It is the same query as if a custom query was executed to extract these alarms from other servers – the remote alarms are not cashed or saved on the user's local server. When a user logs into the Operator Console, he will then see a list of alarms – the alarms from his logged in server. Then, chunks of alarms will be added to this list as other Global Servers respond to the query and send their alarms to the Operator Console.
- A few seconds after start-up the user's Alarm list will contain all old unhandled alarms from all available Global Servers. When a new alarm is generated on the currently logged in (local) server, all logged in users with rights will immediately receive the alarm. When an alarm is generated on another Global Server and it is set to be pushed, it will be forwarded to the user's Operator Console. The queried Alarm list will thus be kept updated as local as well as remote alarms are generated.

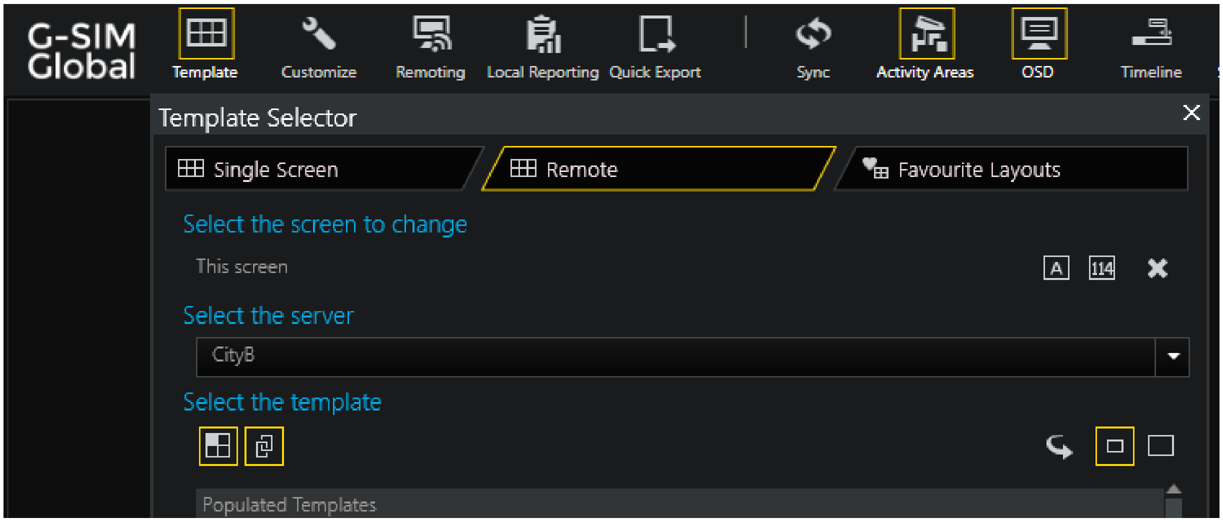
Global Handling of Process Data

The filter criteria selector for process data searches was modified to work in a cross server environment where not all process data types may be queried or exist on all Global Servers. Like for all other lists, a Server criteria was added, and the list of available process data types will be populated depending on the selected server.

Pre-installed (default) process data filters are not synchronized between Global Servers. If default filter is changed it must be changed manually on all Global Server respectively. Otherwise severs will have different filter configurations. Solution: The default filter can be cloned. Then the filter clone can be changed as needed and will be synchronized between Global Servers.

Template Selection in G-SIM Global

A new tab was added to the Template Selector enabling the user to select a Populated Template or Linked Layout from a remote server. The Single Screen tab will only show screen templates on the currently logged in server. Empty templates may only be selected from templates available on the logged in server.



Template Selector

Select the screen to change

This screen

Select the server

CityB

Select the template

Populated Templates

Connection Failure Notification

G-SIM has safety mechanisms to compensate for network failures and to re-establish connections to clients autonomously.

The behavior of the operator console (OpCon) and remote console (ReCon) in case of a network failure, are explained below for the different G-SIM systems. Select your system in the list to display the corresponding explanations and recommended actions:

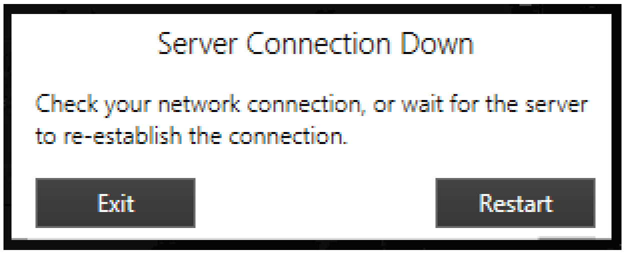
- **Standalone System**
- **Standalone Cluster System**
- **Global System with Cluster**
- **Global System without Cluster**

Standalone System

In case of a loss of the network connection, the standalone system will automatically reconnect to the OpCon and ReCon as soon as the server is available again.

Notification in the Operator Console

The warning message that appears in the OpCon of the standalone system advises the user to restart the OpCon directly by clicking the **Restart** button or to close it completely by clicking the **Exit** button.

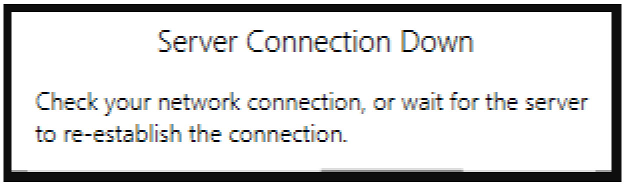


Server Connection Down

Check your network connection, or wait for the server to re-establish the connection.

Notification in the Remote Console

The warning message that appears in the ReCon of the standalone system informs the user about the network failure.



Server Connection Down

Check your network connection, or wait for the server to re-establish the connection.

This message box disappears automatically as soon as the server is available again.

Standalone Cluster System

Since the standalone cluster system has a primary and a secondary (failover) server, there are two types of network failure that result in loss of network connection as well as corresponding behaviors of the system:

- Failure of the primary server
- Failure of the primary and secondary server

Failure of the Primary Server

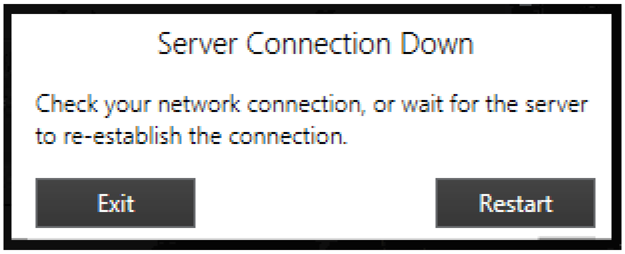
In case of a network failure of the primary server, the OpCon and ReCon of the standalone cluster system automatically connects to the secondary (failover) server if it is available. As soon as the primary server is available again, the system automatically reconnects to the OpCon and ReCon.

Failure of the Primary and Secondary Server

In case of a network failure of the primary and secondary server, the standalone cluster system independently re-establishes the connection to the OpCon and ReCon as soon as one of the servers is available again

Notification in the Operator Console

The warning message that appears in the OpCon of the standalone cluster system advises the user to restart the OpCon directly by clicking the **Restart** button or to close it completely by clicking the **Exit** button.

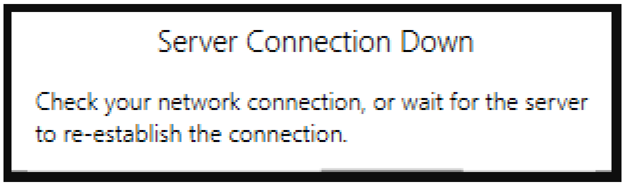


Server Connection Down

Check your network connection, or wait for the server to re-establish the connection.

Notification in the Remote Console

The warning message that appears in the ReCon of the standalone cluster system informs the user about the network failure.



Server Connection Down

Check your network connection, or wait for the server to re-establish the connection.

This message box disappears automatically as soon as the server is available again.

Global System with Cluster

Since the global cluster system has a primary and a secondary (failover) server, there are two types of network failure that result in loss of network connection and corresponding behaviors of the system:

- Failure of the primary server
- Failure of the primary and secondary server

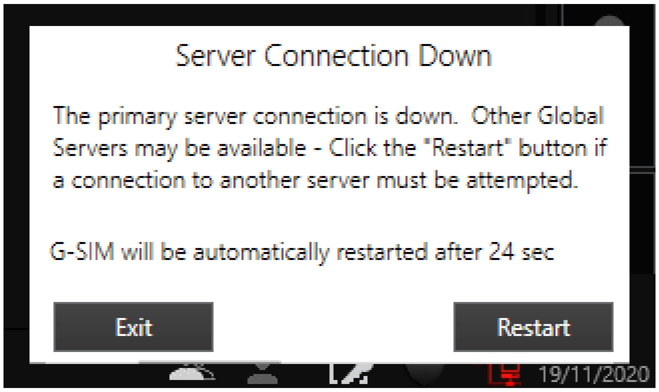
Failure of the Primary Server

In case of a network failure of the primary server, the OpCon and ReCon of the global cluster system automatically connects to the secondary (failover) server if it is available. As soon as the primary server is available again, the system reconnects to the OpCon and ReCon independently.

Failure of the Primary and Secondary Server

In case of a network failure of the primary and secondary server, the global cluster system independently establishes the connection to the next available global server.

This requires a restart of the OpCon and the ReCon, which is performed automatically. A corresponding warning message appears in both consoles to notify the user of the required restart.



Server Connection Down

The primary server connection is down. Other Global Servers may be available - Click the "Restart" button if a connection to another server must be attempted.

G-SIM will be automatically restarted after 24 sec

IMPORTANT: Restarting the console is necessary to ensure a consistent data state and to avoid a console malfunction.

- It is recommended to restart the consoles directly by clicking the Restart button.

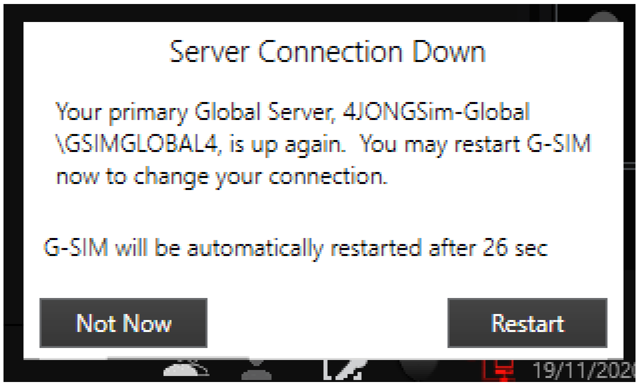
  → After the restart an unhindered operation of the OpCon and the ReCon is guaranteed again.

- If you do not want to restart the OpCon or ReCon directly, you can close the console by clicking on the Exit button.
- If you do not click either button, the OpCon and ReCon will automatically restart and connect to the next available global server as soon as the countdown timer reaches 0.

  → Information on setting the countdown timer can be found here: **Set up Countdown Timer for Automatic Restart**

As soon as the primary server is available again while the OpCon or ReCon is connected to a non-primary or secondary server, the system re-establishes the connection independently.

This requires a restart of the OpCon and the ReCon, which is performed automatically. A corresponding warning message appears in both consoles to notify the user of the required restart.



Server Connection Down

Your primary Global Server, 4JONGSim-Global \GSIMGLOBAL4, is up again. You may restart G-SIM now to change your connection.

G-SIM will be automatically restarted after 26 sec

⚠ **IMPORTANT:** Restarting the console is necessary to ensure a consistent data state and to avoid a console malfunction.

- It is recommended to restart the consoles directly by clicking the Restart button.

  → After the restart an unhindered operation of the OCon and the ReCon is guaranteed again.

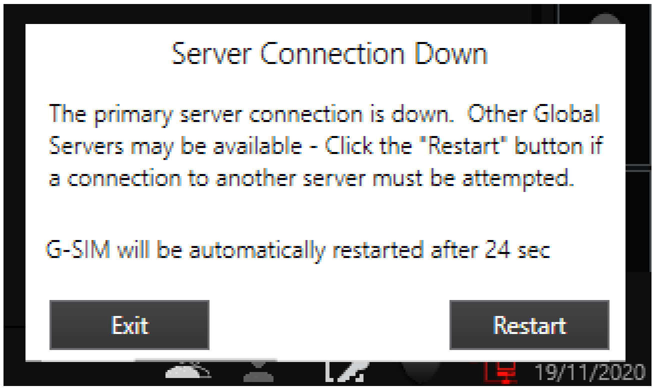
- If you do not want to restart the OpCon or ReCon directly, but want to continue working with the currently connected G-SIM server, click the Not Now button.
- If you do not click either button, the OpCon and ReCon will automatically restart and connect to the primary server as soon as the countdown timer reaches 0.

  → Information on setting the countdown timer can be found here: **Set up Countdown Timer for Automatic Restart**

Global System without Cluster

In case of a network failure of the primary server, the global system without cluster independently establishes the connection to the next available global server.

This requires a restart of the OpCon and the ReCon, which is performed automatically. A corresponding warning message appears in both consoles to notify the user of the required restart.



Server Connection Down

The primary server connection is down. Other Global Servers may be available - Click the "Restart" button if a connection to another server must be attempted.

G-SIM will be automatically restarted after 24 sec

⚠ **IMPORTANT:** Restarting the console is necessary to ensure a consistent data state and to avoid a console malfunction.

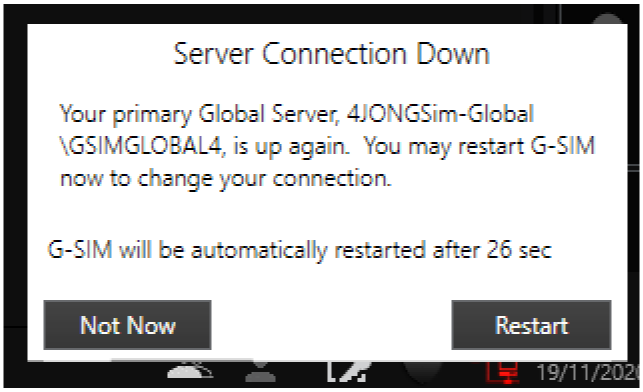
- It is recommended to restart the consoles directly by clicking the Restart button.

  → After the restart an unhindered operation of the OpCon and the ReCon is guaranteed again.
- If you do not want to restart the OpCon or ReCon directly, you can close the console by clicking on the Exit button.
- If you do not click either button, the OpCon and ReCon will automatically restart and connect to the next available global server as soon as the countdown timer reaches 0.

  → Information on setting the countdown timer can be found here: **Set up Countdown Timer for Automatic Restart**

As soon as the primary server is available again while the OpCon or ReCon is connected to another global server, the system re-establishes the connection independently.

This requires a restart of the OpCon and the ReCon, which is performed automatically. A corresponding warning message appears in both consoles to notify the user of the required restart.



Server Connection Down

Your primary Global Server, 4JONGSim-Global \GSIMGLOBAL4, is up again. You may restart G-SIM now to change your connection.

G-SIM will be automatically restarted after 26 sec

⚠ **IMPORTANT:** Restarting the console is necessary to ensure a consistent data state and to avoid a console malfunction.

- It is recommended to restart the consoles directly by clicking the Restart button.

  → After the restart an unhindered operation of the OpCon and the ReCon is guaranteed again.

- If you do not want to restart the OpCon or ReCon directly, but want to continue working with the currently connected G-SIM server, click the Not Now button.
- If you do not click either button, the OpCon and ReCon will automatically restart and connect to the primary server as soon as the countdown timer reaches 0.

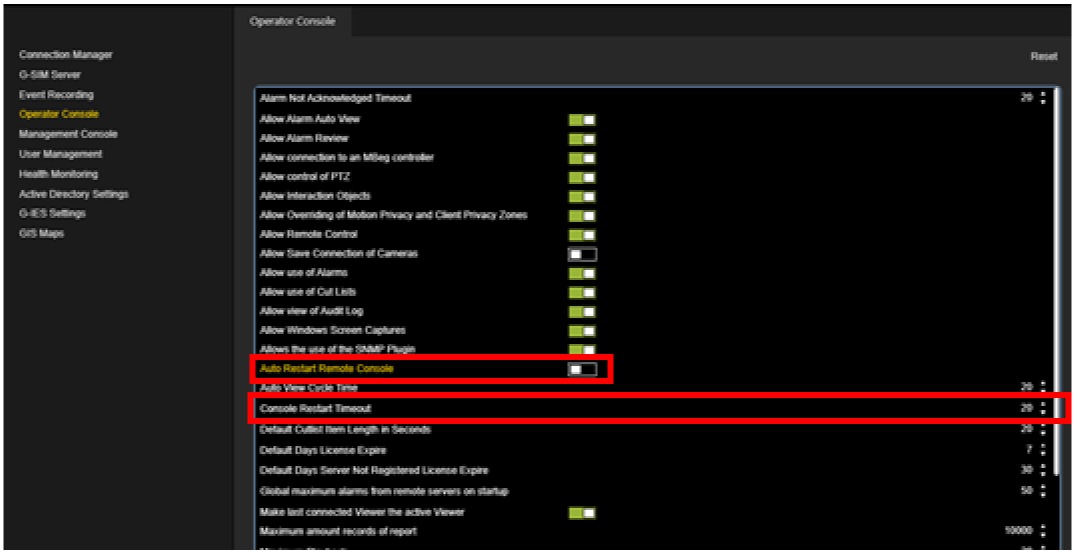
  → Information on setting the countdown timer can be found here: **Set up Countdown Timer for Automatic Restart**

Set up Countdown Timer for Automatic Restart

The countdown timer (in seconds) until the automatic restart of the OpCon or ReCon can be configured in the Management Console in the **System Settings**. To do this, select the category Operator Console and define the time in seconds until restart with the option Console Restart Timeout.

You can also set the same behavior for a ReCon as for an OpCon by deactivating the slider Auto Restart Remote Console.

In this case, the ReCon must be restarted manually via the Restart pop-up window.



Alarm Not Acknowledged Timeout	20
Allow Alarm Auto View	☑
Allow Alarm Review	☑
Allow connection to an MBeg controller	☑
Allow control of PTZ	☑
Allow Interaction Objects	☑
Allow Overriding of Motion Privacy and Client Privacy Zones	☑
Allow Remote Control	☑
Allow Save Connection of Cameras	☐
Allow use of Alarms	☑
Allow use of Cut Lists	☑
Allow view of Audit Log	☑
Allow Windows Screen Captures	☑
Allows the use of the SNMP Plugin	☑
Auto Restart Remote Console	☐
Auto View Cycle Time	20
Console Restart Timeout	20
Default Cutlist Item Length in Seconds	20
Default Days License Expire	7
Default Days Server Not Registered License Expire	30
Global maximum alarms from remote servers on startup	50
Make last connected Viewer the active Viewer	☑
Maximum amount records of report	10000

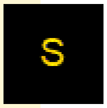
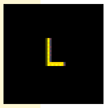
Image Watermark

General Information

You have the option to save a 50x50 image watermark logo as a 256-color bitmap file.

Name this file ExportLogoS.bmp or ExportLogoL.bmp.

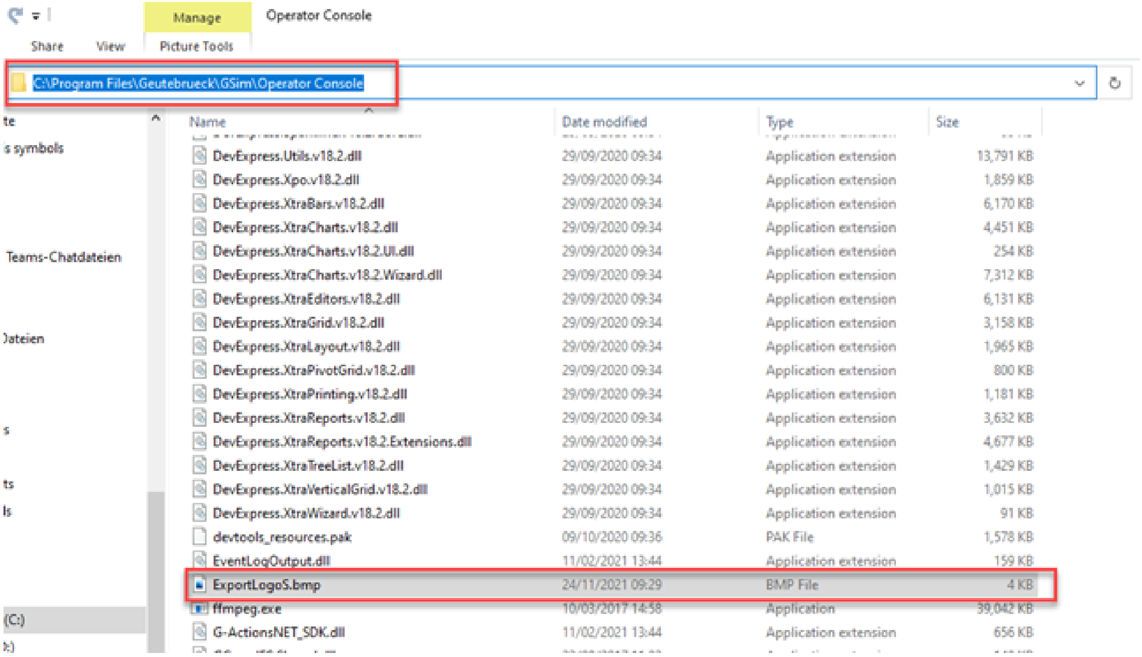
Two example images:

ExportLogoS.bmp	
ExportLogoL.bmp	

In OpCon it is only possible to export a mp4 video with image watermark.

How to Use Image Watermark

1. Copy the image watermark picture to `C:\Program Files\Geutebrueck-\GSim\Operator Console`.



C:\Program Files\Geutebrueck\GSim\Operator Console

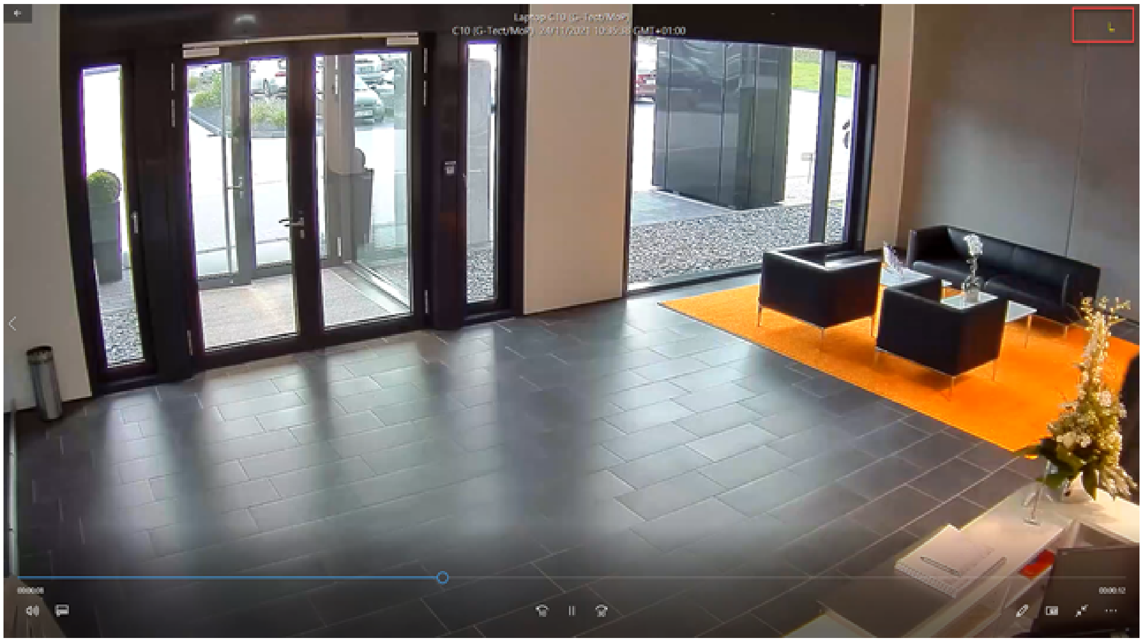
Name	Date modified	Type	Size
DevExpress.Utils.v18.2.dll	29/09/2020 09:34	Application extension	13,791 KB
DevExpress.Xpo.v18.2.dll	29/09/2020 09:34	Application extension	1,859 KB
DevExpress.XtraBars.v18.2.dll	29/09/2020 09:34	Application extension	6,170 KB
DevExpress.XtraCharts.v18.2.dll	29/09/2020 09:34	Application extension	4,451 KB
DevExpress.XtraCharts.v18.2.UI.dll	29/09/2020 09:34	Application extension	254 KB
DevExpress.XtraCharts.v18.2.Wizard.dll	29/09/2020 09:34	Application extension	7,312 KB
DevExpress.XtraEditors.v18.2.dll	29/09/2020 09:34	Application extension	6,131 KB
DevExpress.XtraGrid.v18.2.dll	29/09/2020 09:34	Application extension	3,158 KB
DevExpress.XtraLayout.v18.2.dll	29/09/2020 09:34	Application extension	1,965 KB
DevExpress.XtraPivotGrid.v18.2.dll	29/09/2020 09:34	Application extension	800 KB
DevExpress.XtraPrinting.v18.2.dll	29/09/2020 09:34	Application extension	1,181 KB
DevExpress.XtraReports.v18.2.dll	29/09/2020 09:34	Application extension	3,632 KB
DevExpress.XtraReports.v18.2.Extensions.dll	29/09/2020 09:34	Application extension	4,677 KB
DevExpress.XtraTreeList.v18.2.dll	29/09/2020 09:34	Application extension	1,429 KB
DevExpress.XtraVerticalGrid.v18.2.dll	29/09/2020 09:34	Application extension	1,015 KB
DevExpress.XtraWizard.v18.2.dll	29/09/2020 09:34	Application extension	91 KB
devtools_resources.pak	09/10/2020 09:36	PAK File	1,578 KB
EventLogOutput.dll	11/02/2021 13:44	Application extension	159 KB
ExportLogoS.bmp	24/11/2021 09:29	BMP File	4 KB
ffmpeg.exe	10/03/2017 14:58	Application	39,042 KB
G-ActionsNET_SDK.dll	11/02/2021 13:44	Application extension	656 KB

2. Save this file with the name **ExportLogoS.bmp** or **ExportLogoL.bmp**.

3. A restart of OpCon is required.

   → If you now do an mp4 export, it should be done automatically.

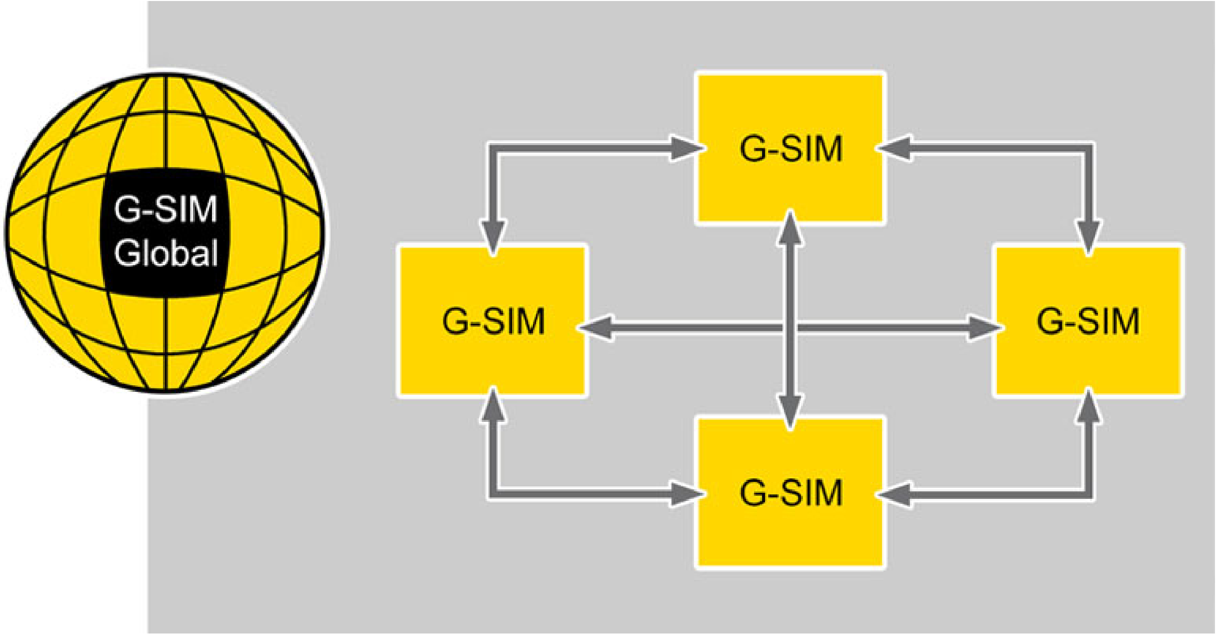
4. Export a mp4 for test.



G-SIM Global

Independent and yet globally networked – this is what distinguishes G-SIM Global.

G-SIM Global is the further development of G-SIM, Geutebrück's Security Information Management – with the difference that it transcends spatial boundaries. With G-SIM, complex video systems and processes can be easily managed and operated. It bundles and overviews all information and data of the Geutebrück world and all connected third-party systems.



The G-SIM Global option gives access to many functions and resources of the connected G-SIM systems at different locations. This includes access to cameras, site plans, alarm processing, process data as well as parameterization of user rights and much more. You gain full control over the connected G-SIM network from any of the connected locations.

- Global management access from any connected G-SIM system to the other G-SIM systems at different locations.
- Alarms can be processed from any G-SIM location.
- Global control is possible by a cross-location search and management of process data.
- Mutual synchronization of G-SIM setups.

- Reduces the cost of operating security centres as they can be concentrated on a small number of locations.
- Increases the availability of G-SIM services as the failure of a G-SIM system at one location is replaced by the synchronized G-SIM system at another location.
- Central alarm and report management.
- Central user and rights management

G-SIM Global is developed on the base of G-SIM 9 and currently allows the connection of up to 30 locations.

Global Structure

Global Servers

G-SIM servers running the Global version of G-SIM will function on their own in the same way as a normal G-SIM server does, but additionally have the ability to synchronize data between them and query data from each other. A Global Server might for example see all the Cameras, G-SIM installations etc. from another Global Server and give a user the ability to view cameras from another server. Data like Alarms and Process Data might be queried from another server or from the whole Global Network. These servers will typically serve different remote G-SIM installations, e.g. different organizations in a city or different cities in an area etc. Data flow can be set up to allow e.g. a scenario where you have organizations in a city (each with its own server only accessing its own data and cameras), then a city level from where all the organizations may be monitored, then a region monitoring cities, up to a national level.

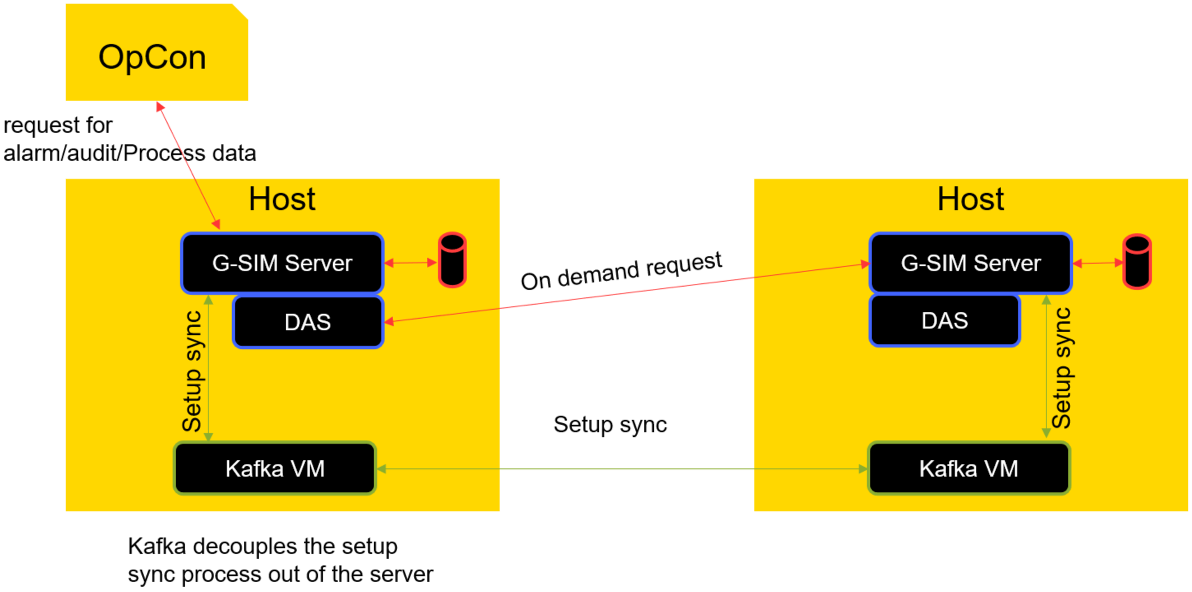
Cluster Servers

A “Global Server” might be a cluster (consisting of two servers: a primary and a failover server). Cluster servers are not unique to G-SIM Global. A cluster operates as a primary/fail-over pair and all data is identical and real-time synced between them. The user will not realize a difference when logged in on the primary or the failover server of a cluster. However the user will experience a difference when logged in on a different Global Server than his usual/preferred server.

Using G-SIM Global with Kafka

These are the various possibilities for using G-SIM Global with Kafka.

G-SIM Structure with Two Global Sites



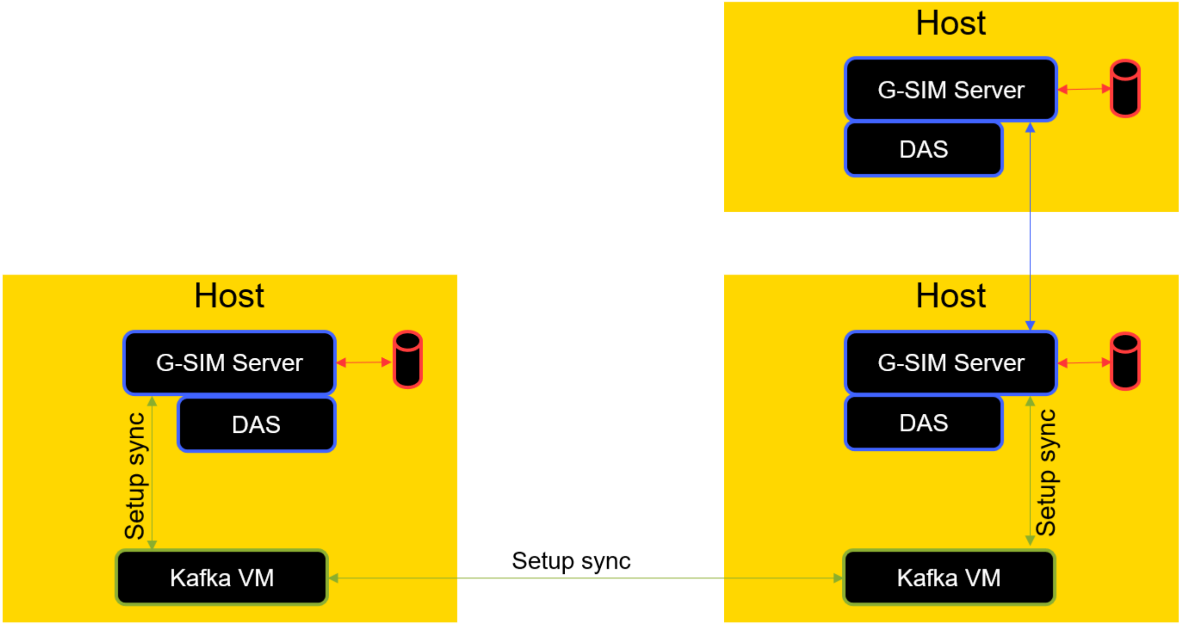
As you can see in the picture, the green colours show the synchronization of the G-SIM setup with the Kafka virtual machines. The G-SIM server sends its setup to the Kafka VM. The Kafka VM translates this into its own Kafka format. On the other side, the Kafka VM receives the data and converts it back into a G-SIM format. The Kafka VM sends the setup to the G-SIM server. The synchronization of the G-SIM setup works in both directions.

The Global server wait between the synchronisations, the default value is 360 minutes. This can be set in the Management Console (default = 360; minimum = 10).

In red you can see how the requests for alarm, audit and process data work. All data is stored in the local SQL database of each G-SIM Global server. When the Operator Console user is looking for an alarm from the second G-SIM Global server, the Data Access Service (DAS) establishes a connection to the second G-SIM Global server. The second G-SIM Global server searches in its SQL database and sends the result back to the first G-SIM Global. The user then sees the alarm result in the Operator Console.

Data Access Service (DAS) communicates with the external G-SIM server.

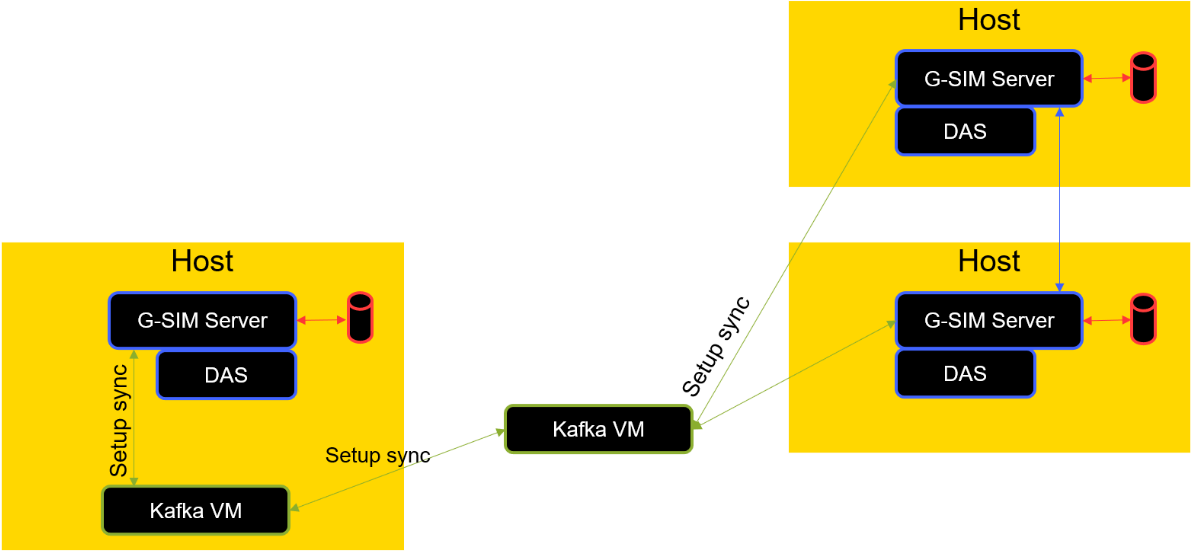
G-SIM Structure with Two Global Sites and One G-SIM Cluster



Kafka decouples the setup sync process out of the server

This example shows that there is a further G-SIM cluster server in addition to the two G-SIM Global servers. The G-SIM cluster server synchronizes the G-SIM setup with the primary global server without a Kafka VM (blue arrow).

G-SIM Structure with Two Global Sites, One G-SIM Cluster and Synchronization with Kafka



Kafka decouples the setup
sync process out of the server

This example shows that the G-SIM cluster server is synced by the Kafka VM.

Install Kafka

Virtual Machine for Kafka

IMPORTANT: The G-SIM Global Synchronization Service (GSS) uses the KAFKA messaging framework. This service is excluded in a virtual machine with a Linux operating system. For each G-SIM Global server a virtual machine must be installed on the host system. By default, the virtual machine gets the IP-Address from a DHCP server. The Cluster Server to be used needs one Kafka service for synchronization. The provided Kafka images are part of the setup files to simplify the setup of G-SIM global. It is possible to exchange the kafka service with your own kafka installation. To use Kafka with G-SIM Global it is necessary to connect via IP address to kafka. Please adapt your listeners settings accordingly.

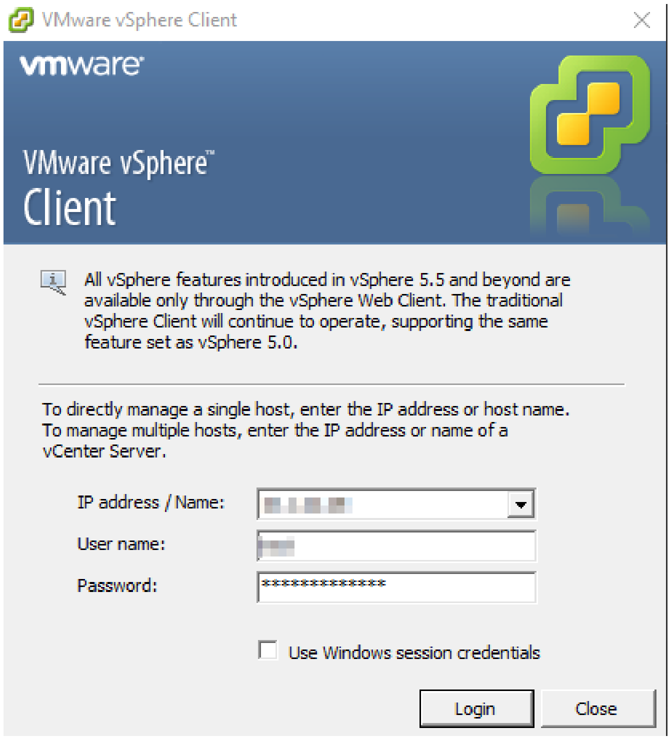
Download Kafka VHD

Contact the Geutebrück support for getting access to the Kafka service VHD download.

Please note that this virtual machine is only available in the OVA format. The OVA format is not supported by Microsoft Hyper-V, therefore Hyper-V cannot be used. Please use VmWare esx, Workstation or Player or Virtual Box from Oracle. The support for Hyper-V will be added later.

VMware Client

1. Start the program **VMware vSphere Client**.



All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

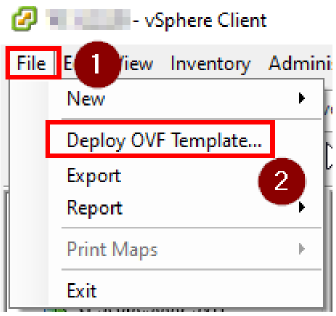
IP address / Name: [redacted]

User name: [redacted]

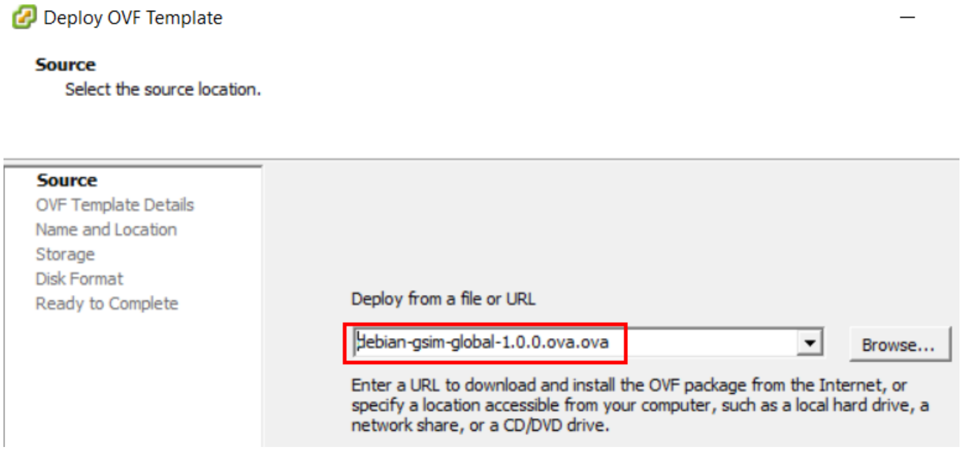
Password: **************

□ Use Windows session credentials

2. Open the **File** > **Deploy OVF Template** and load the Kafka service VHD.



3. Select the source location.



Deploy OVF Template

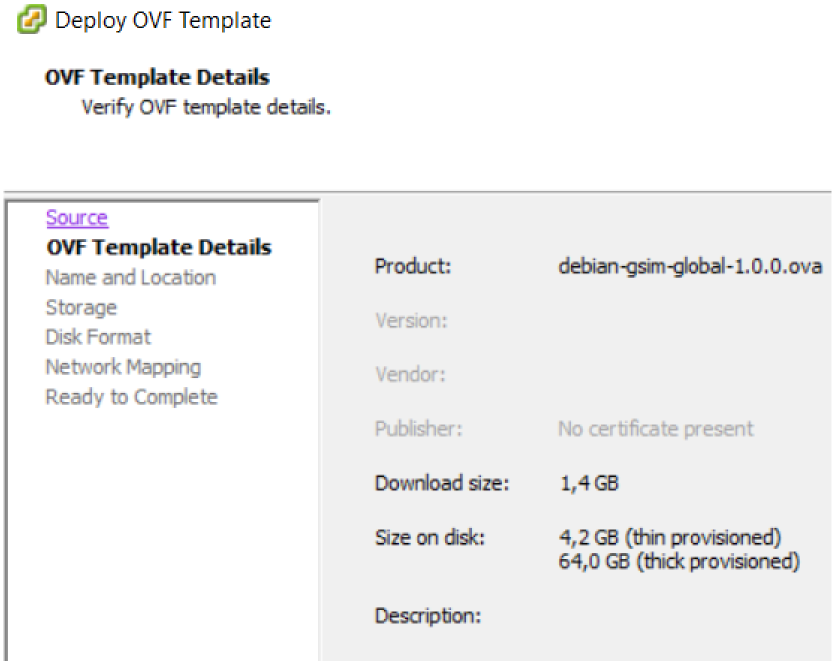
Source
Select the source location.

Deploy from a file or URL

debian-gsim-global-1.0.0.ova.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

4. Verify OVF template details.

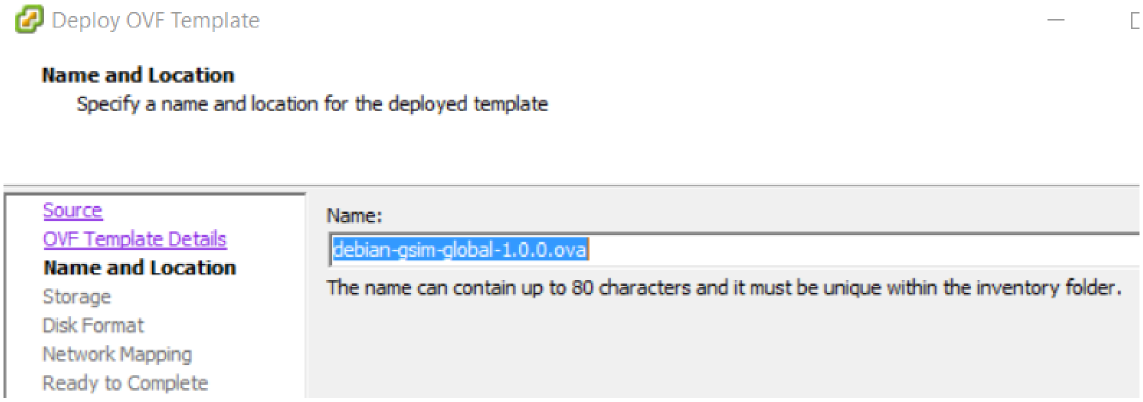


Deploy OVF Template

OVF Template Details
Verify OVF template details.

Product:	debian-gsim-global-1.0.0.ova
Version:	
Vendor:	
Publisher:	No certificate present
Download size:	1,4 GB
Size on disk:	4,2 GB (thin provisioned) 64,0 GB (thick provisioned)
Description:	

5. Specify a name and location for the deployed template.



Deploy OVF Template

Name and Location

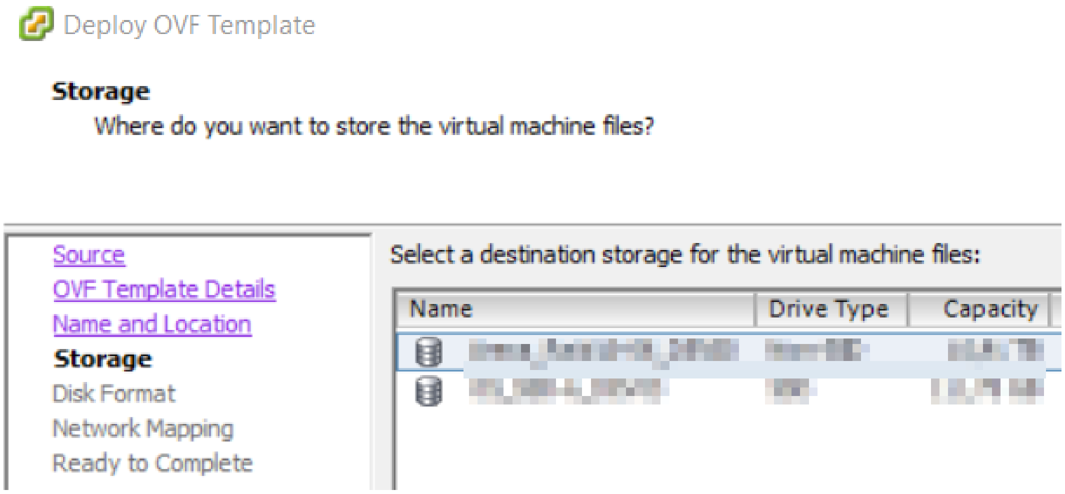
Specify a name and location for the deployed template

Name:

debian-gsim-global-1.0.0.ova

The name can contain up to 80 characters and it must be unique within the inventory folder.

6. Select a destination storage for the virtual machine files.



Deploy OVF Template

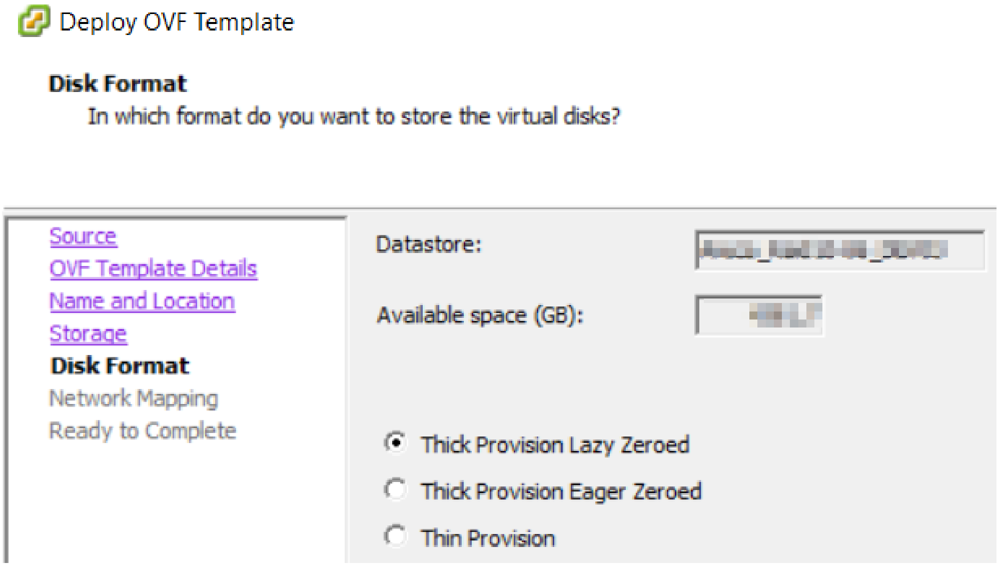
Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

7. Select a storage format for the virtual disks.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: [redacted]

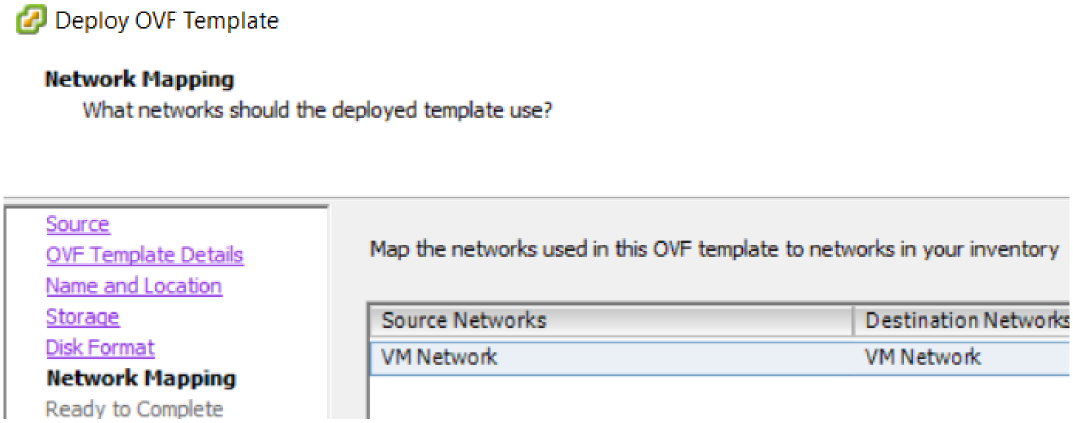
Available space (GB): [redacted]

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

8. Map he networks used in this OVF template to networks in your inventory.



Deploy OVF Template

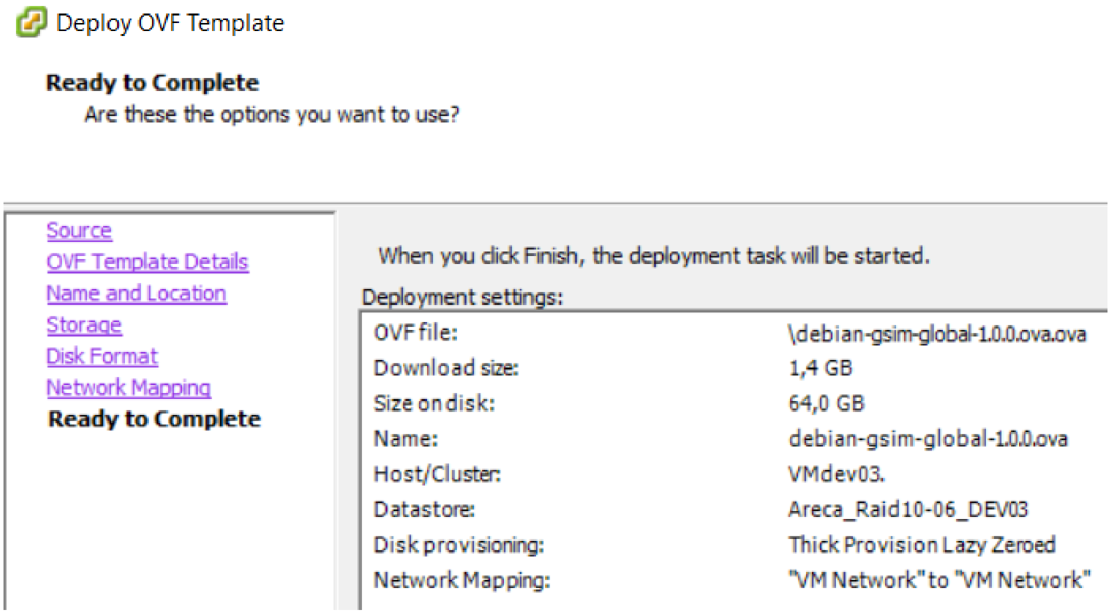
Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	VM Network

9. Verify the deployment settings. When you click **Finish**, the deployment task will be started.



Deploy OVF Template

Ready to Complete
Are these the options you want to use?

Source
OVF Template Details
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete

When you click Finish, the deployment task will be started.

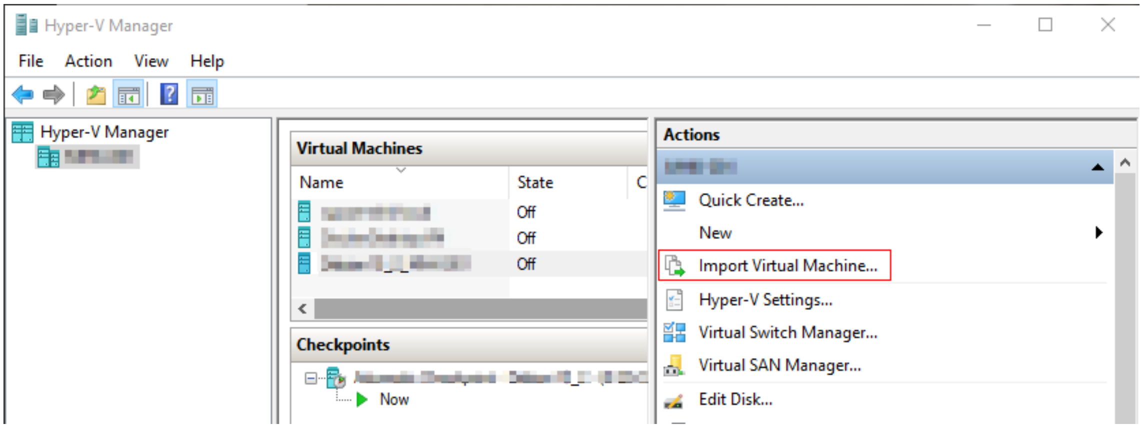
Deployment settings:

OVF file:	\debian-gsim-global-1.0.0.ova.ova
Download size:	1,4 GB
Size on disk:	64,0 GB
Name:	debian-gsim-global-1.0.0.ova
Host/Cluster:	VMdev03.
Datastore:	Areca_Raid10-06_DEV03
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"VM Network" to "VM Network"

Hyper-V Client

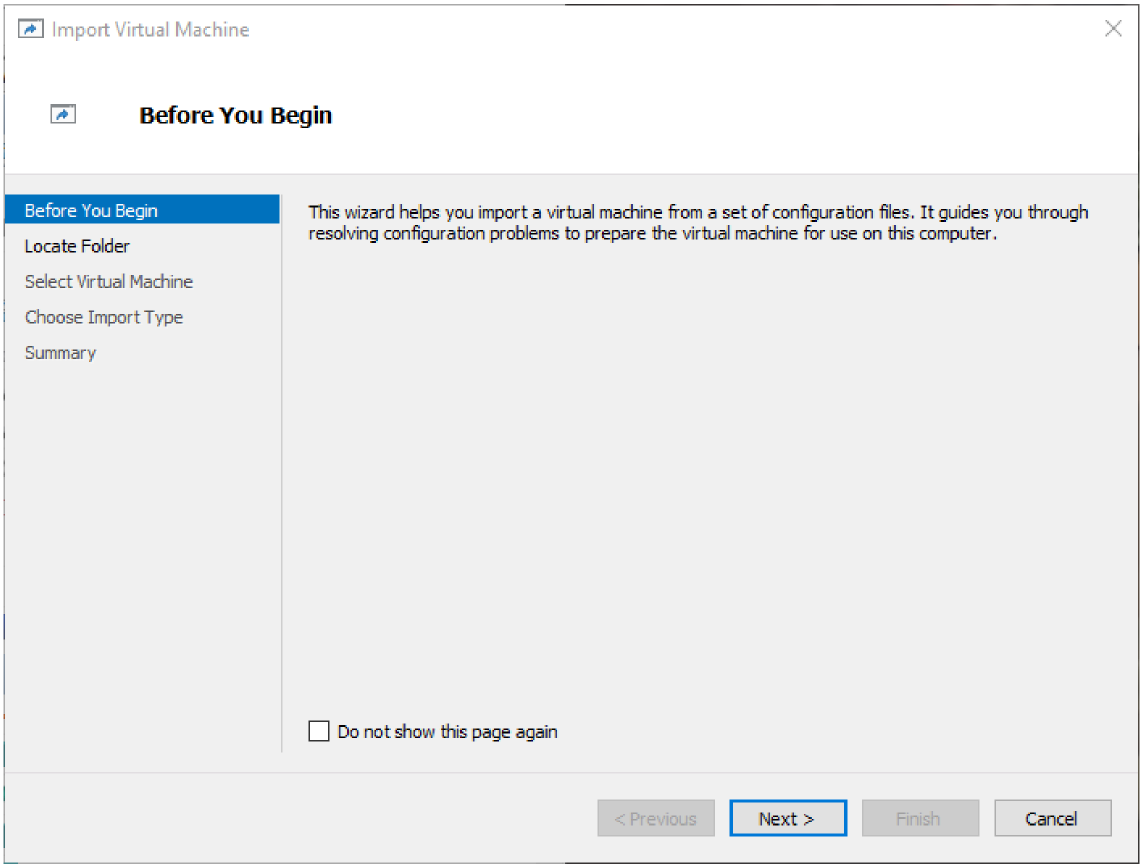
IMPORTANT: Make sure that your local Hyper-V environment is set up correctly.

1. Start the **Hyper-V Manager**.
2. Select **Import Virtual Machine...** from the **Actions** menu.



→ The dialog box **Import Virtual Machine** opens.

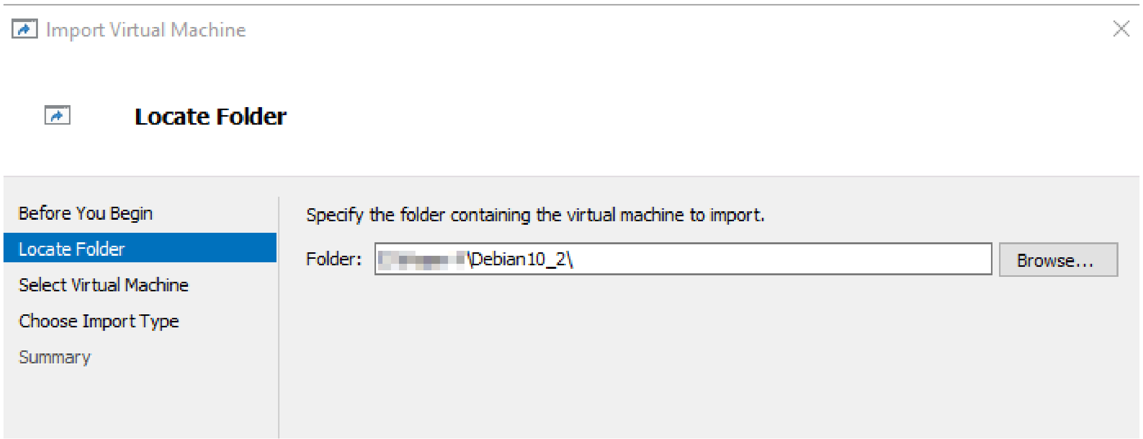
3. The Assistant guides you through the steps of the import procedure. Click the **Next** button.



This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

□ Do not show this page again

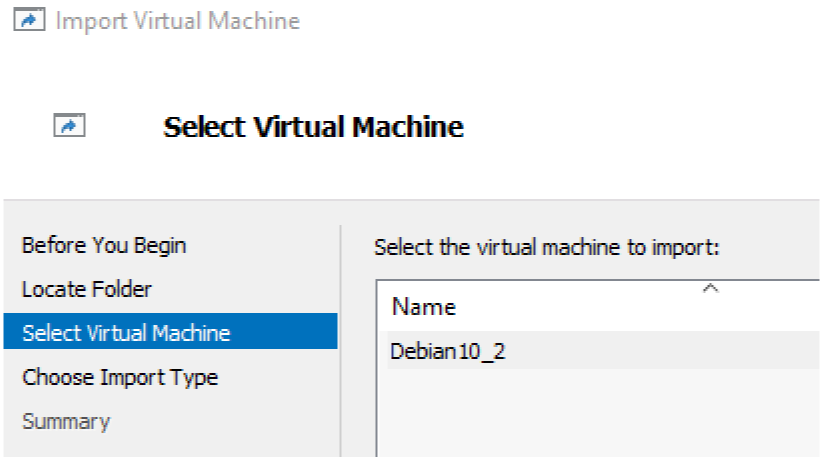
4. Browse to the location of your virtual machine on the disk and specify this folder that contains the virtual machine you want to import.



Specify the folder containing the virtual machine to import.

Folder: [redacted]\Debian10_2\

5. Select the virtual machine you want to import.



Import Virtual Machine

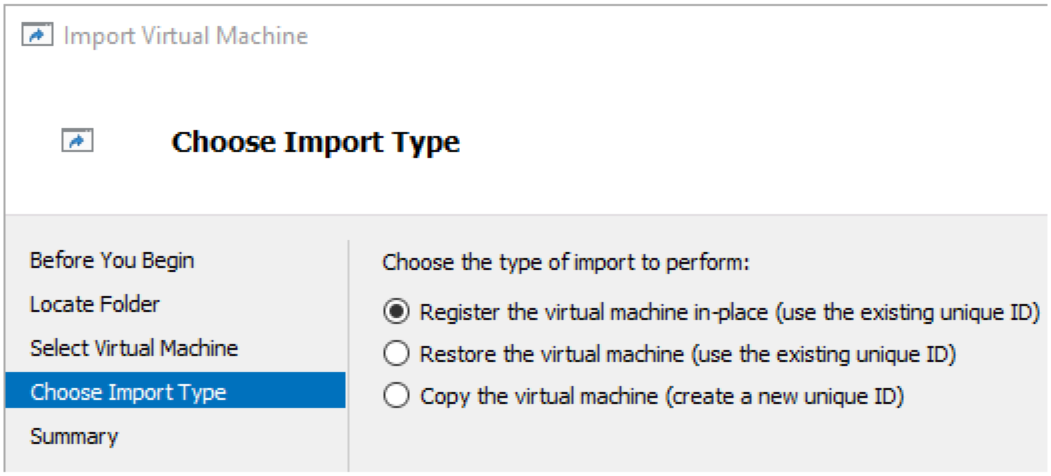
Select Virtual Machine

Before You Begin
Locate Folder
Select Virtual Machine
Choose Import Type
Summary

Select the virtual machine to import:

Name
Debian10_2

6. Choose the type of import to perform.



Import Virtual Machine

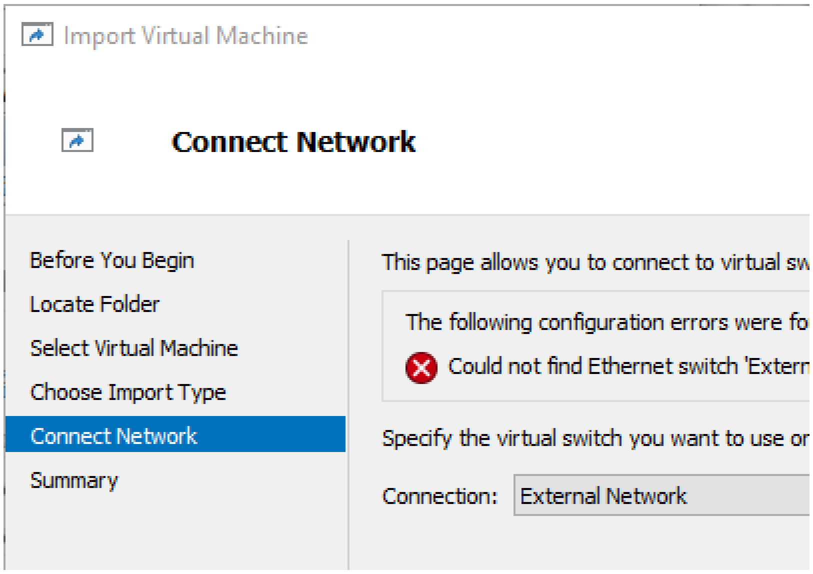
Choose Import Type

Before You Begin
Locate Folder
Select Virtual Machine
Choose Import Type
Summary

Choose the type of import to perform:

● Register the virtual machine in-place (use the existing unique ID)
○ Restore the virtual machine (use the existing unique ID)
○ Copy the virtual machine (create a new unique ID)

7. Specify the network connection.



Connect Network

This page allows you to connect to virtual sw

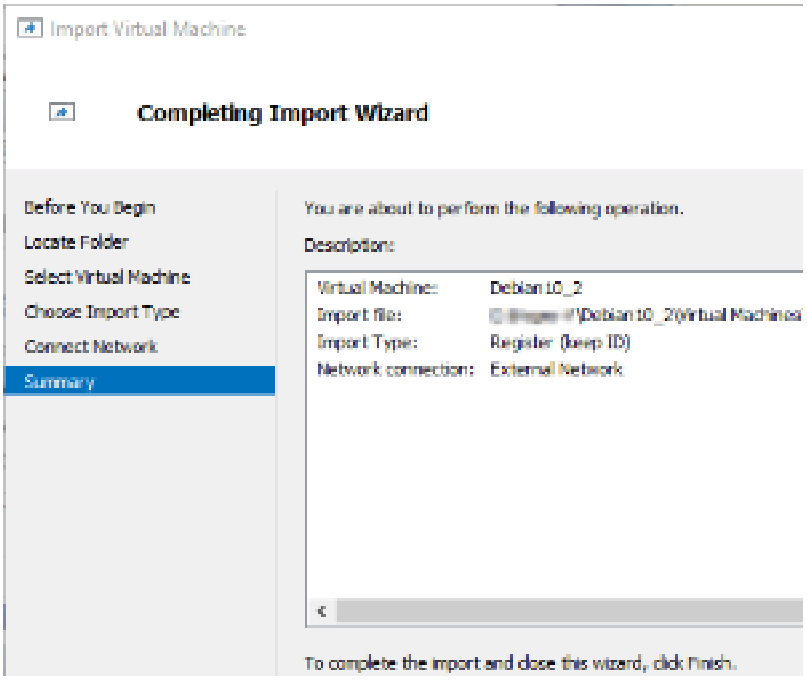
The following configuration errors were fo

Could not find Ethernet switch 'Extern

Specify the virtual switch you want to use or

Connection: External Network

8. Check the summary of your specified data. To complete the import and close the wizard, click the **Finish** button.



Completing Import Wizard

You are about to perform the following operation.

Description:

Virtual Machine: Debian 10_2

Import file: [redacted]\Debian 10_2\Virtual Machines\

Import Type: Register (keep ID)

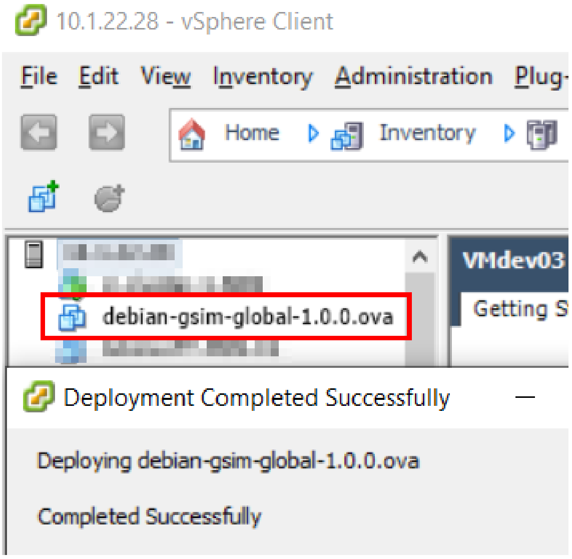
Network connection: External Network

To complete the import and close this wizard, click Finish.

Login Kafka VHD

This part is optional and is only needed for troubleshooting.

1. Start the VM machine.

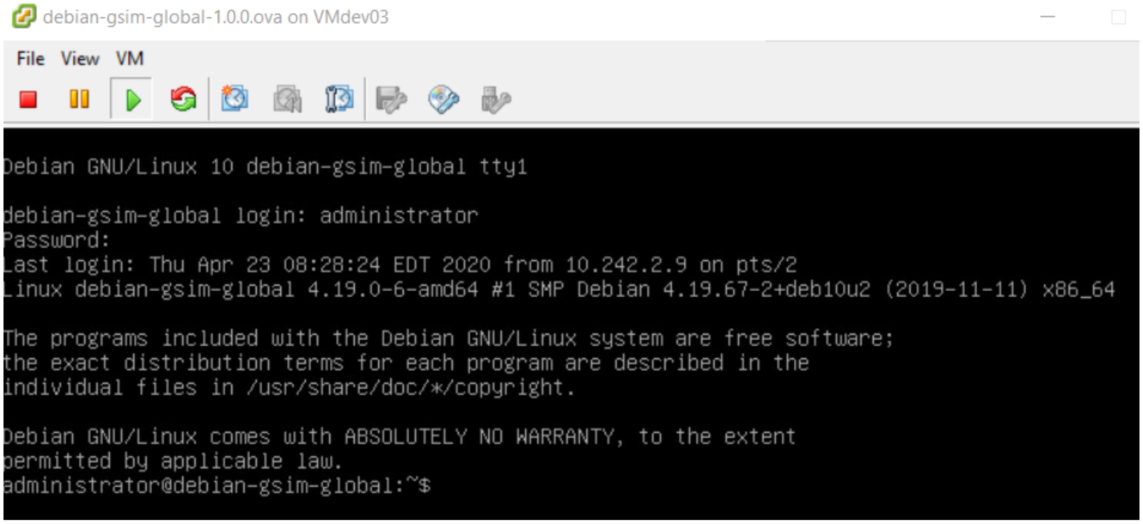

10.1.22.28 - vSphere Client
File Edit View Inventory Administration Plug-
Home
Inventory
[redacted]
[redacted]
debian-gsim-global-1.0.0.ova
[redacted]
VMdev03
Getting S

Deployment Completed Successfully

Deploying debian-gsim-global-1.0.0.ova

Completed Successfully

2. Log in with the login data:
   - **Login**: administrator
   - **Password**: gsimglobal

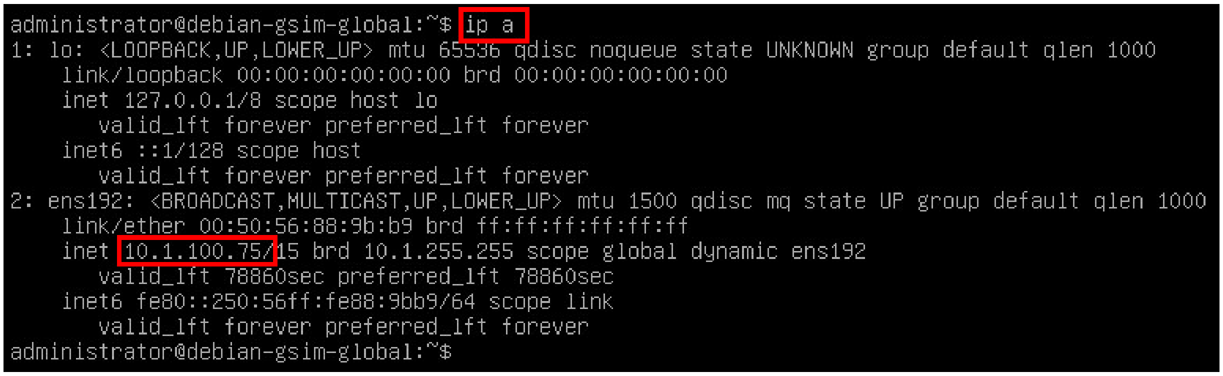


```
Debian GNU/Linux 10 debian-gsim-global tty1

debian-gsim-global login: administrator
Password:
Last login: Thu Apr 23 08:28:24 EDT 2020 from 10.242.2.9 on pts/2
Linux debian-gsim-global 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
administrator@debian-gsim-global:~$
```

Commands

Check the Kafka IP address and use the following command: **ip a**

For example: **10.1.100.75**

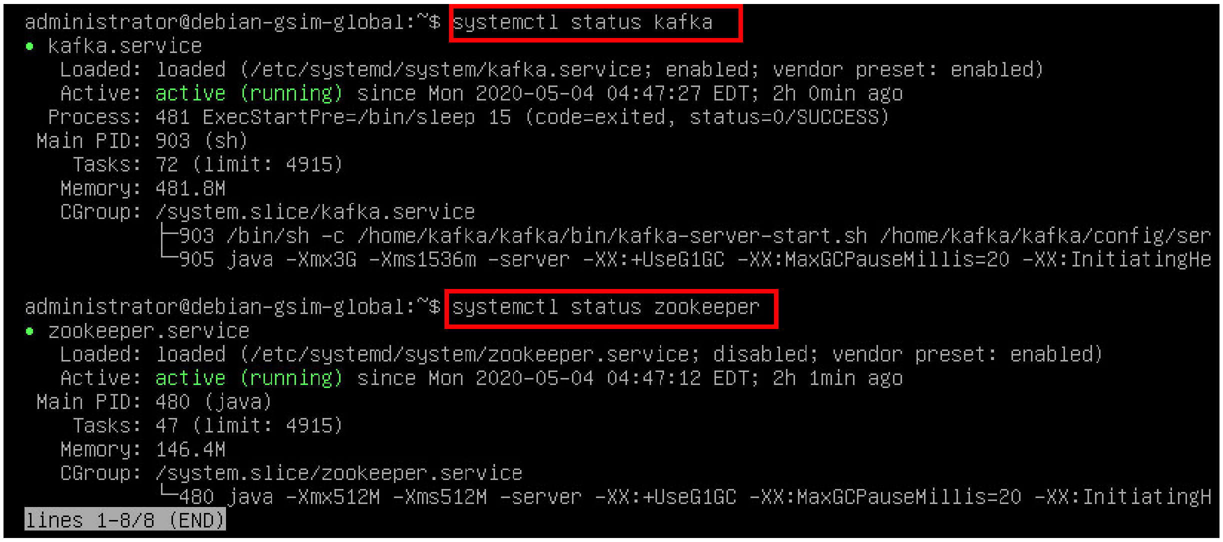


```
administrator@debian-gsim-global:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:88:9b:b9 brd ff:ff:ff:ff:ff:ff
    inet 10.1.100.75/15 brd 10.1.255.255 scope global dynamic ens192
       valid_lft 78860sec preferred_lft 78860sec
    inet6 fe80::250:56ff:fe88:9bb9/64 scope link
       valid_lft forever preferred_lft forever
administrator@debian-gsim-global:~$
```

The virtual Machine is configured to use DHCP.

Use the following commands to control the Kafka and zookeeper service: `systemctl status` **`<service>`**

- `systemctl status kafka`
- `systemctl status zookeeper`



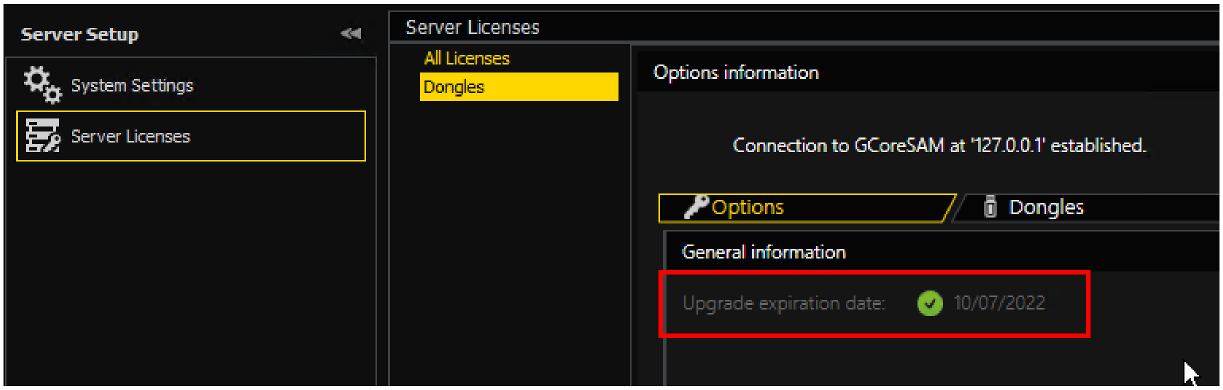
```
administrator@debian-gsim-global:~$ systemctl status kafka
● kafka.service
   Loaded: loaded (/etc/systemd/system/kafka.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-05-04 04:47:27 EDT; 2h 0min ago
  Process: 481 ExecStartPre=/bin/sleep 15 (code=exited, status=0/SUCCESS)
 Main PID: 903 (sh)
    Tasks: 72 (limit: 4915)
   Memory: 481.8M
   CGroup: /system.slice/kafka.service
           ├─903 /bin/sh -c /home/kafka/kafka/bin/kafka-server-start.sh /home/kafka/kafka/config/ser
           └─905 java -Xmx3G -Xms1536m -server -XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingHe

administrator@debian-gsim-global:~$ systemctl status zookeeper
● zookeeper.service
   Loaded: loaded (/etc/systemd/system/zookeeper.service; disabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-05-04 04:47:12 EDT; 2h 1min ago
 Main PID: 480 (java)
    Tasks: 47 (limit: 4915)
   Memory: 146.4M
   CGroup: /system.slice/zookeeper.service
           └─480 java -Xmx512M -Xms512M -server -XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingH
lines 1-8/8 (END)
```

Install and Upgrade Global

Install the Update Test from Release 7.10.1 (old Enterprise version) to the current Global version.

Upgrade License

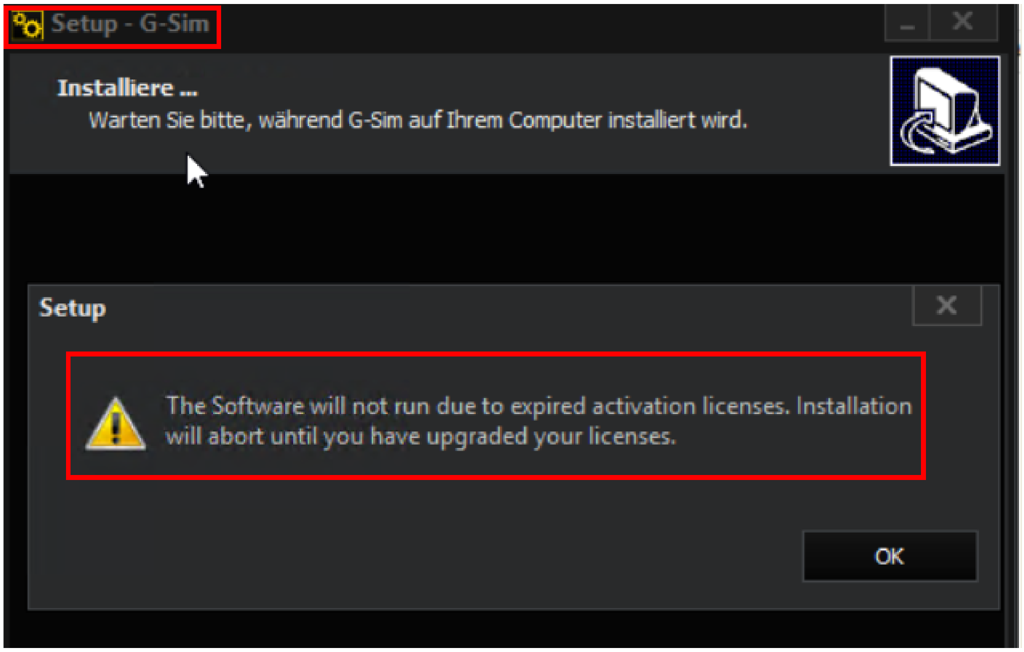
Check the upgrade license in the Management Console **Server Licenses** and the **Upgrade expiration date**.



Connection to GCoreSAM at '127.0.0.1' established.

Upgrade expiration date: ✓ 10/07/2022

If the upgrade licence is not valid, the **Setup - G-SIM** software will be stopped.



Installiere ...

Warten Sie bitte, während G-Sim auf Ihrem Computer installiert wird.

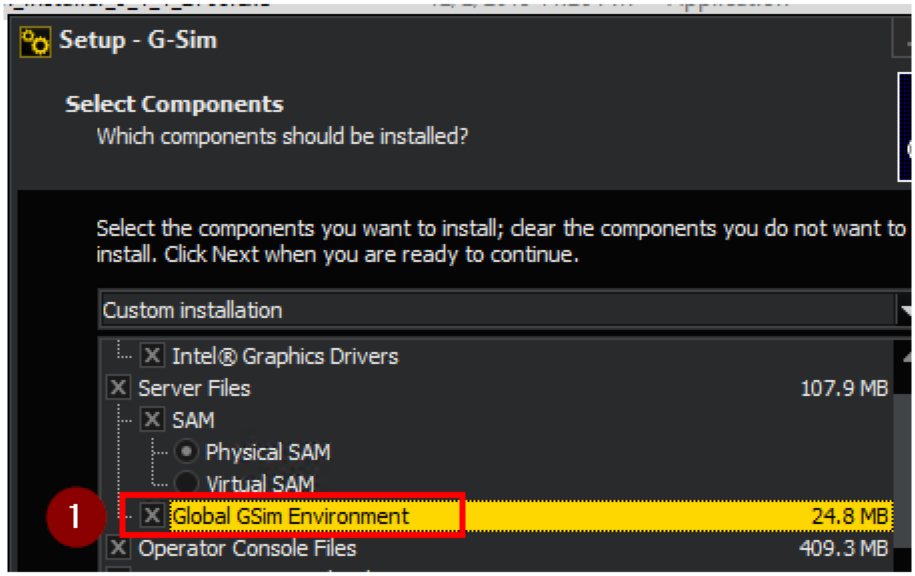
The Software will not run due to expired activation licenses. Installation will abort until you have upgraded your licenses.

Install DotNet Framework 4.7.2 (or higher)

The **Setup - G-SIM** software will be stopped if the .Net Framework 4.7.2 (or higher) is not installed.

Installation G-SIM Software

In the dialog **Select Components** of the G-SIM Setup, select the file **Global GSIM Environment** under **Server Files**.



Setup - G-Sim

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom installation

- ☒ Intel® Graphics Drivers
- ☒ Server Files 107.9 MB
  - ☒ SAM
    - ● Physical SAM
    - ○ Virtual SAM
  - ☒ Global GSim Environment 24.8 MB
- ☒ Operator Console Files 409.3 MB

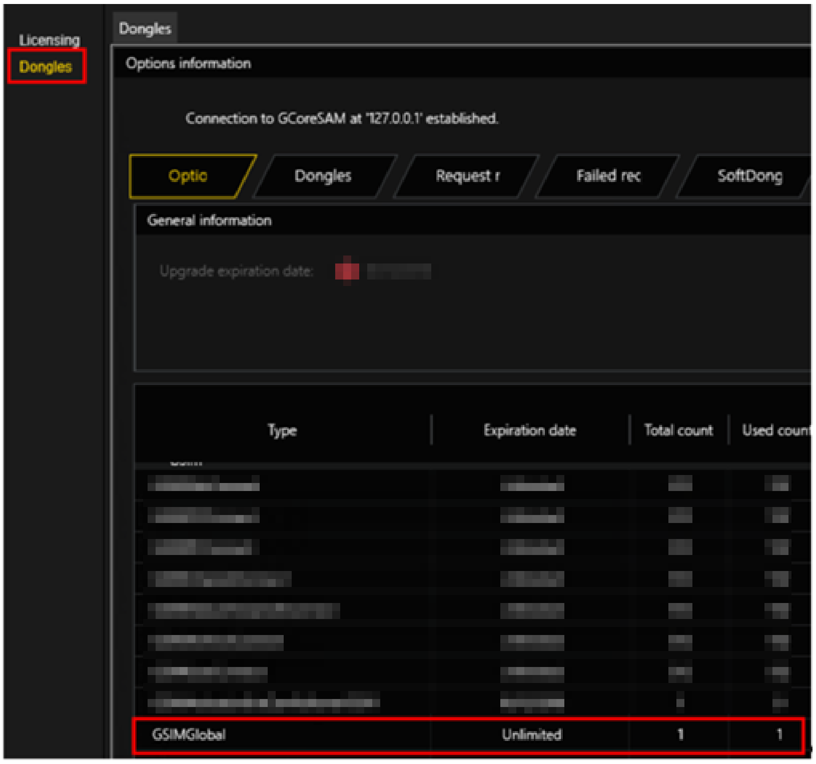
→ The installation of the G-SIM software starts.

Global Setup

IMPORTANT: Before the initial system setup, please ensure that all previously installed services are running properly on the respective servers. Especially the Kafka service is essential for correct behavior and synchronization during the setup process.

Global Option

Start the Management Console and verify the **GSIMGlobal** option. You will find this option under the **Options information** of the tab **Dongles**.



Connection to GCoreSAM at '127.0.0.1' established.

Upgrade expiration date: [redacted]

Type	Expiration date	Total count	Used count
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
GSIMGlobal	Unlimited	1	1

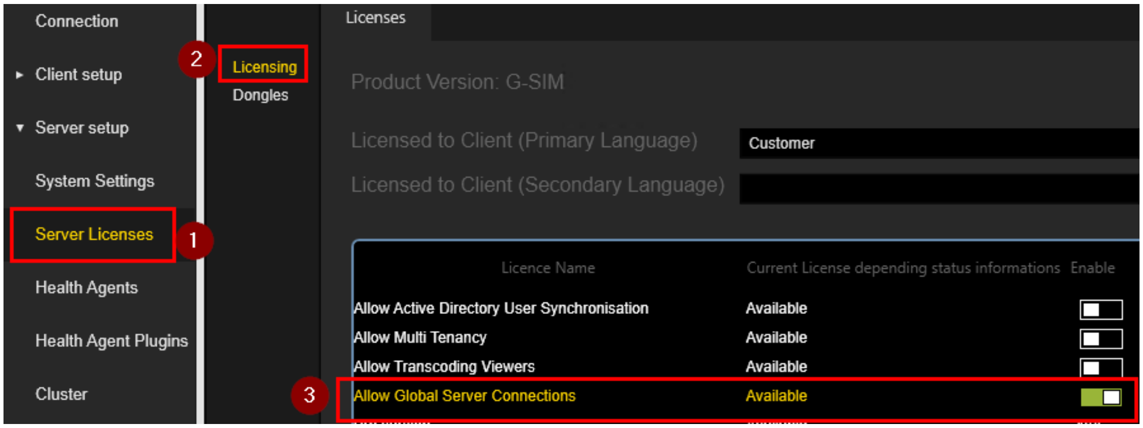
Server Licenses

Enable the license name **Allow Global Server Connections**.

To enable the license name, do the following:

1. Start the Management Console.
2. Open the **Server Setup** view and select the **Server Licenses** view (1) from the drop-down menu items.
3. Select **Licensing** (2).

4. Enable the license name **Allow Global Server Connections** (3).



Product Version: G-SIM

Licensed to Client (Primary Language): Customer

Licensed to Client (Secondary Language):

Licence Name	Current License depending status informations	Enable
Allow Active Directory User Synchronisation	Available	☐
Allow Multi Tenancy	Available	☐
Allow Transcoding Viewers	Available	☐
Allow Global Server Connections	Available	☑

Global Server Sync

The Global Server waits between the synchronizations, the default value is 360 minutes. This can be set in the Management Console (default = 360; minimum = 10).

To set the **Global Server Sync Minutes**, do the following:

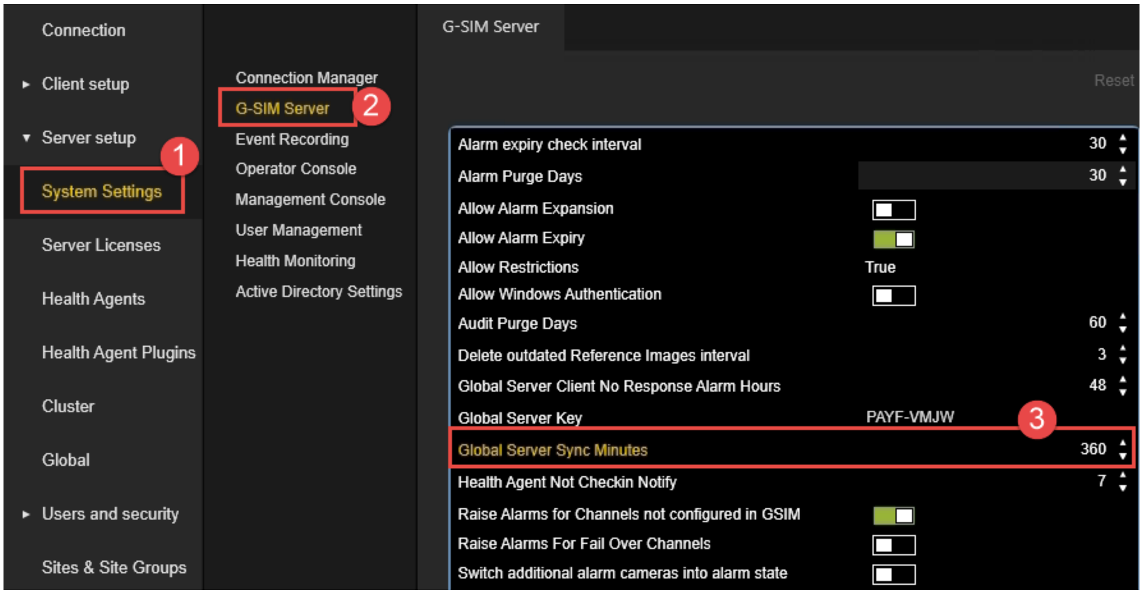
1. Start the Management Console.

2. Open the **Server Setup** view and select the **System Settings** view (1) from the drop-down menu items.

3. Select **G-SIM Server** (2).

4. Select the setting option **Global Server Sync Minutes** (3) and set the

required value.



Alarm expiry check interval	30
Alarm Purge Days	30
Allow Alarm Expansion	☐
Allow Alarm Expiry	☑
Allow Restrictions	True
Allow Windows Authentication	☐
Audit Purge Days	60
Delete outdated Reference Images interval	3
Global Server Client No Response Alarm Hours	48
Global Server Key	PAYF-VMJW
Global Server Sync Minutes	360
Health Agent Not Checkin Notify	7
Raise Alarms for Channels not configured in GSIM	☑
Raise Alarms For Fail Over Channels	☐
Switch additional alarm cameras into alarm state	☐

Global Server Key

Start the Management Console and add the **Global Server Key** from each G-SIM Global Server to the filed **Server Authentication**.

The same setting must be made for all G-SIM Global Master, but not for the G-SIM Cluster!

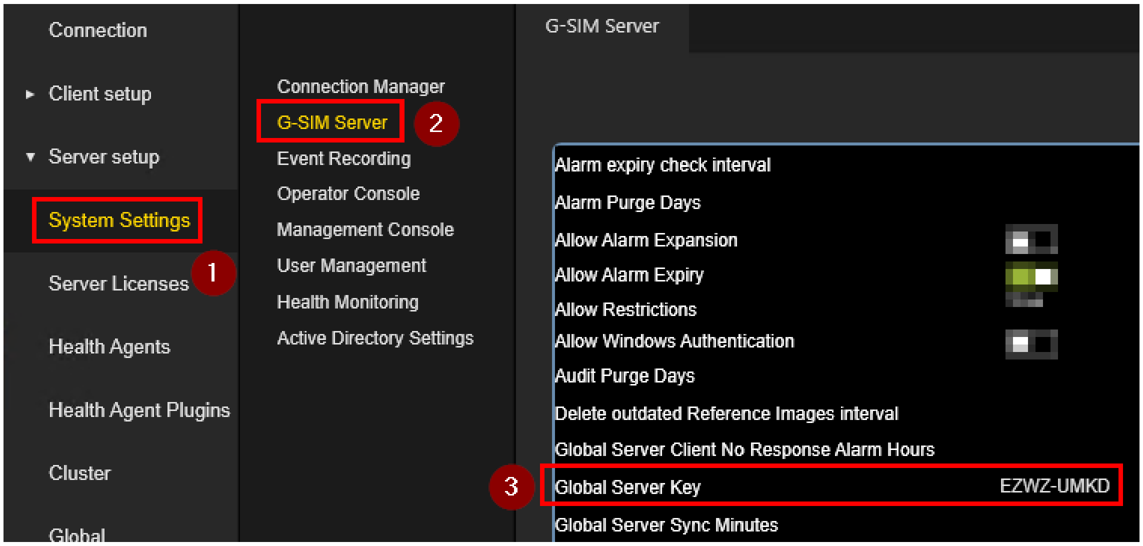
Follow the steps below:

Verification of Local Value Key

Verify the local value key of the Global Server:

1. Open the **Server Setup** view and select the **System Settings** view (1) from the drop-down menu items.
2. Select **G-SIM Server** (2).

3. Verify the local value key in the field **Global Server Key** (3).



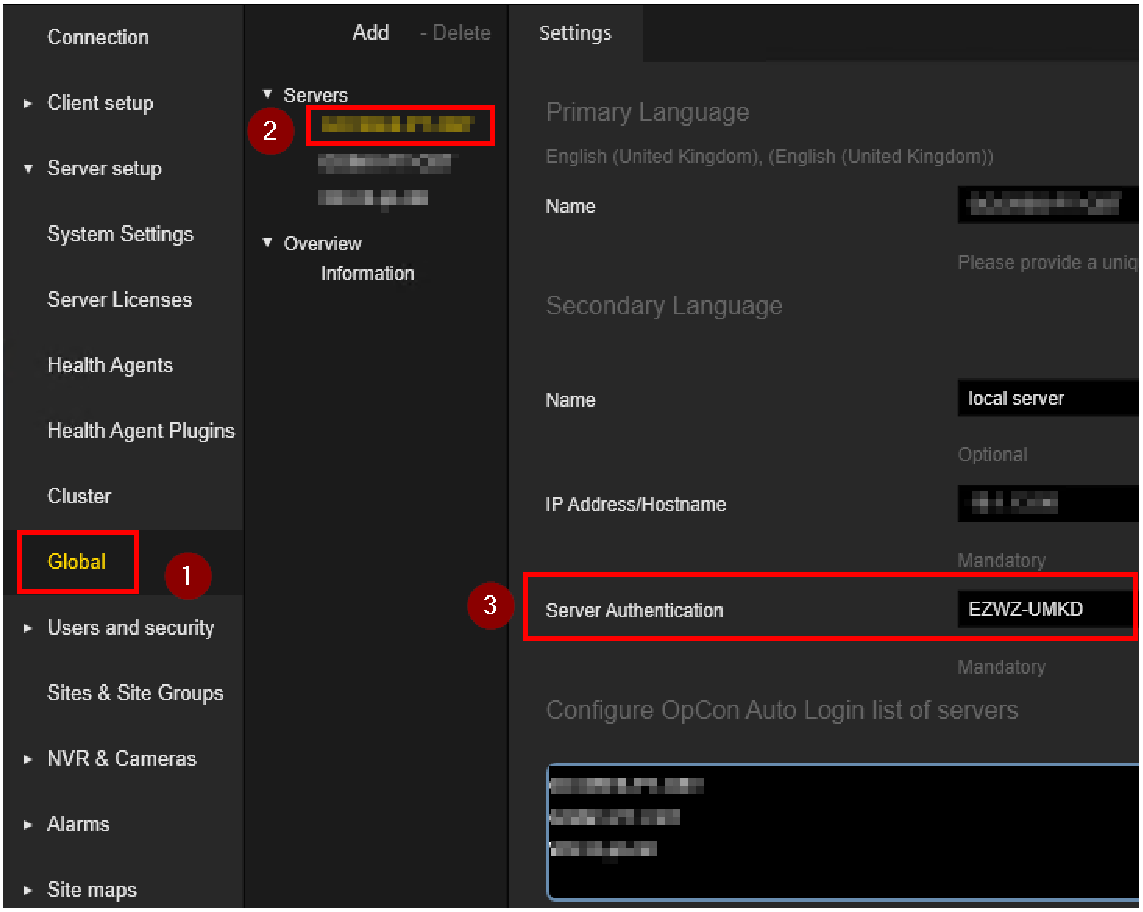
Alarm expiry check interval
Alarm Purge Days
Allow Alarm Expansion
Allow Alarm Expiry
Allow Restrictions
Allow Windows Authentication
Audit Purge Days
Delete outdated Reference Images interval
Global Server Client No Response Alarm Hours
Global Server Key EZWZ-UMKD
Global Server Sync Minutes

Verify the local value key in the field **Server Authentication** in the Global Server settings:

1. Open the **Server Setup** view and select the **Global** view (1) from the drop-down menu items.

2. Select the corresponding server (2).

3. Verify the local value key in the **Server Authentication** field (3).



Primary Language

English (United Kingdom), (English (United Kingdom))

Name [redacted]

Please provide a uniq

Secondary Language

Name local server

Optional

IP Address/Hostname [redacted]

Mandatory

Server Authentication EZWZ-UMKD

Mandatory

Configure OpCon Auto Login list of servers

[redacted]

Add Remote Global Server

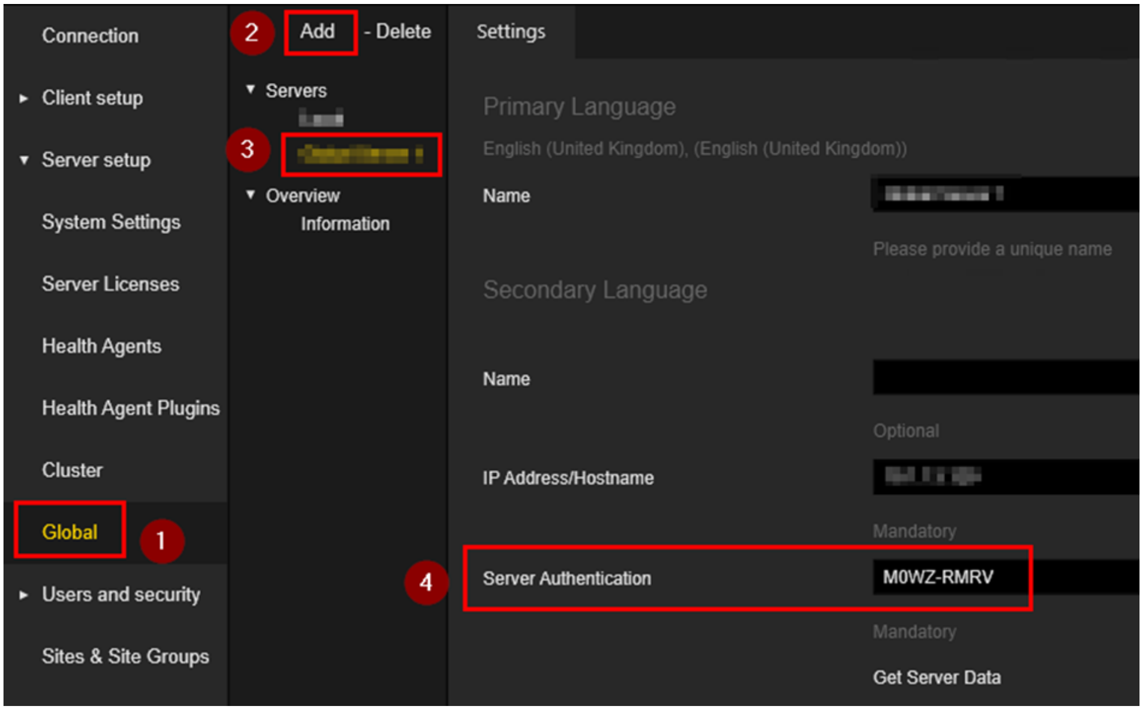
Add the Remote Global Servers and copy the Remote Global Server Key in the **Server Authentication** field:

1. Open the **Server Setup** view and select the **Global** view (1) from the drop-down menu items.

2. Click the **Add** button (2).

3. Add the Remote Global Server (3).

4. Copy the Remote Global Server Key in the **Server Authentication** field (4).



[redacted]

[redacted]

Primary Language

English (United Kingdom), (English (United Kingdom))

Name: [redacted]

Please provide a unique name

Secondary Language

Name:

Optional

IP Address/Hostname: [redacted]

Mandatory

Server Authentication: M0WZ-RMRV

Mandatory

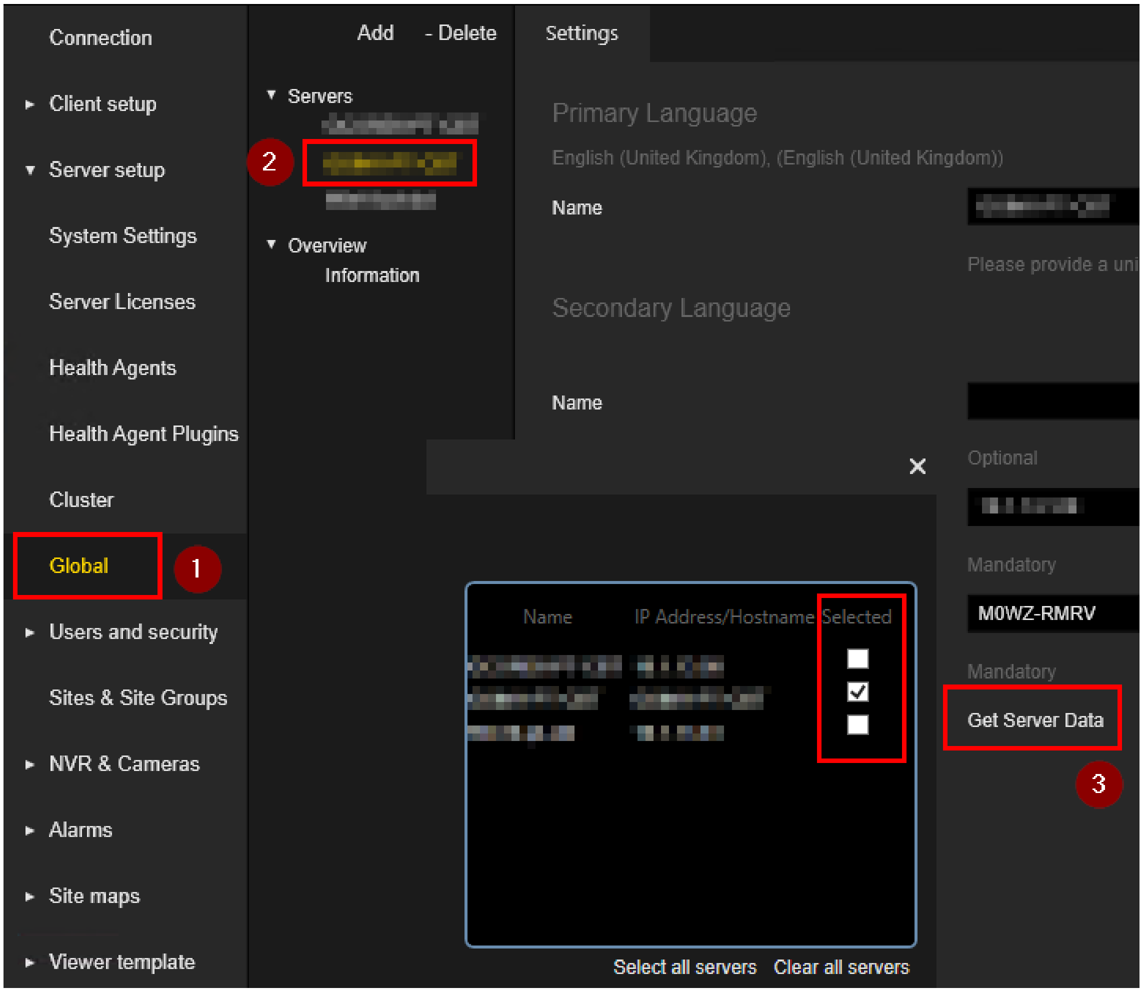
Get Server Data for Remote Global Servers

Select the **Get Server Data** button for the Remote Global server and select the corresponding servers:

1. Open the **Server Setup** view and select the **Global** view (1) from the drop-down menu items.

2. Select the Remote Global Server (2).

3. Click the **Get Server Data** button (3) and select the corresponding servers.



Primary Language

English (United Kingdom), (English (United Kingdom))

Name

Please provide a uni

Secondary Language

Name

Optional

Mandatory

M0WZ-RMRV

Mandatory

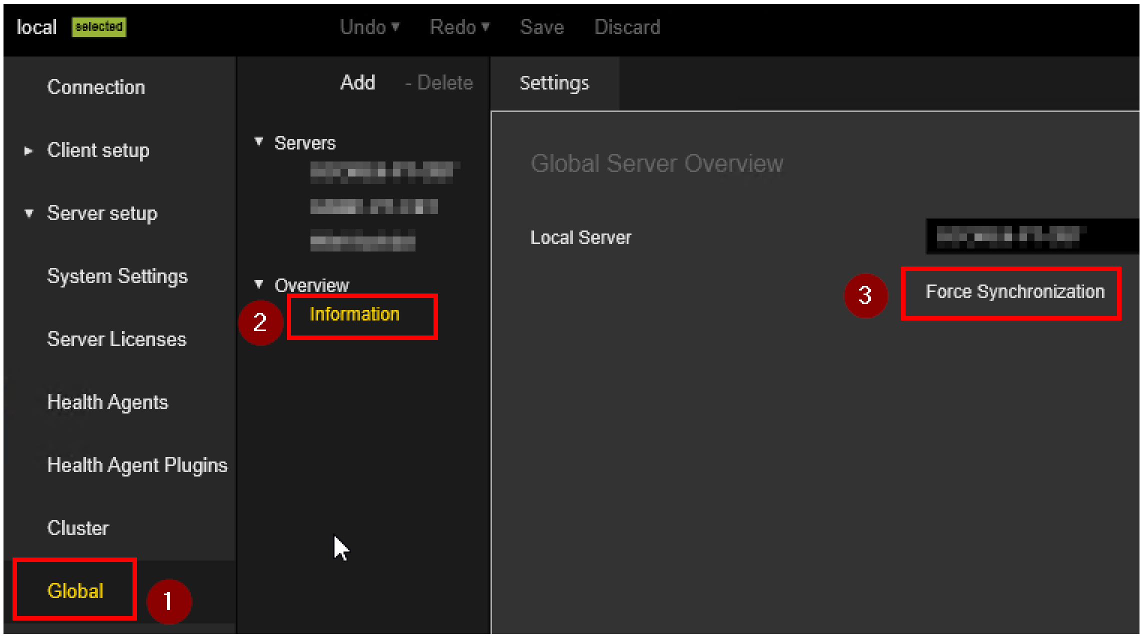
Name	IP Address/Hostname	Selected
		□
		☑
		□

Start Synchronization Immediately

The synchronization will be started immediately by selecting **Force Synchronization**:

1. Open the **Server Setup** view and select the **Global** view (1) from the drop-down menu items.
2. Select **Information** (2).
3. Click the **Force Synchronization** button (3).

→ The synchronization will be started immediately.



Mapping G-SIM Server with Kafka

Start the Windows PowerShell on each G-SIM Global Server for port mapping between Kafka service. This configuration was only done during setup to enable the firewall and allow communication.

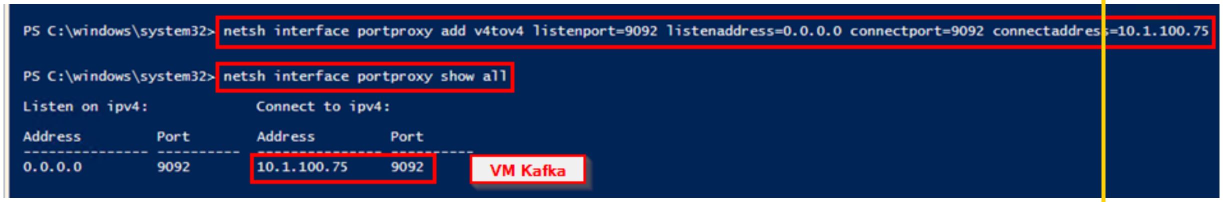
Default Port 9092

Use the following commands:

- `netsh interface portproxy add v4tov4 listenport=9092 listen-address=0.0.0.0 connectport=9092 connectaddress=`**`<<IP VM Kafka>>`**
- `netsh interface portproxy show all`

Example

```
netsh interface portproxy add v4tov4 listenport=9092 listen-address=0.0.0.0 connectport=9092 connectaddress=10.1.100.75
```

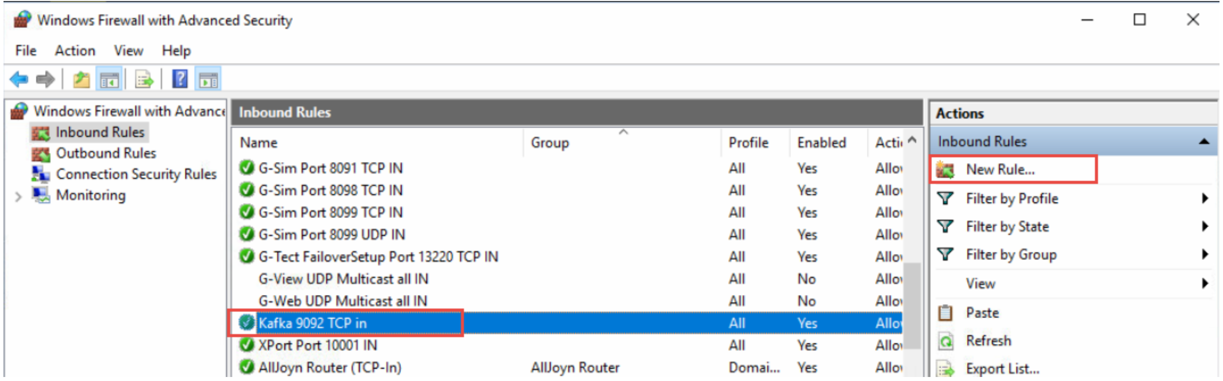


```
PS C:\windows\system32> netsh interface portproxy add v4tov4 listenport=9092 listenaddress=0.0.0.0 connectport=9092 connectaddress=10.1.100.75

PS C:\windows\system32> netsh interface portproxy show all

Listen on ipv4:             Connect to ipv4:

Address         Port        Address         Port
--------------- ----------  --------------- ----------
0.0.0.0         9092        10.1.100.75     9092
```

If you want to delete the interface, use the following command:

```
netsh interface portproxy delete v4tov4 listenport=9092 listen-address=0.0.0.0
```

Set up the firewall:



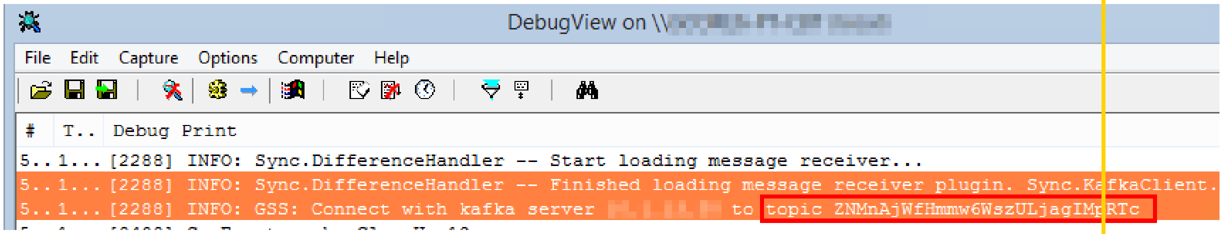
Inbound Rules

Name	Group	Profile	Enabled	Acti
G-Sim Port 8091 TCP IN		All	Yes	Allo
G-Sim Port 8098 TCP IN		All	Yes	Allo
G-Sim Port 8099 TCP IN		All	Yes	Allo
G-Sim Port 8099 UDP IN		All	Yes	Allo
G-Tect FailoverSetup Port 13220 TCP IN		All	Yes	Allo
G-View UDP Multicast all IN		All	No	Allo
G-Web UDP Multicast all IN		All	No	Allo
Kafka 9092 TCP in		All	Yes	Allo
XPort Port 10001 IN		All	Yes	Allo
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allo

Connect G-SIM with Kafka

Each G-SIM Global Server will be connected to a Kafka server. This output will be logged with the tool DeBugView.

Example topic: ZNMnAj.........



```
#   T..  Debug Print
5..1... [2288] INFO: Sync.DifferenceHandler -- Start loading message receiver...
5..1... [2288] INFO: Sync.DifferenceHandler -- Finished loading message receiver plugin. Sync.KafkaClient.
5..1... [2288] INFO: GSS: Connect with kafka server [redacted] to topic ZNMnAjWfHmmw6WszULjagIMpRTc
```

Auto Login

Auto Login is a G-SIM Global feature, which allows an Operator Console to log into another server if the preferred server is not available. A list of servers may be specified which will be tried to connect to in sequence.

⚠ **IMPORTANT:** In the case of a cluster primary/fail-over pair, the setup is identical on both servers. Also a setup must be exported from one server and imported on the other to ensure all resource IDs etc. to be identical.
When setting up a Global Server environment, it is very important to start with a clean database on every server. The identifiers for each type of resource must be unique and must be generated on the specific server to make them belong to the server. Therefore, you should never import one Global Server's setup on another server and just edit names, descriptions etc. IDs will not be regenerated, resulting in resources on different servers with identical IDs, which in turn will cause the sync process to fail.
When setting up several servers, the same Management Console on the same machine may be used to connect to all other servers and to do a remote setup. Never use the local 127.0.0.1 IP in any of the setups.

Synced Data of Global

9.1.2.x

- ConfigData.Users,
- ConfigData.UserGroups,
- ConfigData.Sites,
- ConfigData.SiteGroups,
- ConfigData.TemplateGroups,
- ConfigData.ViewerGroups,
- ConfigData.CameraGroups,
- ConfigData.ScreenDefinitions (TemplateDefinitions),

- ConfigData.CameraLookups,
- ConfigData.CameraPTZPresets,
- ConfigData.CameraRefFrames, SQL: T_CameraRefFrames,
- ConfigData.Cameras,
- ConfigData.CameraTypes,
- ConfigData.MapObjects,
- ConfigData.MapObjectStateSymbols,
- ConfigData.MapObjectTypes,
- ConfigData.MediaSources,
- ConfigData.MapButtonTemplates,
- ConfigData.HSTemplates, (HotspotTemplates),
- ConfigData.SiteMaps
- ConfigData.SystemUsers,
- ConfigData.SystemUserGroups,
- ConfigData.Restrictions,
- ConfigData.ProcessDataFilters,
- ConfigData.ProcessSearchLines,
- ConfigData.ProcessSearchLineSelectorItems,
- ConfigData.ScreenContent,
- ConfigData.GuardTours,
- ConfigData.GuardTourItems
- ConfigData.HealthEvents, (Alarm Template),
- ConfigData.AlarmResponseTypes,

- ConfigData.SystemComponents,
- ConfigData.SystemComponentCategories,
- ConfigData.OperatorConsoles,
- ConfigData.UnmannedConsoleGroups, (RemoteConsoles),
- ConfigData.ExportLocations,
- ConfigData.CustomButtons,
- ConfigData.CustomButtonSets,
- ConfigData.CustomButtonSetToCustomButtonRelations,
- ConfigData.CustomButtonSetToUserRelations,
- ConfigData.VideoEventTypes, (CutList Types)

Knowledge Base

Architecture

In this manual we look at the G-SIM architecture from quite a high vantage point. We thus do not go into anything in great depth, as the aim here is to give you an overview of how it all works.

It is extremely important that you be sure that your network infrastructure suppliers, installers, and maintainers understand the requirements on the network. What constitutes a good business network does not make for a good video network. The needs are different, and it really is a case of all or nothing: one cannot cut corners here.

We have seen video running on a 10Gbps network be useless because it was not configured properly. Therefore please see to it that the correct people get your installer's recommendations in good enough time to implement them.

With that out of the way, we can now proceed with an overview of G-SIM as a whole. That is then followed by more in-depth discussions of the client-server approach and the health agent/monitoring side of things, along with whatever else is necessary to understand how that works.

A Note on Terminology

It may be confusing at first, but the word "server" is used in two different contexts: at the hardware level it means a physical machine, usually expensive, on which the server software is running. This already shows the second meaning of "server": a program running on a machine. In our case, we have the G-SIM server which accepts connections from its various client machines, which is all explained in the chapter **The Client-Server Approach**.

High-Level Overview

Although G-SIM is a very easy program to use, it is nevertheless a large product when all its options are installed, and it deals with potentially complex issues. This chapter aims to strike a balance between glossing over topics and delving into them. As the readership is expected to be diverse, we have opted for an approach which tries not to gloss over anything, while not going into too much detail on any one topic.

The Client-Server Approach

A fundamental building block is the use of a client-server approach. The most basic version of this is where we have a single central machine running a server program, and one or more distributed machines running client programs. The clients connect to the server as required in order to have it do some function that only it can do. In this way each part of the infrastructure does only what it is best at, and we centralise those aspects which everyone needs.

Software Components

G-SIM is purely software, so it consists of program code. Its design revolves around the following 5 core components:

Component	Description
G-SIM Server	At the heart of the system is the G-SIM Server. In short it is the communication and control hub of the system. All system requests, commands and notifications are routed via the G-SIM Server. It is installed as a service on a Windows® -based operating system. Part of the server package is the Connection Manager, which handles all communication in a smooth and predictable manner.
Health Agents	Software components called Health Agents can be installed on various Windows®-based computers in G-SIM. These Health Agents gather health data from various system components which they report to the G-SIM Server. The Server in turn makes decisions on the supplied information, e.g. notifying users of the health state.
Operator Console	As far as the operators are concerned, the Operator Console is G-SIM. It is their only interaction with the system, even taking into account video walls or unmanned consoles.
Management Console	The Management Console is the program which is used to do the configuration and maintenance tasks associated with G-SIM. It stands alone, making it impossible for operators "accidentally" to gain access to administrative functions via a misconfigured Operator Console.
Updater Service	Configured via the Management Console, this is used to make sure that all the various parts of G-SIM are up-to-date, wherever they may run.

Architecture Components

The G-SIM Server architecture is extremely agile and streamlined. It removes the burden of the physical video connection and its control from the server by authorising and managing video connections via a component called the Connection Manager. Instead of routing video through the server, the Connection Manager authorises connection requests from operator workstations, allowing them to connect directly to the NVRs in question, placing no further burden on the server.

The G-SIM Server has at its core a TCP/IP application layer protocol communication mechanism. This simply means that all the software components in G-SIM communicate with network messages. The implication of this is that software components in a G-SIM are identified by an IP address (or computer name if DNS is in use). IP address identification is preferable. In most cases, a single message represents a command or request. The G-SIM Server replies to every command or request with a result. This implies that a single conversation between the operator workstation and the server requires at least 2 messages at the application layer.

The persistent backbone of the G-SIM Server is Microsoft® SQL Server™. G-SIM Server connects to a SQL Server™ database to retrieve the configuration of the G-SIM. This is the first thing the G-SIM Server does on start-up. After a successful connection is established by the G-SIM Server to a valid SQL Server™ configuration database, it loads the configuration data and waits for client connections. G-SIM Server is therefore the only data provider and store for clients (the exception is that the map cache and limited user-related settings are stored on the client workstations).

Client-Server Architecture

From the G-SIM Server's perspective, all other G-SIM software components are clients. The Server distinguishes between the following types of clients:

- Operator Console
- Management Console
- Health Agent
- G-SIM Updater

The responsibilities of the G-SIM Server towards its clients are basically the following:

- Validate client
- Authorise client actions

- Supply client with data requested
- Request data from client
- Perform actions on behalf of client
- Notify other clients of a specific client’s behavior
- Log client actions and requests to the audit log

Health Agents

G-SIM provides an extensible health monitoring framework used to monitor the health of various system components. "System health" is a generic term describing the well-being of a system. Health information includes:

- Current state of various system parameters
- Failure history or stability
- Performance information of various system components

Health Monitoring Architecture

A Health Agent (HA) is a software component with the ability to communicate health information to the G-SIM server. A Health Monitor (HM) is a software component with the ability to monitor the health of one or more system components parameters. The most important system components monitored are hardware, software, system usage, and network parameters.

G-SIM has an extensive library of health monitors to provide out-of-the-box health monitoring functionality. Because the Health Monitor is an architecturally modular software component, the G-SIM health framework can therefore be extended by custom developed Health Monitors. These modular software components or Health Monitors are called plug-ins (or HM plug-ins). The most important out-of-the-box Health Monitor plug-ins are the 3 plugins GeViSoft, SSC and SNMP.

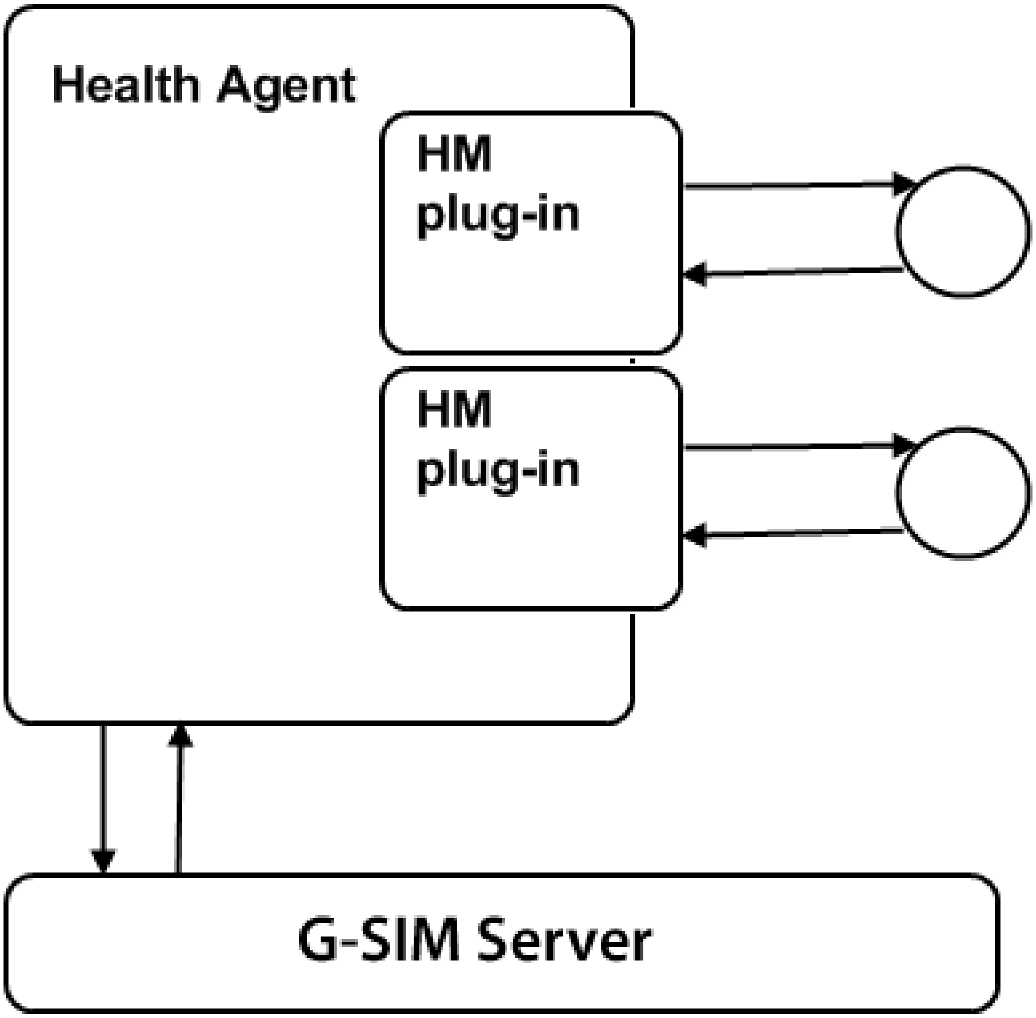
It is important to understand how the G-SIM health framework works to be able to configure it successfully. A Health Agent is configured to use specified Health Monitor plug-ins and to monitor specified sites.

Plugin Architecture

The Health Agent is a software component that runs as a service on a designated computer. Its only function is to communicate health information collected from Health Monitors to the G-SIM server. Health Monitors are software components that can only run as plug-ins inside the Health Agent process. At start-up, the

Health Agent loads plug-ins installed on the computer. A Health Monitor, depending on its design and function, might need system data to perform its task successfully. The plug-in architecture supports data requests from plug-ins: data is requested from the Health Agent which in turn requests data from the G-SIM server, which supplies the requested data to the plug-in. The current Health Monitor plug-in architecture supports requests for the following system data:

- Video source information (NVR and camera information). These data are grouped per site.
- Storage device information. These data include the NVRs using the storage device.
- Health Monitor plug-in parameters.



Start-up of the Health Agent

The health agent follows a set procedure at start-up. Understanding the procedure is important for troubleshooting and maintenance. It is as follows:

At start-up the health agent loads all the health monitors:

- It supplies the health monitor with system data.
- It sets up the health monitor parameters.
- It starts the health monitor.

After the health monitors have been loaded the health agent synchronizes with the G-SIM server:

- It connects to G-SIM server Connection Manager and logs in as a health agent.
- It sends alarms (if any) to the G-SIM server.
- It gets the latest system data and health monitor parameters from the server.
- It updates the health monitor with the latest system data and parameters.

Health Event Generation

A Health Agent has the capacity to generate health events. It most instances, health events are referred to as alarms. It is true that all alarms are health events but not all health events are alarms.

Health Events	
Sync-loss and Camera Failure	This happens when a NVR detects that a camera is not transmitting a signal.
CPA Event	This will be triggered when the camera is moved.
Login Failures	If a user attempts to log in with an invalid user name or password.
System Errors and System Terminating	Any system errors or termination events that are sent from the GeViScope.
Errors and Warn-	Numerous errors and warnings can be sent from the

Health Events	
ings from RAID	GeViRAID, which can range from hard drive failures to over-heating.
FRC Notification	This happens when the iSCSI port is disconnected.
Digital input or Camera Contact	A physical relay or button is pressed by a user.
Custom Alarms	GeViSoft Actions mapped to alarms.

A health monitor plug-in defines its own health events and its primary function is to monitor these events. If a health event is detected and filtered through the plug-in rule set, then the health monitor creates a generic health event structure and populates it with the required detail. It then passes the event to the Health Agent to forward to the G-SIM server. Health events have three severity levels that determine how they are passed to the G-SIM server. These levels describe the time criticality of the events.

Health Event Severity	Health Agent Action
Critical	Critical health events are immediately published to the G-SIM server.
Non-Critical	Non-critical health events are published to the G-SIM server at the next scheduled synchronisation time.
Information	Non critical health events are published to the G-SIM server at the next scheduled synchronisation time only if requested by the server.

Alarm Architecture

An alarm is a health event that should be brought to the attention of an Operator Console user. It therefore requires human intervention. For this reason an alarm has a state that indicates where in the intervention process it is and it also may have actions that guide a user in the intervention process.

The Operator Console has a list called the Alarm List that contains all raised health events. See the **Alarms** for more detail. When alarms are flooding in from the Health Agent, the Server could go into a locked state when trying to update all the

Map Objects' global states. To guard against that, the server and the Operator Console have special code to deal with alarm floods. They also co-operate to cope with floods.

Alarm Terminology

The following table explains the most pertinent terminology that is used when dealing with alarms. It is important to stick to this, as it will vastly reduce the chances of miscommunication.

Alarm Terminology	Description
Source	Represents the source or origin of the alarm. Possible sources are: • Computers or NVRs • Cameras • Digital inputs • Other hardware sources This value can contain a unique identifier that can be interpreted by the G-SIM system and then linked to a G-SIM component. In the case where the source is not a G-SIM component, this value represents a text description of the source. For instance, for camera failures, the source might contain the unique identifier of the camera or it might contain a text description containing a site reference and camera name in the format: Site - Camera
Location	Represents a text description of the physical location of the alarm source. It should refer to a location within a site.
Site	Represents the site the alarm originates from. A site is basically a grouping of locations and cameras which has been created by the G-SIM administrator. For some installations it is best to group physically (those close together), while in others logically (those which do the same thing, for example).
Camera	Represents the default camera associated with the alarm.

Alarm Terminology	Description
	Associating a camera with an alarm has two meanings: • With camera failures, it represents the camera that failed. • With all other events, it represents a camera that can be used to monitor the event.

As you can see, the terminology cements the concepts, and makes clear communication possible.

Alarm State

The following table gives an overview of the states that an alarm may be in.

Alarm State	Description
New	A new health notification (i.e. alarm) was created in the system and appears in the Active Alarm List of appropriate users. The alarm will already be visible in the Alarm History List.
Acknowledged	An alarm was acknowledged by a user implying the user took ownership of the alarm. The Alarm Task List (i.e. procedure list as wizard) is visible in write mode to this user.
Forwarded	The alarm was forwarded to another user but the user was not logged in. This is appropriate for example where a shift change will take place and the next user to handle the alarm is to use the same workstation. (It should be noted that all alarms older than 24 hours will be flagged. This is therefore a viable option.)
ForwardedAcknowledged	The alarm was forwarded to another online user and the user acknowledged and accepted the alarm. This user is now the new user and can view the Alarm Task List in write mode.
Handled	The alarm was handled, i.e. the Alarm Task List was completed. This alarm will disappear from the Active Alarm List and will be only viewable form the Alarm History List.

See the User manual for more detail on alarm states and how to deal with them.

Alarm Actions

In essence, an alarm action is a traceable task that guides the user to follow a certain procedure when an alarm arrives. By default, an alarm has no actions. All actions can be configured with the Maintenance console. Alarm actions are therefore specific to the implementation and more detail can be found in the G-SIM Configuration and Implementation Manual.

The alarm action directs a user to perform a certain task as a result of the alarm condition. To allow for the traceability of the action, the user is forced to provide an action result or response. The health monitor plug-in architecture provides the following alarm action response types to facilitate its traceability and to allow the Operator console to interpret the action into a user response graphical interface.

Action Response Type	Description
Text	The user is forced to supply a text description as a response to the action request.
Check	The user is forced to acknowledge that the action item was attended to.
YesNo	The user is forced to supply a Yes or No answer to the action request.

Maintenance

From a risk management perspective, this is probably the most important aspect of G-SIM: keeping things stable. If the planning and installation were done properly, then system maintenance will not be a burden, and can be completed with relative ease. The only real issues would then be external, and particular to your installation.

This manual focuses on three main topics:

- **Monitoring** the installation.
- **Data base** maintenance.
- Using the **updater service** to see that everything remains synchronised.

At present, events and counters are prefixed with the term **GeViCentral**, which was the development project name for G-SIM. These entries will most likely change to G-SIM in future, so please bear this in mind when developing any monitoring scripts.

Monitoring

Monitoring is a critically important aspect of maintaining the health and stability of a G-SIM installation. In this chapter we look at two types of monitoring: event and performance.

- Event monitoring makes use of the Windows event logs. Here you will find descriptive text outlining problems that G-SIM and other parts of the installation pick up.
- Performance monitoring can be used for such diverse purposes as seeing where a current problem is, to identifying trends.

Event Monitoring

The events we refer to here are those which are written by various parts of the G-SIM installation to the Windows Event Logs.

It is important to note that more than only the G-SIM named events should be considered when trouble-shooting. Sometimes a system event will be the reason for whatever problem there may be. It is thus best to view event log entries as clues: they are usually not definitive, but rather point to the real reason.

Performance Monitoring

In the introductory text of this chapter, the point was made that performance monitoring includes identifying trends. While this is seldom seen as urgent, it is very important. If you do not check for trends, you will usually discover an underlying problem only once it has become an issue that needs immediate attention. It is far better to identify and deal with it during scheduled maintenance, for example.

Counters

The following table outlines the counters which G-SIM writes to the Windows Performance Monitoring System.

Counters	**Description**
Active Client Connections	The cache of active client connections to the server.

Counters	Description
Active Site Connections	The number of open connections to sites.
Active Video Connections	The number of active video connections across all sites.
Avg Message Processing Time (sec)	The average message processing time in fractional-second resolution.
Messages Processed	The number of messages processed since server start-up.
Messages Processed per second (sec)	The average number of messages processed per second for the monitoring interval.
Moving Average Message Processing Time (ms)	The moving average (over last 1000 messages) processing time per message in milliseconds (ms).
Moving Average Video Connect Request Time (ms)	The moving average (over last 1000 connection attempts) video connection time in milliseconds.
Open ISDN Connections	The number of open ISDN connections.

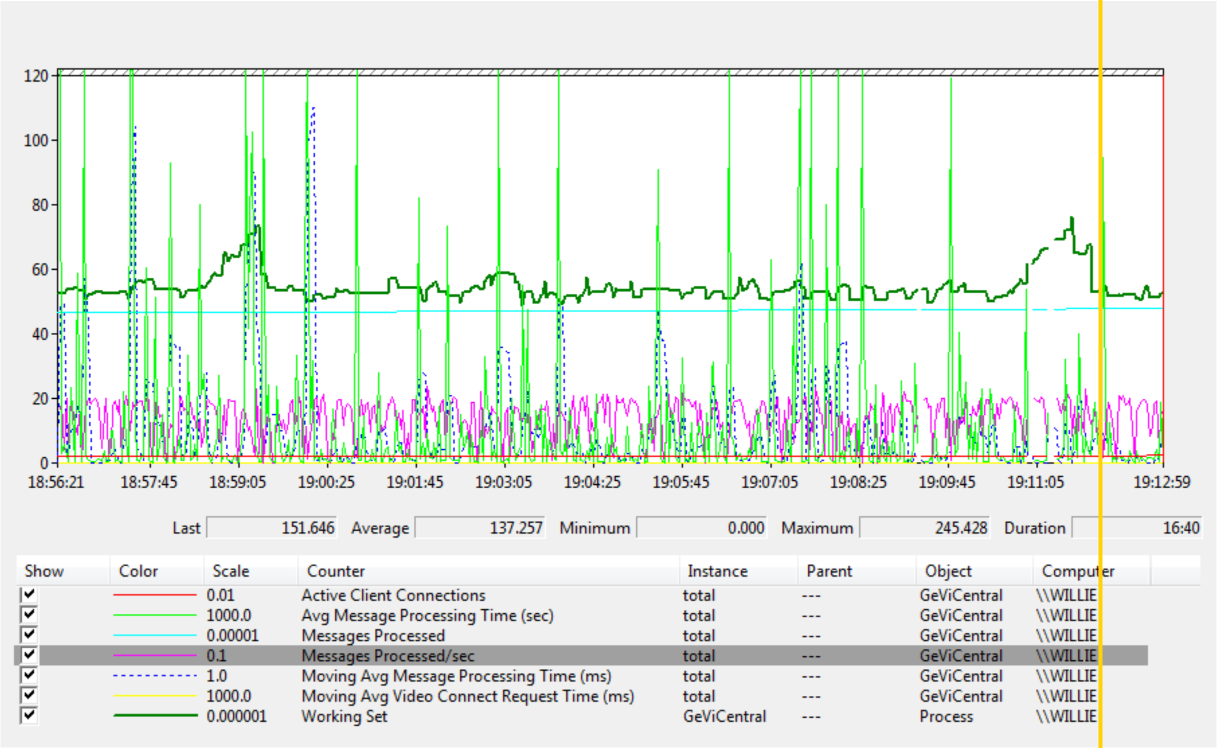
Preventative Maintenance

This simply involves monitoring performance counters and sending out notifications to maintenance staff when certain predefined values are crossed or certain criteria are met. These are known as performance counter alerts. Performance counter alerts can be accessed in Windows by creating a Data Collector Set in the Computer Management console.

For example, a notification (e-mail / SMS) can be sent when the memory usage of the G-SIM Server reaches a certain threshold, or a notification can be sent when the Moving Avg Message Processing Time (ms) counter exceeds 3000 ms (3 seconds).

Example: Connection Performance Test

> Example In this example we look at the usage of the performance counters to measure client connection performance. This specific performance test was designed to test the client connection performance of the G-SIM server.



Last 151.646 Average 137.257 Minimum 0.000 Maximum 245.428 Duration 16:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	0.01	Active Client Connections	total	---	GeViCentral	\\WILLIE
☑	—	1000.0	Avg Message Processing Time (sec)	total	---	GeViCentral	\\WILLIE
☑	—	0.00001	Messages Processed	total	---	GeViCentral	\\WILLIE
☑	—	0.1	Messages Processed/sec	total	---	GeViCentral	\\WILLIE
☑	┄	1.0	Moving Avg Message Processing Time (ms)	total	---	GeViCentral	\\WILLIE
☑	—	1000.0	Moving Avg Video Connect Request Time (ms)	total	---	GeViCentral	\\WILLIE
☑	—	0.000001	Working Set	GeViCentral	---	Process	\\WILLIE

An additional performance counter that would give relevant informative data is the memory **Working Set** of the G-SIM Server.

Data Base Maintenance

The G-SIM Server uses Microsoft SQL Server for persistent storage. Persistent data consist of system configuration data (static), system state data (dynamic), and the system audit log.

Although default automated backups are configured during the system installation, it is imperative that a database backup procedure is drafted for every G-SIM installation. Such a procedure should address the following concerns:

- Automated backup procedures
- Backup frequency
- Off-site backup
- Data security and integrity
- System integrity during backup

- System restoration from backups
- Rebuilding the data base index

What these are and how they are defined is entirely up to you, but would most likely have to fit in with existing corporate backup processes. Just be sure to verify with your data security officer that the defined procedures are sufficient.

Maps and Graphics

A map is used as a visual reference of an area to display cameras, alarms and other objects of importance on. One site can have many maps for different areas. We use two types of maps: overview and detail. Overview maps typically won't have individual device status information, but are used to aid in navigation. They will thus have labels such as street or building names, and hot-spots which, when clicked upon, take the operator to the relevant map (usually detail, though it could be an overview map if the area is really large).

A typical map will show a position layout as clearly and as simply as possible to assist in alarm handling, and maintenance, and will also try not to be cluttered with useless info. All interactive elements (such as cameras) are drawn and placed during the compilation process in G-SIM and are not part of the original map images.

Overview

As beautiful and as functional as the maps are that you see in G-SIM demos, they can require considerable planning and work, depending on where you get them. In this document we outline the steps required to get to a set of workable maps.

We will be talking about inter alia the following:

- Differences between raster and vector images and their implications for maps
- Sources we can use for maps
- How best to map different scenarios
- How to prepare map images
- Overview maps

- Detail maps
- Hot-spot links

The most important aspect to generating good maps is comprehensive planning and fanatical documentation. We will go into details later, but for now the following will give you a good idea of what to consider and how to plan.

Example

Say that a customer's site comprises of 5 buildings, where each building has 4 floors with cameras on each floor, and some of the floors have clusters of cameras in certain areas (such as stairwells and elevators). In planning the map we need to keep in mind our ultimate goal: to locate areas easily (implying clarity and area recognition on maps) and get to cameras/alarms quickly (cameras and alarm sections must not overlap or obscure each other, and there can't be too many levels of overview maps).

Keeping these goals in mind, this customer will probably need the following map levels:

- An Overview map of the grounds, showing all 5 buildings. Hotspots are added afterwards in G-SIM to navigate to each sector's Close-up (in this case each building).
- The next level can either be Overview or Close-up maps, depending on the size of each sector and the number of cameras. Since these buildings have more than one floor with cameras on each, we will need a map for each floor, thus a total of 20 maps for this level. When working with a building, you can consider using either a side view or top view of the building/each floor, depending on the placement of the cameras and the building's layout. If unsure, use a top view.
    - Consider that a map is viewed inside a G-SIM viewer, which is by default not very large. If you are viewing the cameras at a decent size and the map is too large for the viewer, it becomes impossible to scroll between cameras near opposite ends; if you resize that same map to fit inside the viewer and the cameras don't fit inside the space any longer,

    then the map needs to be an Overview map that links to smaller sections (Close-up maps) of the floor.

    - If the map is suitable for most of the cameras except for an area of clustered cameras, you can make a combination Overview/Close-up map by placing all cameras on it except the clustered cameras, then mark that area as a section that links to its own Close-up map.

- The lowest level is the Detail map that shows cameras and alarm areas. The map's size must be large enough that none of the cameras overlap but not too wide to make navigation from one end to the other a tedious task.

Because of the huge difference in size between an Overview and Close-up map, it is recommended to render two different maps at different sizes. It is tempting to make a Close-up map and then use that map for the overview too, but that is completely the wrong way around. You first need to do the overview map, and from there you will know where to split it for the various detail maps.

MultiTenancy

The G-SIM multitenancy is enabled on the dongle via a software option. If the option is on the dongle, the customer can switch on this functionality in the management console (Management Console).

The multitenancy changes the behavior of created G-SIM users and user groups. The objective is to separate users at the user group level so that, for example, different customers can be created on the system, but they cannot see each other in the operator console (OpCon).

G-SIM provides this functionality through user groups. Here, a G-SIM user group is created for each client.

Once the multitenancy is switched on, in the user list of the Operator Console, only users are shown that originate from the same user group as the logged in user. In addition, for status changes such as which user is currently observing the camera, only users from the same user group are shown. A superordinate instance or group that has access to all resources does not exist.

Notifications and tasks can only be sent and received to and from users in the same user group.

Camera tours that are marked **public** are displayed when the tour has been created by a user of the same user group.

Evaluation in the audit log are limited to users of the same user group.

In general, all resources such as alarms, cameras, sites, etc., are available for all users. They are restricted via for the corresponding user groups in the restrictions present in G-SIM. The following restrictions can be set up:

- Alarm instances
- Alarms
- Cameras
- Export locations
- Viewer layouts (scenes)
- Sites
- Remote consoles
- Process data filters
- Process data search for a site
- Resources that are not available for the user group are not shown. Examples:
    - Cameras that are blocked for the user are no longer shown on the map.
    - Users cannot see which users from other groups are currently observing a camera
    - A customer operates their own remote console. So that users of the customer can control it, a restriction must be set up that blocks this remote console for other user groups.

Multiple Addition of a Recorder

Since a NVR can only be assigned to one site, it is possible that the same NVR is added twice. In this case, G-SIM provides the option of importing the function **Only to certain channels** for the import function for the video channels.

The G-SIM NVR Failover Function covers this configuration. The functionality of a recorder that is added multiple times is not directly a component of the multitenancy, but it may be used by it.

Limitations

- Currently, the cameras of the second site, for NVR Failover with a recorder added multiple times, are not reconnected in case of a failover.
- More than one user group per client is not currently possible. Mixed operation where only one customer contains multiple user groups is not foreseen.
- Multitenancy relates exclusively to Operator Console!
- Process data searches cannot currently be limited at the user group level. It is possible for users or user groups to limit the process data filter using a restriction, however the search will be performed on the entire site. This can only be bypassed when the user has been created for their own site in G-SIM.

Technical alterations reserved.

GEUTEBRÜCK GmbH
Im Nassen 7-9 | D-53578 Windhagen
Tel. +49 (0)2645 137-0 | Fax-999
info@geutebrueck.com

www.geutebrueck.com