

Geutebrück Platform
Documentation

08.09.2026

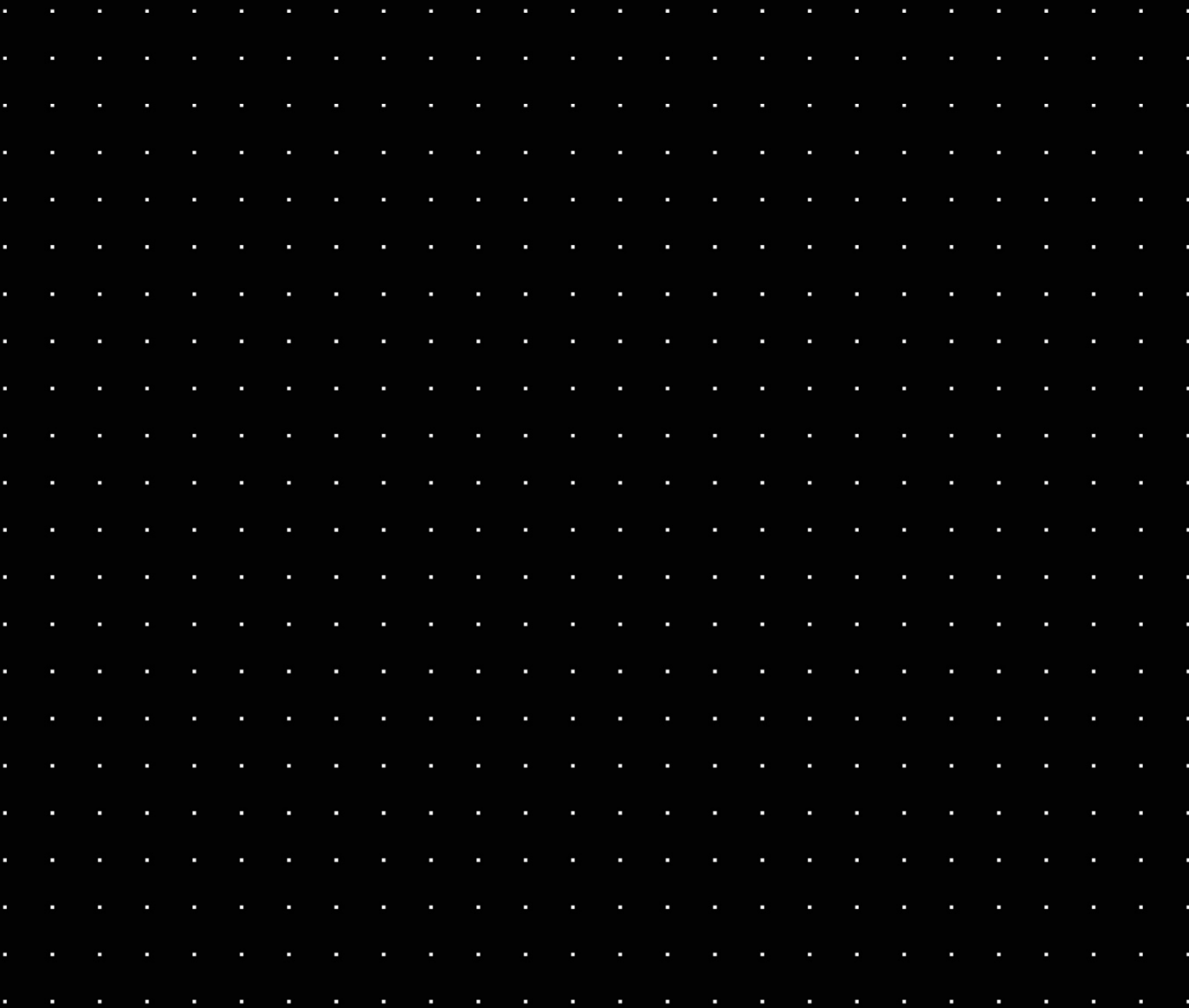


Table Of Contents

About This Documentation	7
Legal Notice	8
Installation	9
Prerequisites	9
Order of Installation	10
Geutebrück Hub Installation	12
Install Geutebrück Hub	12
Create Administrator Account	14
Plugin Loader Installation	16
Local Installation	16
Remote Installation (Optional)	20
Without Geutebrück Hub Connection	23
Local Installation	23
Remote Installation (Optional)	26
Linux Installation (Optional)	37
Failover Installation (Optional)	40
G-Insights Installation	41
Install NVIDIA CUDA Toolkit (Optional)	41
Install G-Insights	42
Initial Setup	44
Set Up Plugin Loader	44
Set Up G-SIM (Optional)	45
Set Up G-Insights	46
Set Up Geutebrück Hub	49
Plugin Loader	50
Overview	50
Feature Overview	50
Plugin Features	50
Upgrade	52
Upgrade 1.1 to 1.2	52
Upgrade 1.2 to 1.3	53
Using Plugin Loader	53
Open the Plugin Loader	53

Manage Devices	54
Add Device	55
Create Multiple Devices	60
Edit Device	63
Delete Device	63
Use CameraRAWOutput Action	64
Manage Mappings	66
Add Custom Mapping	67
Edit Custom Mapping	70
Delete Custom Mapping	70
Development	71
SDK Installation	71
SDK Backend	72
Components	72
Interfaces	73
Write a Remote Plugin	73
Write a Plugin Module	76
Multihead Support	81
Include Your Own Settings UI	82
Add a Plugin to a Plugin Loader	83
Example Plugins	84
Plugin Loader Simulator	84
SDK Frontend	85
Geutebrück Hub	87
User Account Management	87
Confirm User Account	87
Change Password	88
Reset Password	89
Apps	91
Users	91
Order of Initial Setup	91
Manage Users	92
Add User	93
Create Password Reset Link	94
Edit User	95
Delete User	97

Manage User Groups	97
Add User Group	97
Edit User Group	100
Delete User Group	102
Manage Roles	102
Add Role	102
Edit Role	104
Delete Role	106
Manage Permission Sets	106
Add Permission Set	107
Edit Permission Set	108
Delete Permission Set	109
Manage Resource Sets	109
Add Resource Set	110
Edit Resource Set	111
Delete Resource Set	113
Resources	113
Manage Resources	113
Add Tag	114
Open Resource	114
Rename Resource	114
Remove Resource	115
Settings	115
System Settings	115
G-Insights Settings	117
Geutebrück Hub Security Guide	120
Purpose	120
Administrator Accounts	120
Authentication And Authorization	120
Certificates And TLS	121
Token-Signing Certificate Rollover	121
Network Hardening	121
G-Insights	122
Overview	122
System Overview	122
Main Features	122

Functional Role of AI in Scope	122
Storage Layout	123
Data Flow	123
Bestshot Generation	124
Path	125
What This Means	126
User Query Paths	126
Compliance Information	127
EU AI Act Compliance & Prohibited Practices (Article 5)	128
What This Means	128
System Behavior	128
Model Accountability and Governance	129
Model Limitations and Biases	130
Security Information	130
System Limits and Known Limitations	131
System Capacity and Sizing Guide	131
Server Limits	131
Channel Limits	131
General Limitations	133
Data Storage and Retention Time	133
G-Insights Settings	134
Using G-Insights	137
Open G-Insights	137
History	138
Search	139
Camera Metadata Search	139
AI-Powered Similarity Search	141
Search Results	142
Analysis	143
FAQ and Troubleshooting	144
Hardware	144
Data Flow	144
Security / RBAC	144
Supported Languages	145
AI Model Accountability	145
Search Results in Camera Metadata Search	145

Search Results in AI-Powered Similarity Search	145
G-Insights Security Guide	146
Geutebrück Hub Trust And Service Token	146
Certificates And HTTPS	146
Local Data Protection	147
Grafana Dashboards	147

About This Documentation

Current software versions:

- Geutebrück Hub 1.1.0
- Plugin Loader 1.6
- G-Insights 1.1.0

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



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.



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

© 2026 GEUTEBRÜCK GmbH. All rights reserved world wide.

Installation

Prerequisites

Before you begin the installation, make sure that the following prerequisites are met, additional to the system requirements in the Release Notes.

Component	Prerequisite
Installed Software	The following software must be installed: • G-Core version 10 or newer • Optional: G-SIM version 13 or newer, including G-SIM Web API
G-Insights Storage and Partitioning	Camera metadata and AI-generated similarity vectors must be stored on separate partitions to guarantee correct operation. • Drive type: Use high-speed NVMe drives for both storage locations. • Operating system partition: Do not use the operating system drive for either storage location. The 4 TB NVMe SSD dedicated to G-Insights must be configured with two separate partitions: • Camera metadata partition: Allocated for the SQLite database. • AI-generated similarity vectors partition: Allocated for the Qdrant database.
G-Insights GPU	A CUDA-capable GPU is required to use the AI-powered similarity search. Supported GPUs: • NVIDIA RTX 2000 Ada • NVIDIA RTX PRO 2000 Blackwell
Camera Configuration	Metadata: Make sure you have enabled the generation of metadata on your cameras to ensure correct func-

Component	Prerequisite
	tionality. Bounding boxes: Make sure that the object bounding boxes are only sent via the metadata stream. Bounding boxes embedded in the video stream might lead to incorrect results in the AI-powered similarity search. Fisheye: Fisheye cameras can be used with either dewarping on edge or with G-Core dewarping. Privacy zones: If privacy zones are required, they must be configured in the camera. G-Core privacy masking is not supported in G-Insights. Time synchronization: To ensure that metadata are correctly assigned in G-Insights and that the Plugin Loader uses the same event timestamp as the system time, your cameras must be time-synchronized. It is also important that the settings for daylight saving time and standard time are configured correctly. Incorrect assignment of timestamps leads to discrepancies, and event data may not be recorded with the correct timestamps. To synchronize cameras and servers, you can use an NTP server. If there are time differences between the cameras in the network, it is recommended that you set up an NTP server on the G-Insights server and synchronize all cameras to it.
Supported Browsers	The browsers Microsoft Edge and Google Chrome (Chromium-based browsers) are supported.

Order of Installation

It is important to install and set up the components in the following order, as there are dependencies between the different components.

1. **Geutebrück Hub Installation**
 - a. **Install Geutebrück Hub**
 - b. **Create Administrator Account**
2. **Plugin Loader Installation**
 - a. **Local Installation**
 - b. **Remote Installation (Optional)**
3. **G-Insights Installation**
 - a. **Install NVIDIA CUDA Toolkit (Optional)**
 - b. **Install G-Insights**
4. **Initial Setup**
 - a. **Set Up Plugin Loader**
 - b. **Set Up G-SIM (Optional)**
 - c. **Set Up G-Insights**
 - d. **Set Up Geutebrück Hub**

Before you install a component, download the installer to the server where you want to install that component.

Component	Installer
Geutebrück Hub	Installer: Geutebrueck_Hub_Installer_xxx.xxx.exe Where to install: G-Core server or remote server
Plugin Loader	Installer: • Local installation: G-Core_Installer_xxx.exe • Remote installation (optional): PluginLoader_Installer_xxx.exe Where to install: • Local installation: G-Core server • Remote installation: Remote server

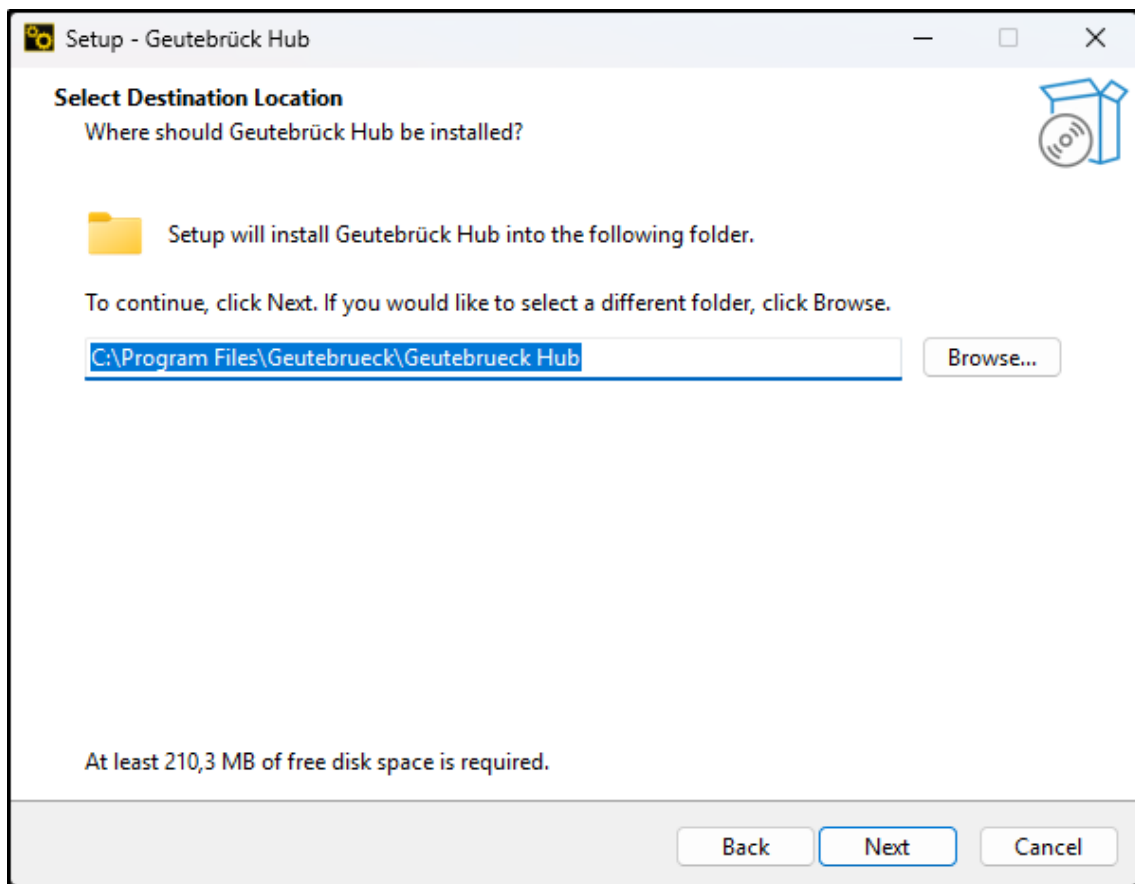
Component	Installer
G-Insights	Installer: • G-Insights: GInsights_xxx.exe • NVIDIA Cuda Toolkit (optional): https://developer.nvidia.com/cuda-12-9-0-download-archive Where to install: • G-Insights: G-Core server or remote server • NVIDIA Cuda Toolkit (optional): G-Insights server

Geutebrück Hub Installation

Install Geutebrück Hub

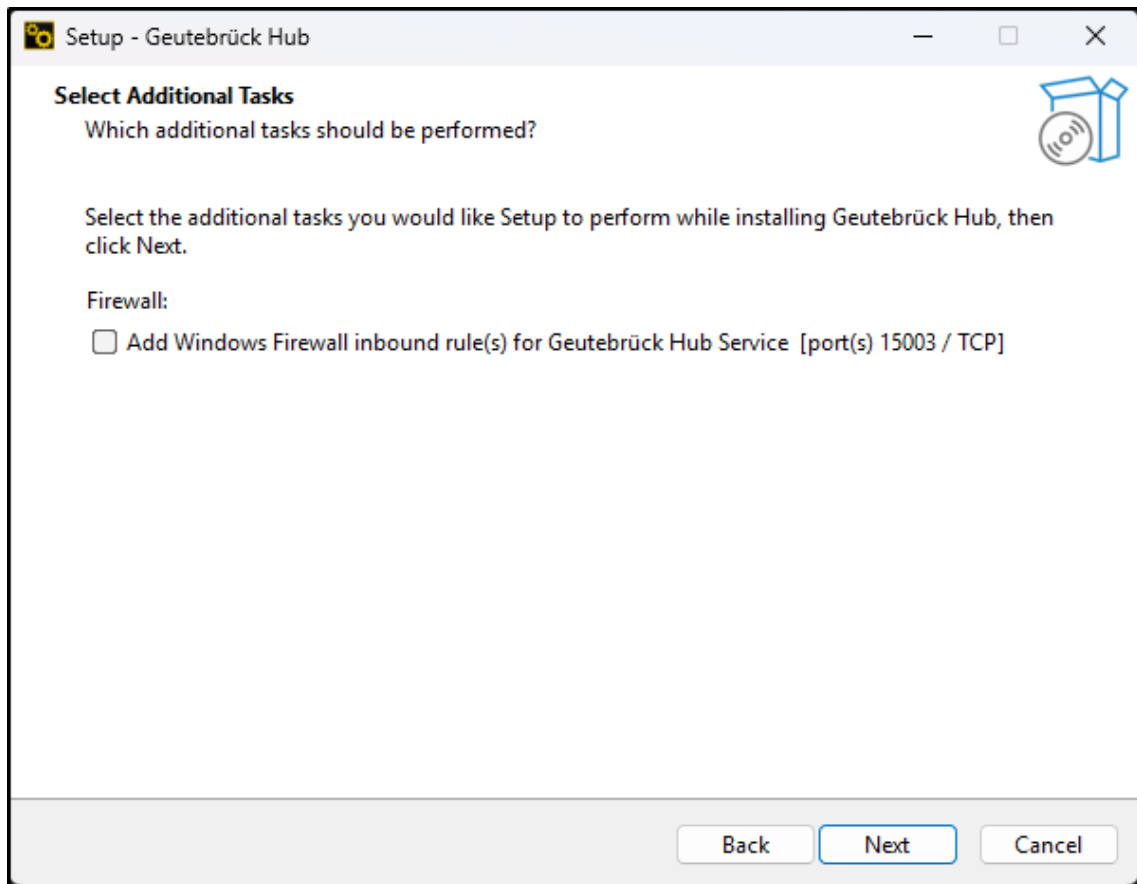
Install the Geutebrück Hub on the G-Core server or a remote server.

1. Run the Geutebrueck Hub_Installer_xxx.xxx.exe file. The installation window opens.
2. On the **License Agreement** page, accept the agreement and click **Next**.
3. On the **Select Destination Location** page, select the installation directory.



4. On the **Select Additional Task** page, select the **Firewall** option if you want to open the TCP port 15003.

i This option is only required if you want to install the **Plugin Loader** and **G-Insights** on a server other than the **Geutebrück Hub** server, as the port is needed for the connection of the **Geutebrück Hub** to the services.



5. On the **Ready to Install** page, click **Install**.
6. To complete the installation, restart the computer. Select **Yes, restart the computer now** or **No, I will restart the computer later** and click **Finish**.

Create Administrator Account

To log in to the Geutebrück Hub, you must first create an administrator account.

1. Open the Geutebrück Hub via the desktop icon. The **Create Initial Administrator** page opens.

The screenshot shows the 'Create Initial Administrator' form on the GEUTEBRUCK Hub interface. The form is centered on a dark background. It contains three input fields: 'E-Mail*', 'Please enter your password*', and 'Please repeat your password*'. Each password field has an eye icon to toggle visibility. A 'Submit' button is located at the bottom right of the form.

2. Enter an e-mail address and a password.
3. Click **Submit**. The **Login** page opens.

The screenshot shows the 'Login' form on the GEUTEBRUCK Hub interface. The form is centered on a dark background. It contains two input fields: 'E-Mail*' and 'Password*'. The 'Password*' field has an eye icon to toggle visibility. A 'Login' button is located at the bottom of the form.

4. Enter the login details and click **Login**. The **Apps** page opens.
No applications or resources are available yet. Continue with the installation of the Plugin Loader.

Plugin Loader Installation

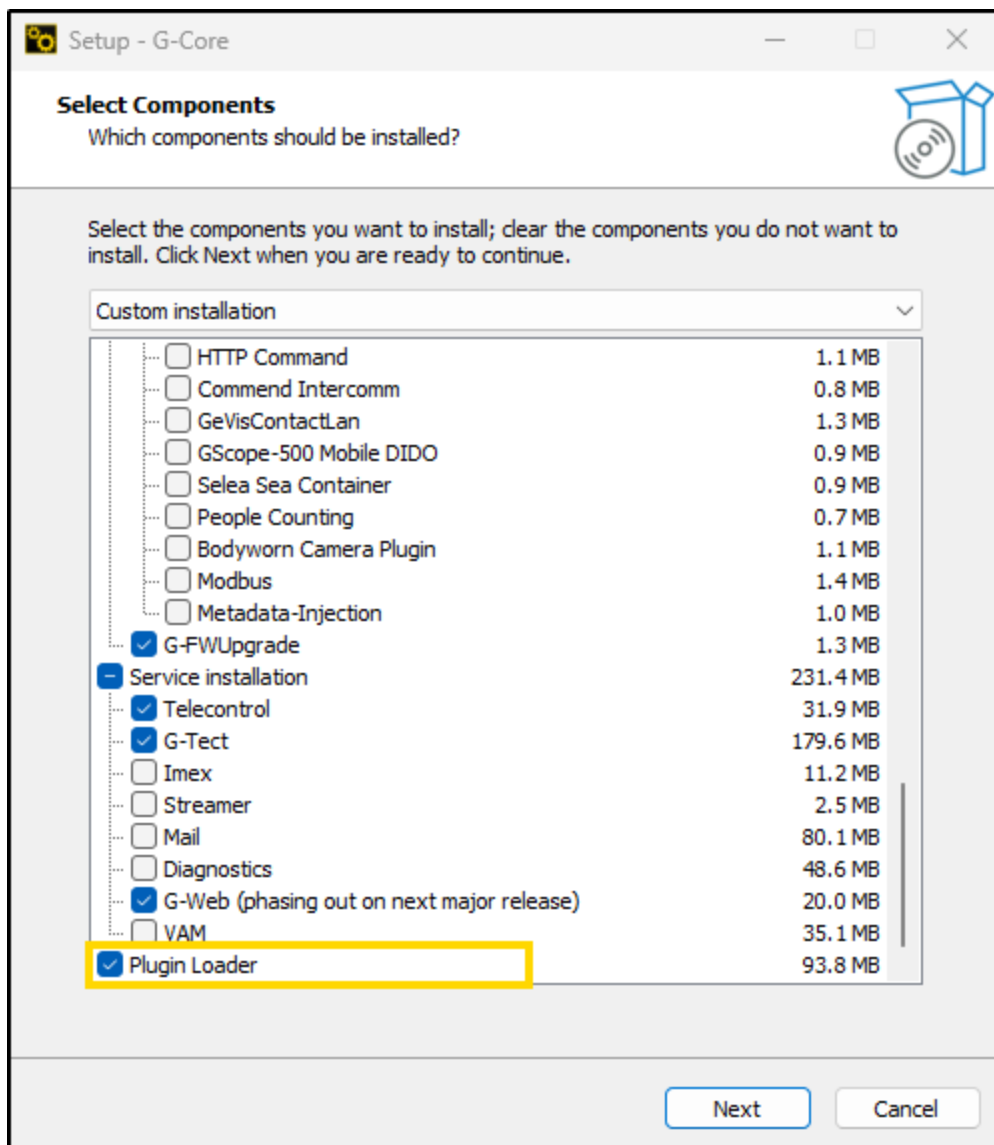
The Plugin Loader consists of two components: Gateway and Plugin Loader.

- Install Gateway and Plugin Loader on the G-Core server (see **Local Installation**).
- Optional: Install the Plugin Loader component also on remote servers to use the Plugin Loader remotely at multiple sites (see **Remote Installation (Optional)**).

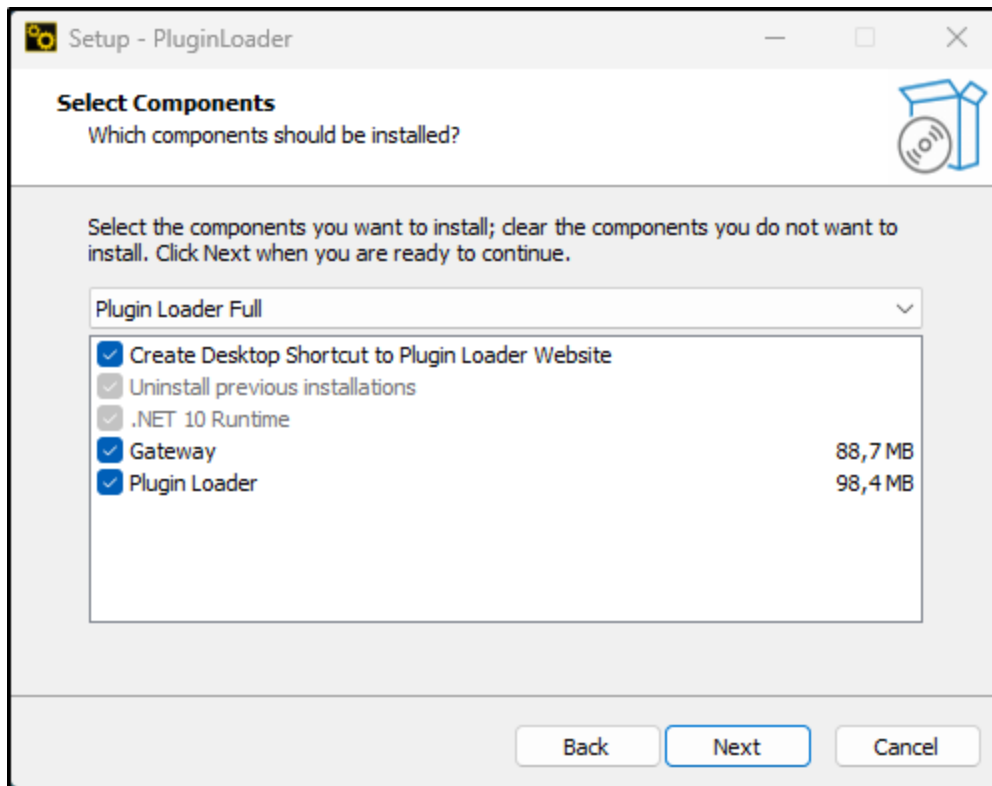
Local Installation

Install the Gateway and the Plugin Loader on the G-Core server.

1. Run the `G-Core_Installer_xxx.exe` file. The installation window opens.
2. On the **License Agreement** page, accept the agreement and click **Next**.
3. On the **Select Components** page, select **Plugin Loader** and the further components you want to install. Click **Next**.

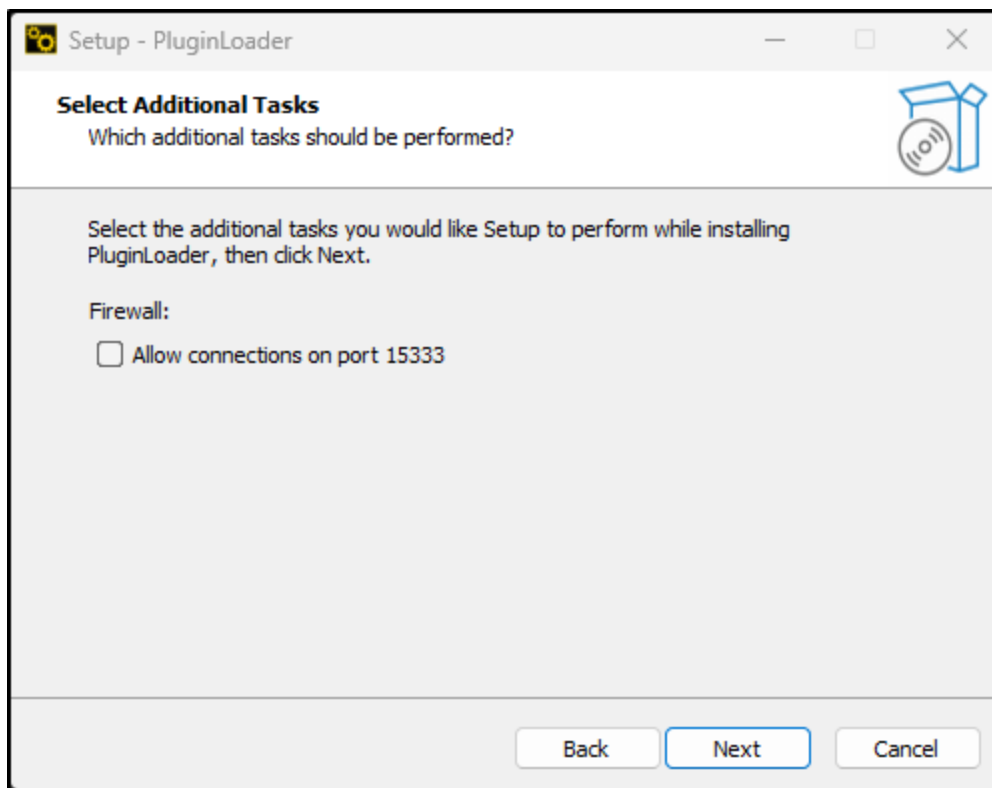


4. On the **Additional Tasks** page, select the **Additional icons** option if you want to create a desktop icon.
5. On the **Ready to Install** page, click **Install**. The Plugin Loader installation window opens.
6. On the **License Agreement** page, accept the agreement and click **Next**.
7. On the **Select Components** page, select **Plugin Loader Full** from the drop-down menu and click **Next**.



8. On the **Select Additional Tasks** page, select the **Firewall** option if you want to open the port 15333.

i This option is only required if you want to install a **Plugin Loader on a server other than the G-Core server (see Remote Installation (Optional))**, as the port is needed for the connection of the **Gateway and the Plugin Loader**.



9. On the **Ready to Install** page, click **Install**.
10. A dialog appears asking whether to connect the Gateway to the Geutebrück Hub. Click **Yes**.
For information on installation without a Geutebrück Hub connection, see **Installation Without Geutebrück Hub Connection**.
11. The **Configure service** dialog appears. Enter your Geutebrück Hub login details.
 - a. In the **Address** field, enter the IP address of the Geutebrück Hub. The default address is `https://localhost:15003`.
 - b. In the **User** field, enter the e-mail address of the Geutebrück Hub user. The user must be an administrator or must have the Service Registration permission.
 - c. In the **Password** field, enter the password of the Geutebrück Hub user.
 - d. Click **Configure**.



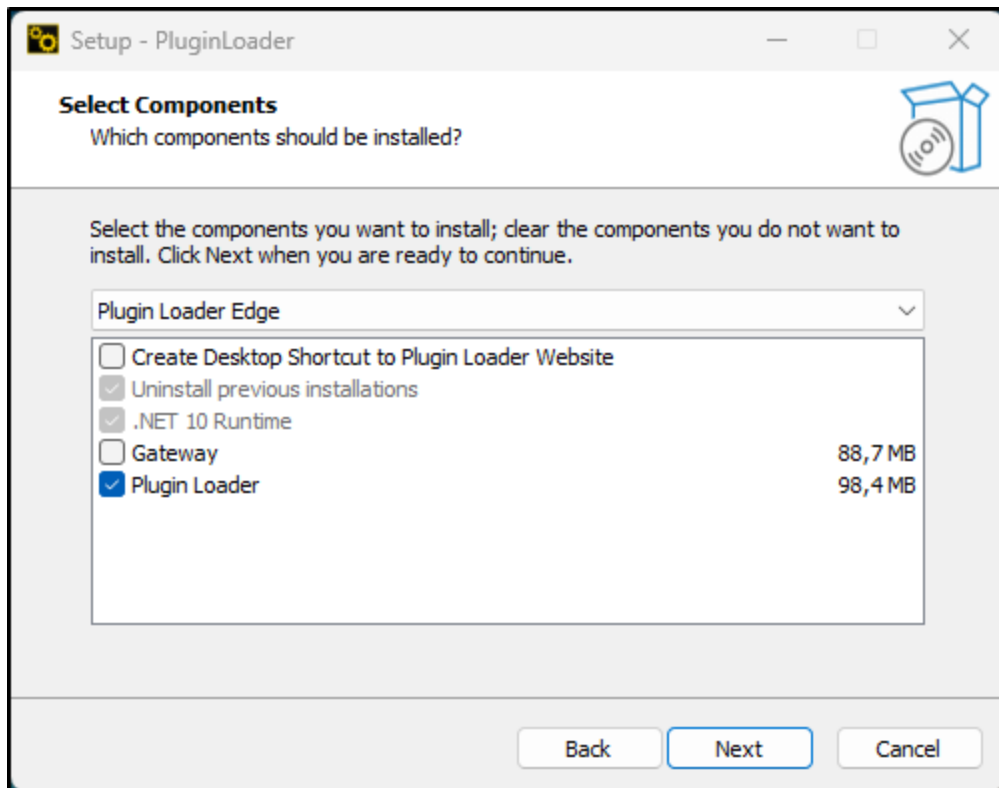
12. A confirmation dialog appears. Click **OK**.
13. A dialog appears asking whether to connect the Plugin Loader to the Geutebrück Hub. Click **Yes**.
For information on installation without a Geutebrück Hub connection see **Installation Without Geutebrück Hub Connection**.
14. The **Configure service** dialog appears again. Enter your Geutebrück Hub login details and click **Configure**.
15. A confirmation dialog appears. Click **OK**.
16. To complete the installation, restart the computer. Select **Yes, restart the computer now** or **No, I will restart the computer later** and click **Finish**.

Remote Installation (Optional)

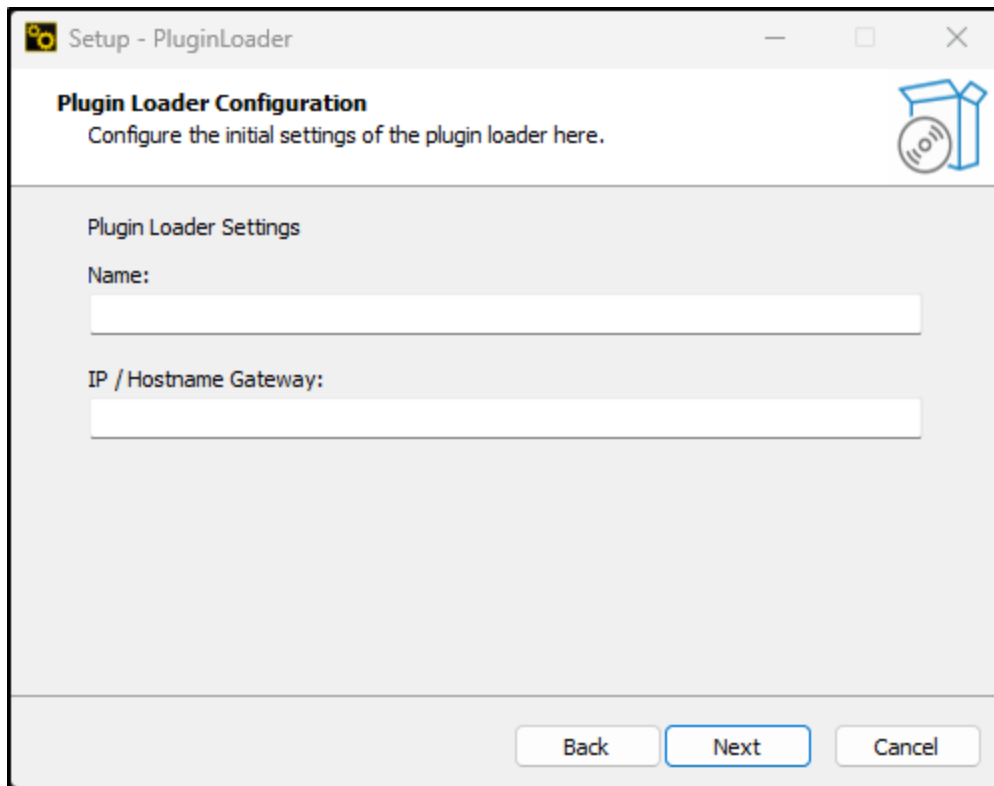
Install the Plugin Loader on a remote server.

i **Make sure that the Gateway is installed on the G-Core server and that port 15333 is open (see Local Installation).**

1. Run the `PluginLoader_Installer_xxx.exe` file. The installation window opens.
2. On the **License Agreement** page, accept the agreement and click **Next**.
3. On the **Select Components** page, select **Plugin Loader Edge** from the drop-down menu and click **Next**.



4. On the **Plugin Loader Configuration** page, enter the Plugin Loader settings.
 - a. In the **Name** field, enter the name for your Plugin Loader.
 - b. In the **IP / Hostname Gateway** field, enter the IP address or hostname of the G-Core server on which the Gateway is installed.
 - c. Click **Next**.



5. On the **Ready to Install** page, click **Install**.
6. A dialog appears asking whether to connect the Plugin Loader to the Geutebrück Hub. Click **Yes**.
For information on installation without a Geutebrück Hub connection, see **Installation Without Geutebrück Hub Connection**.
7. The **Configure service** dialog appears. Enter your Geutebrück Hub login details.
 - a. In the **Address** field, enter the IP address of the Geutebrück Hub. The default address is `https://localhost:15003`.
 - b. In the **User** field, enter the e-mail address of the Geutebrück Hub user. The user must be an administrator or must have the Service Registration permission.
 - c. In the **Password** field, enter the password of the Geutebrück Hub user.
 - d. Click **Configure**.



8. A confirmation dialog appears. Click **OK**.
9. To complete the installation, restart the computer. Select **Yes, restart the computer now** or **No, I will restart the computer later** and click **Finish**.

Without Geutebrück Hub Connection

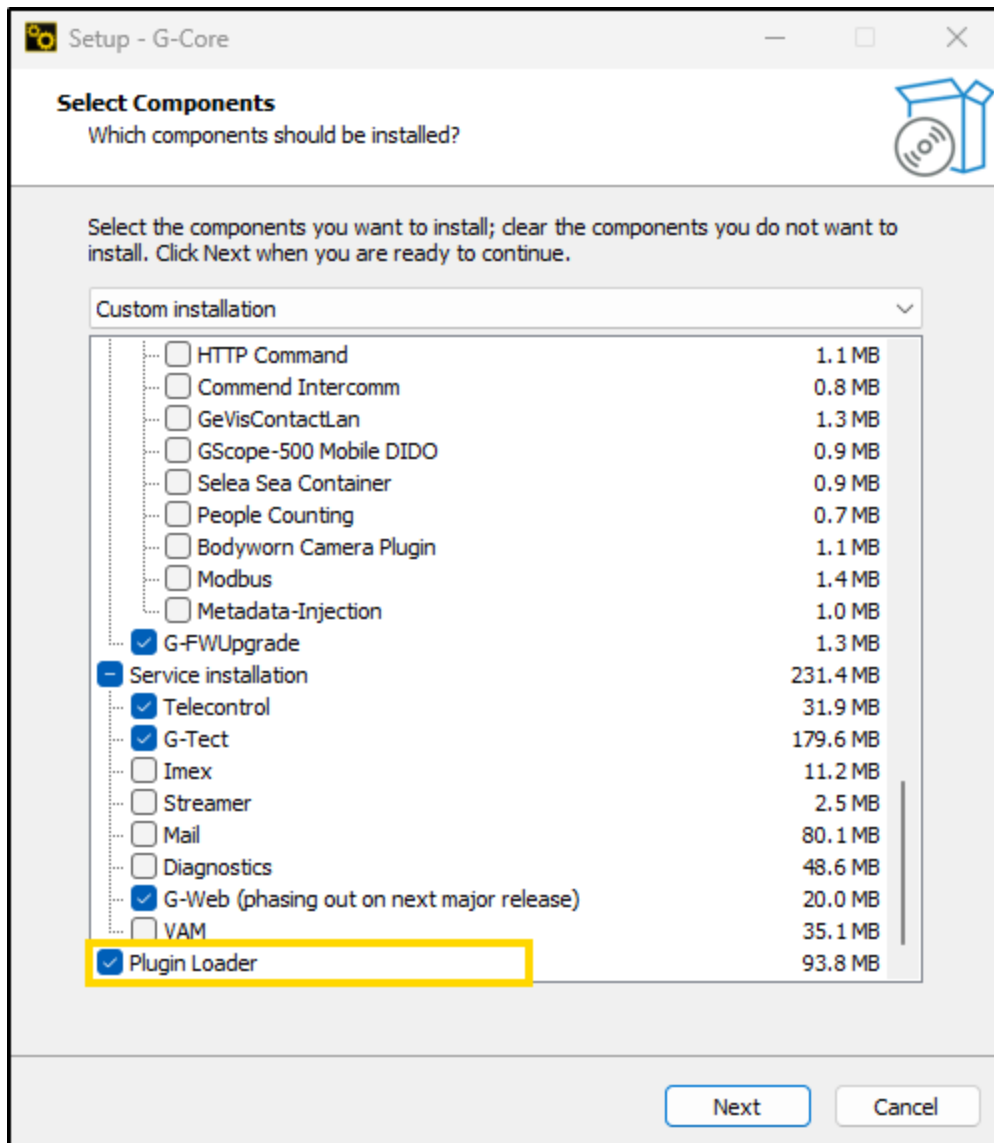
The Plugin Loader consists of two components: Gateway and Plugin Loader.

- Install Gateway and Plugin Loader on the G-Core server (see **Local Installation**).
- Optional: Install the Plugin Loader component also on remote servers to use the Plugin Loader remotely at multiple sites (see **Remote Installation (Optional)**).

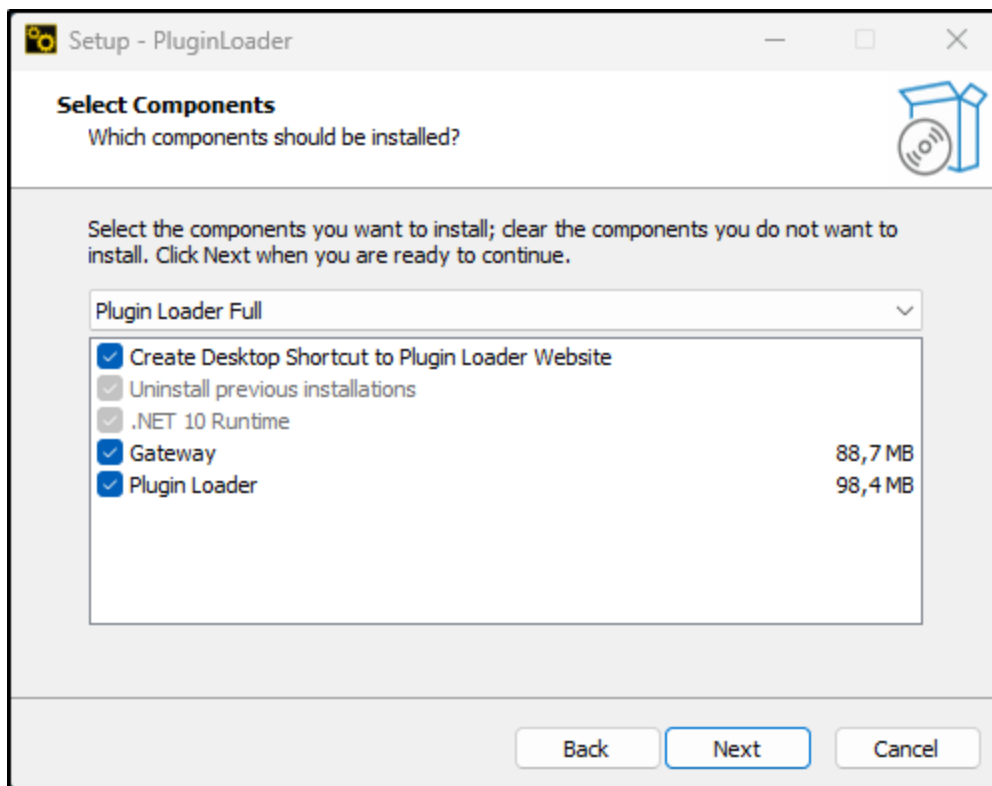
Local Installation

Install the Gateway and the Plugin Loader on the G-Core server.

1. Run the `G-Core_Installer_xxx.exe` file. The installation window opens.
2. On the **License Agreement** page, accept the agreement and click **Next**.
3. On the **Select Components** page, select **Plugin Loader** and the further components you want to install. Click **Next**.

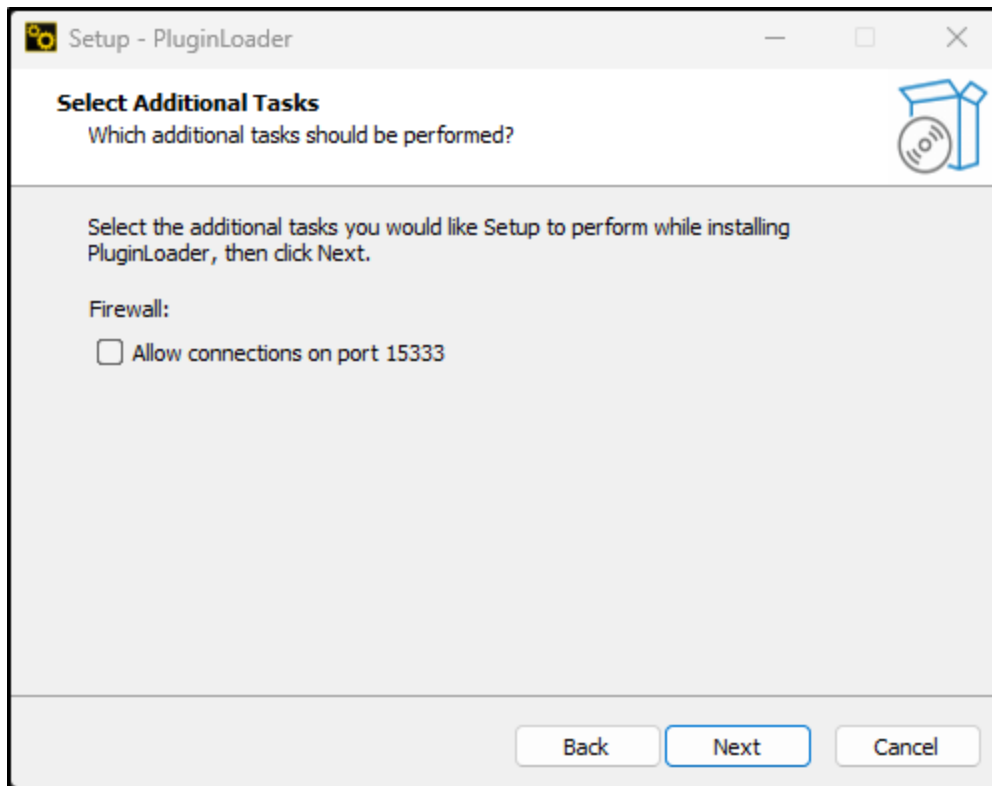


4. On the **Additional Tasks** page, select the **Additional icons** option if you want to create a desktop icon.
5. On the **Ready to Install** page, click **Install**. The Plugin Loader installation window opens.
6. On the **License Agreement** page, accept the agreement and click **Next**.
7. On the **Select Components** page, select **Plugin Loader Full** from the drop-down menu and click **Next**.



8. On the **Select Additional Task** page, select the **Firewall** option if you want to open the port 15333.

i **This option is only required if you want to install a Plugin Loader on a server other than the G-Core server (see Remote Installation (Optional)), as the port is needed for the connection of the Gateway and the Plugin Loader.**



9. On the **Ready to Install** page, click **Install**.
10. A dialog appears asking whether to connect the Gateway to the Geutebrück Hub. Click **No**.
For information on installation with a Geutebrück Hub connection, see **Plugin Loader Installation**.
11. To complete the installation, restart the computer. Select **Yes, restart the computer now** or **No, I will restart the computer later** and click **Finish**.

Remote Installation (Optional)

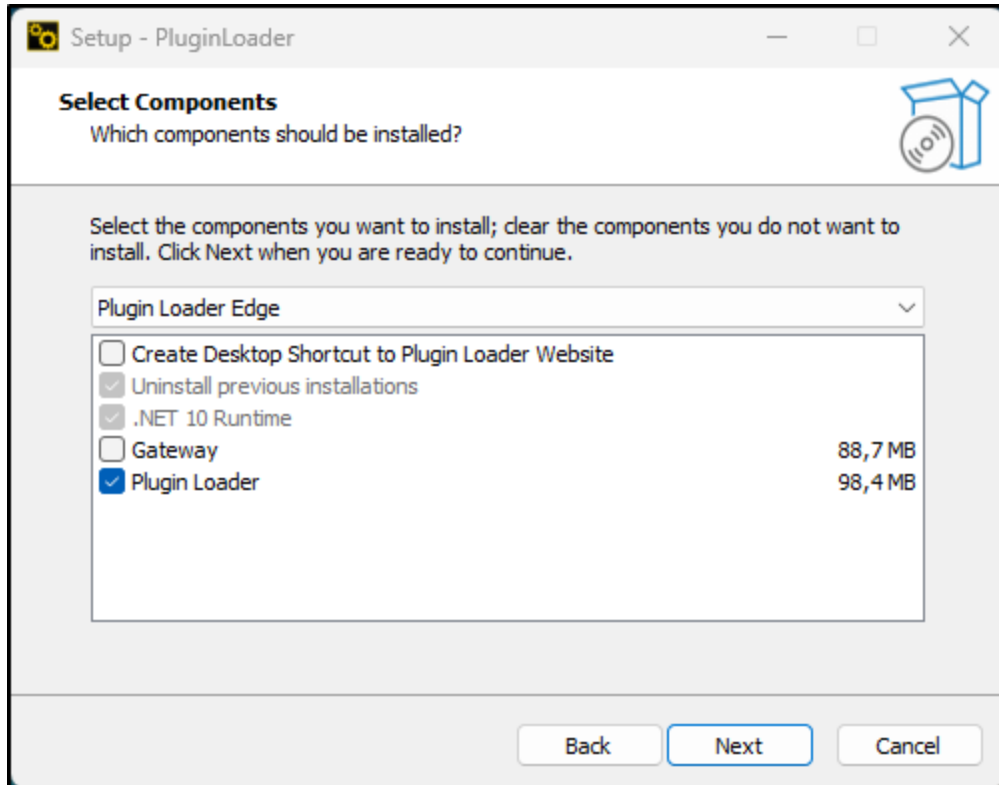
To use the Plugin Loader remotely at multiple sites, install the Plugin Loader component on the respective remote servers (see **Install Plugin Loader**) and import the authentication certificate (see **Import Authentication Certificate**).

i Requirement:
Make sure that the Gateway is installed on the G-Core server and that the port 15333 is open (see Local Installation).

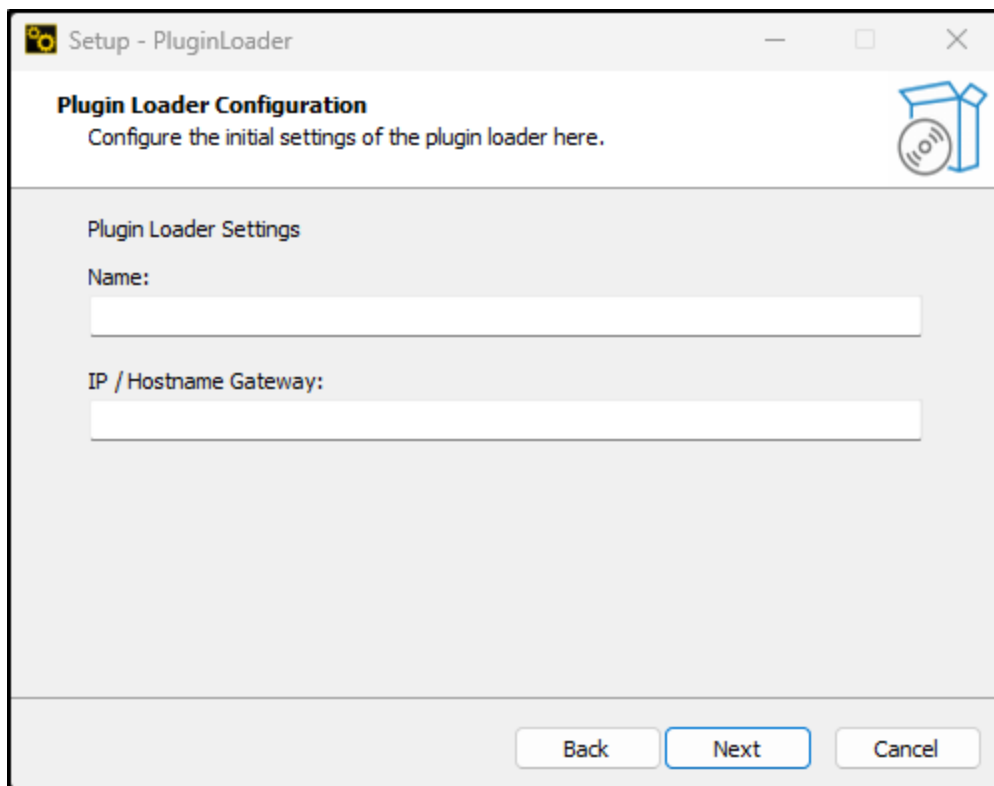
Install Plugin Loader

Install the Plugin Loader on the remote server.

1. Run the `PluginLoader_Installer_xxx.exe` file. The installation window opens.
2. On the **License Agreement** page, accept the agreement and click **Next**.
3. On the **Select Components** page, select **Plugin Loader Edge** from the drop-down menu and click **Next**.

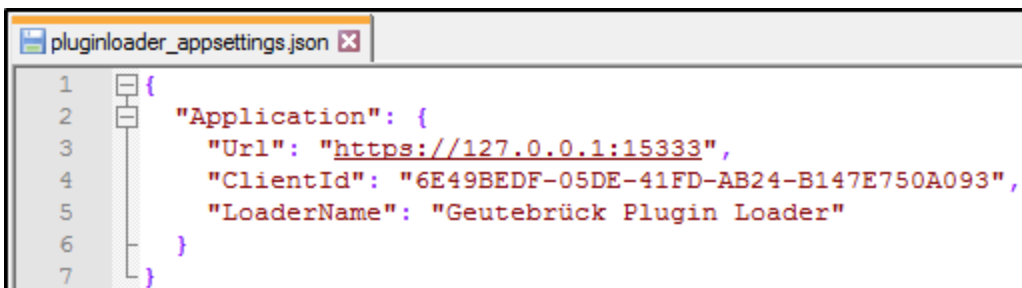


4. On the **Plugin Loader Configuration** page, enter the Plugin Loader settings.
 - a. In the **Name** field, enter the name for your Plugin Loader.
 - b. In the **IP / Hostname Gateway** field, enter the IP address or hostname of the G-Core server on which the Gateway is installed.
 - c. Click **Next**.



5. On the **Ready to Install** page, click **Install**.
6. A dialog appears asking whether to connect the Gateway to the Geutebrück Hub. Click **No**.
For information on installation with a Geutebrück Hub connection, see **Plugin Loader Installation**.
7. To complete the installation, restart the computer. Select **Yes, restart the computer now** or **No, I will restart the computer later** and click **Finish**.

The Plugin Loader settings are saved in the `pluginloader_appsettings.json` file in the installation directory `C:\Program Files\Geutebrueck\PluginLoader`. You can subsequently change the settings in this file. If you have made changes, you must restart the **Geutebrueck.PluginLoader.Service** service.



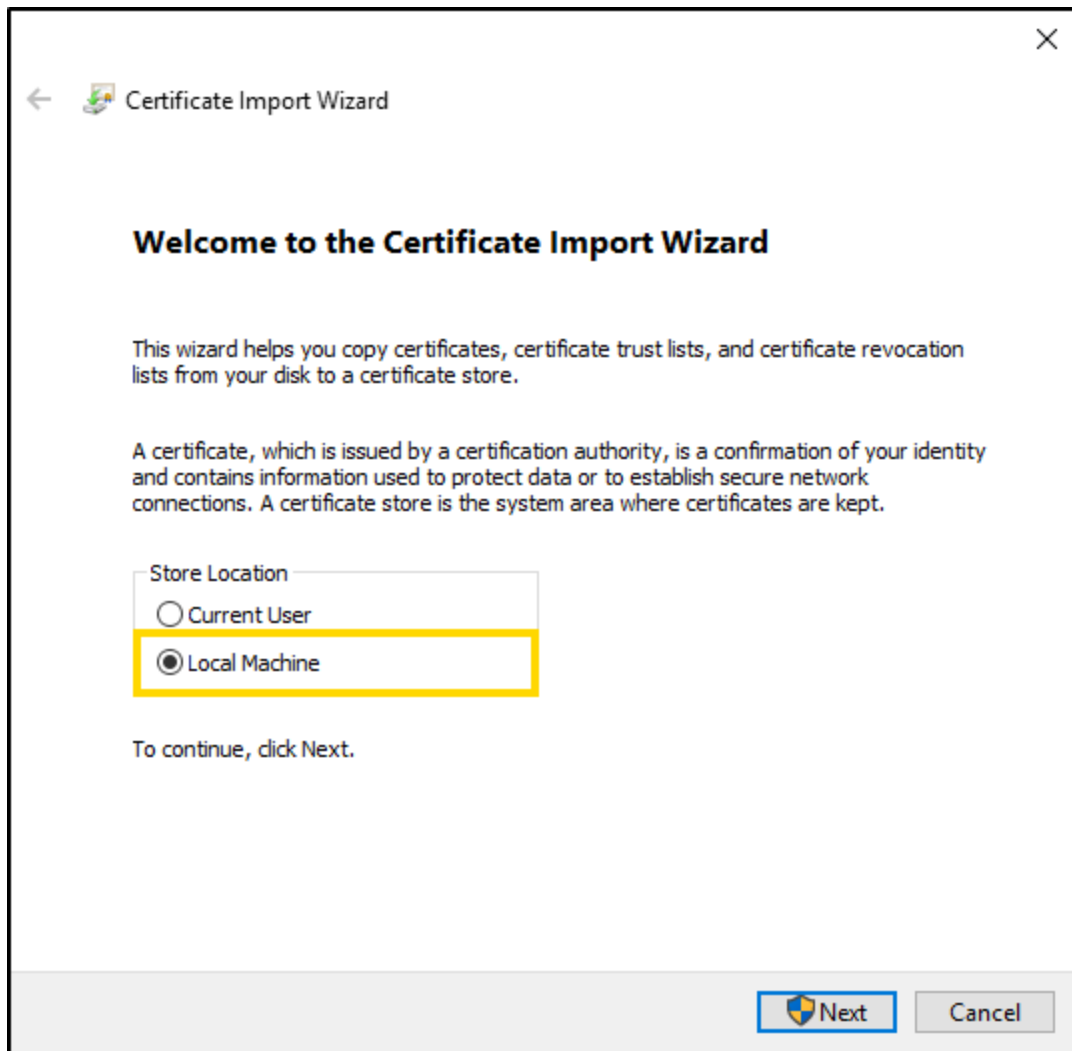
Import Authentication Certificate

You must import the authentication certificate into the following store locations:

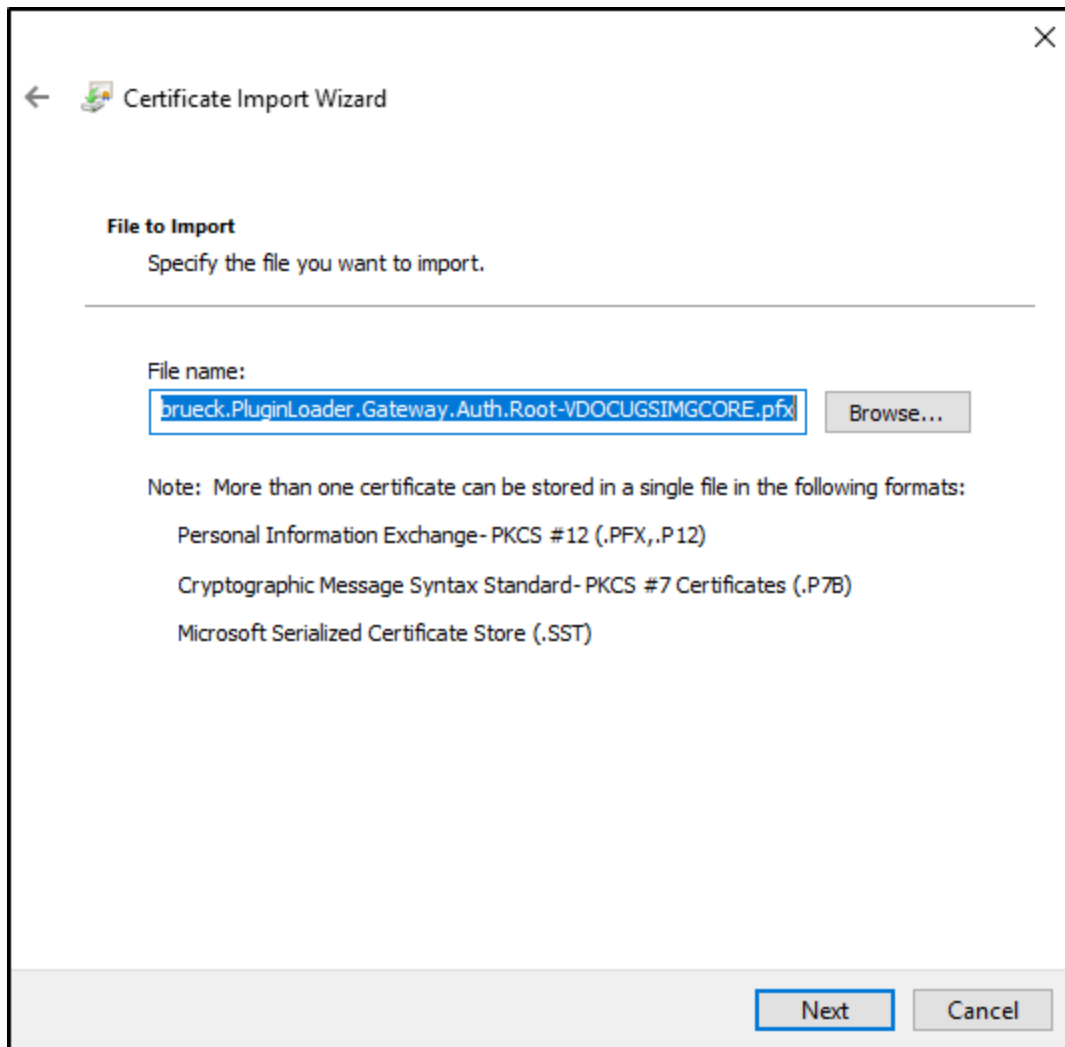
- **Local Machine:** To connect the remote Plugin Loader to the Gateway on the G-Core server.
- **Current User:** To access the Plugin Loader web interface remotely.

Import the authentication certificate to the remote server.

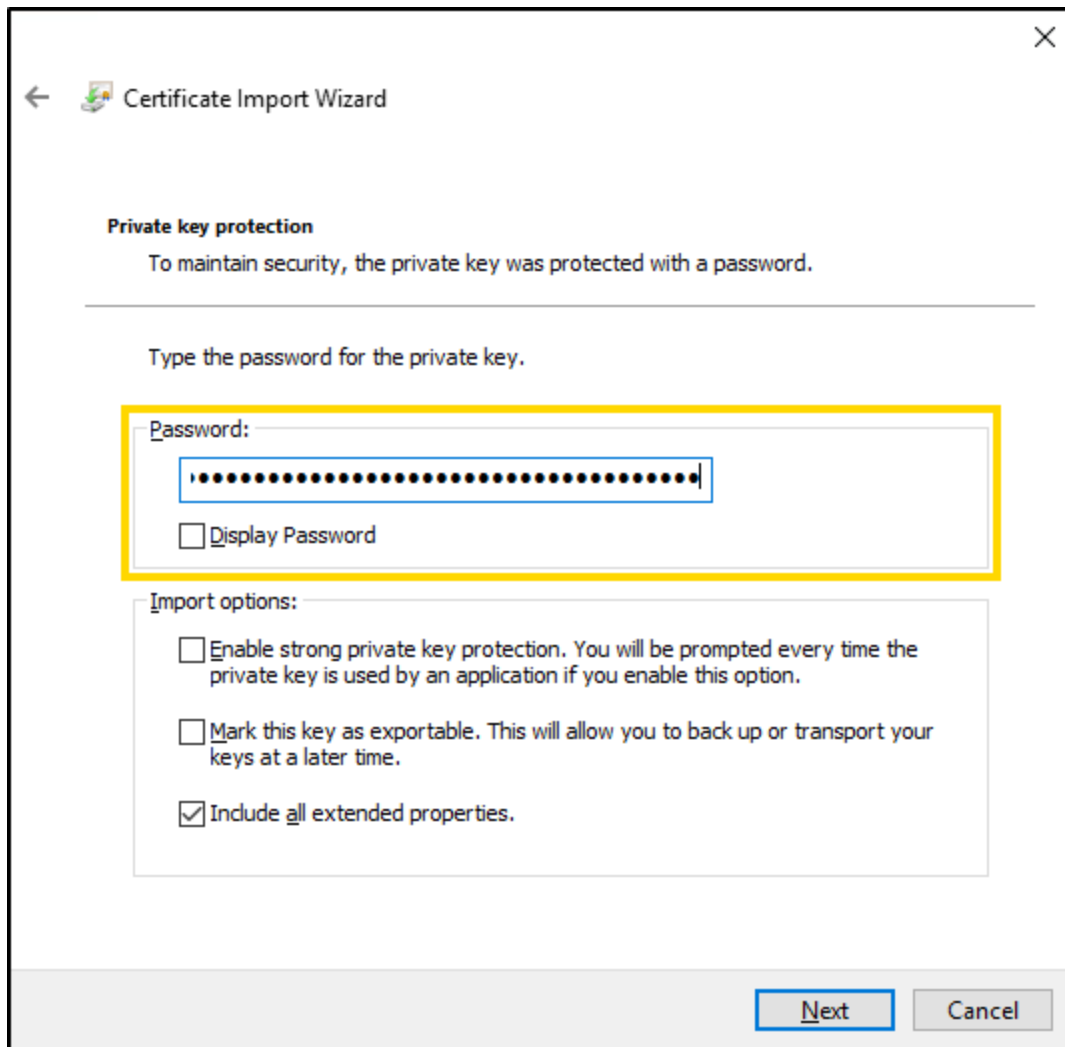
1. After installing the Gateway on the G-Core server (see **Local Installation**), you will find the certificate files in the folder `C:\Program Files\Geutebrueck-\GCore\RemotePlugins\child-root`. Copy these files to the remote client.
2. Run the certificate file `child-Geutebrueck-.PluginLoader.Gateway.Auth.Root-<hostname>.pfx`. The Certificate Import Wizard window opens.
3. On the **Welcome to the Certificate Import Wizard** page, select **Local Machine** and click **Next**.



4. On the **File to Import** page, the certificate file is already selected by default. Click **Next**.



5. On the **Private key protection** page, type the password for the private key. This password is noted in the certificate file `child-Geutebrueck-.PluginLoader.Gateway.Auth.Root-<hostname>.pfx.$password.txt`. Click **Next**.



The image shows a Windows 'Certificate Import Wizard' window. The title bar says 'Certificate Import Wizard' with a back arrow and a close button. The main content area is titled 'Private key protection' and contains the text 'To maintain security, the private key was protected with a password.' Below this is a prompt 'Type the password for the private key.' followed by a 'Password:' label and a text box filled with dots. A yellow rectangular box highlights the password input area and the 'Display Password' checkbox. Below the password section is the 'Import options:' section, which contains three checkboxes: 'Enable strong private key protection...' (unchecked), 'Mark this key as exportable...' (unchecked), and 'Include all extended properties.' (checked). At the bottom right are 'Next' and 'Cancel' buttons.

← 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:

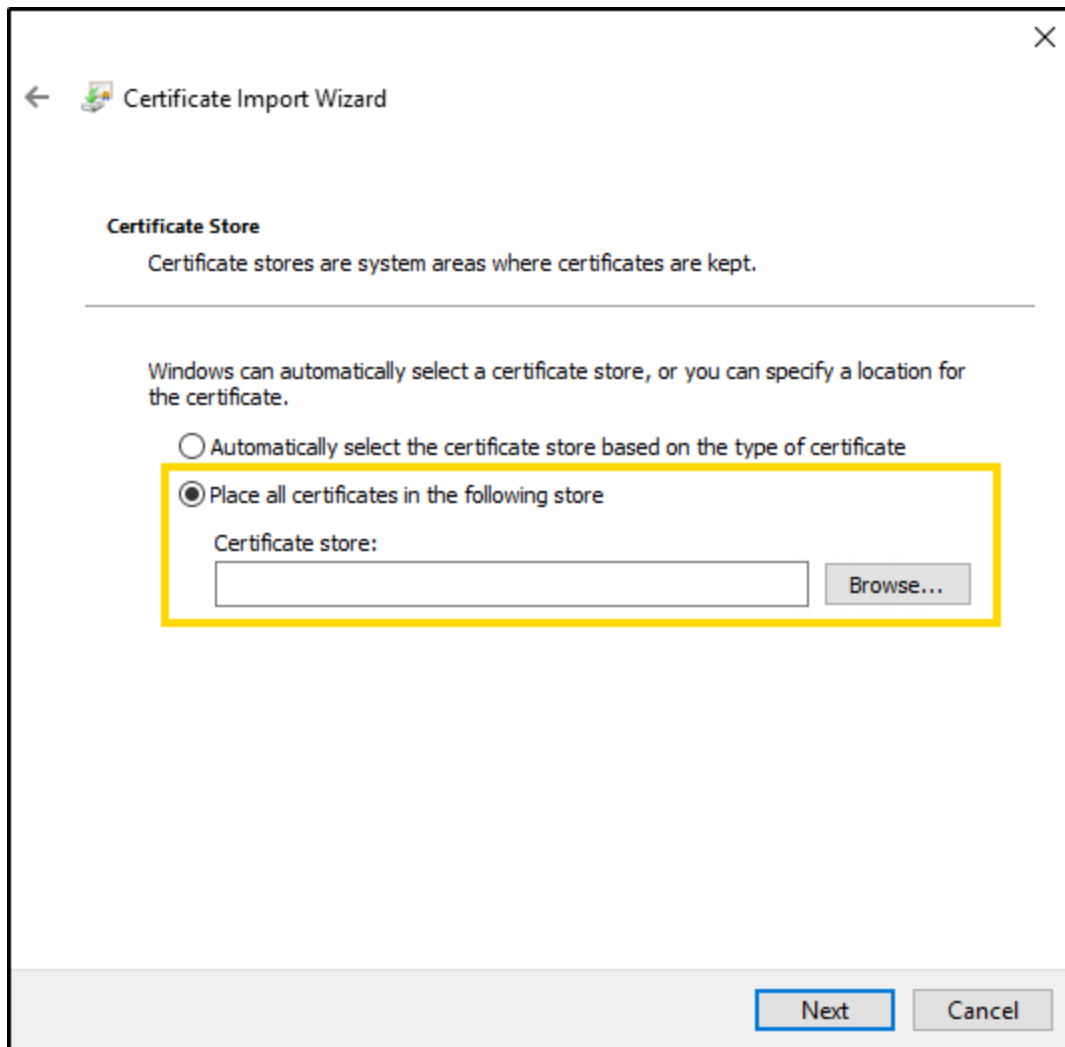
☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

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

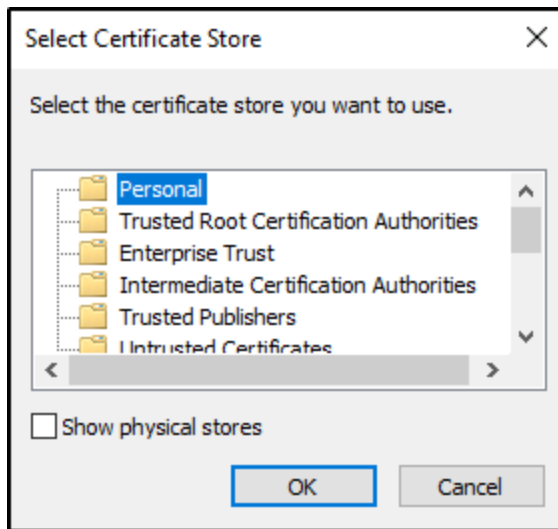
☒ Include all extended properties.

Next Cancel

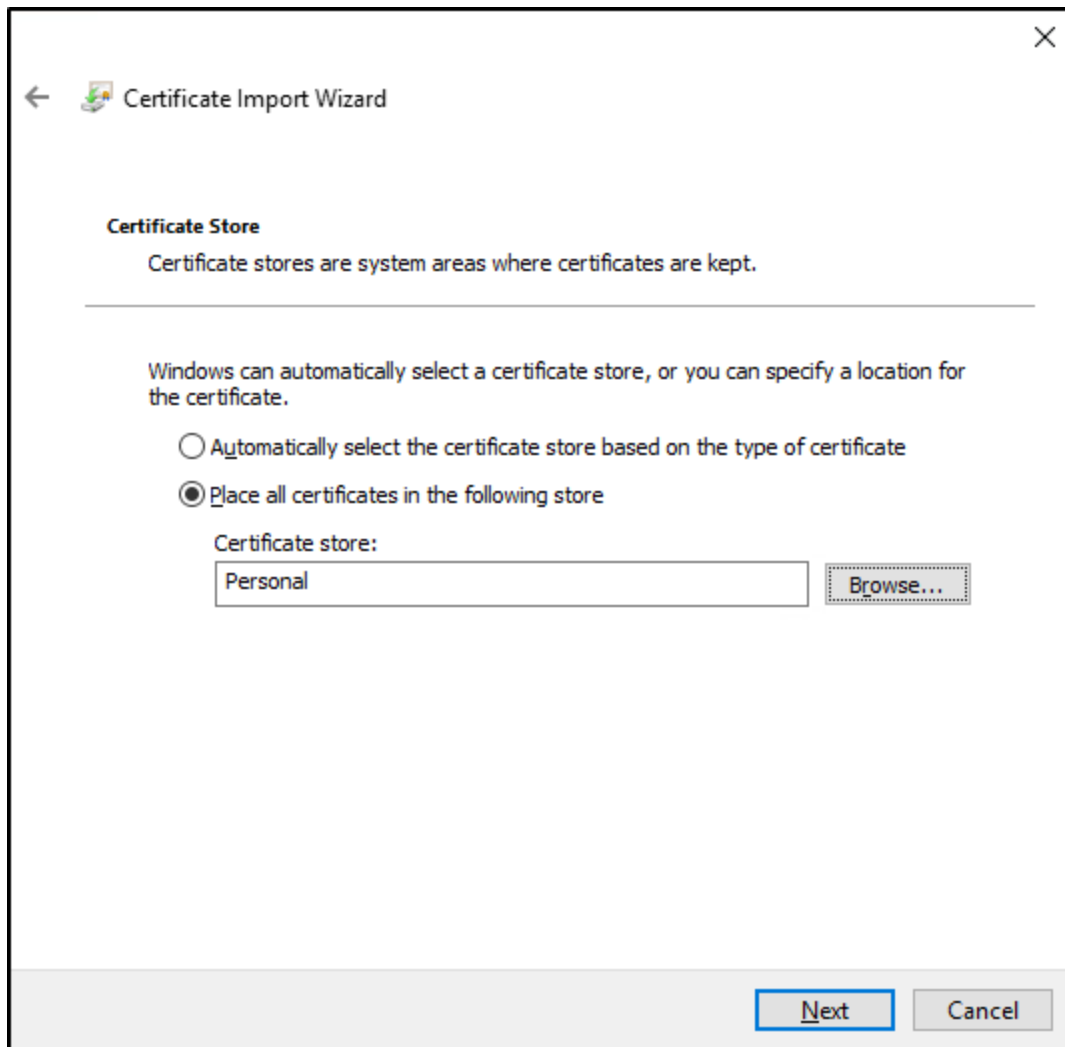
6. On the **Certificate Store** page, select **Place all certificates in the following store** and click **Browse...**



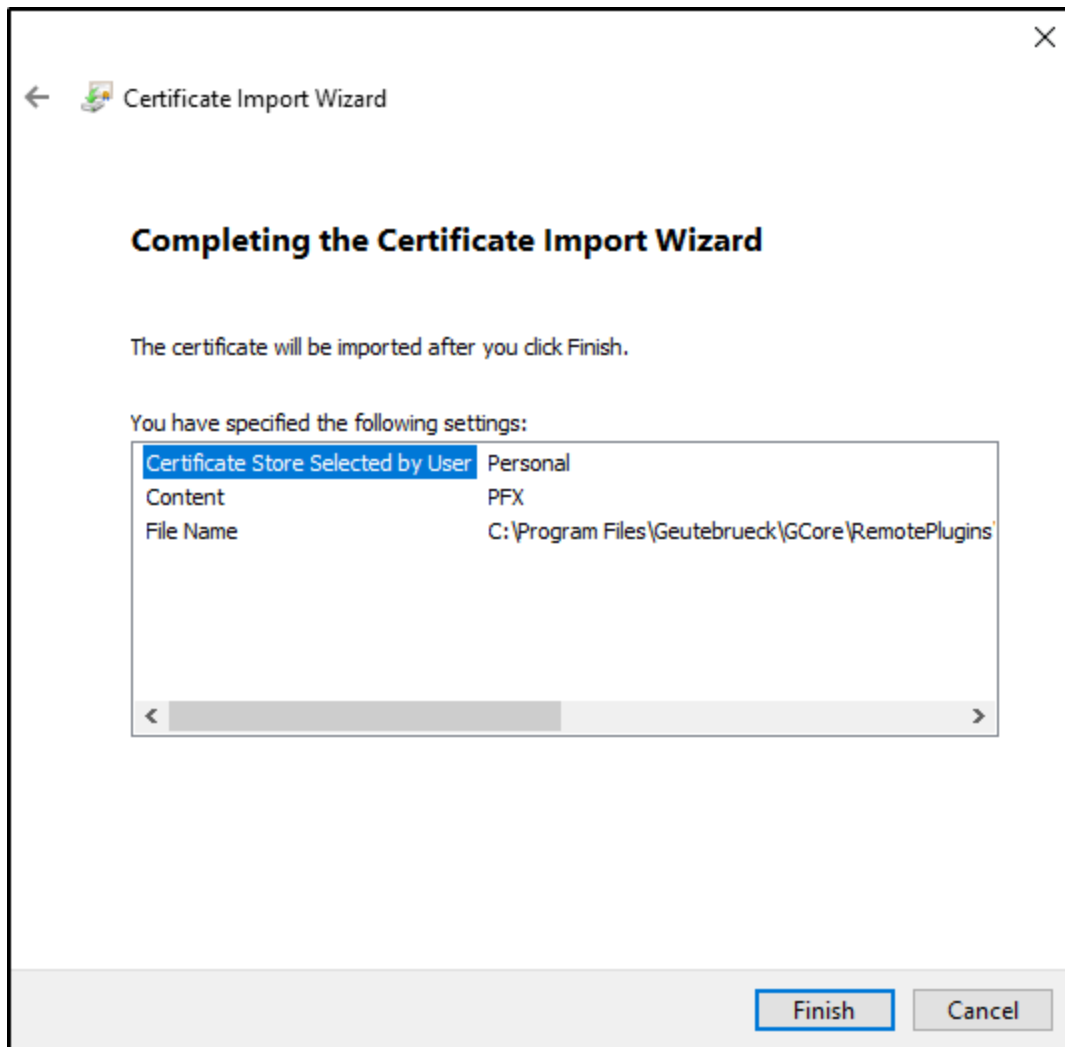
7. In the **Select Certificate Store** dialog, select the **Personal** folder and click **OK**.



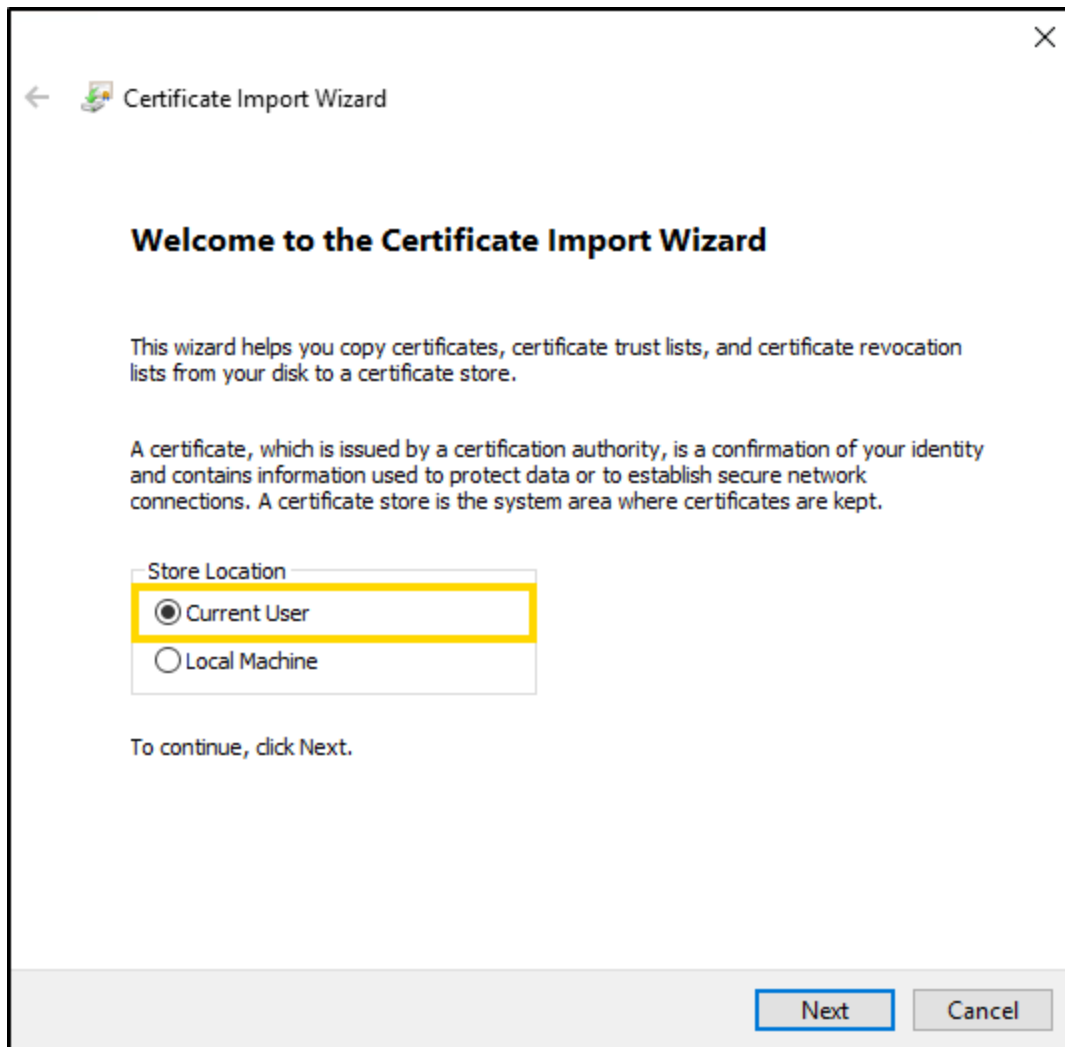
8. On the **Certificate Store** page, click **Next**.



9. On the Completing the Certificate Import Wizard page, click Finish.



10. Run the certificate file `child-Geutebrueck-.PluginLoader.Gateway.Auth.Root-<hostname>.pfx` again. The Certificate Import Wizard window opens.
11. On the **Welcome to the Certificate Import Wizard** page, select **Current User** and click **Next**.



12. Follow the steps described above again.
13. Restart the `Geutebrueck.PluginLoader.Service` service.

Linux Installation (Optional)

i The installation file for Linux installation is only available on request.

To use the Plugin Loader remotely at multiple sites, install the Plugin Loader component on the respective Linux remote servers (see **Install Plugin Loader**) and import the authentication certificate (see **Import Authentication Certificate**).



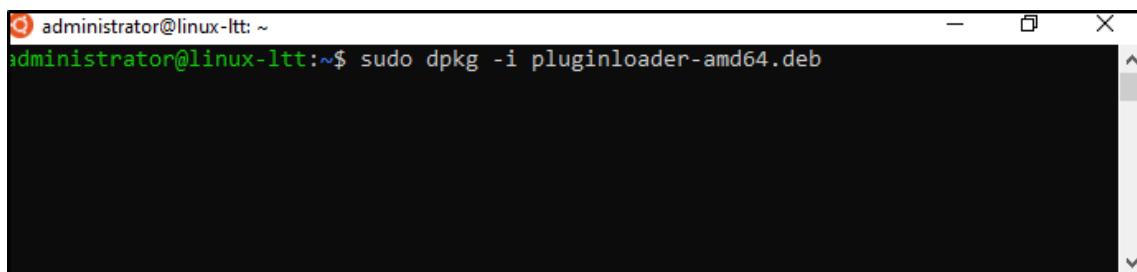
Requirements:

- Make sure that the Gateway is installed on the G-Core server and that port 15333 is open (see Local Installation).
- The Linux system must have the Debian Package Manager (dpkg).

Install Plugin Loader

Install the Plugin Loader on the Linux remote server.

1. Copy the installation file `pluginloader-amd64.deb` to the Linux server.
2. Run the `pluginloader-amd64.deb` using the command `dpkg -i pluginloader-amd64.deb`.



```
administrator@linux-ltt: ~  
administrator@linux-ltt:~$ sudo dpkg -i pluginloader-amd64.deb
```

3. In the Please enter the host of PluginLoader Gateway prompt **1**, enter the IP address of the G-Core server on which the Gateway is installed (see **Local Installation**).
4. Take the default values for the port of the Gateway and the Plugin Loader GUID by skipping the prompt with enter. If you change the GUID, you must specify a unique GUID.
5. In the Please enter the PluginLoader name prompt **2**, enter the name for your Plugin Loader.



The settings are saved at `/etc/geutebrueck-`

`/pluginloader/pluginloader_appsettings.json` and can also be changed in this `appsettings.json` file. If you change the settings in this file, you must restart the Plugin Loader service using the `systemctl restart pluginloader` command.

```
administrator@linux-itt: ~$ sudo dpkg -i pluginloader-amd64.deb
./ormals nicht ausgewähltes Paket pluginloader wird gewählt.
./lese Datenbank ... 224440 Dateien und Verzeichnisse sind derzeit installiert.)
./orbereitung zum Entpacken von pluginloader-amd64.deb ...
./ntpacken von pluginloader (1.1) ...
pluginloader (1.1) wird eingerichtet ...
Please enter the host of Pluginloader Gateway (default: localhost): 10.1.2.180
Please enter the port of Pluginloader Gateway (default: 15333):
Please enter the Pluginloader GUID (default: fbade2f8-51e5-4ecf-bdf6-d527192a954c):
Please enter the Pluginloader name (default: Default Plugin Loader): Linux pluginloader
Pluginloader URL: https://10.1.2.180:15333
Pluginloader Name: Linux pluginloader
Pluginloader GUID: fbade2f8-51e5-4ecf-bdf6-d527192a954c
Note: The config can also be changed at '/etc/geutebrueck/pluginloader/pluginloader.appsettings.json'.
Created symlink /etc/systemd/system/multi-user.target.wants/pluginloader.service → /etc/systemd/system/pluginloader.service.
administrator@linux-itt: ~$
```

6. You can query the status of the Plugin Loader using the `systemctl status pluginloader` command 1.
7. The Plugin Loader service is restarted after installation. You can restart the service manually using the `systemctl restart pluginloader` command 2.

```
administrator@linux-itt: ~$ sudo dpkg -i pluginloader-amd64.deb
./ormals nicht ausgewähltes Paket pluginloader wird gewählt.
./lese Datenbank ... 224440 Dateien und Verzeichnisse sind derzeit installiert.)
./orbereitung zum Entpacken von pluginloader-amd64.deb ...
./ntpacken von pluginloader (1.1) ...
pluginloader (1.1) wird eingerichtet ...
Please enter the host of Pluginloader Gateway (default: localhost): 10.1.2.180
Please enter the port of Pluginloader Gateway (default: 15333):
Please enter the Pluginloader GUID (default: fbade2f8-51e5-4ecf-bdf6-d527192a954c):
Please enter the Pluginloader name (default: Default Plugin Loader): Linux pluginloader
Pluginloader URL: https://10.1.2.180:15333
Pluginloader Name: Linux pluginloader
Pluginloader GUID: fbade2f8-51e5-4ecf-bdf6-d527192a954c
Note: The config can also be changed at '/etc/geutebrueck/pluginloader/pluginloader.appsettings.json'.
administrator@linux-itt: ~$ sudo dpkg -i pluginloader-amd64.deb
./lese Datenbank ... 225365 Dateien und Verzeichnisse sind derzeit installiert.)
./orbereitung zum Entpacken von pluginloader-amd64.deb ...
./ntpacken von pluginloader (1.1) über (1.1) ...
pluginloader (1.1) wird eingerichtet ...
Pluginloader URL: https://10.1.2.180:15333
Pluginloader Name: Linux pluginloader
Pluginloader GUID: fbade2f8-51e5-4ecf-bdf6-d527192a954c
Note: The config can also be changed at '/etc/geutebrueck/pluginloader/pluginloader.appsettings.json'.
administrator@linux-itt: ~$ systemctl status pluginloader
pluginloader.service - Geutebrueck Remote Plugin Loader
Loaded: loaded (/etc/systemd/system/pluginloader.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2024-02-21 15:14:46 CET; 1min 48s ago
Main PID: 6950 (RemotePlugins.P)
Tasks: 22 (limit: 9285)
Memory: 68.1M
CPU: 18.765s
CGroup: /system.slice/pluginloader.service
└─6950 /opt/pluginloader/RemotePlugins.Pluginloader.Service

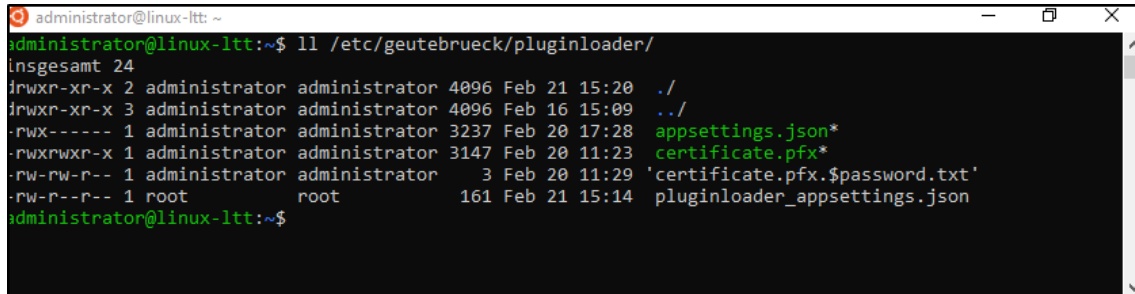
eb 21 15:16:27 linux-itt RemotePlugins.Pluginloader.Service[6950]: [D] Grpc.Net.Client: Sending message.
eb 21 15:16:27 linux-itt RemotePlugins.Pluginloader.Service[6950]: [T] Grpc.Net.Client: Serialized 'PluginCommandReturnValue' to 4 byte message.
eb 21 15:16:27 linux-itt RemotePlugins.Pluginloader.Service[6950]: [T] Grpc.Net.Client: Message sent.
eb 21 15:16:30 linux-itt RemotePlugins.Pluginloader.Service[6950]: [T] Grpc.Net.Client: Deserializing 124 byte message to 'PluginCommandWrapper'.
eb 21 15:16:30 linux-itt RemotePlugins.Pluginloader.Service[6950]: [T] Grpc.Net.Client: Received message.
eb 21 15:16:30 linux-itt RemotePlugins.Pluginloader.Service[6950]: [D] RemotePlugins.M: Plugin Command ClientAvailableParams @ 14 took 00:00:00.00007
eb 21 15:16:30 linux-itt RemotePlugins.Pluginloader.Service[6950]: [D] Grpc.Net.Client: Reading message.
eb 21 15:16:30 linux-itt RemotePlugins.Pluginloader.Service[6950]: [D] Grpc.Net.Client: Sending message.
eb 21 15:16:30 linux-itt RemotePlugins.Pluginloader.Service[6950]: [T] Grpc.Net.Client: Serialized 'PluginCommandReturnValue' to 2 byte message.
eb 21 15:16:30 linux-itt RemotePlugins.Pluginloader.Service[6950]: [T] Grpc.Net.Client: Message sent.

administrator@linux-itt: ~$ systemctl restart pluginloader
*** AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ***
Authentication is to restart the 'pluginloader.service' notwendig.
Authenticating as: administrator,, (administrator)
password:
*** AUTHENTICATION COMPLETE ***
administrator@linux-itt: ~$
```

Import Authentication Certificate

Import the authentication certificate to the Linux remote server.

1. After installing the Gateway on the G-Core server (see **Local Installation**), you will find the certificate files in the folder `C:\Program Files\Geutebrueck-\GCore\RemotePlugins\child-root`. Copy these .pfx and .txt files to the Linux remote server in the directory `/etc/geutebrueck/pluginloader/`.



```
administrator@linux-ltt: ~  
administrator@linux-ltt:~$ ll /etc/geutebrueck/pluginloader/  
insgesamt 24  
drwxr-xr-x 2 administrator administrator 4096 Feb 21 15:20 ./  
drwxr-xr-x 3 administrator administrator 4096 Feb 16 15:09 ../  
-rwx----- 1 administrator administrator 3237 Feb 20 17:28 appsettings.json*  
-rwxrwxr-x 1 administrator administrator 3147 Feb 20 11:23 certificate.pfx*  
-rw-rw-r-- 1 administrator administrator   3 Feb 20 11:29 'certificate.pfx.$password.txt'  
-rw-r--r-- 1 root root 161 Feb 21 15:14 pluginloader_appsettings.json  
administrator@linux-ltt:~$
```

2. If you import the certificate during the installation of the Plugin Loader, the Plugin Loader service is automatically restarted after the import. Otherwise, you must restart the service manually with the `systemctl restart pluginloader` command.

Failover Installation (Optional)

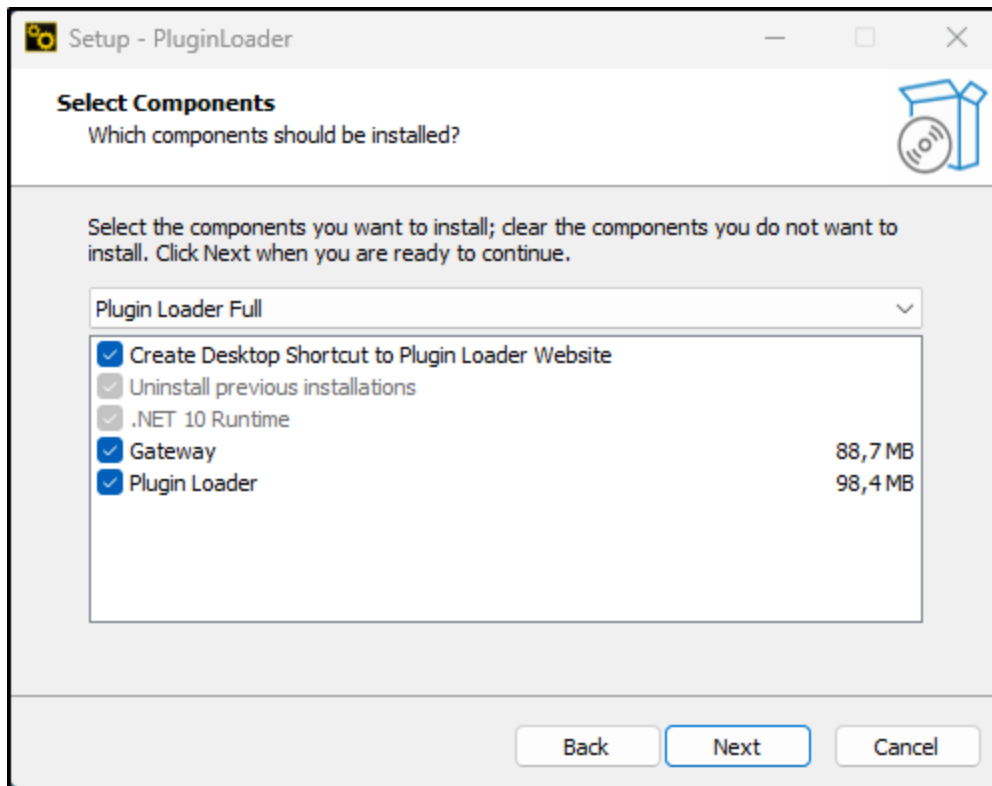
You can use the G-Core failover for the Plugin Loader. The Gateway checks whether a failover case occurs on the primary G-Core server. If the failover case occurs, the Gateway pushes all Remote Plugins to the connected Plugin Loader, regardless of the Plugin Loader ID, so that the G-Core spare device can use the plugins.

i Requirement:
G-SIM system with a primary G-Core server and configured spare devices. For more information on failover, see the G-SIM documentation.

Install the Gateway and the Plugin Loader on the G-Core server and on the respective G-Core spare devices.

1. Install the **Plugin Loader Full** installation (see **Local Installation**) on the G-Core server.
2. Install the **Plugin Loader Full** installation (see **Local Installation**) on the G-Core spare device.

i Install the Plugin Loader on all G-Core spare devices to avoid losing Plugin Loader channels on failover. If a failover occurs on a G-Core spare device without a Plugin Loader, the channels become unavailable.



3. In G-SIM, ensure that failover is configured. For more information on failover, see the G-SIM documentation.

Further configuration of the G-Core spare device is not necessary.

G-Insights Installation

Install NVIDIA CUDA Toolkit (Optional)

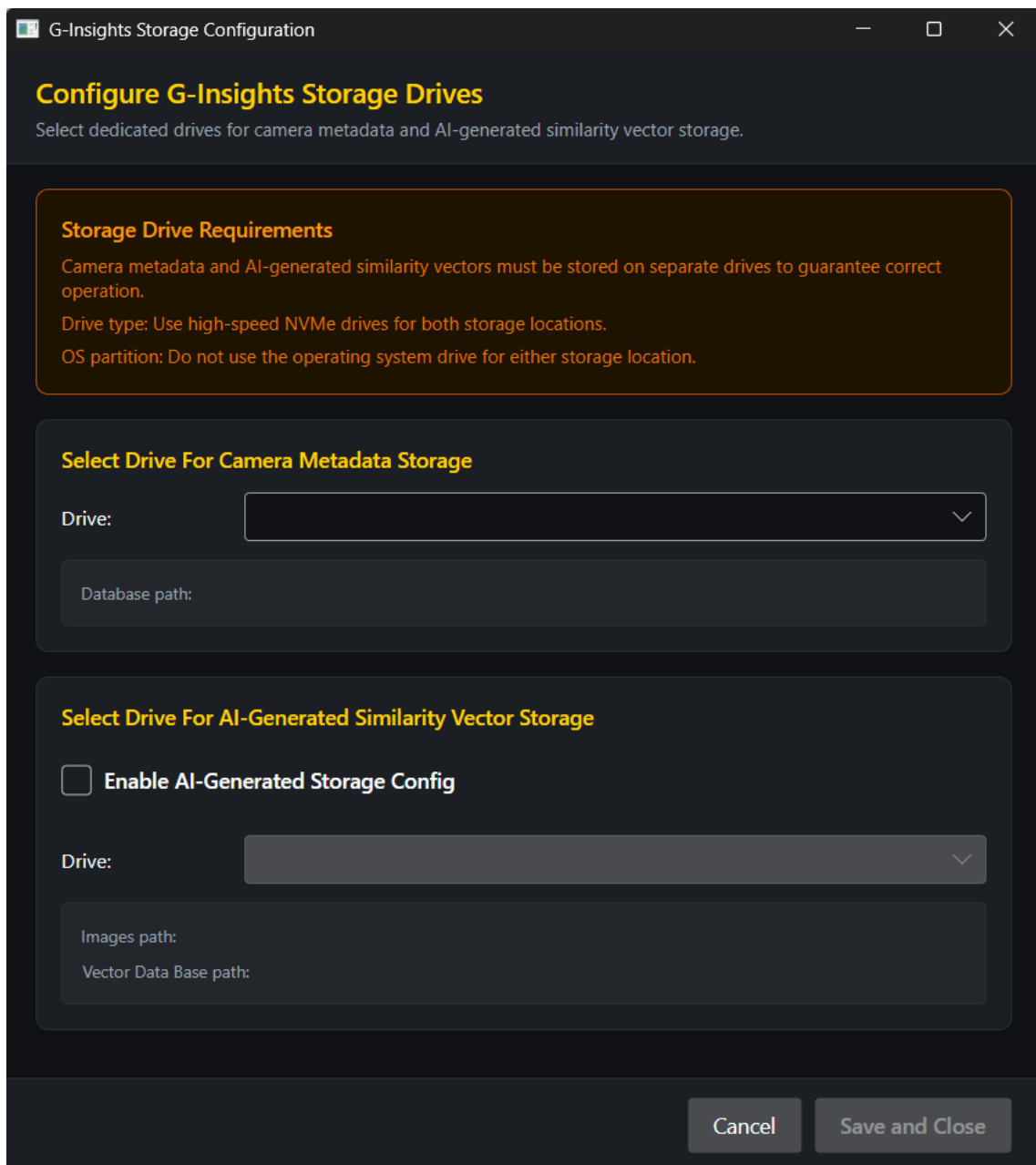
If you want to use the AI-powered similarity search, install the NVIDIA CUDA Toolkit on the server where you will install G-Insights. Tested with CUDA Toolkit version 12.9.

1. Download the NVIDIA CUDA Toolkit version 12.9.0 from the [CUDA Toolkit 12.9 Downloads](#) page.
2. Run the installer file.
3. Follow the installation steps. For more information, see the [CUDA documentation](#).
4. Complete the installation.

Install G-Insights

Install G-Insights on the G-Core server or a remote server.

1. Mount the `GInsights_Setup_xxx_main_xxx.iso` file. The virtual drive opens.
2. Run the `G-Insights_xxx.exe` file. The installation window opens.
3. On the **License Agreement** page, accept the agreement and click **Next**.
4. The **G-Insights Storage Configuration** dialog opens.
 - a. Select the drive for the camera metadata storage.
 - b. If you want to use the AI-powered similarity search, enable the **Enable AI-Generated Storage Config** option and select the drive for the AI-generated similarity vector storage.
 - c. Click **Save and Close**.



The image shows a 'G-Insights Storage Configuration' dialog box with a dark theme. At the top, the title bar says 'G-Insights Storage Configuration'. Below it, the main heading is 'Configure G-Insights Storage Drives' in yellow, followed by the instruction 'Select dedicated drives for camera metadata and AI-generated similarity vector storage.' in light gray. A yellow-bordered box contains 'Storage Drive Requirements' in bold, with three lines of text: 'Camera metadata and AI-generated similarity vectors must be stored on separate drives to guarantee correct operation.', 'Drive type: Use high-speed NVMe drives for both storage locations.', and 'OS partition: Do not use the operating system drive for either storage location.' Below this, there are two main sections. The first is 'Select Drive For Camera Metadata Storage' in yellow, containing a 'Drive:' dropdown menu, a 'Database path:' text field, and a 'Save' button. The second is 'Select Drive For AI-Generated Similarity Vector Storage' in yellow, containing an unchecked 'Enable AI-Generated Storage Config' checkbox, a 'Drive:' dropdown menu, 'Images path:' and 'Vector Data Base path:' text fields, and a 'Save' button. At the bottom right are 'Cancel' and 'Save and Close' buttons.

Configure G-Insights Storage Drives
Select dedicated drives for camera metadata and AI-generated similarity vector storage.

Storage Drive Requirements
Camera metadata and AI-generated similarity vectors must be stored on separate drives to guarantee correct operation.
Drive type: Use high-speed NVMe drives for both storage locations.
OS partition: Do not use the operating system drive for either storage location.

Select Drive For Camera Metadata Storage

Drive:

Database path:

Select Drive For AI-Generated Similarity Vector Storage

☐ Enable AI-Generated Storage Config

Drive:

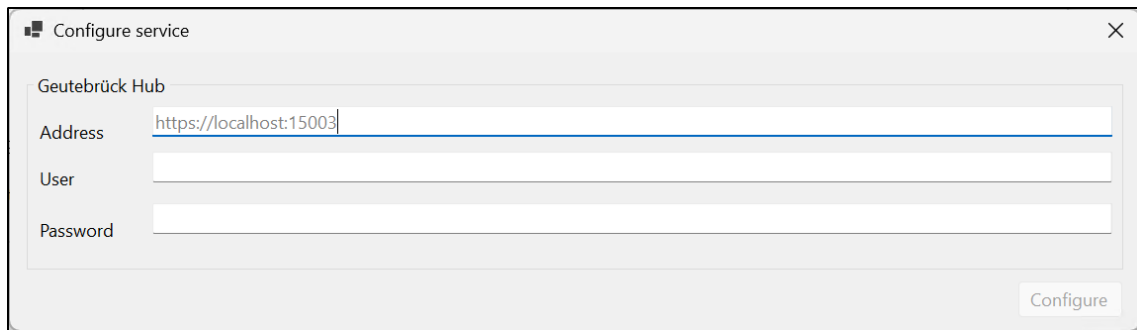
Images path:

Vector Data Base path:

Cancel Save and Close

5. On the **Ready to Install** page, click **Install**.
6. The **Configure service** dialog opens. Enter your Geutebrück Hub login details.
 - a. In the **Address** field, enter the IP address of the Geutebrück Hub. The default address is `https://localhost:15003`.

- b. In the **User** field, enter the e-mail address of the Geutebrück Hub user. The user must be an administrator or must have the Service Registration permission.
- c. In the **Password** field, enter the password of the Geutebrück Hub user.
- d. Click **Configure**.



7. A confirmation dialog appears. Click **OK**.
8. To complete the installation, restart the computer. Select **Yes, restart the computer now** or **No, I will restart the computer later** and click **Finish**.

Initial Setup

The initial setup of the installation components is part of the installation process and is required to use G-Insights. It is important to set up the components in the following order, as there are dependencies between the different components.

Set Up Plugin Loader

Add and configure your cameras.

1. Open Geutebrück Hub via the desktop icon.
2. Go to the **Resources** page. In the resources list, click the  icon of the resource named G-Core_xxx to open the Plugin Loader web interface.
3. On the Plugin Loader page, click **Connect** to connect the Plugin Loader to G-Set.
4. On the **Devices** page, add and configure the cameras (see **Add Device**).

5. Click **Save** to send your configuration to G-Core.
6. Click **Disconnect** to disconnect the Plugin Loader from G-Set.

Set Up G-SIM (Optional)

Set up the use of G-Insights in G-SIM in the Management Console.

i Requirement:
G-SIM and G-Insights must be connected to the same G-Core server.
The global channel numbers for the media channels must be identical in G-Core and G-SIM.

1. Open the Management Console.
2. Go to **Server setup > Server Licenses > Licensing**. In the details pane, enable the **Allow the usage of Web Browser feature** license.
3. Go to **Server setup > System Settings > Web Browser Management**. In the details pane, enable the **Use cookies in the Webbrowser** setting.
4. Go to **Server setup > System Settings > G-Insights**. In the details pane, configure the settings.
 - a. In the **Forensic Search URL** field, enter the following URL:

```
https://<localhost or ip address>:15003/<G-Insights ID>/search?mediachannel={mediachannel}&timestamp={timestamp}&x1={x1}&x2={x2}&y1={y1}&y2={y2}
```

- b. Replace `<localhost or ip address>` with the IP address of the server in which G-Insights is installed.
 - c. Replace `<G-Insights ID>` with the ID of G-Insights (e.g. 91455d0b-019d-8000-8000-000474943530). You can find the ID in the **ID** column of the resource list in the Geutebrück Hub or in the G-Insights URL.
 - d. In the **Rectangle Border Color** field, select the color you want the rectangle for the G-Insights Forensic Search to have in the Operator Console viewer.
5. Go to **Media Sources & Cameras > Camera Types**. In the item list, select a camera type.
 6. In the details pane, open the **Configuration** tab. Enable the **G-Insights Forensic Search Camera** option. Perform this step for all camera types that are allowed to use G-Insights Forensic Search.

7. Go to **Client Setup > Consoles**. In the item list, select the Operator Console that is allowed to use the G-Insights Forensic Search.
8. In the details pane, open the **Settings** tab. In the **Console Global Number** field, enter a console global number.

i You can enter any number other than 0. If the number is set to 0, the console does not allow remote actions.

9. Go to **Users & Security > Users**.
10. Configure a user who is allowed to use the G-Insights Forensic Search.
 - a. In the item list, add or select a user.
 - b. In the details pane, open the **Settings** tab. In the **E-Mail** field, enter the e-mail address of the user, which is also used in the Geutebrück Hub.

i The email address of the G-SIM user must be identical to the email address of the user in the Geutebrück Hub.

- c. In the details pane, open the **Privileges** tab. In the **Cameras and Video** section, enable the **Allow Forensic Search via G-Insights** privilege.
 - d. Perform this for all users who are allowed to use G-Insights Forensic Search.
11. Configure a G-SIM Web API user.
 - a. In the item list, add a user.
 - b. In the details pane, open the **Settings** tab. Enter **Name**, **Login Name** and **Password** for the user.
 - c. In the details pane, open the **Privileges** tab. In the **General / Control** section, enable the **Allow connection to G-SIM Web API** privilege. If this privilege is enabled for a user, all other privileges are disabled and the user cannot log in to the Management Console and make changes.
12. Click **Save** to save your configuration.

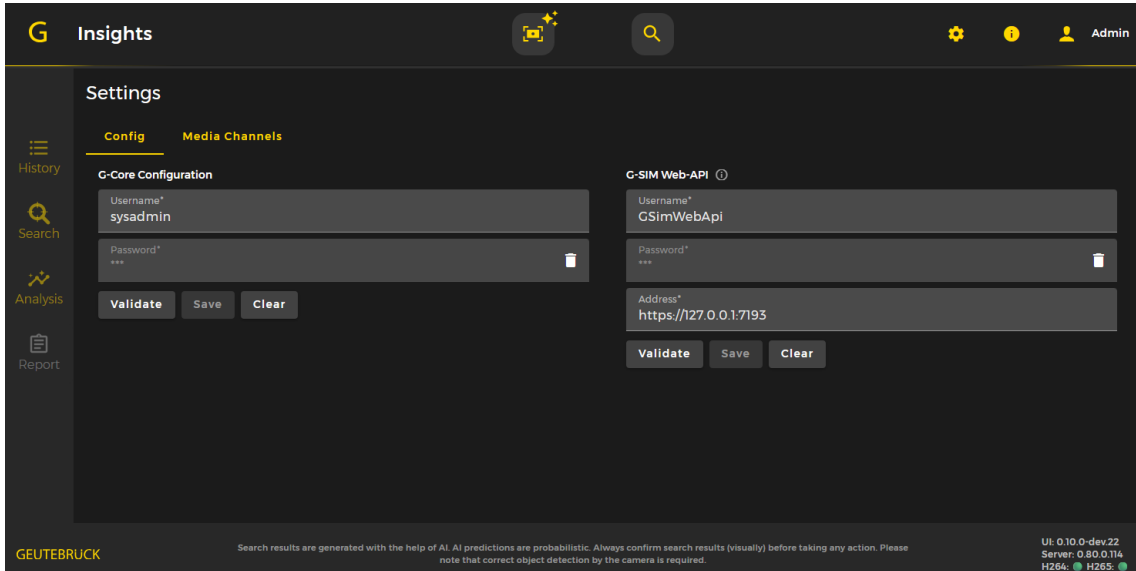
Set Up G-Insights

Set up the G-Insights settings for G-Core and, optionally, for G-SIM.

1. Open Geutebrück Hub via the desktop icon and go to **Settings > G-Insights** or click the  icon in the G-Insights toolbar. The G-Insights **Settings** page opens.

 **The G-Insights settings are only visible if you have the Edit G-Insights Settings permission and G-Insights is connected.**

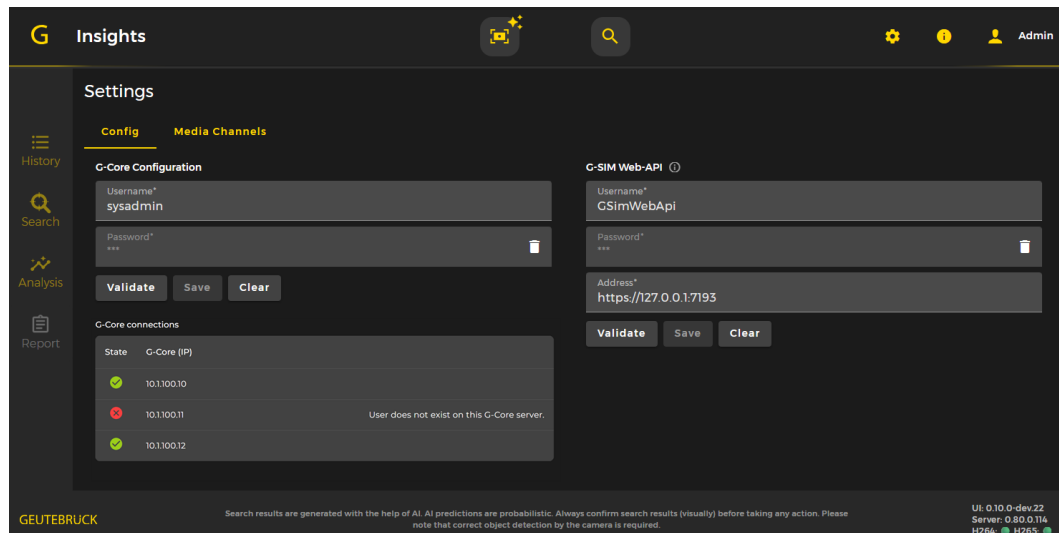
2. Go to the **Config** tab.



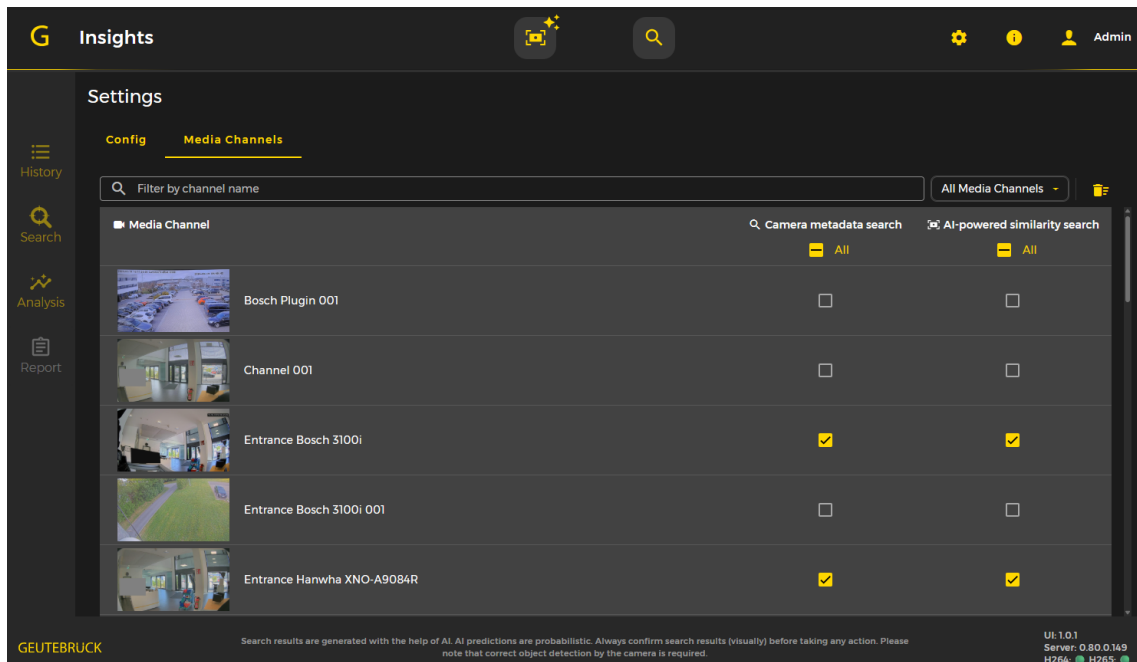
The screenshot shows the 'G Insights' settings page with the 'Config' tab selected. The page is divided into two main sections: 'G-Core Configuration' and 'G-SIM Web-API'. Each section contains input fields for 'Username', 'Password', and 'Address', along with 'Validate', 'Save', and 'Clear' buttons. The 'G-Core Configuration' section has a trash icon next to the password field. The 'G-SIM Web-API' section also has a trash icon next to the password field. The 'G-Core Configuration' section shows 'sysadmin' in the username field. The 'G-SIM Web-API' section shows 'GSimWebApi' in the username field and 'https://127.0.0.1:7193' in the address field. The page also features a sidebar with 'History', 'Search', 'Analysis', and 'Report' options, and a footer with the 'GEUTEBRÜCK' logo and version information.

3. G-Core Configuration (required):
 - a. Enter the **Username** and **Password** of G-Core.

 **All G-Core systems that you want to use in G-Insights must have a user with an identical username and password. Enter this username and password. These can be the default login details `sysadmin` and `masterkey`.**
 - b. Click **Validate**, to verify in which G-Core systems the specified user exists. The **G-Core connections** list appears, displaying all G-Core servers connected to the Geutebrück Hub and indicating whether the specified user exists.



- c. Click **Save** to save the G-Core configuration.
4. G-SIM Configuration (optional):
 - a. In the **Username** and **Password** fields, enter the username and password of the G-SIM user with the G-SIM Web API privilege (see **Set Up G-SIM (Optional)**).
 - b. In the **Host** field, enter the IP address and port of the G-SIM Web API (https://<localhost or ip address>:7193).
 - c. Click **Validate**, to verify the connection to the G-SIM Web API. If the connection is successful, a green check mark is displayed.
 - d. Click **Save** to save the G-SIM configuration.
5. Go to the **Media Channels** tab.
6. In the media channel list, enable the **Camera metadata search** option for the media channels you want to use in G-Insights. If you use AI-powered similarity search, also enable the **AI-powered similarity search** option.



7. Click **Save**.

Set Up Geutebrück Hub

Once you have completed the initial setup of the installation components, you can proceed with configuring the user management in the Geutebrück Hub.

1. Open Geutebrück Hub via the desktop icon.
2. On the **Resource Sets** page, add a resource set and assign resources to the set (see **Add Resource Set**).
3. On the **Permission Sets** page, add a permission set and select the permissions for the set (see **Add Permission Set**).
4. On the **Roles** page, add a role and assign permission sets and resource sets to the role (see **Add Role**).
5. On the **User Groups** page, add a user group and assign users and roles to the user group (see **Add User Group**).
6. On the **Users** page, add a user (see **Add User**).

Plugin Loader

Overview

With the Plugin Loader, you can integrate your camera devices into your G-Core system remotely and site-independent. You can connect several Plugin Loaders, which are distributed across different sites, to your G-Core system and control and manage them centrally.

Feature Overview

Device Management:

You can add and configure your camera devices via Remote Plugins and connect them to your G-Core system (see **Add Device**).

Event Mapping:

You can receive and use metadata from Geutebrück H-Series, Hanwha, Bosch or ONVIF Profile M cameras. The camera events are converted into the Geutebrück metadata format and mapped to predefined G-Core actions. You can also map the camera events to the G-Core actions manually (see **Add Custom Mapping**). For information on metadata mapping, see the PDF document [ONVIF Metadata Mapping](#).

SDK Development:

You can independently develop camera integrations for your Geutebrück system. With the provided **SDK Backend** and **SDK Frontend** you can develop custom plugins and integrate them into your system.

Plugin Features

This table lists the features of the Remote ONVIF Plugin and compares them with the G-Core ONVIF Plugin.

-  = Feature is supported.
 = Feature is not supported.

Feature	G-Core ONVIF Plugin	Remote ONVIF Plugin
General:		

Feature	G-Core ONVIF Plugin	Remote ONVIF Plugin
PTZ		
Area zoom and Click to move		
Multihead camera		
Video:		
Video streaming (H.264, H.265, JPEG)		
Dual streaming		
Dynamic live streaming (DLS)		
Dynamic stream selection (DSS)		
Audio:		
Audio streaming		
Audio backchannel (2-way audio)		
Event handling:		
Camera-side motion detection		
Event handling		
Event filter	per camera	per Plugin Loader
Event mapping to G-Core actions		
Additional:		
Digital inputs and outputs		
Edge recording		
Time synchronization		
Disable G-Core settings		

Upgrade

Upgrade 1.1 to 1.2

If you upgrade the Plugin Loader version 1.1 to 1.2, you must first uninstall version 1.1 and delete the installation directories. The Plugin Loader settings are saved in the `pluginloader_appsettings.json` file. Save this file to backup the settings.

Upgrade the Plugin Loader on the G-Core server (see **Local Installation**) and the Plugin Loader on a remote client (see **Remote Installation (Optional)**).

Upgrade Plugin Loader on G-Core server:

1. Save a backup copy of the `pluginloader_appsettings.json` file, which is located in the installation directory `C:\Program Files\Geutebrueck-\PluginLoader`.
2. Uninstall the **G-Core Hub** program via the Windows control panel.
3. Remove the installation directories `C:\Program Files\Geutebrueck-\PluginLoader` and `C:\Program Files\Geutebrueck-\GCore\RemotePlugins`.
4. Run the `PluginLoader_Installer_1.2.0.exe` on the G-Core server to install the Plugin Loader 1.2 (see **Local Installation**).
5. Replace the `pluginloader_appsettings.json` file in the installation directory `C:\Program Files\Geutebrueck\PluginLoader` with the backup copy.
6. Restart the **GCoreServer** and **Geutebrueck.PluginLoader.Service** service.

Upgrade Plugin Loader on remote client:

1. Save a backup copy of the `pluginloader_appsettings.json` file, which is located in the installation directory `C:\Program Files\Geutebrueck-\RemotePluginLoader`.
2. Uninstall the **Geutebrück PluginLoader** program via the Windows control panel.
3. Remove the installation directory `C:\Program Files\Geutebrueck-\RemotePluginLoader`.
4. Run the `PluginLoader_Installer_1.2.0.exe` on the remote client to install the Plugin Loader 1.2 (see **Remote Installation (Optional)**).

5. Replace the `pluginloader_appsettings.json` file in the installation directory `C:\Program Files\Geutebrueck\PluginLoader` with the backup copy.
6. Restart the `Geutebrueck.PluginLoader.Service` service.

Upgrade 1.2 to 1.3

If you upgrade the Plugin Loader version 1.2 to 1.3, you must first install G-Core 8.3 before installing the Plugin Loader 1.3. The Plugin Loader settings are saved in the `pluginloader_appsettings.json` file. Save this file to backup the settings.

Upgrade the Plugin Loader on the G-Core server (see **Local Installation**) and the Plugin Loader on a remote client (see **Remote Installation (Optional)**).

How to upgrade the Plugin Loader:

1. Install G-Core 8.3 on the G-Core server.



The problem may occur that outdated Plugin Loader files could not be completely removed and therefore G-Core cannot start. Proceed with the installation of Plugin Loader 1.3, which will update all relevant files and restart the G-Core server. After installation, check that G-Core has been restarted correctly with the new files.

2. Install the Plugin Loader 1.3 on the G-Core server (see **Local Installation**). The Plugin Loader installer restarts the G-Core service during installation.
3. Optional: Install the Plugin Loader 1.3 on the remote client (see **Remote Installation (Optional)**).

Using Plugin Loader

Open the Plugin Loader

With Geutebrück Hub connection:

In the Geutebrück Hub, go to the **Resources** page. In the resources list, click the



icon of the resource named `G-Core_XXX`.

Without Geutebrück Hub connection:

- On the G-Core server: `https://localhost:15333` or desktop icon
- On a remote server: `https://<hostname or host-ip>:15333`

Manage Devices

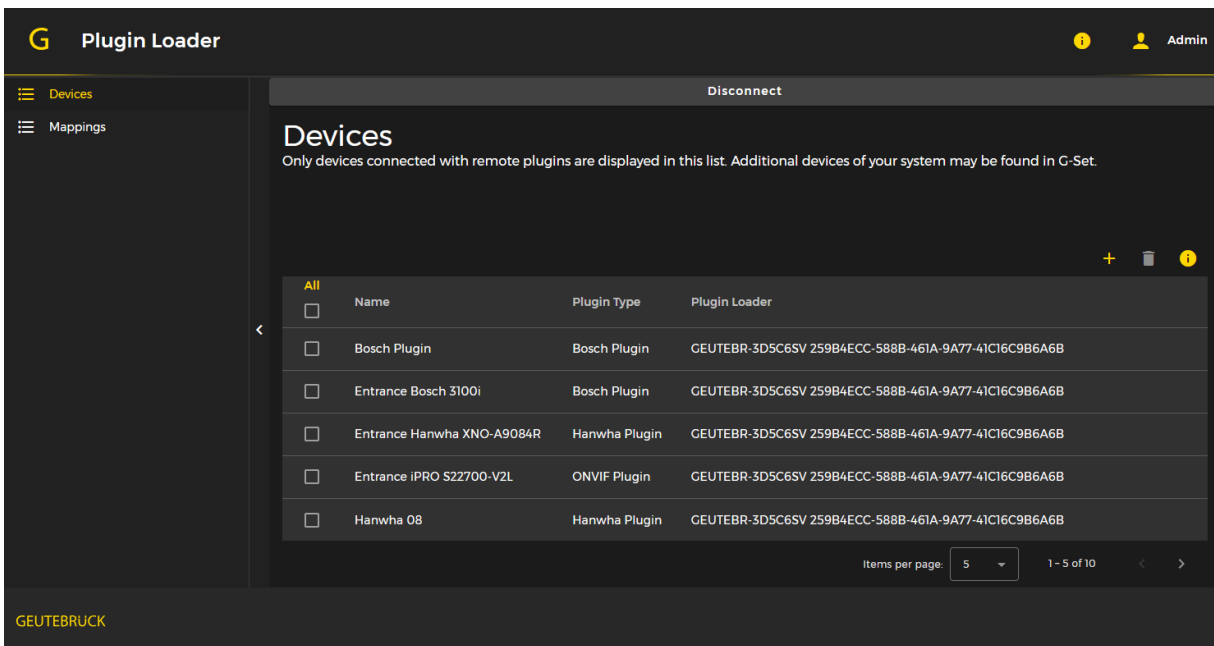
The **Devices** page provides an overview of all configured devices connected to G-Core via Remote Plugins.

The following information is listed:

- **Name:** Name of the Device.
- **Plugin Type:** Type of the selected Remote Plugin.
- **Plugin Loader:** Client ID of the selected Plugin Loader. Click the  icon to copy it to the clipboard.

 **The client ID is also specified in the `pluginloader_appsettings.json` file in the installation directory `C:\Program Files\Geutebrueck\RemotePluginLoader` of the respective Plugin Loader.**

If the selected Plugin Loader of a device is not available, the error message **Plugin loader unavailable!**  appears and the device cannot be edited. Make sure that the G-Core server and the `Geutebrueck.PluginLoader.Service` service are running and restart them if necessary.

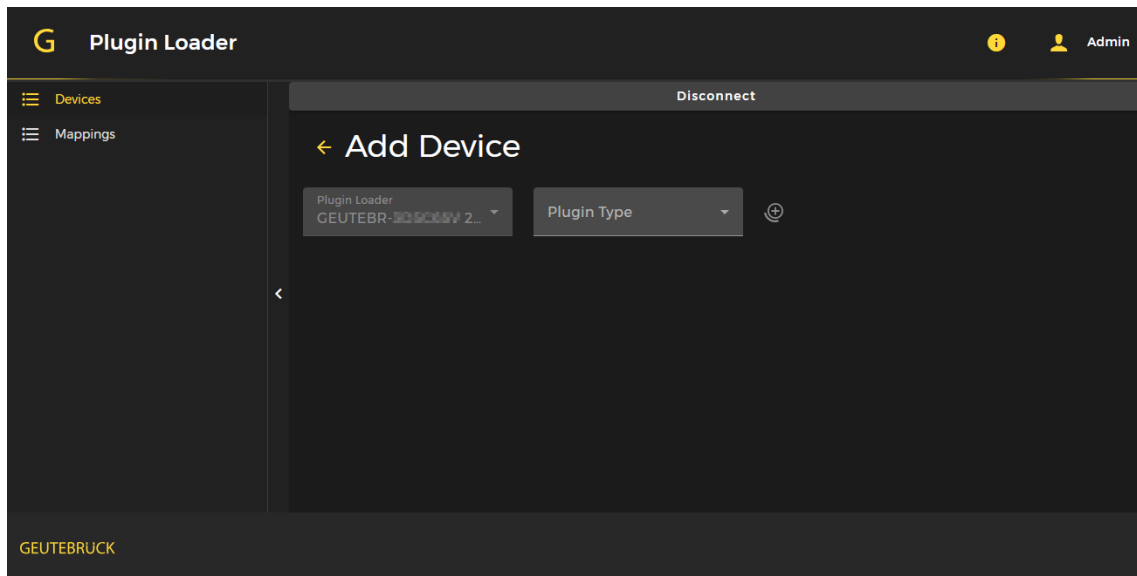


The screenshot shows the 'G Plugin Loader' application interface. On the left is a sidebar with 'Devices' and 'Mappings' options. The main area is titled 'Devices' and contains a table of connected devices. The table has columns for 'Name', 'Plugin Type', and 'Plugin Loader'. There are 5 items listed, all with the same Plugin Loader ID. At the bottom right, there is a pagination control showing 'Items per page: 5' and '1 - 5 of 10'.

Name	Plugin Type	Plugin Loader
Bosch Plugin	Bosch Plugin	GEUTEBR-3D5C6SV 259B4ECC-588B-461A-9A77-41C16C9B6A6B
Entrance Bosch 3100i	Bosch Plugin	GEUTEBR-3D5C6SV 259B4ECC-588B-461A-9A77-41C16C9B6A6B
Entrance Hanwha XNO-A9084R	Hanwha Plugin	GEUTEBR-3D5C6SV 259B4ECC-588B-461A-9A77-41C16C9B6A6B
Entrance iPRO S22700-V2L	ONVIF Plugin	GEUTEBR-3D5C6SV 259B4ECC-588B-461A-9A77-41C16C9B6A6B
Hanwha 08	Hanwha Plugin	GEUTEBR-3D5C6SV 259B4ECC-588B-461A-9A77-41C16C9B6A6B

Add Device

1. On the **Devices** page, click the **+** icon. The **Add Device** page opens.



2. In the **Plugin Loader** drop-down menu, select the Plugin Loader. If there is only one Plugin Loader, it is selected by default.
3. In the **Plugin Type** drop-down menu, select the plugin type. The **Edit Device** page opens.
4. In the **Device name** field, enter the name of the device.
5. Enter the **Connection Settings**:

Name	Description
Protocol	Select HTTP or HTTPS. If you are using HTTPS communication, you must set up the camera to use HTTPS. To do this, you must install or create a certificate on the camera.
Connection String	Enter the IP address or DNS name of the camera. i If you insert an URL such as <http/https>://<domain>:<port> the Protocol and Port will be filled in automatically.
Port	Enter the port of the camera.

Name	Description
	The port is determined by the selected protocol. If HTTP is selected, the default port automatically changes to 80 and if HTTPS is selected, the default port changes to 443. You can edit the port and enter the port of the camera.
RTSP Port	Enter the RTSP port of the camera. The default port is 554.
Username	Enter the username of the camera.
Password	Enter the password of the camera.

6. Click **Connect + Configure**.
7. Configure the camera sensors. The system automatically adds as many sensors as channels are available for the respective camera.
 - Click **+ Add Sensor** to manually add a sensor or click the  icon of the selected sensor to delete it. A maximum of 5 sensors can be added.
 - Activate or deactivate the **Disabled/ Enabled** slider, to enable or disable the selected sensor.
 - You can change the **Sensorname** of the selected sensor.
 - Click the  icon to apply the settings of the selected sensor to all sensors.
8. A new media channel is created for each sensor. You can also select a media channel from the **Media Channels** drop-down menu, which lists all available media channels from G-Core that are not already linked to a hardware.
9. Select the type of **Streaming Behaviour**:

Stream	Description
Single	Select this option to retrieve only one stream from the camera. The specified streaming settings apply to both the live stream and recordings.
Dual	Select this option to retrieve two streams from the camera, one for live stream and one for recordings. You can specify the streaming settings for both live stream and recordings

Stream	Description
	to avoid live stream and recordings using the same resolution.
DSS (Dynamic Stream Selection)	Select this option to not permanently bind the live and recording streams of G-Core to streams of the camera. Instead, multiple streams with different resolutions are configured in the camera. Depending on the requirements for the live and recording stream, one of them is selected. With this option, it is possible to switch between different resolutions depending on the event without creating a gap in the stream. Therefore, this option is recommended if you want event-driven changes in resolution.

10. Specify the settings for **Recording and live**:

Name	Description
Video codec	As video codec you can choose between H.264, H.265 and JPEG.
GOP size	With GOP (Group of Picture) size you can specify the ratio of IDR to P frames. The GOP size is internally adjusted to the configured frame rate, maintaining an interval of one second (e.g., a maximum GOP of 30 for 30 fps).
Protocol format	Select the transport protocol format: • TCP: Streaming communication with the camera takes place via port 554 by default. All communication (audio, video and control data) takes place only via this port. TCP is the preferred and best option of transport protocols. • UDP: With UDP, streaming also takes place via port 554, but video, audio and control data are transmitted via up to four additional ports. These ports are selected by the camera. Due to the higher number of ports and the associated firewall configuration issues, UDP is less suitable than TCP. • Multicast: With multicast, streaming also takes place

Name	Description
	via port 554. Audio, video and control data are streamed via an additional multicast address plus port. i Each camera in the network must be assigned to a unique multicast address. Multiple cameras must not be assigned to the same multicast address. It is possible for multiple cameras to use the same port, but they must not have the same multicast address because the primary separation in switches is performed using the multicast addresses. Using identical multicast addresses leads to network and device overload and incorrect display of the images. • HTTP: With HTTP, an RTSP stream is established via HTTP port 80 (RTSP and RTP via HTTP). In this case, the streaming protocol is established in the same way as with TCP, with the difference that port 80 is used instead of port 554, as this is not blocked by most firewalls. • HTTPS: With HTTPS, an encrypted RTSP stream is established via HTTPS port 443 (RTSP and RTP via HTTP). i Some cameras may not be able to support encrypted streaming. In this case, you need to select another transport protocol.
Constant / Variable	You choose between a variable bitrate and a constant bitrate. With a variable bitrate, the quality settings are used for the profile that is assigned to the media channel. A variable bitrate is generally recommended to ensure good image quality. However, if the stream should not exceed a certain bandwidth, you should use a constant bitrate.

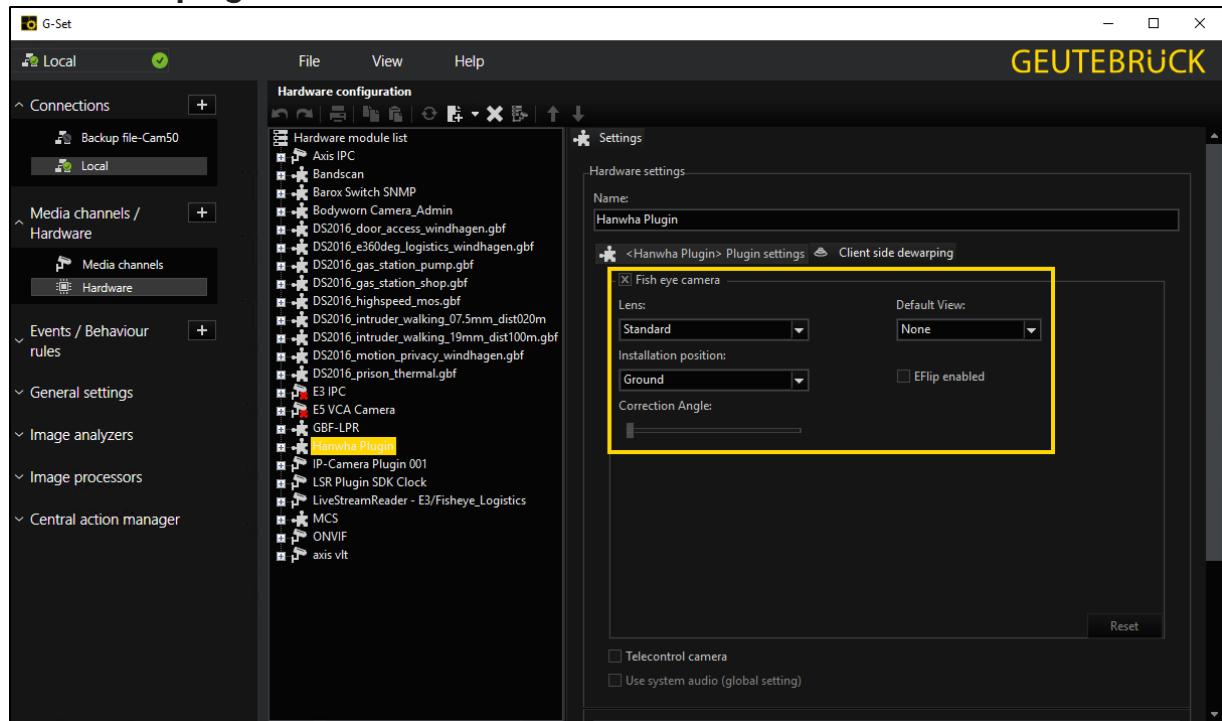
Name	Description
Bitrate	Enter the bitrate. You can choose between the unit kbit and mbit.
Merge behaviour	i Only for streaming behaviour Single. Select how the possibly different settings for live and storage under media channels are combined: • Best wins: The highest value specified in the corresponding settings is used for all parameters. • Worst wins: The worst value specified in the corresponding settings is used for all parameters. • Live wins: The settings for the live stream are used. • Storage wins: The settings for the storage are used. • Quality of storage wins but highest framerate: Resolution and quality are selected via the settings for the storage channel. The higher frame rate of the two, live or storage, is used.
Resolution	i Only for streaming behaviour DSS. Select which resolutions are to be set up in the camera.

11. Activate the **PTZ control** option, if your camera supports PTZ.
12. The device is added to the **Manage Devices** and your configuration is buffered. To complete your configuration and update G-Set, click **Save**.

The Remote Plugin and associated media channels are added in G-Set. Permanent recording is enabled per default for the added media channels.

i In G-Set, you can activate and configure the fisheye dewarping for the device. Select the corresponding Remote Plugin in the Hardware

module list and activate the Fish eye camera option on the Client side dewarping tab.



Create Multiple Devices

Create multiple devices based on the settings of an existing device.

1. On the **Edit Device** page, click the  icon or on the **Devices** page, hover your mouse over the row of the device you want to use as base for the multiple devices and click the  icon. The **Create Multiple Devices** page opens.

Some of your changes have not been sent to G-Core

Disconnect

← Create Multiple Devices

Create multiple devices based on an existing device.

Plugin Loader: GEUTEBR-XXXXXXXX-XXXX

Plugin Type: H-Series Plugin

Configuration

Device Name* H-Series Plugin 1

First IP*

Amount of Devices* 1

Last IP*

User name

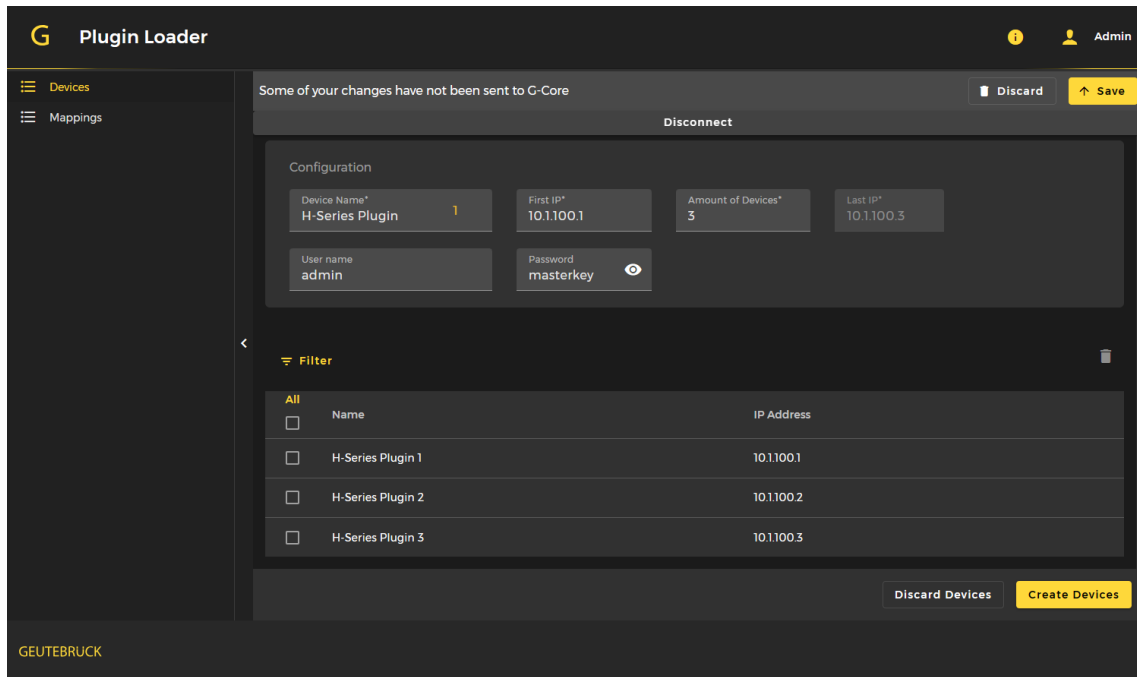
Password

GEUTEBRUCK

2. Enter the settings for the multiple devices:

Name	Description
Device Name	Enter the name of the device and the index with which the name of the first in the list of devices to be created should begin.
First IP	Enter the IP address with which the first device in the list of devices to be created should begin. The IP address is incremented for all subsequent devices. The list of devices to be created appears.
Amount of Devices	Specify the number of devices you want to create. You can create a maximum of 64 devices at the same time. i Note that if you change the number of devices, the multiple device list will be updated and any changes you have already made will be discarded.
Last IP	The IP address of the last device in the list of devices to be created.
User name	Specify a username that is used for all devices to be created (optional).
Password	Specify a password that is used for all devices to be created (optional).

3. The list of devices to be created appears if you have specified the **First IP**.



4. To edit the settings of a device, click in the row of the respective device. The **Edit Device** dialog opens. Edit the settings of the device (see **Add Device**) and click **Submit**.
5. To delete a device, select one or more devices by selecting the respective checkboxes and click the  icon.
6. Click **Create Devices**.

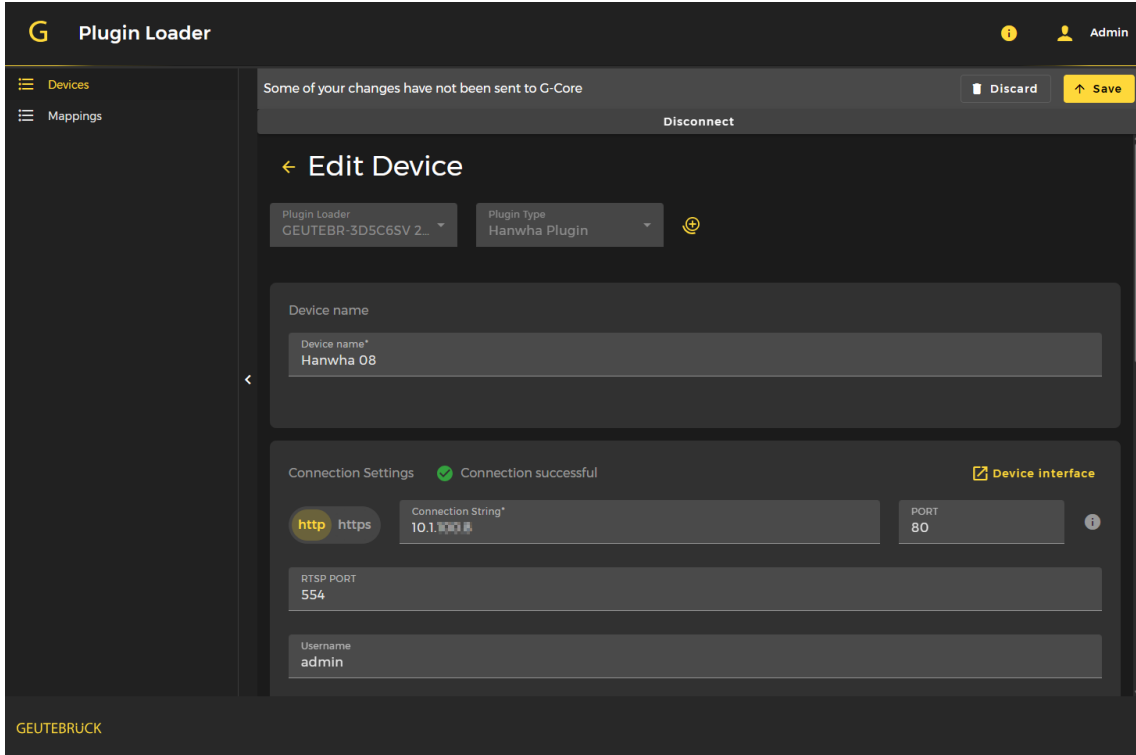
 **If you do not click **Create Devices**, the devices are prepared but not created. In the Manage Devices and the Add Device view,**

an indicator appears next to the  icon showing how many multiple devices are prepared for the selected device. Click the drop-down menu icon and select whether you want to  Edit or  Delete the prepared devices.

7. The devices are added to the **Manage Devices** and your configuration is buffered. To complete your configuration and update G-Set, click **Save**.

Edit Device

1. On the **Devices** page, hover your mouse over the row of the device you want to edit and click the  icon. The **Edit Device** page opens.



The screenshot shows the 'Edit Device' page in the 'Plugin Loader' web interface. The page has a dark theme. At the top, there's a header with a 'G' logo, 'Plugin Loader' text, and a user profile 'Admin'. Below the header, a sidebar on the left contains 'Devices' and 'Mappings' links. The main content area has a title 'Edit Device' with a back arrow. Below the title, there are two dropdown menus: 'Plugin Loader' (set to 'GEUTEBR-3D5C6SV 2...') and 'Plugin Type' (set to 'Hanwha Plugin'). A yellow warning icon is next to the 'Plugin Type' dropdown. Below these, there's a 'Device name' field with the value 'Hanwha 08'. Further down, there's a 'Connection Settings' section with a green checkmark and the text 'Connection successful'. To the right of this section is a 'Device interface' link. The 'Connection Settings' section includes a protocol selector (set to 'http'), a 'Connection String*' field (containing '10.1.100.1'), a 'PORT' field (containing '80'), an 'RTSP PORT' field (containing '554'), and a 'Username' field (containing 'admin'). At the bottom left, the text 'GEUTEBRUCK' is visible.

2. Edit the device settings (see **Add Device**).
3. Your configuration is buffered. To complete your configuration and update G-Set, click **Save**.

The Remote Plugin and associated media channels are updated in G-Set.



IMPORTANT: Do not manually add a Remote Plugin in G-Set and do not make any changes to the plugin settings. The plugin should only be added and changed via the Plugin Loader web interface.

Delete Device

1. On the **Devices** page, select the device you want to delete by selecting the checkbox.
2. Click the  icon.

3. A confirmation dialog opens. Click **Confirm**.
4. To complete your configuration and update G-Set, click **Save**.

Use CameraRAWOutput Action

The `CameraRAWOutput` action enables you to send HTTP requests to a camera, allowing you to interact with the settings or functions of the camera via raw HTTP requests.

Parameters

The action uses a combination of parameters to define the request details.

Parameter	Description
Camera (required)	Specify the camera to which the request should be sent. You can use a unique identifier or a name. Example: <code>Camera: {2, 1, "ONVIF Plugin 001"}</code>
Output (required)	Specify the relative URL path to which the HTTP request should be sent. This is the path component of the base URL of the camera for the HTTP request. Example: <code>Output: "/cgi-bin/admin/param.cgi?action=update&Image.I0.Text.String=Example"</code>
HTTPRequestMethod (optional)	Specify the HTTP method to be used for the request. The following methods are possible: • <code>GET</code>: Retrieves data from the camera (default). • <code>POST</code>: Sends data to the camera. Example: <code>HTTPRequestMethod: "POST"</code>
HTTPRequestBody (optional)	Specify the message body content to be sent with the HTTP request. This is used with <code>POST</code> requests. Specify the parameters or data to be included in the message body of the request. Example: <code>HTTPRequestBody: "param=value"</code>

Behavior

If the **Output** parameter is set, the Plugin Loader constructs the URL to send the request. The protocol (`http` or `https`), host/IP address and port are derived from the plugin configuration for the selected camera.

If only **Output** is specified, a GET request is sent to `<protocol>://<host>:<port><Output>`.

- `<protocol>` is determined from the plugin configuration (either `http` or `https`).
- `<host>` and `<port>` are taken from the plugin configuration.
- `<Output>` is the specified path component.

If **HTTPRequestMethod** is set to `POST`, then **HTTPMessageBody** is used to define the content of the request messagebody.

Example

GET request

```
CameraRAWOutput (Camera: { 2, 1, "ONVIF Plugin 001" }, Out-  
put: "/cgi-bin/ad-  
min/param.cgi?action=update&Image.I0.Text.String=Hallo  
Review")
```

This sends a GET request to:

```
<protocol>://<host>:<port>/cgi-bin/ad-  
min/param.cgi?action=update&Image.I0.Text.String=Example
```

Example

POST request with message body

```
CameraRAWOutput (Camera: { 2, 1, "ONVIF Plugin 001" }, Out-  
put: "/cgi-bin/path?param=value", HTTPRequestMethod:"POST",  
HTTPMessageBody:"param=value")
```

This sends a POST request to:

```
<protocol>://<host>:<port>/cgi-bin/path?param=value
```

The request message body contains param=value.

Manage Mappings

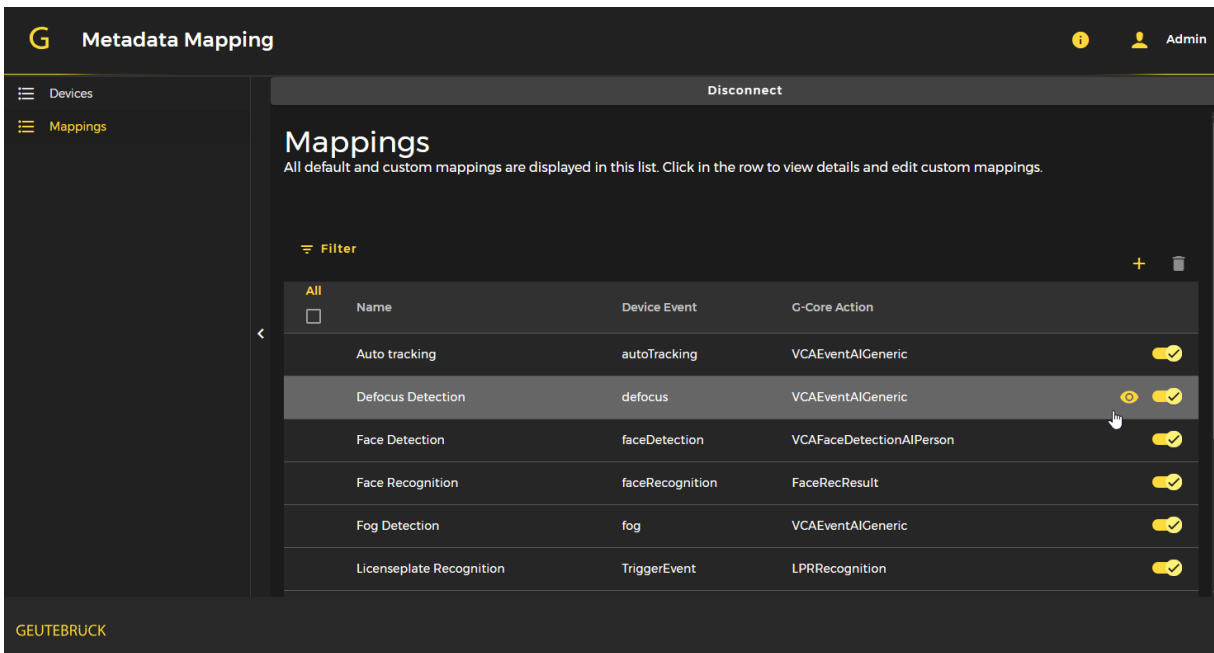
The **Mappings** page provides an overview of all default and custom mappings.

The following information is listed:

- **Name:** Name of the mapping.
- **Device Event:** Name of the mapped device event.
- **G-Core Action Name:** Name of the mapped G-Core action.

Default mappings are marked with the  icon. Click on the row to display the predefined settings.

Activate or deactivate a mapping by toggling the slider. Activated mappings are applied to all available cameras connected with remote plugins (see **Manage Devices**).

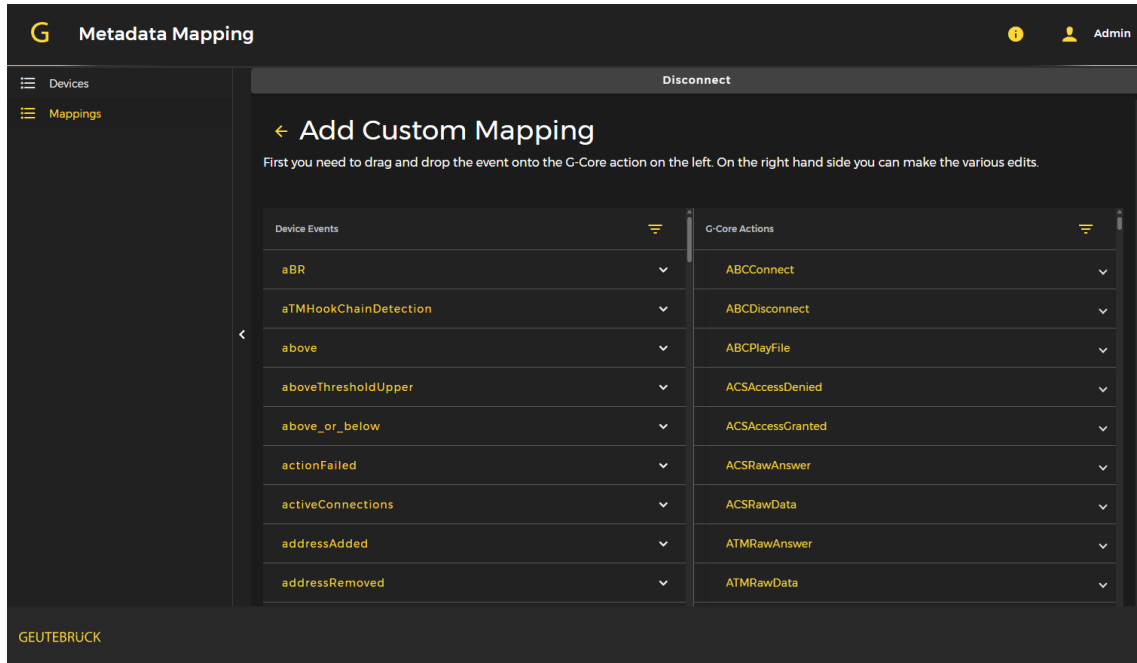


The screenshot shows the 'Metadata Mapping' page in a web application. The page has a dark theme. On the left is a sidebar with 'Devices' and 'Mappings' (selected). The main area is titled 'Mappings' and contains a table of mappings. The table has columns: Name, Device Event, G-Core Action, and a toggle switch. The 'Defocus Detection' row is highlighted, and its toggle switch is being clicked by a mouse cursor. The bottom of the page shows the 'GEUTEBRUCK' logo.

Name	Device Event	G-Core Action	Toggle
Auto tracking	autoTracking	VCAEventAIGeneric	On
Defocus Detection	defocus	VCAEventAIGeneric	On
Face Detection	faceDetection	VCAFaceDetectionAllPerson	On
Face Recognition	faceRecognition	FaceRecResult	On
Fog Detection	fog	VCAEventAIGeneric	On
Licenseplate Recognition	TriggerEvent	LPRRecognition	On

Add Custom Mapping

1. On the **Mappings** page, click the **+** icon. The **Add Custom Mapping** page opens.



2. Map a device event from the **Device Events** list to a G-Core action in the **G-Core Actions** list using drag and drop. The **Edit Custom Mappings** page opens.
3. Specify the **Essentials** settings:

Essentials

Mapping Name*
VCACountingAIOObject - counting

Extensions
counting ×

G-Core Action
VCACountingAIOObject

Condition
e.g. class == "person"

Name	Description
Mapping Name	Specify the name of the mapping. The default name is composed of <G-Core Action> - <Device Event>.
Extensions	Click in this field and select the extensions you want to add to your mapping from the drop-down menu.
G-Core Action	Name of the G-Core action (not editable).
Condition	Specify which extension data should be displayed for an event.

- You can select an extension value for each **G-Core Action Parameter** to display only this value for the action parameter. The value for the parameter **Channel** is set by default and cannot be selected.

G-Core Action Parameter
Direction

Default
Extended

counting
^
name
countingIndex
reportType
objectType
count

class

imagePos

Value
counting.countingIndex
X

If you want to select multiple values for a G-Core action parameter, click on the **Extended** slider. Enter the values in the **Custom value** input field. To enter a custom value, use the Scriban scripting language. Click on the **i** icon at the top right to display examples of custom values.

G-Core Action Parameter
Direction

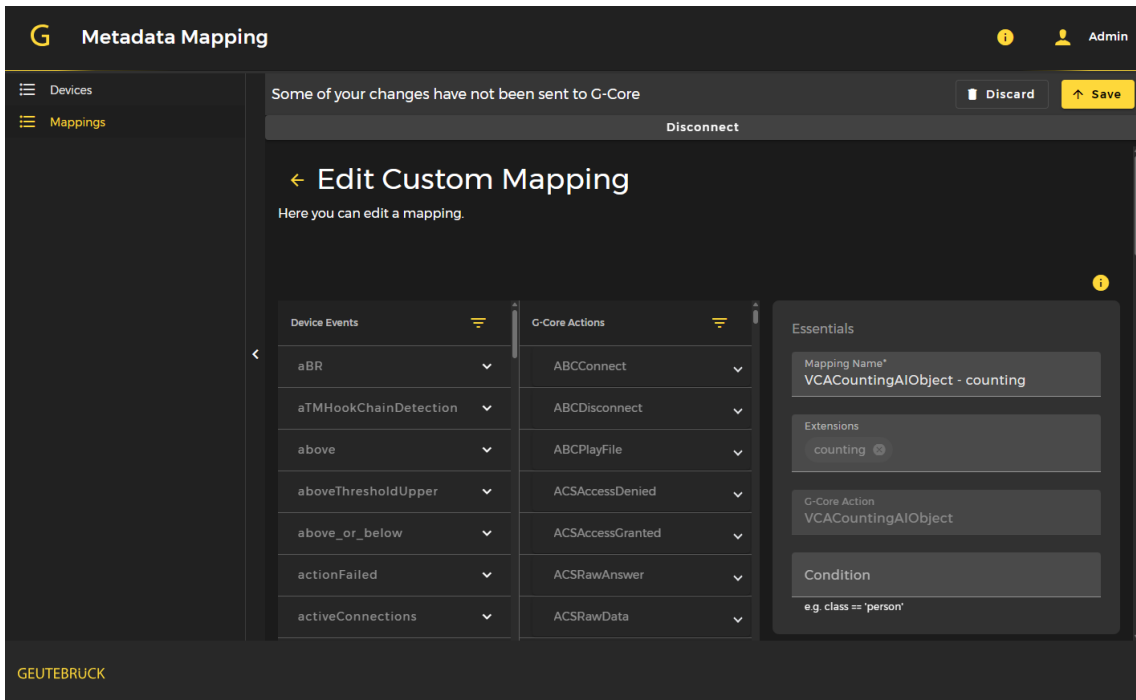
Default
Extended

Custom value

5. The mapping is added to the **Manage Mappings** and your configuration is buffered. To complete your configuration and update G-Set, click **Save**.

Edit Custom Mapping

1. On the **Mappings** page, hover your mouse over the row of the custom mapping you want to edit and click the  icon. The **Edit Custom Mapping** page opens.



2. Edit the mapping settings (see **Add Custom Mapping**).
3. Your configuration is buffered. To complete your configuration and update G-Set, click **Save**.

Delete Custom Mapping

1. On the **Mappings** page, select the custom mapping you want to delete by selecting the checkbox.
2. Click the  icon.
3. A confirmation dialog opens. Click **Confirm**.
4. To complete your configuration and update G-Set, click **Save**.

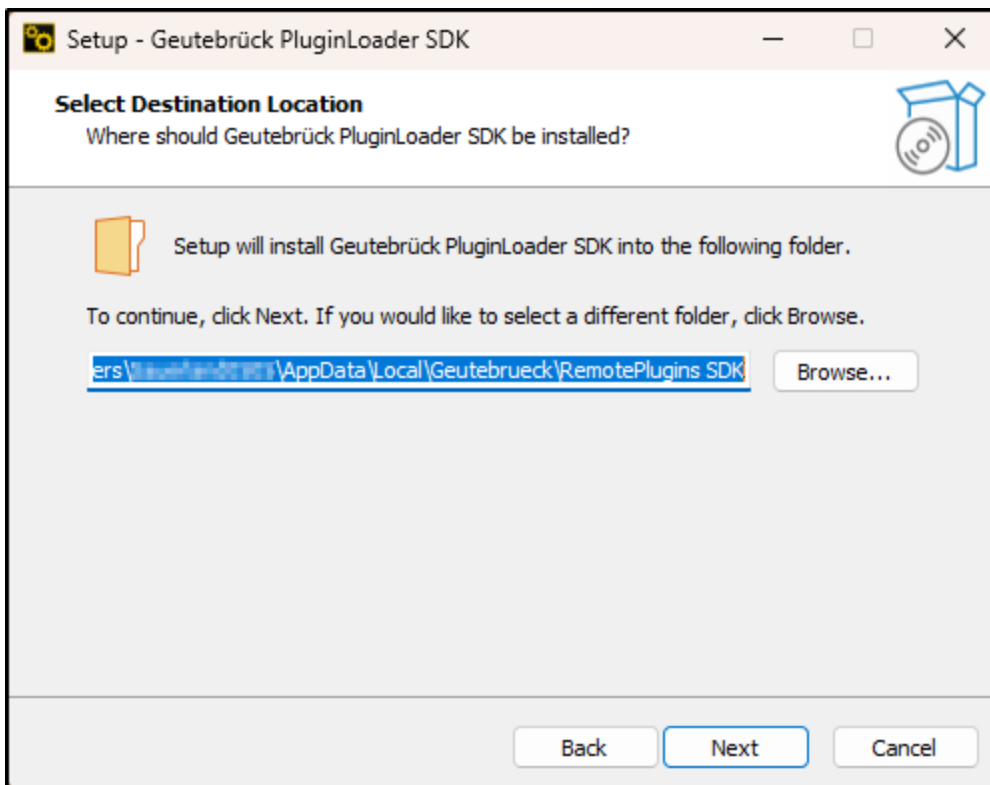
Development

SDK Installation

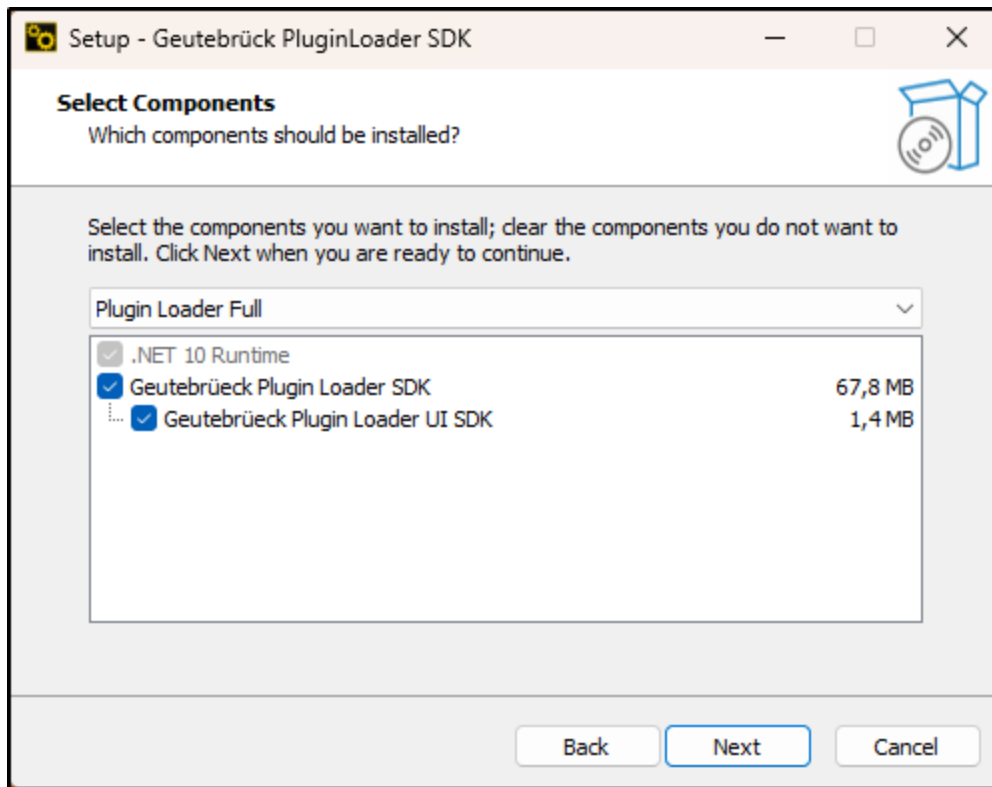
 **The installer for SDK installation is only available at sdk.geutebrueck.com.**

To develop your own Remote Plugins, install the Plugin Loader SDK. The SDK installer contains several example projects to explain different workflows (ImageModules, PTZ and I/Os) of the Remote Plugin architecture. It also contains a Plugin Loader Simulator that can be used to test newly developed plugins directly without the need of an entire G-Core system.

1. Run the Geutebrück PluginLoader SDK_xxx.exe file. The installation window opens.
2. On the **License Agreement** page, accept the agreement and click **Next**.
3. On the **Select Destination Location** page, you can change the installation path and click **Next**.



- On the **Select Components** page, select the components you want to install and click **Next**.



- On the **Ready to Install** page, click **Install**.
- When the installation is complete, click **Finish**.

SDK Backend

i You can also find this technical documentation for the SDK backend in the `README.md` file in the installation directory of the SDK.

Components

A Remote Plugin consists of the following components:

Component	Description
Plugin	The main instance of the Remote Plugin. Manages the entire life cycle of an instance of the Remote Plugin and instantiates modules.

Component	Description
Plugin provider	Provides information about the plugin. Aggregates metadata and default settings.
Module	Processes events and commands of an interaction category. - Image modules stream image data from a camera to the server (IImageModule). - IO modules handle input/output capabilities of a camera (IIOModule). - PTZ modules forward pan, tilt, and zoom capabilities to a camera as commanded by an operator (IPtzModule).
Individual settings	Represents the individual configuration of the plugin.

Interfaces

The following interfaces must be considered during SDK development:

Interface	Description
IPluginProvider	Provides information about the plugin. Aggregates metadata and default settings.
RemotePluginBase IImagePlugin	These interfaces are crucial for creating a plugin. They contain basic methods about the ID, information, and modules that a plugin can contain, as well as methods for creating and retrieving modules.
ImageModuleBase	In order to add modules for plugins, this interface must be inherited so that it is possible to work with the streams.
IImageStreamer	This interface is used by plugins to push the images.

Write a Remote Plugin

These imports are used in the following example:

```
using Google.Protobuf.WellKnownTypes;
using Google.Protobuf;
```

```

using Microsoft.Extensions.DependencyInjection;
using RemotePlugins.Api.Interfaces;
using RemotePlugins.Api.Structures.Enums;
using RemotePlugins.Sdk;
using RemotePlugins.Sdk.Modules;
using SkiaSharp;
using RemotePlugins.Api.Structures;

```

How to write a Remote Plugin:

1. Create a C# class library project (.NET 8.0).
2. Use Geutebrueck.RemotePlugins.Sdk as SDK and specify the version to use.

To do this, replace `Microsoft.NET.Sdk` with `Geutebrueck.RemotePlugins.Sdk/<version>`. The `.csproj` file should now look like this:

```

<Project Sdk="Geutebrueck.RemotePlugins.Sdk/1.0.0">

  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <ImplicitUsings>enable</ImplicitUsings>
    <Nullable>enable</Nullable>
  </PropertyGroup>

</Project>

```

3. Write a plugin class derived from the base class `PluginBase`.

The virtual method `OnSettingsChanged()` can be overridden and is called when the JSON configuration of the instance has changed. Services are automatically injected into the constructor (if any).

```

public class SamplePlugin : PluginBase
{
    //protected override void OnSettingsChanged() { }

    protected override void OnDispose() { }
}

```

4. Write a provider class that extends `PluginProviderBase<T>`.

```

public class SamplePluginProvider : PluginProviderBase<SamplePlugin>
{
    private readonly int _maxImageModules = 1;

    protected override IBasePluginSettings GetPluginDefaultSettings()
    {
        return PluginSettings.Create(_maxImageModules);
    }

    protected override PluginDefinition GetPluginDefinition()
    {
        return new("Sample Plugin")
        {
            MaxInstances = 16,
            MaxImageModules = _maxImageModules,
            InputChannels = 0,
            OutputChannels = 0,
        };
    }

    /* Optionally configure your services */
    public void ConfigureServices(IServiceCollection services)
    {
        // Register your plugin services here
    }

    /* Optionally configure the app */
    public void Configure(IPluginLoaderApplication app)
    {
        // configure your plugin here
        // app.Services.GetRequiredService<SampleService>
        ().DoAtStartup();
    }
}

```

5. You can define individual settings for the plugin in addition to the default settings.
 - a. Define the individual settings as public properties in an additional class derived from `IndividualPluginSettingsBase`.

```
public class SamplePluginIndividualSettings : IndividualPluginSettingsBase
{
    public int Test1 { get; set; } = 10;
    public string Test2 { get; set; } = "test";
}
```

- b. Pass the type of the settings class in `GetPluginDefaultSettings()`.

```
protected override IBasePluginSettings GetPluginDefaultSettings()
{
    return PluginSettings.Create<SamplePluginIndividualSettings>(_maxImageModules);
}
```

Write a Plugin Module

There are many functionalities that plugins can support, but not every plugin has to support all functionalities. For this reason, there are the modules that a plugin can provide to support certain functionalities. To do this, the module must implement the corresponding module interface. A plugin can have several modules, even several instances of the same module.

In this example, an `ImageModule` is implemented that allows streaming of images.

The currently available interface types for modules which are recognized by the framework are:

- `IImageModule` for image modules
- `IIOModule` for IO modules
- `IPtzModule` for PTZ modules

How to write a plugin module:

1. Write a module class derived from the base class `PluginModuleBase` and implementing the interface `IImageModule`.

Call the `StopStream()` method from the `OnDispose()` method in order to stop the image stream if a module instance is removed. The private fields and properties are specific to this module and may be different for other modules.

- `_streamActive` controls starting and stopping the image stream.
- `_imageBase` holds the static image to stream.
- `IndividualSettings` gives access to the individual settings of our `SamplePlugin`.

In addition, a small set of virtual methods can be overridden if necessary:

- `RegisterSubmodules(IList<>)` informs the module about other modules of the same plugin instance. Module instances shared in this way must be added to the `CreateModuleParams.SubmoduleReferences` property in the plugin before calling `CreatePluginModule()`.
- `SetPluginSettings()` is called when new settings have been deserialized. The base implementation can handle this and calls `OnSettingsChanged()`.
- `OnSettingsChanged()` is called once all settings have been set.

Additional base classes are provided (`ImageModuleBase`, `IOModuleBase`, `PTZModuleBase`) that contain frequently used code for their respective module type and encapsulate events into abstract methods that can be overridden.

Services are automatically injected into the constructor.

```
public class SamplePluginImageModule : ImageModuleBase
{
    private readonly SamplePluginImageStreamer _streamer;

    public SamplePluginIndividualSettings IndividualSettings =>
        PluginSettings.DeviceSettings.IndividualSettings as
        SamplePluginIndividualSettings ?? new();

    public SamplePluginImageModule()
    {
        _streamer = new(this);
    }

    protected override void StartStream(Guid streamId)
    {
        _streamer.StartStream();
    }
}
```

```

    }

    protected override void StopStream(Guid streamId)
    {
        _streamer.StopStream();
    }

    protected override IEnumerable<IImageStreamer>
    GetImageStreamers()
    {
        yield return _streamer;
    }

    protected override IImageStreamer SelectStream(string tag,
    ImageResolution resolution, StreamSelectionBehaviour stream-
    ingBehaviour)
    {
        return _streamer;
    }

    //protected override void Initialize() { }

    //protected override void RegisterSubmodules(IList<IBaseMod-
    ule> modules) { }

    //protected override void SetPluginSettings(IBasePlu-
    ginSettings settings) => base(settings);

    //protected override void OnSettingsChanged() { }

    protected override void OnDispose()
    {
        _streamer.StopStream();
    }
}

```

2. Register the module as module capability to your plugin inside the plugin constructor.

See the example plugins for reference on how to use the other overloads of `AddModuleCapability`.

```

public class SamplePlugin : PluginBase

```

```

{
    [...]

    public SamplePlugin()
    {
        // register the image module using the default factory
        AddModuleCapability<IImageModule, SamplePlu-
ginImageModule>();
    }

    [...]
}

```

3. Implement an image streamer defined by `IImageStreamer`.

Start with the `RunStream` function. The task of this function is to stream images continuously. For this purpose, the static image is initialized at the beginning. Then the function `CreateAndPublishCommand` is called in an infinite loop to stream the image along with a current time stamp. The gateway receives the stream and forwards it to the G-Core server.

```

public class SamplePluginImageStreamer : IImageStreamer
{
    public Guid Id {get;} = Guid.NewGuid();
    private readonly SamplePluginImageModule _imageModule;

    private bool _streamActive = false;

    public SamplePluginImageStreamer(SamplePluginImageModule
imageModule)
    {
        _imageModule = imageModule;
    }

    private async Task RunStream()
    {
        _streamActive = true;
        var imageBase = new SKBitmap(800, 600);
        using (SKCanvas canvas = new(imageBase))
            canvas.DrawRect(new SKRect(0, 0, 800, 600),
new SKPaint() { Style = SKPaintStyle.Fill, Color = SKColors.Blue
});

        while (_streamActive)

```

```

        {
            var img = imageBase.Encode(SKEncodedImageFormat.Jpeg, 100).ToArray();
            var picTime = Timestamp.FromDateTimeOffset
(DateTimeOffset.UtcNow);

            _imageModule.PushImage(
                ByteString.CopyFrom(img),
                ImageCodecType.Jpg,
                Id
            );

            await Task.Delay(1000);
            Console.WriteLine($"{_imageModule.IndividualSettings?.Test1 ?? -1} {_imageModule.IndividualSettings?.Test2 ?? "null"}");
        }
    }

    public void StartStream()
    {
        if (!_streamActive)
            _ = RunStream();
    }

    public void StopStream()
    {
        _streamActive = false;
    }

    public ImageStreamInfo GetStreamInfo()
    {
        return new()
        {
            Id = Id.Wrap()
        };
    }

    public void HandleStreamTask(StreamTask streamTask, ImageResolution resolution) { }

    public void UpdateImageResolution(ImageResolution resolution) { }
}

```


Multihead Support

Some cameras have several heads, each with its own sensor and usually looking in different directions. Each camera head corresponds to an `IImageModule` in the plugin. The number of camera heads supported by the plugin can be set in the `PluginProviderBase<T>.GetPluginDefinition` via the parameter `MaxImageModules`. Individual settings for the different heads (derived from the base class `IndividualChannelSettingsBase`) can be registered in the method `GetPluginDefaultSettings`, as well as the global individual settings for all channels (derived from the base class `IndividualPluginSettingsBase`).

```
public class ExampleMultiheadPluginProvider : PluginProviderBase<ExampleMultiheadPlugin>
{
    private readonly int _maxImageModules = 5;

    protected override IBasePluginSettings GetPluginDefaultSettings()
    {
        return PluginSettings.Create<ExampleMultiheadIndividualSettings, ExampleMultiheadIndividualChannelSettings>(_maxImageModules);
    }

    protected override PluginDefinition GetPluginDefinition()
    {
        return new("Example Multihead Plugin")
        {
            MaxInstances = 16,
            MaxImageModules = _maxImageModules,
            InputChannels = 0,
            OutputChannels = 0,
        };
    }
}
```

A useful default channel setting is the `HeadId` which is predefined as a sequential number starting by zero. This index can be used to access the corresponding camera head in the streaming URL, and can be adjusted in the setup. It can be easily requested by `PluginSettings?.GetChannelSettings(ModuleId)?.HeadId` from the image modules.

Include Your Own Settings UI

1. Create a new UI project and an initial component for the settings UI using the UI SDK. You will find this in the installation directory of the SDK.
2. Write the frontend SDK. See **SDK Frontend** for detailed information.
3. You need to define two values:
 - `UiModule`: The name of the entry module, usually `./<your-project-name>`. You can find this name inside the `module-federation.config.js` as key for `exposed`.
 - `UiComponent`: The component of the entry module, usually `<your-project-name>Component`.
4. Provide the defined values to the framework via the `PluginDefinition` object from the `PluginProvider` (see [Write a Provider Class](#)).

```
public class ExampleMultiheadPluginProvider : PluginProviderBase<ExampleMultiheadPlugin>
{
    [...]

    protected override PluginDefinition GetPluginDefinition()
    {
        return new()
        {
            [...]

            UiApp = "<public-dist-dir>",
            UiModule = "./<entry-module>",
            UiComponent = "<entry-component>"
        };
    }
}
```

5. Build the UI files and copy the built UI files, which are located in `dist` after building, to the plugin directory that can be accessed by the Plugin Loader. The default directory structure of a plugin is:

```
YourPlugin/
├─ net8.0/
├─ public/
```

```
└─ <public-dist-dir>/
   └─ ** PLACE THE UI DIST FILES HERE **
plugin.json
```

i Do not place your files directly in the `public` directory. The value for `<public-dist-dir>` must be unique for your plugin.

The directory `public` is specified in the `plugin.json` as the root directory for public files that the browser can access. While it is recommended to keep the default value, you can change the value for `PublicFiles > Root` in `plugin.json` to any directory relative to the directory containing `plugin.json` or to an absolute path. The path provided via `RemotePluginInfo.UiApp` is always considered relative to this path. This value can also be changed at design time within the `.csproj` of your plugin. Set the property `PublicFilesDir` to the desired path. It will automatically be placed in the `plugin.json` during the build.

For example, if you want your assets to be loaded from `C:\MyPublicAssets`, the `.csproj` file should look like this:

```
<Project Sdk="Geutebrueck.RemotePlugins.Sdk/1.0.0">

  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <ImplicitUsings>enable</ImplicitUsings>
    <Nullable>enable</Nullable>
    <PublicFilesDir>C:\MyPublicAssets</PublicFilesDir>
  </PropertyGroup>

</Project>
```

Add a Plugin to a Plugin Loader

Every plugin has a `plugin.json` file which defines the path to load the plugin assembly. All relative paths in this file are relative to the directory containing it. Absolute paths can also be specified.

The default installation path of the Plugin Loader is `C:\Program Files\Geutebrueck\PluginLoader`. To add a plugin to a plugin loader, copy the plugin files to a new `plugins/<your-plugin-name>` directory. The actual name of the directory inside `plugins` is not important. Then restart the Plugin Loader.

```

RemotePluginLoader/
├── plugins/
│   └── <your-plugin-name>/
│       ├── net8.0/
│       │   └── ...
│       └── plugin.json
└── ...

```

Example Plugins

The examples of the plugin implementation source code are located in the **Examples** folder in installation directory of the SDK.

Plugin	Description
ExamplePlugin	A blank, loadable plugin without any functionality.
ExampleJpegPlugin	Streams continuously generated JPEG frames to the server.
ExampleH264Plugin	Takes H.264 frames from a file and streams them to the server in a loop. Uses individual settings to configure the file location.
ExamplePtzPlugin	Visualizes pan, tilt and zoom commands with generated JPEG frames.
ExampleMultiheadPlugin	Supports up to five image modules per instance, each simulating a camera head.
SDKPlugin	A comprehensive example that combines and demonstrates most of the possible functions.

Plugin Loader Simulator

The Remote Plugin Simulator is a tool to test your plugin and view its images. The plugin is loaded into a simulated environment, no G-Core system is required.

1. To make your plugin available to the simulator, copy it to the `simulator/plugins` directory as described for the Plugin Loader (see **Add a Plugin to a Plugin Loader**):

```
Simulator/  
├── plugins/  
│   └── <your-plugin-name>/  
│       ├── net8.0/  
│       │   └── ...  
│       └── plugin.json  
└── ...
```

2. Run the `PluginLoaderSimulator.exe` file located in the **Simulator** folder in the installation directory of the SDK.

SDK Frontend

The frontend SDK is installed with the Plugin Loader SDK Installer. After the installation the frontend SDK is located in the **RemotePluginsUISDK** folder in the installation directory of the SDK.

Documentation:

You can find the technical documentation for the SDK frontend in the file `documentation.md` in the subdirectory `RemotePluginsUISDK\docs\plugin-loader-doc`. Follow the steps in this documentation to write the frontend SDK.

i **This documentation describes the technologies used as well as the setup of the development environment. The Compodoc environment described there gives an overview and describes the available source code.**

Frontend Plugin:

The documentation file `documentation.md` describes how a plugin is created and integrated in the Plugin Loader service. This is necessary to load the created plugin in the Geutebrück system or in the appropriate web user interface.

For more information on creating a user interface for a plugin and integrating it into the Geutebrück system, refer to the technical documentation in the project.

Standalone Plugin:

In addition to the provided frontend SDK, which provides a number of useful libraries for connecting Angular specific applications, there is also the possibility to use another frontend framework or even only HTML, CSS and JavaScript for the development of the user interfaces.

Integrating other frameworks may lead to unexpected problems. Implementation using only HTML, CSS and JavaScript requires hosting the web application independently and must be used as a standalone web application.

The Angular libraries provided allow for easy use, implementation, and integration. Using other frontend frameworks or only HTML, CSS, and JavaScript require standalone implementation by using the provided API.

Geutebrück Hub

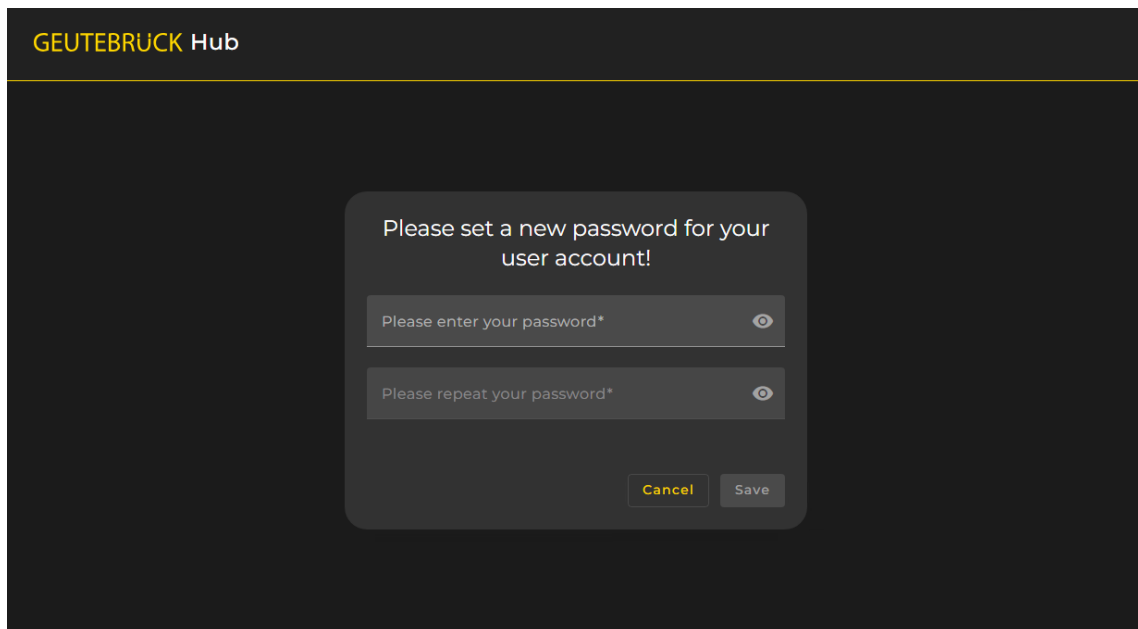
User Account Management

Confirm User Account

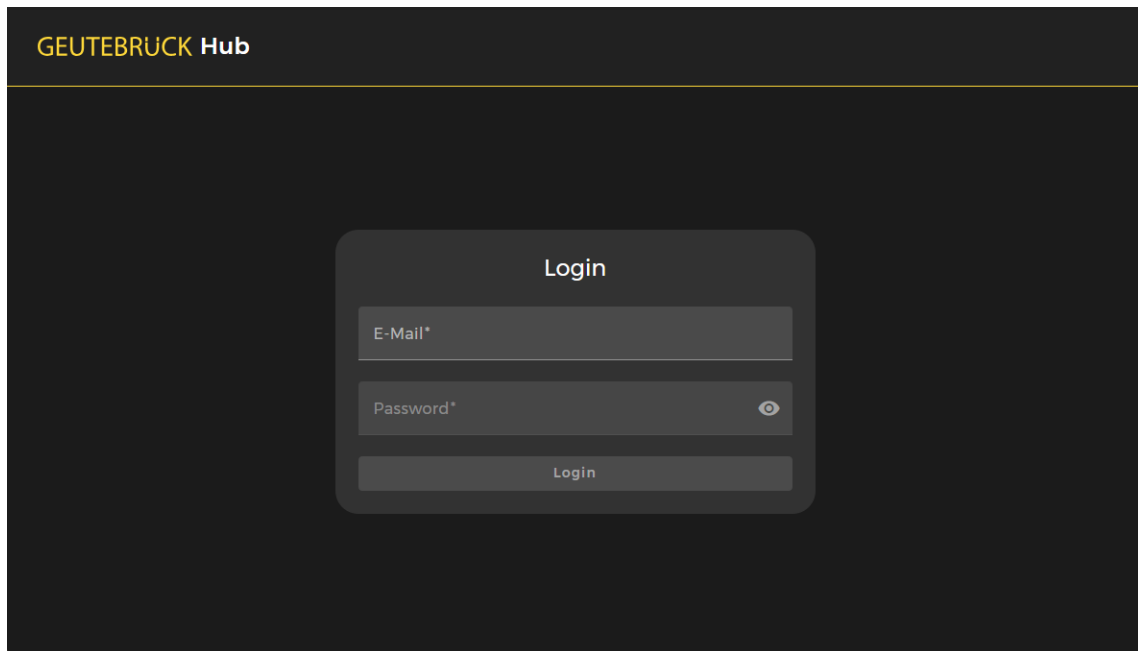
When you open the Geutebrück Hub for the first time, you'll need to confirm your user account.

1. Open the Geutebrück Hub via the registration Link. The **Set a new password** page opens.

i A registration link is generated for newly created users; this link will redirect you to the Geutebrück Hub login page to complete your registration. You'll receive this link from the administrator who created your user account.

The screenshot shows a dark-themed web interface. At the top left, the text 'GEUTEBRÜCK Hub' is displayed in a light color. Below this, a central modal form is shown. The form has a title 'Please set a new password for your user account!'. It contains two input fields: 'Please enter your password*' and 'Please repeat your password*'. Each field has a small eye icon to its right, indicating a password field. At the bottom of the form, there are two buttons: 'Cancel' and 'Save'.

2. Enter a password for your user account.
3. Click **Save**. The **Login** page opens.

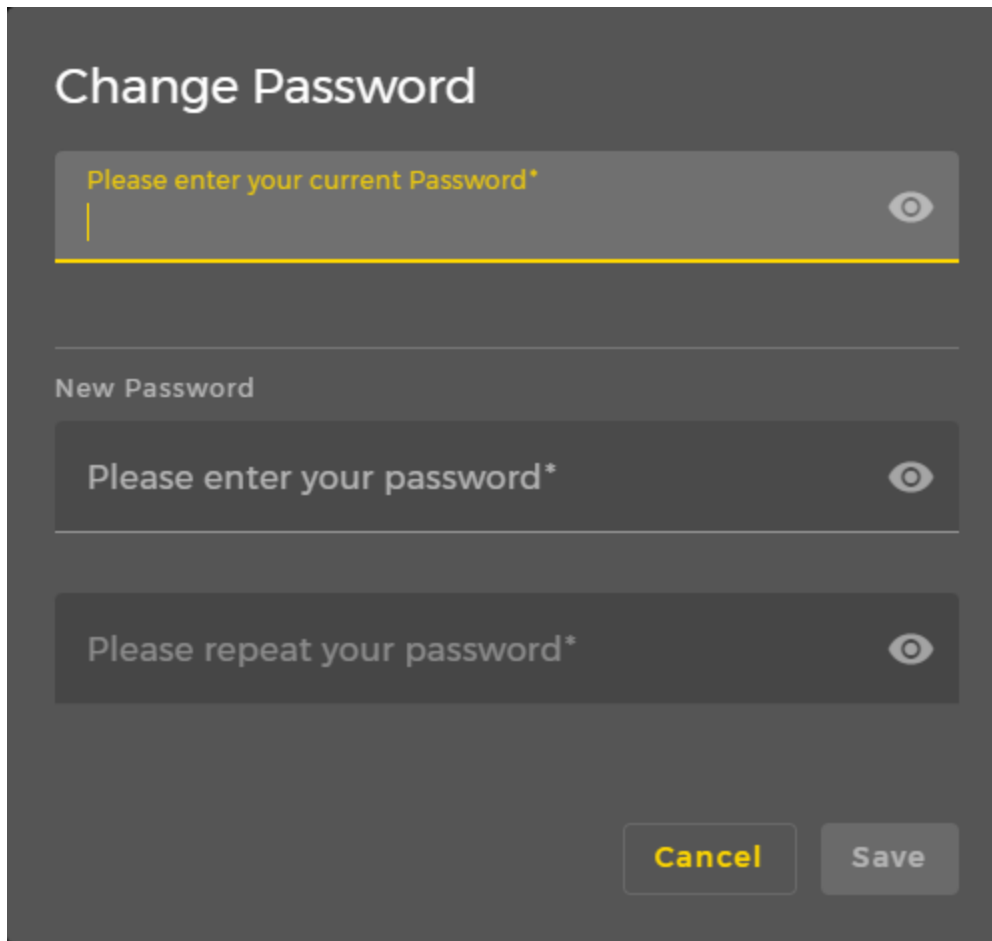


4. Enter your login details and click **Login**.

Change Password

You can change the password of your user account.

1. Log in to the Geutebrück Hub.
2. In the user menu, click **Change Password**. The **Change Password** dialog opens.

A dark-themed user interface for changing a password. At the top, the title "Change Password" is displayed in white. Below it, there are three input fields. The first field is labeled "Please enter your current Password*" in yellow text and has a yellow underline. The second and third fields are grouped under the label "New Password" in white text; the second is labeled "Please enter your password*" and the third is labeled "Please repeat your password*", both in white text. Each input field has a white eye icon on the right side to toggle visibility. At the bottom right, there are two buttons: "Cancel" in yellow text and "Save" in white text, both on dark gray backgrounds.

Change Password

Please enter your current Password*

New Password

Please enter your password*

Please repeat your password*

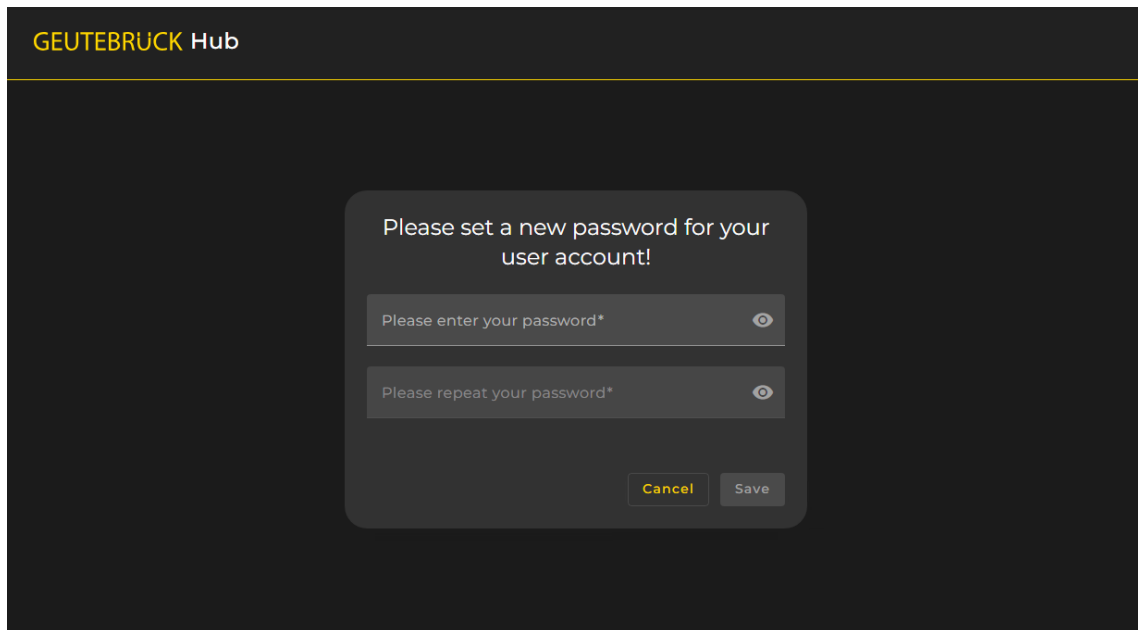
Cancel Save

3. Enter your current password.
4. Enter your new password.
5. Click **Save**.

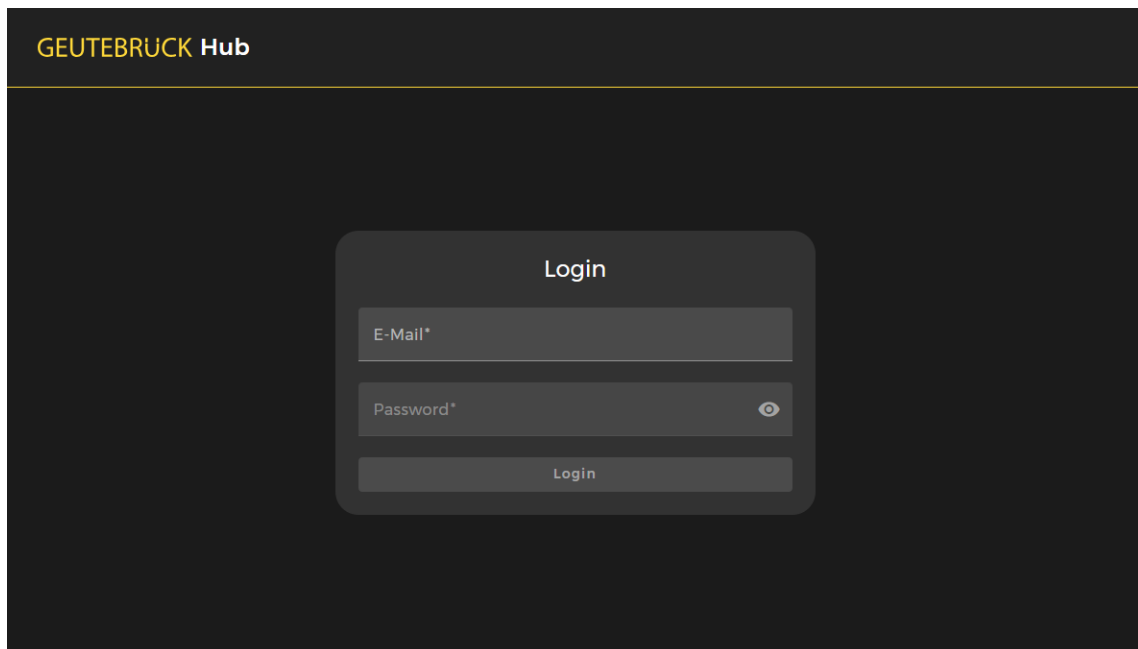
Reset Password

If you have forgotten your password, contact your administrator. They can generate a password reset link for your user account (see **Create Password Reset Link**), which you can use to reset your password.

1. Open the Geutebrück Hub via the password reset Link. The **Set a new password** page opens.



2. Enter a new password for your user account.
3. Click **Save**. The **Login** page opens.



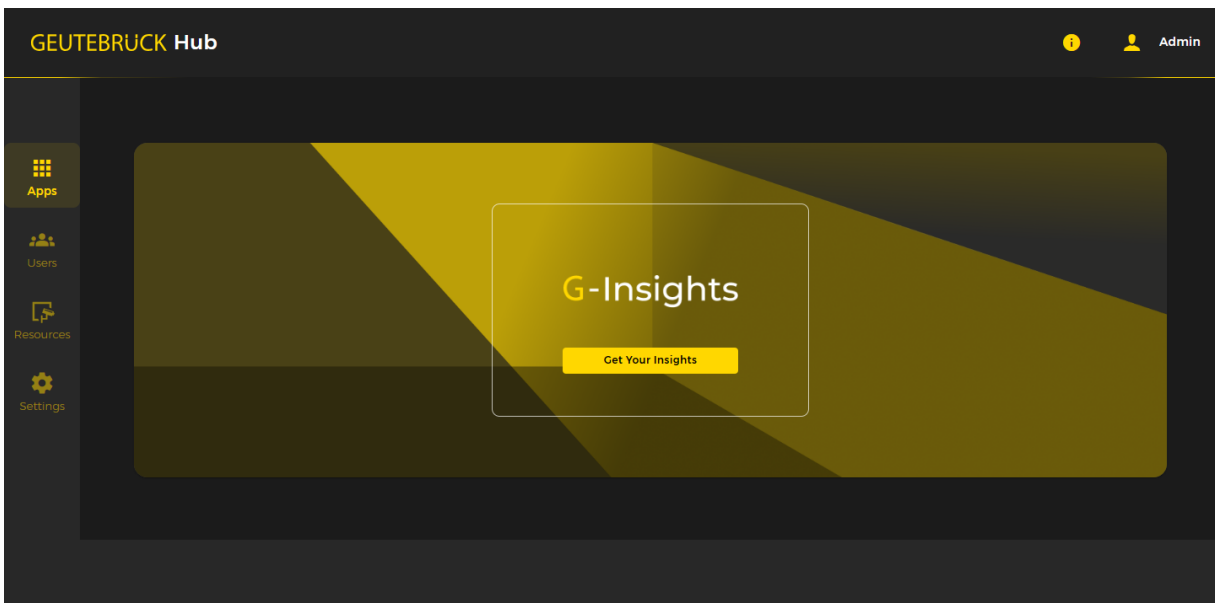
4. Enter your login details and click **Login**.

Apps

The **Apps** page provides an overview of all available services that include their own user interface.

Click the **Get Your Insights** button, to open the G-Insights app in a new tab.

i You only see services for which you have the required permissions.



Users

Order of Initial Setup

Once you have completed the initial setup of the installation components(see **Initial Setup**), you can proceed with configuring the user management.

During initial setup, you should follow this order, as there are dependencies between the different components.

1. Open Geutebrück Hub via the desktop icon.
2. On the **Resource Sets** page, add a resource set and assign resources to the set (see **Add Resource Set**).

3. On the **Permission Sets** page, add a permission set and select the permissions for the set (see **Add Permission Set**).
4. On the **Roles** page, add a role and assign permission sets and resource sets to the role (see **Add Role**).
5. On the **User Groups** page, add a user group and assign users and roles to the user group (see **Add User Group**).
6. On the **Users** page, add a user (see **Add User**).

Manage Users

The **Users** page provides an overview of all user accounts in your system, as well as the status of each account.

-  **User account confirmed:** The user has completed the registration of their user account.
-  **User account not confirmed:** The user has been created but must still confirm their user account (see **Confirm User Account**) or reset their password (see **Reset Password**).
-  **User account is expired:** The user account has expired and cannot be used again until the password has been reset (see **Create Password Reset Link**).

GEUTEBRUCK Hub


 Admin

Apps

Users

Resources

Settings

Users

This is the overview of all Users. If you want to add a User, click on the "+" above the table.




		First Name	Last Name	Groups	E-Mail	Phone	Added On	Last Modified
☒				Administrators	default@administrator.com	/	4/21/26, 12:06 PM	4/21/26, 12:06 PM
☐		asdf	dsfg		test3@test.com		6/15/26, 12:28 PM	6/15/26, 12:28 PM
☐		Marta	Marketing	Operators G-Insights	marketing@administrator.com		4/28/26, 9:49 AM	4/28/26, 11:12 AM
☐		sdaf	sdfg	Operators G-Insights	test2@test.com		6/15/26, 12:28 PM	6/15/26, 12:28 PM
☐		test	test	Administrators	test@test.de		6/15/26, 12:27 PM	6/15/26, 12:27 PM
☐		Tobias	Hörmann, B.	Operators G-Insights	tobias.hoermann@geutebruck.com		4/28/26, 11:51 AM	4/28/26, 11:51 AM

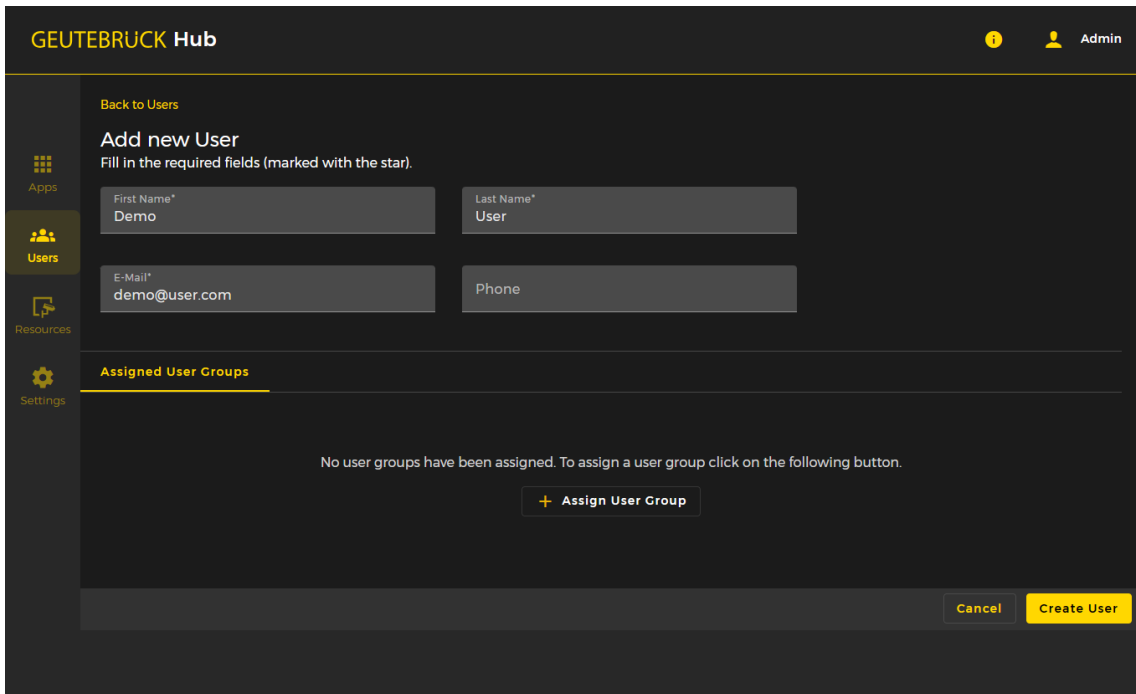
Items per page: 10
1 - 6 of 6

Add User

Add a user to your system, assign them to a user group, and then send the registration link to the newly created user so they can complete their registration.

1. On the **Users** page, click the **+** icon. The **Add new User** page opens.
2. Enter the user's first name, last name, e-mail address, and (optional) phone number. The **Assigned User Groups** tab appears.

 **The e-mail address must not already exist in the system.**



GEUTEBRÜCK Hub

Back to Users

Add new User

Fill in the required fields (marked with the star).

First Name*
Demo

Last Name*
User

E-Mail*
demo@user.com

Phone

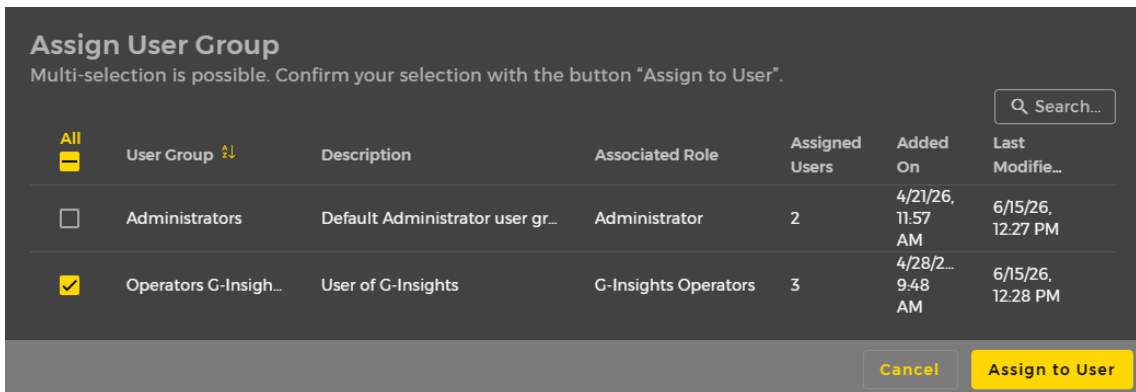
Assigned User Groups

No user groups have been assigned. To assign a user group click on the following button.

[+ Assign User Group](#)

[Cancel](#) [Create User](#)

3. Click the **+ Assign User Group** button. The **Assign User Group** dialog opens, listing the available user groups.



Assign User Group

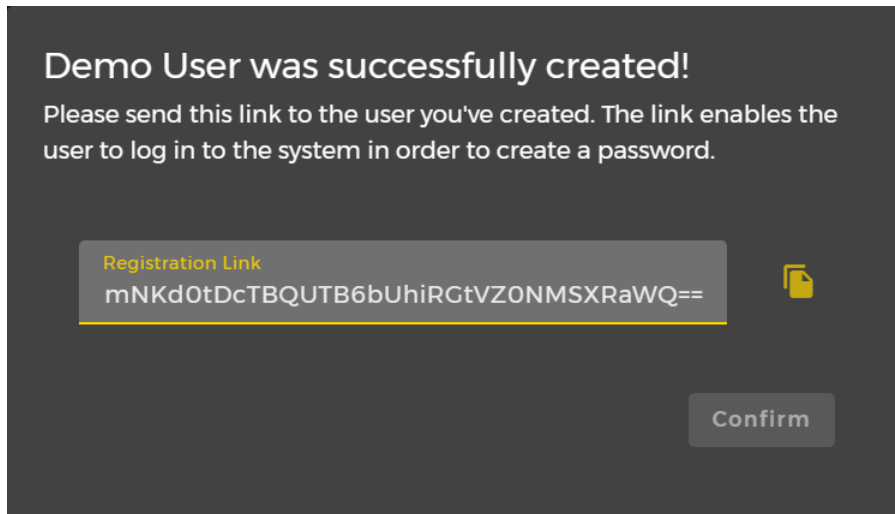
Multi-selection is possible. Confirm your selection with the button "Assign to User".

[Q Search...](#)

All	User Group	Description	Associated Role	Assigned Users	Added On	Last Modifie...
☐	Administrators	Default Administrator user gr...	Administrator	2	4/21/26, 11:57 AM	6/15/26, 12:27 PM
☒	Operators G-Insigh...	User of G-Insights	G-Insights Operators	3	4/28/2..., 9:48 AM	6/15/26, 12:28 PM

[Cancel](#) [Assign to User](#)

4. Select the user groups to which you want to assign the user by selecting the checkbox. If no user groups have been created yet, go to **Add User Group**.
5. Click **Assign to User**.
6. Click **Create User**. A confirmation dialog opens, displaying the registration link for the newly created user.



7. Click the  icon.
8. Click **Confirm**.
9. Send the link to the newly created user. The user must then complete the registration process by creating a password for their user account via this link (see **Confirm User Account**).

Create Password Reset Link

If a user has forgotten their password or you want to reset the password for that user account, you can create a password reset link for that user account.

1. On the **Users** page, hover your mouse over the row of the user for whom you want to reset the password link and click the  icon. A confirmation dialog opens.

 **You can only see this icon if you have the required permissions.**

New password link for Demo User was successfully created!

Please send this new link to the user. The link enables the user to log in to the system in order to reset their password.

Reset Link

iZVZ2WVA2ODdkMmVKamFtaXFsv0I3SkJ3QQ==



Confirm

2. Click the  icon.
3. Click **Confirm**.
4. Send the link to the appropriate user. The user must then complete the process by resetting the password for their user account via this link (see **Reset Password**).

Edit User

1. On the **Users** page, hover your mouse over the row of the user you want to edit and click the  icon. The **Edit <User Name>** page opens.

GEUTEBRUCK Hub Admin

[Back to Users](#)

Edit Demo User

Fill in the required fields (marked with the star).

First Name* Demo Last Name* User

E-Mail* demo@user.com Phone

Assigned User Groups

☐	User Group	Description	Associated Role	Assigned Users	Added On	Last Modified
☐	Operators G-Insights	User of G-Insights	G-Insights Operators	4	4/28/26, 9:48 AM	6/15/26, 8:41 PM

Items per page: 10 1 - 1 of 1

2. Edit the user's first name, last name, e-mail address, and (optional) phone number.
3. Assign a user group:
 - a. Go to the **Assigned User Groups** tab.
 - b. Click the icon. The **Assign User Group** dialog opens, listing the available user groups.

Assign User Group

Multi-selection is possible. Confirm your selection with the button "Assign to User".

☐	User Group	Description	Associated Role	Assigned Users	Added On	Last Modified
☒	Administrators	Default Administrator user gr...	Administrator	2	4/21/26, 11:57 AM	6/15/26, 12:27 PM
☐	Demo			2	6/15/26, 8:47 PM	6/15/26, 8:47 PM

- c. Select the user groups to which you want to assign the user by selecting the checkbox. If no user groups have been created yet, go to **Add User Group**.
 - d. Click **Assign to User**.
4. Delete a user group assignment:

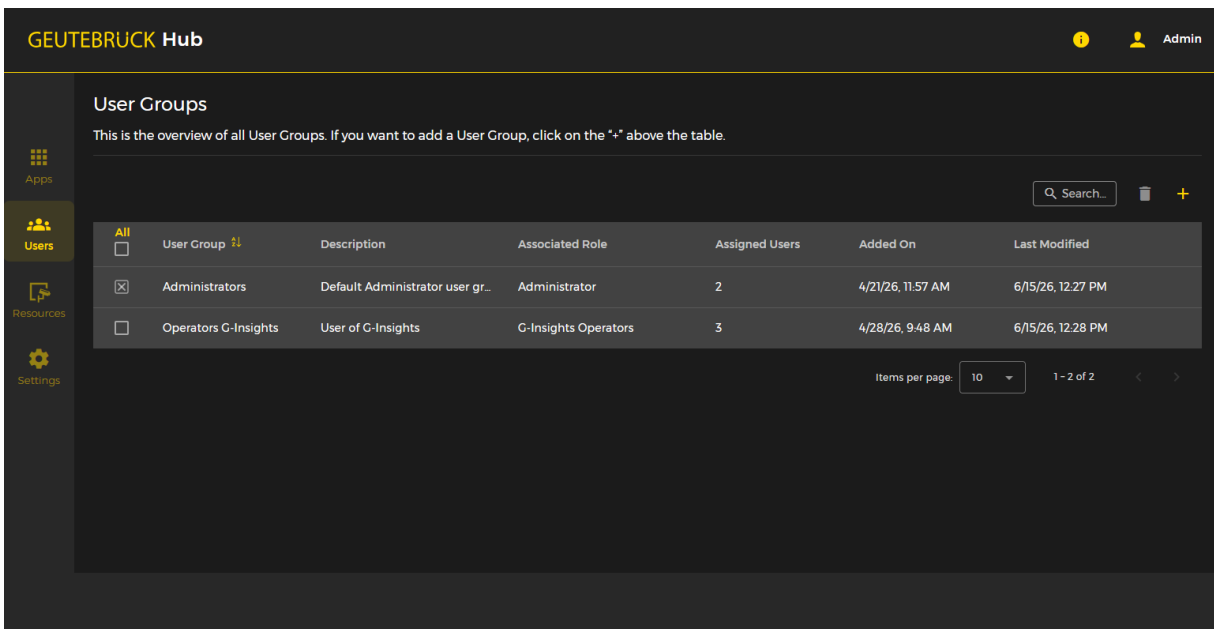
- a. Go to the **Assigned User Groups** tab.
 - b. Select a user group from the list by selecting the checkbox and click the  icon.
 - c. A confirmation dialog appears. Click **Confirm**.
5. Click **Update User**.

Delete User

1. On the **Users** page, select the user you want to delete from the list by selecting the checkbox.
2. Click the  icon.
3. A confirmation dialog appears. Click **Confirm**.

Manage User Groups

The **User Groups** page provides an overview of all user groups in your system.



GEUTEBRUCK Hub Admin

User Groups

This is the overview of all User Groups. If you want to add a User Group, click on the "+" above the table.

All	User Group	Description	Associated Role	Assigned Users	Added On	Last Modified
☒	Administrators	Default Administrator user gr...	Administrator	2	4/21/26, 11:57 AM	6/15/26, 12:27 PM
☐	Operators G-Insights	User of G-Insights	G-Insights Operators	3	4/28/26, 9:48 AM	6/15/26, 12:28 PM

Items per page: 10 1 - 2 of 2

Add User Group

Add a user group to your system and assign users and roles to it.

1. On the **User Groups** page, click the **+** icon. The **Add new User Groups** page opens.
2. Enter the name and (optional) the description of the user group. The **Users** and **Roles** tabs appear.

i The user group name must not already exist in the system.

The screenshot shows the 'Add new User Group' page in the GEUTEBRUCK Hub. The page has a dark theme with a sidebar on the left containing icons for 'Apps', 'Users', 'Resources', and 'Settings'. The 'Users' icon is highlighted. The main content area has a header 'Add new User Group' with a subtitle 'Fill in the required fields (marked with the star)'. Below this are two input fields: 'Name*' with the value 'Demo' and 'Description'. Below the input fields are two tabs: 'Users' (active) and 'Roles'. The 'Users' tab shows a message: 'No user have been assigned. To assign a user click on the following button.' followed by a button '+ Assign User to this User Group'. At the bottom right of the page are two buttons: 'Cancel' and 'Create User Group'.

3. Go to the **Users** tab.
4. Click the **+** **Assign User to this User Group** button. The **Assign User** dialog opens, listing the available users.

Assign User
Multi-selection is possible. Confirm your selection with the button "Assign to User Group".

Q Search...

All		First Name	Last Name	Groups	E-Mail
☐	✓			Administrators	default@administrator.com
☐	✓	asdf	dsfg		test3@test.com
☒	✓	Marta	Marketing	Operators G-Insights	marketing@administrator.com
☐	⚠	sdaf	sdfg	Operators G-Insights	test2@test.com
☒	✓	test	test	Administrators	test@test.de

Cancel Assign to User Group

- Select the users you want to assign to the user group by selecting the checkbox. If no users have been created yet, go to **Add User**.
- Click **Assign to User Group**.
- Go to the **Roles** tab.
- Click the **+ Assign Role to this User Group** button. The **Assign Role** dialog opens, listing the available roles.

Assign Role
Multi-selection is possible. Confirm your selection with the button "Assign to User Group".

Q Search...

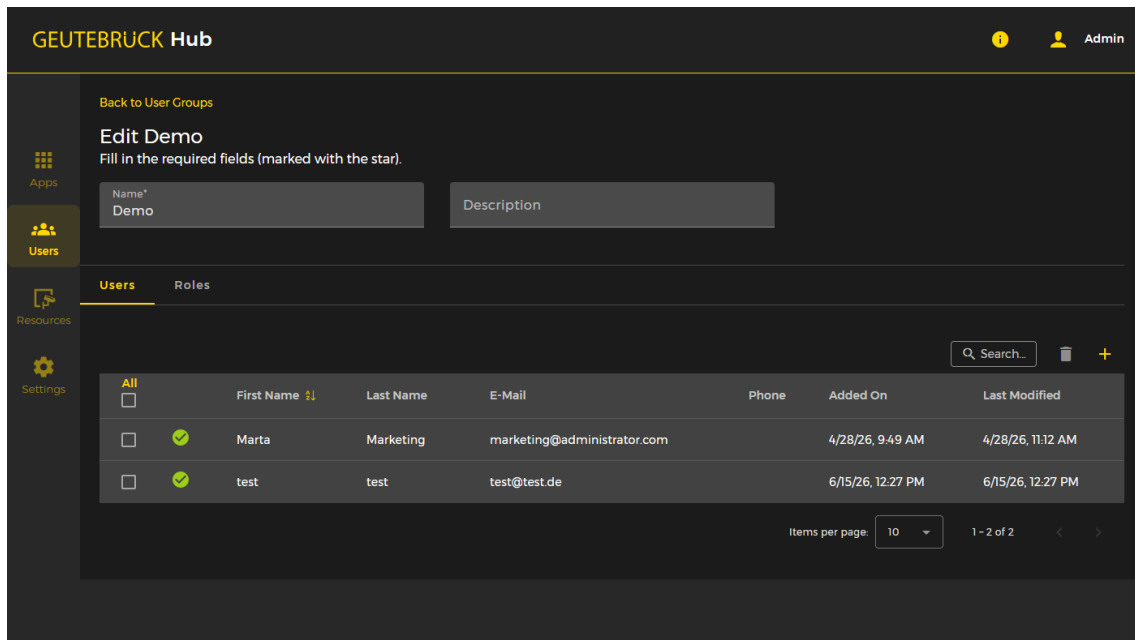
All	Role	Description	Added On	Last Modified
☐	Administrator	Default Administrator Role	4/21/26, 11:57 AM	4/21/26, 11:57 AM
☒	G-Insights Operators		4/28/26, 11:52 AM	4/28/26, 12:28 PM

Cancel Assign to User Group

- Select the roles you want to assign to the user group by selecting the checkbox. If no roles have been created yet, go to **Add Role**.
- Click **Assign to User Group**.
- Click **Create User Group**.

Edit User Group

1. On the **User Group** page, hover your mouse over the row of the user group you want to edit and click the  icon. The **Edit <User Group Name>** page opens.



GEUTEBRUCK Hub

Back to User Groups

Edit Demo

Fill in the required fields (marked with the star).

Name*
Demo

Description

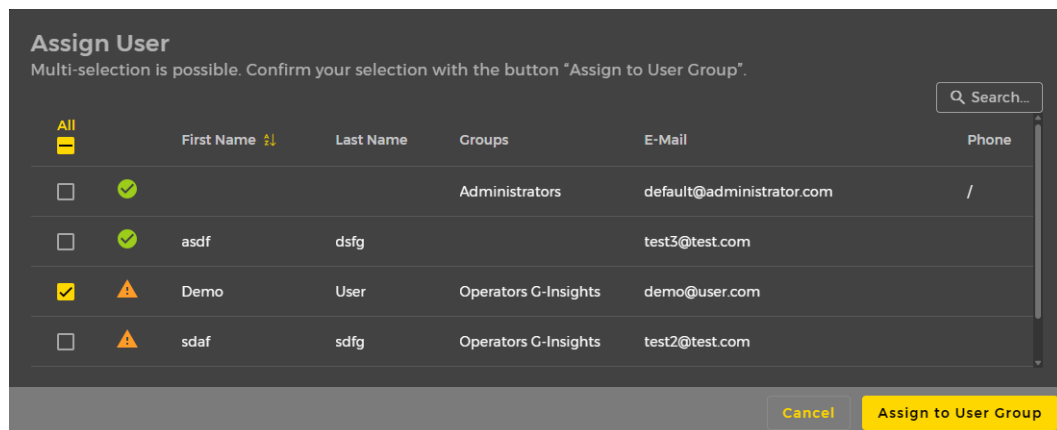
Users Roles

Search...

All	First Name	Last Name	E-Mail	Phone	Added On	Last Modified
☐	Marta	Marketing	marketing@administrator.com		4/28/26, 9:49 AM	4/28/26, 11:12 AM
☐	test	test	test@test.de		6/15/26, 12:27 PM	6/15/26, 12:27 PM

Items per page: 10 1 - 2 of 2

2. Edit the name and (optional) the description of the user group.
3. Assign a user:
 - a. Go to the **Users** tab.
 - b. Click the  icon. The **Assign User** dialog opens, listing the available users.



Assign User

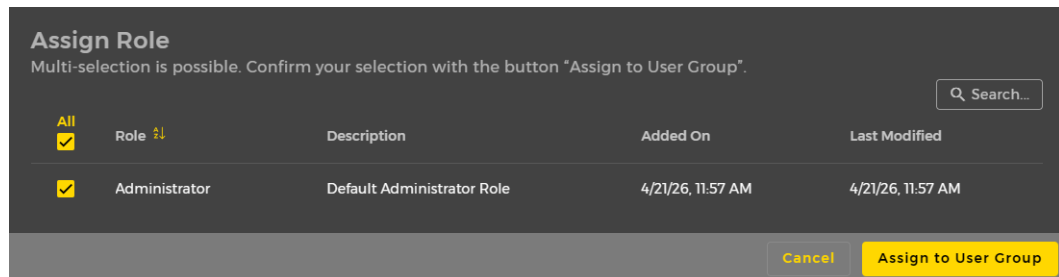
Multi-selection is possible. Confirm your selection with the button "Assign to User Group".

Search...

All	First Name	Last Name	Groups	E-Mail	Phone
☐			Administrators	default@administrator.com	/
☐	asdf	dsfg		test3@test.com	
☒	Demo	User	Operators G-Insights	demo@user.com	
☐	sdfg	sdfg	Operators G-Insights	test2@test.com	

Cancel Assign to User Group

- c. Select the users you want to assign to the user group by selecting the checkbox. If no users have been created yet, go to **Add User**.
 - d. Click **Assign to User Group**.
4. Delete a user assignment:
 - a. Go to the **Users** tab.
 - b. Select a user from the list by selecting the checkbox and click the  icon.
 - c. A confirmation dialog appears. Click **Confirm**.
5. Assign a role:
 - a. Go to the **Roles** tab.
 - b. Click the **+** button. The **Assign Role** dialog opens, listing the available roles.



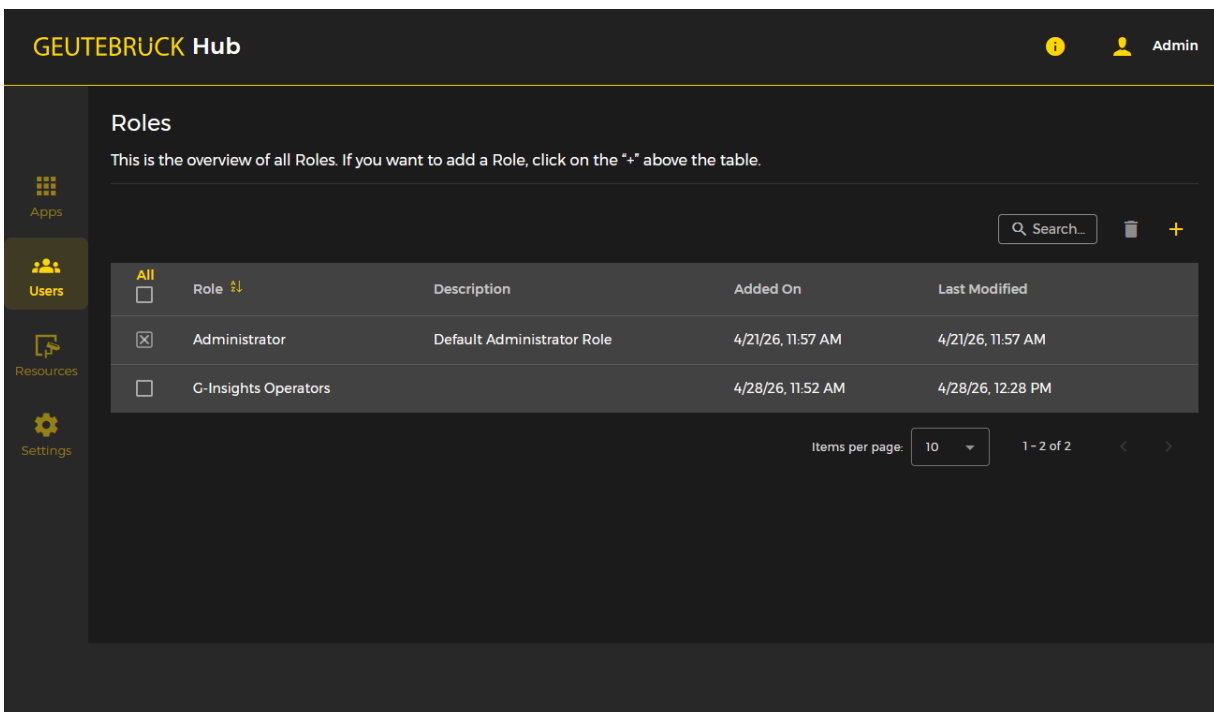
- c. Select the roles you want to assign to the user group by selecting the checkbox. If no roles have been created yet, go to **Add Role**.
 - d. Click **Assign to User Group**.
6. Delete a role assignment:
 - a. Go to the **Roles** tab.
 - b. Select a role from the list by selecting the checkbox and click the  icon.
 - c. A confirmation dialog appears. Click **Confirm**.
7. Click **Update User Group**.

Delete User Group

1. On the **User Groups** page, select the user group you want to delete from the list by selecting the checkbox.
2. Click the  icon.
3. A confirmation dialog appears. Click **Confirm**.

Manage Roles

The **Roles** page provides an overview of all roles in the system.



GEUTEBRUCK Hub Admin

Roles

This is the overview of all Roles. If you want to add a Role, click on the "+" above the table.

Search...

All	Role	Description	Added On	Last Modified
☒	Administrator	Default Administrator Role	4/21/26, 11:57 AM	4/21/26, 11:57 AM
☐	G-Insights Operators		4/28/26, 11:52 AM	4/28/26, 12:28 PM

Items per page: 10 1 - 2 of 2

Add Role

Add a role to your system and assign permission sets and resource sets to it.

1. On the **Roles** page, click the  icon. The **Add new Role** page opens.
2. Enter the name and (optional) the description of the role. The **Permission Sets** and **Resource Sets** tabs appear.

 **The role name must not already exist in the system.**

GEUTEBRUCK Hub

Back to Roles

Add new Role

Fill in the required fields (marked with the star).

Name* Demo

Description

Apps

Users

Resources

Settings

Permission Sets Resource Sets

No permission set have been assigned. To assign a permission set click on the following button.

+ Assign Permission Set to this Role

Cancel Create Role

- Go to the **Permission Sets** tab.
- Click the **+ Assign Permission Set to this Role** button. The **Assign Permission Set** dialog opens, listing the available permission sets.

Assign Permission Set

Multi-selection is possible. Confirm your selection with the button "Assign to Role".

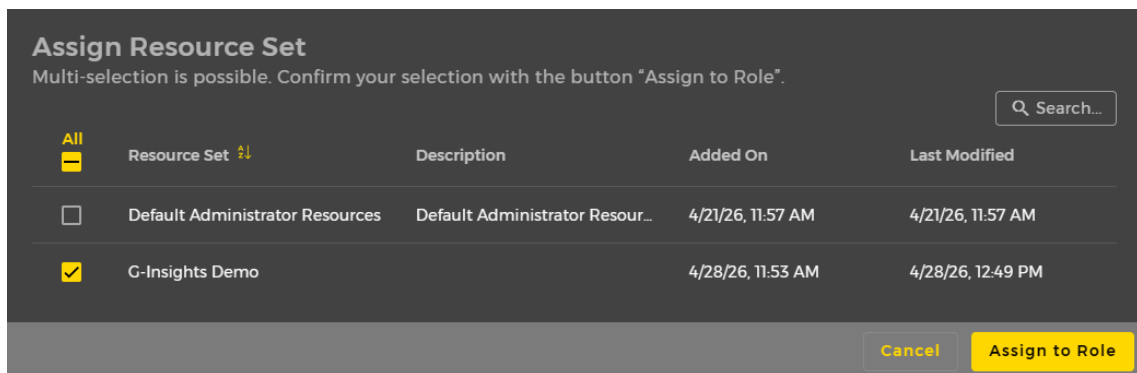
Search...

All	Permission Set	Description	Added On	Last Modified
☐	Default Administrator Permissions	Default Permission Set	4/21/26, 11:57 AM	4/21/26, 11:57 AM
☒	Access G-Insights	Access G-Insights	4/28/26, 11:27 AM	4/28/26, 11:27 AM
☐	test	test	5/19/26, 12:28 PM	5/19/26, 12:28 PM

Cancel Assign to Role

- Select the permission sets you want to assign to the role by selecting the checkbox. If no permission sets have been created yet, go to **Add Permission Set**.
- Click **Assign to Role**.
- Go to the **Resource Sets** tab.

- Click the **+ Assign Resource Set to this Role** button. The **Assign Resource Set** dialog opens, listing the available resource sets.



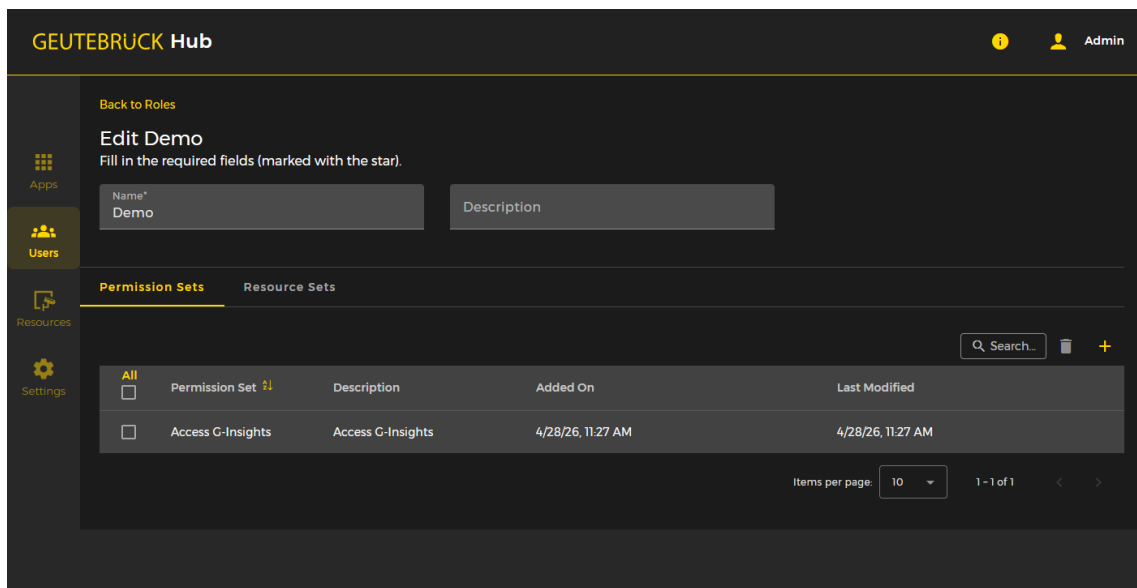
The **Assign Resource Set** dialog is shown. It has a title bar and a subtitle: "Multi-selection is possible. Confirm your selection with the button 'Assign to Role'". There is a search bar in the top right corner. Below the search bar is a table with columns: "All" (with a dropdown arrow), "Resource Set" (with a sort icon), "Description", "Added On", and "Last Modified". The table contains two rows: "Default Administrator Resources" and "G-Insights Demo". The "G-Insights Demo" row has a checked checkbox in the "All" column. At the bottom right, there are two buttons: "Cancel" and "Assign to Role".

All	Resource Set	Description	Added On	Last Modified
☐	Default Administrator Resources	Default Administrator Resour...	4/21/26, 11:57 AM	4/21/26, 11:57 AM
☒	G-Insights Demo		4/28/26, 11:53 AM	4/28/26, 12:49 PM

- Select the resource sets you want to assign to the role by selecting the checkbox. If no resource sets have been created yet, go to **Add Resource Set**.
- Click **Assign to Role**.
- Click **Create Role**.

Edit Role

- On the **Roles** page, hover your mouse over the row of the role you want to edit and click the  icon. The **Edit <Role Name>** page opens.



The **Edit Demo** page is shown. It has a header with "GEUTEBRUCK Hub" and a user profile "Admin". The page has a sidebar with "Apps", "Users", "Resources", and "Settings". The main content area has a "Back to Roles" link and a "Fill in the required fields (marked with the star)." instruction. There are two input fields: "Name*" (with the value "Demo") and "Description". Below these fields are two tabs: "Permission Sets" (selected) and "Resource Sets". The "Permission Sets" tab shows a table with columns: "All" (with a dropdown arrow), "Permission Set" (with a sort icon), "Description", "Added On", and "Last Modified". The table contains one row: "Access G-Insights". At the bottom right, there is a pagination control showing "Items per page: 10" and "1 - 1 of 1".

All	Permission Set	Description	Added On	Last Modified
☐	Access G-Insights	Access G-Insights	4/28/26, 11:27 AM	4/28/26, 11:27 AM

- Edit the name and (optional) the description of the role.
- Assign a permission set:

- a. Go to the **Permission Sets** tab.
- b. Click the **+** icon. The **Assign Permission Set** dialog opens, listing the available permission sets.

Assign Permission Set

Multi-selection is possible. Confirm your selection with the button "Assign to Role".

All

Permission Set

Description

Added On

Last Modified

☒	Default Administrator Permissions	Default Permission Set	4/21/26, 11:57 AM	4/21/26, 11:57 AM
☐	test	test	5/19/26, 12:28 PM	5/19/26, 12:28 PM

Cancel

Assign to Role

- c. Select the permission sets you want to assign to the role by selecting the checkbox. If no permission sets have been created yet, go to **Add Permission Set**.
 - d. Click **Assign to Role**.
4. Delete a permission set assignment:
 - a. Go to the **Permission Sets** tab.
 - b. Select a permission set from the list by selecting the checkbox and click the **🗑** icon.
 - c. A confirmation dialog appears. Click **Confirm**.
 5. Assign a resource set:
 - a. Go to the **Resource Sets** tab.
 - b. Click the **+** button. The **Assign Resource Set** dialog opens, listing the available resource sets.

Assign Resource Set

Multi-selection is possible. Confirm your selection with the button "Assign to Role".

All

Resource Set

Description

Added On

Last Modified

☒	Default Administrator Resources	Default Administrator Resour...	4/21/26, 11:57 AM	4/21/26, 11:57 AM
-------------------------------------	---------------------------------	---------------------------------	-------------------	-------------------

Cancel

Assign to Role

- c. Select the resource sets you want to assign to the role by selecting the checkbox. If no resource sets have been created yet, go to **Add Resource Set**.
 - d. Click **Assign to Role**.
6. Delete a resource set assignment:
 - a. Go to the **Resource Sets** tab.
 - b. Select a resource set from the list by selecting the checkbox and click the  icon.
 - c. A confirmation dialog appears. Click **Confirm**.
7. Click **Update Role**.

Delete Role

1. On the **Roles** page, select the role you want to delete from the list by selecting the checkbox.
2. Click the  icon.
3. A confirmation dialog appears. Click **Confirm**.

Manage Permission Sets

The **Permission Sets** page displays a list of all permission sets in your system.

GEUTEBRUCK Hub

Admin

Apps

Users

Resources

Settings

Permission Sets

This is the overview of all Permission Sets. If you want to add a Permission Set, click on the "+" above the table.

Q Search...

+

All	Permission Set	Description	Roles	Added On	Last Modified
☐	Permission Set				
☒	Default Administrator Permissions	Default Permission Set	Administrator	4/21/26, 11:57 AM	4/21/26, 11:57 AM
☐	Access G-Insights	Access G-Insights	G-Insights Operators	4/28/26, 11:27 AM	4/28/26, 11:27 AM
☐	test	test		5/19/26, 12:28 PM	5/19/26, 12:28 PM

Items per page: 10

1 - 3 of 3

<

>

Add Permission Set

Add a permission set to your system and assign the permissions to it.

- On the **Permission Sets** page, click the **+** icon. The **Add new Permission Set** page opens.
- Enter the name and (optional) the description of the permission set.

i **The permission set name must not already exist in the system.**

GEUTEBRUCK Hub Admin

[Back to Permission Sets](#)

Add new Permission Set

Fill in the required fields (marked with the star).

Name* Demo Description

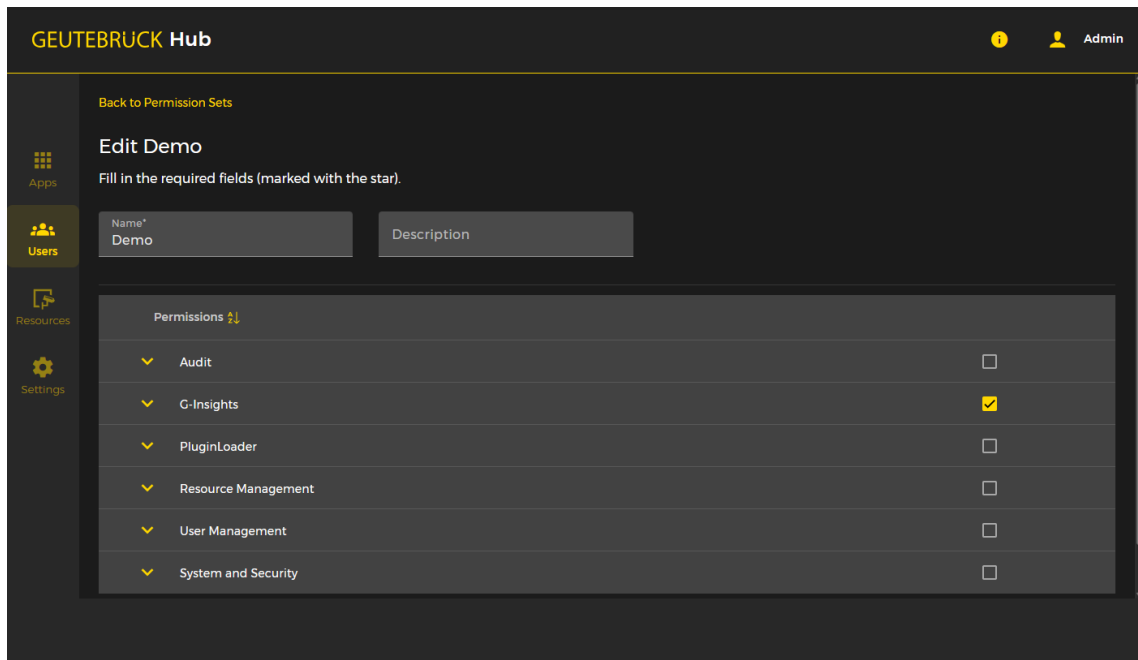
Permissions	
▼ Audit	☐
▼ G-Insights	☐
▼ PluginLoader	☐
▼ Resource Management	☐
▼ User Management	☐
▼ System and Security	☐

[Cancel](#) [Create Permission Set](#)

3. Select the permissions you want to assign to the permission set by selecting the checkbox.
4. Click **Create Permission Set**.

Edit Permission Set

1. On the **Permission Sets** page, hover your mouse over the row of the permission set you want to edit and click the  icon. The **Edit <Permission Set Name>** page opens.



2. Edit the name and (optional) the description of the permission set.
3. Select the permissions you want to assign to the permission set by selecting the checkbox.
4. Click **Update Permission Set**.

Delete Permission Set

1. On the **Permission Sets** page, select the permission set you want to delete from the list by selecting the checkbox.
2. Click the  icon.
3. A confirmation dialog appears. Click **Confirm**.

Manage Resource Sets

The **Resource Sets** page displays all resource sets in your system.

GEUTEBRÜCK Hub

Admin

Apps

Users

Resources

Settings

Resource Sets

This is the overview of all Resource Sets. If you want to add a Resource Set, click on the "+" above the table.

All	Resource Set	Description	Roles	Added On	Last Modified
☒	Default Administrator Resources	Default Administrator Resour...	Administrator	4/21/26, 11:57 AM	4/21/26, 11:57 AM
☐	G-Insights Demo		G-Insights Operators	4/28/26, 11:53 AM	4/28/26, 12:49 PM

Items per page: 10
1 - 2 of 2

Add Resource Set

Add a resource set to your system and assign the resources to it.

- On the **Resource Sets** page, click the **+** icon. The **Add new Resource Set** page opens.
- Enter the name and (optional) the description of the resource set.

The resource set name must not already exist in the system.

GEUTEBRÜCK Hub

Admin

Apps

Users

Resources

Settings

Back to Resources

Add new Resource Set

Fill in the required fields (marked with the star).

Name*
Demo

Description

Select all resources

No resource have been assigned. To assign a resource click on the following button.

Assign Resource to this Resource Set

Cancel

Create Resource Set

- Click the **+** **Assign Resource to this Resource Set** button. The **Assign Resource** dialog opens, listing the available resources (see **Manage Resources**).

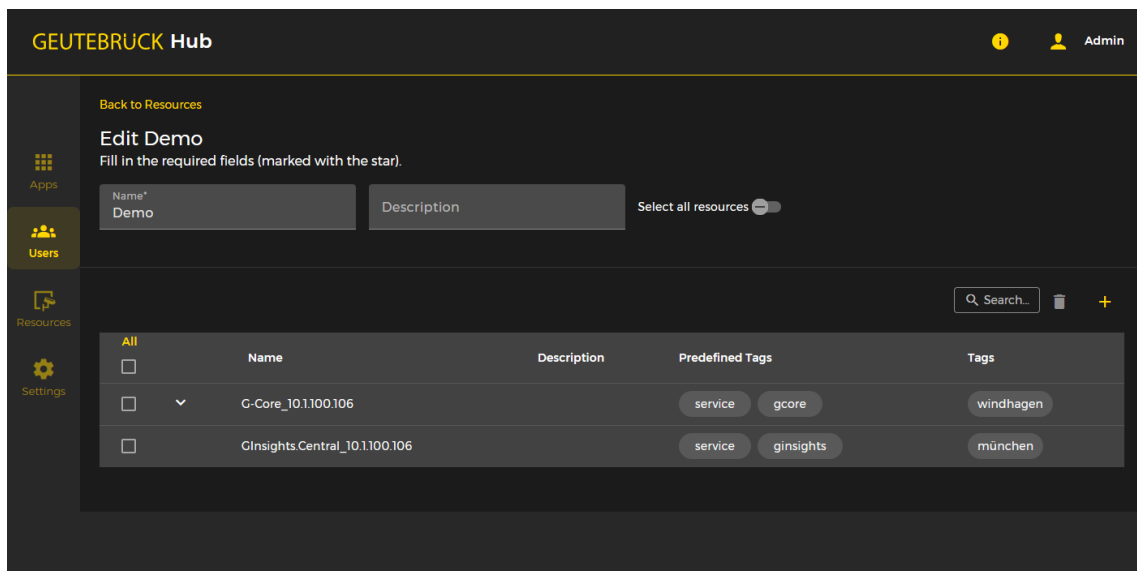
i Alternatively, you can enable the **Select all resources** option to **synchronize the resource set with the resources** (see **Manage Resources**). **All available resources will be added to the resource set, as well as any resources added in the future.**

All	Name	Description	Predefined Tags	Tags
☐	PluginLoader_127.0.0.1		service pluginloader	test tag
☒	G-Core_10.1.100.106		service gcore	windhagen
☒	GInsights.Central_10.1.100.106		service ginsights	münchen

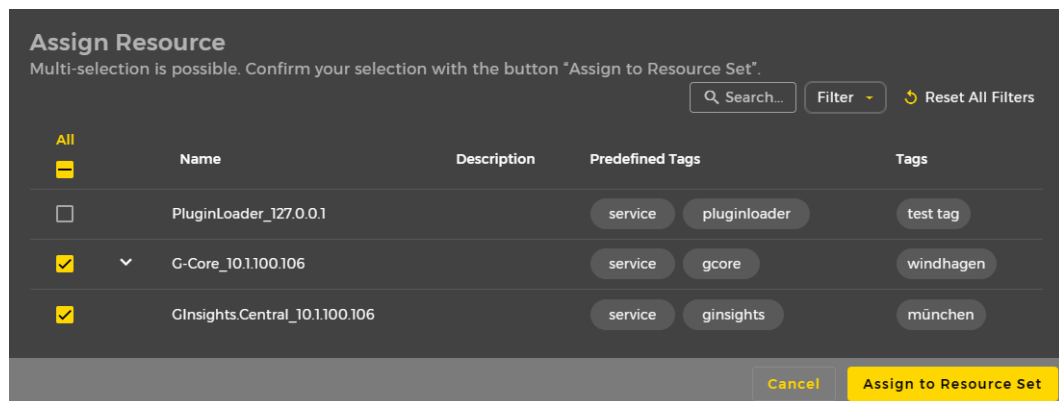
- Select the resources you want to assign to the resource set by selecting the checkbox.
- Click **Assign to Resource Set**.
- Click **Create Resource Set**.

Edit Resource Set

- On the **Resource Sets** page, hover your mouse over the row of the resource set you want to edit and click the  icon. The **Edit <Resource Set Name>** page opens.



2. Edit the name and (optional) the description of the resource set.
3. Assign a resource:
 - a. Click the **+** icon. The **Assign Resource** dialog opens, listing the available resources (see **Manage Resources**).



i Alternatively, you can enable the **Select all resources** option to synchronize the resource set with the resources (see **Manage Resources**). All available resources will be added to the resource set, as well as any resources added in the future.

- b. Select the resources you want to assign to the resource set by selecting the checkbox.
- c. Click **Assign to Resource Set**.

4. Delete a resource assignment:
 - a. Select a resource from the list by selecting the checkbox and click the  icon.
 - b. A confirmation dialog appears. Click **Confirm**.
5. Click **Update Resource Set**.

Delete Resource Set

1. On the **Resource Sets** page, select the resource set you want to delete from the list by selecting the checkbox.
2. Click the  icon.
3. A confirmation dialog appears. Click **Confirm**.

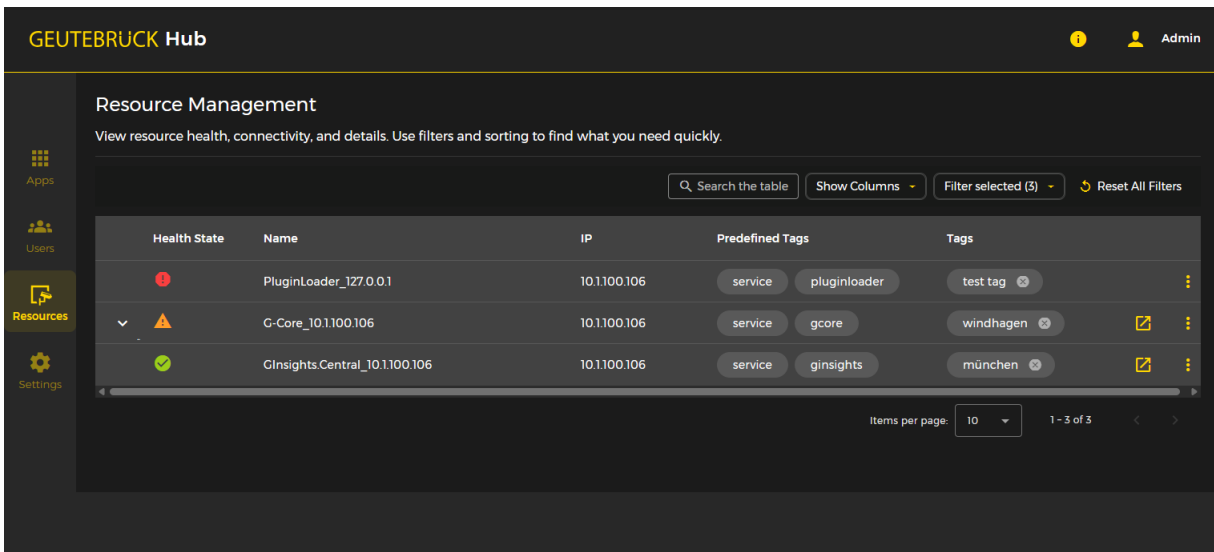
Resources

Manage Resources

The **Resource Management** page provides an overview of all resources connected to your system or were previously connected but are now disconnected.

 **You only see resources for which you have the required permissions.**

You can filter the list by text, predefined tags, custom tags (see **Add Tag**) and health state.



Add Tag

You can add custom tags to filter the resource list.

1. On the **Resource Management** page, double-click the Tags column of the resource to which you want to add a tag, or open the context menu and click **Add tags**.
2. In the **Type new tag** field, enter the name of the tag.
3. Click the icon.

Open Resource

You can open the user interface for resources that have their own user interface

via the resource list. To do this, click the icon for the resource whose interface you want to open.



You only see the icon if you have the required permissions.

Rename Resource

You can rename the resource services in the resource list.

1. On the **Resource Management** page, double-click the Name column of the resource you want to rename, or open the context menu and click **Rename service**.
2. In the **Enter new Name** field, enter the name of the resource service.
3. Click the  icon.

Remove Resource

You can remove a resource from the resource list.

1. On the **Resource Management** page, open the context menu of the resource you want to delete.
2. Click **Remove resource**. If a resource is connected, you cannot remove it. Disconnect the resource first.

 **You only see this option if you have the required permissions.**

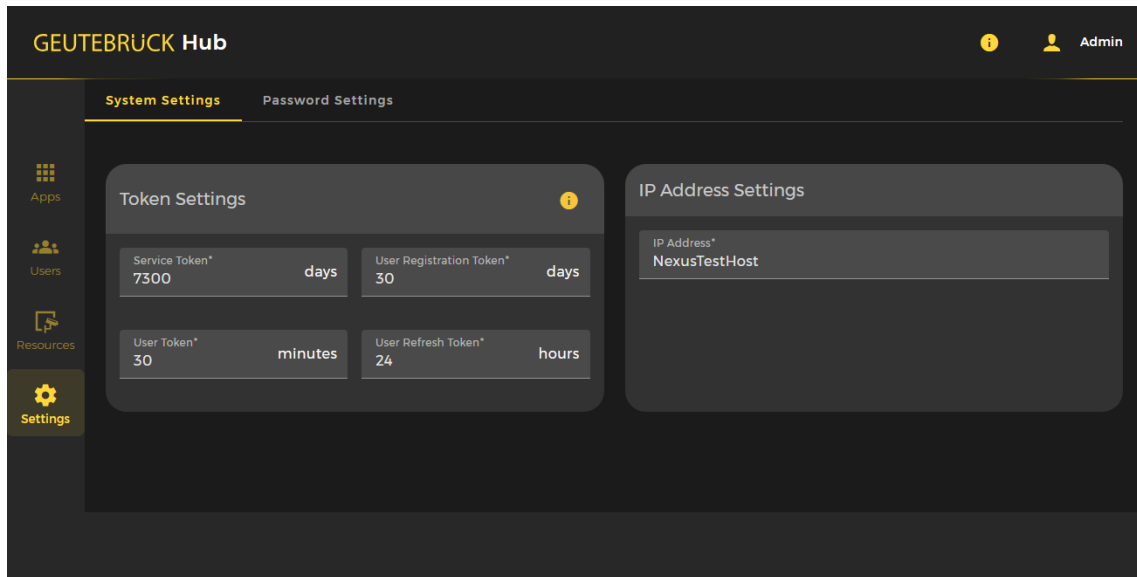
3. A confirmation dialog opens. Click **Remove**.

Settings

System Settings

Configure the system and password settings for the Geutebrück Hub.

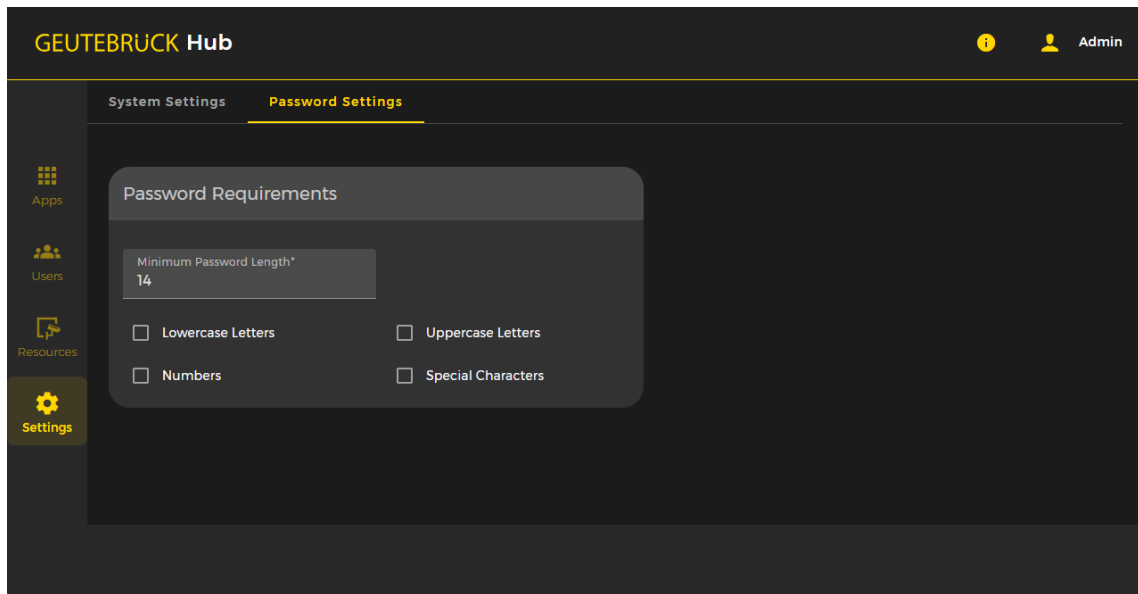
1. Open the **Settings** page and got to the **System Settings** tab.



2. In the **Token Settings** pane, configure the token expiration time.

Token	Description	Default
Service Token	Access token for system-to-system communication. Used by services instead of users.	7300 days
User Token	Grants access to the system after successful authentication. Required for all protected requests.	30 minutes
User Registration Token	Provides initial access during user registration. Enables the registration of new users. Once the token expires, the link for initial registration is no longer valid.	30 days
User Refresh Token	Used to renew an expired user token. Generates a new user and user refresh token pair.	24 hours

3. In the **IP Address Settings** pane, you can change the IP address or hostname used by the Geutebrück Hub.
4. Go to the **Password Settings** tab.



5. Configure the **Password Requirements**. Set the minimum password length and, optionally, additional password requirements.
6. Click **Save**.

G-Insights Settings

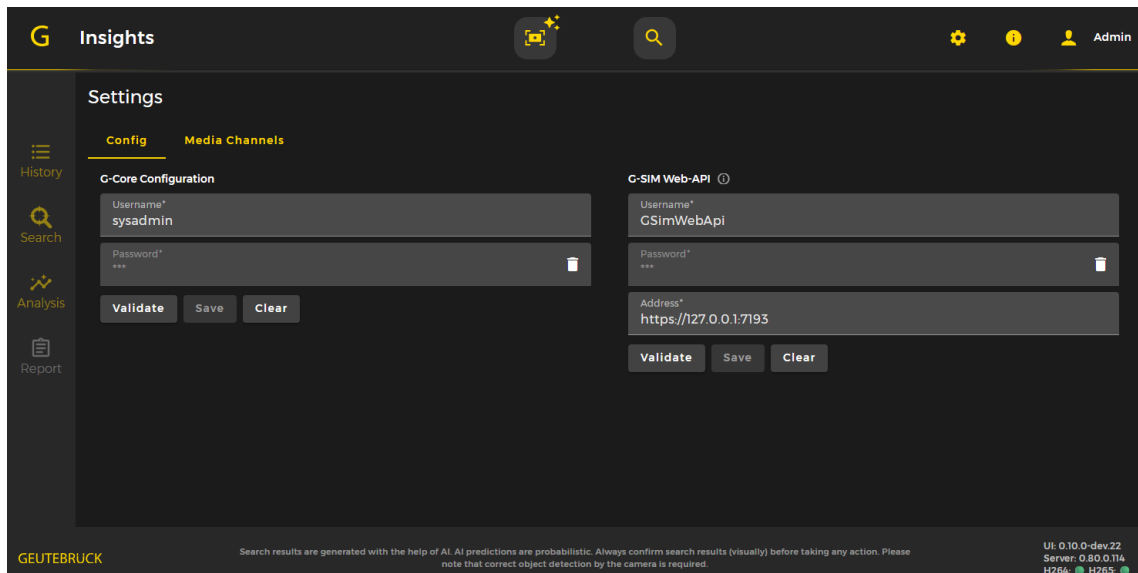
Set up the G-Insights settings for G-Core and, optionally, for G-SIM.

1. Open Geutebrück Hub via the desktop icon and go to **Settings > G-Insights**

or click the  icon in the G-Insights toolbar. The G-Insights **Settings** page opens.

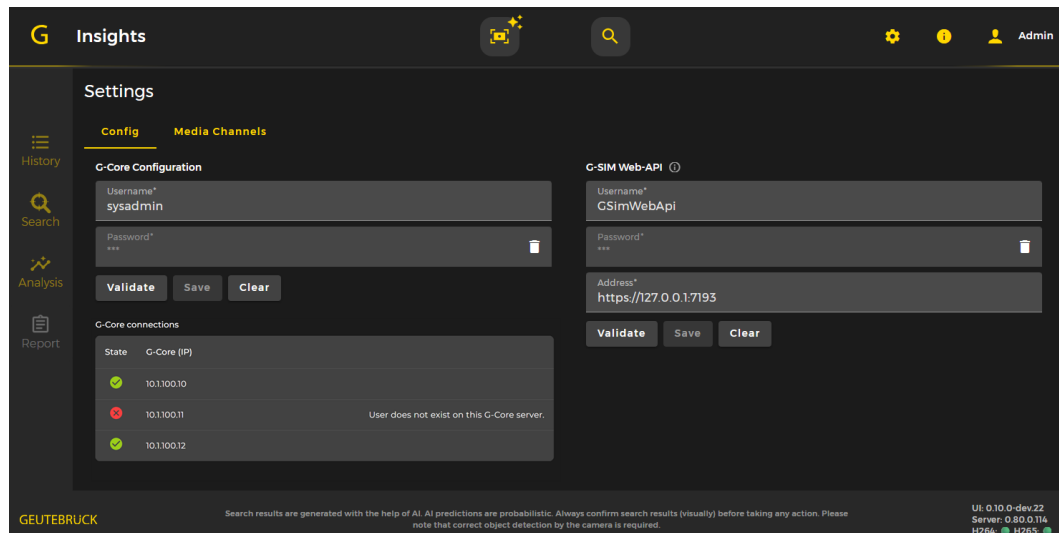
 **The G-Insights settings are only visible if you have the Edit G-Insights Settings permission and G-Insights is connected.**

2. Go to the **Config** tab.

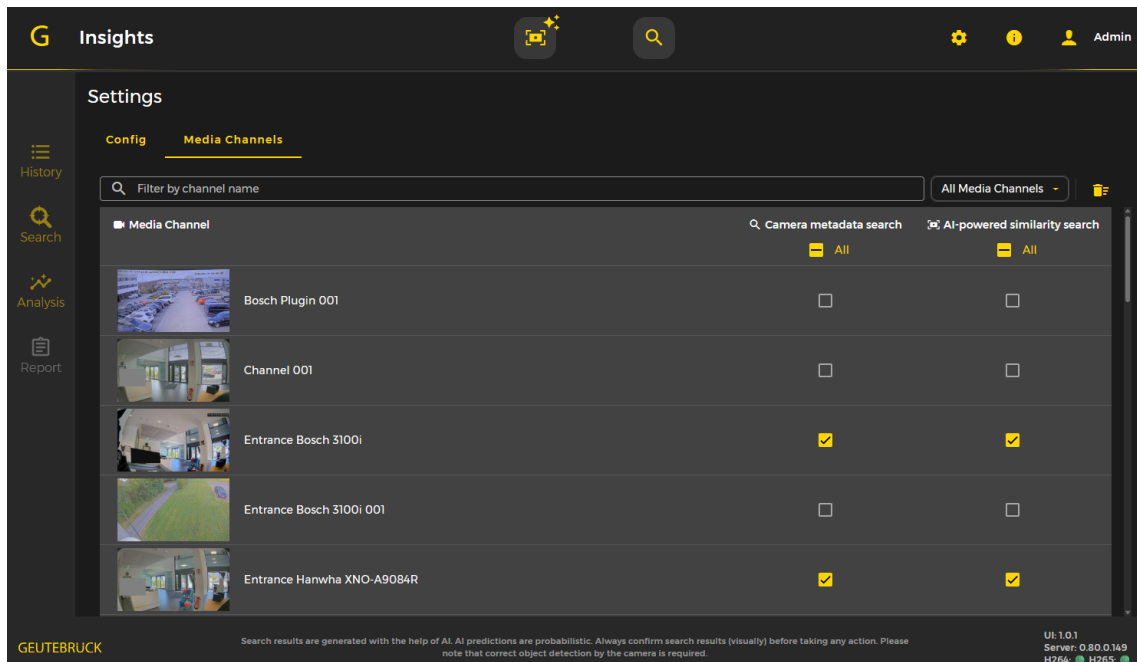


i All G-Core systems that you want to use in G-Insights must have a user with an identical username and password. Enter this username and password. These can be the default login details sysadmin and masterkey.

- Click **Validate**, to verify in which G-Core systems the specified user exists. The **G-Core connections** list appears, displaying all G-Core servers connected to the Geutebrück Hub and indicating whether the specified user exists.



- c. Click **Save** to save the G-Core configuration.
4. G-SIM Configuration (optional):
 - a. In the **Username** and **Password** fields, enter the username and password of the G-SIM user with the G-SIM Web API privilege (see **Set Up G-SIM (Optional)**).
 - b. In the **Host** field, enter the IP address and port of the G-SIM Web API (`https://<localhost or ip address>:7193`).
 - c. Click **Validate**, to verify the connection to the G-SIM Web API. If the connection is successful, a green check mark is displayed.
 - d. Click **Save** to save the G-SIM configuration.
5. Go to the **Media Channels** tab.
6. In the media channel list, enable the **Camera metadata search** option for the media channels you want to use in G-Insights. If you use AI-powered similarity search, also enable the **AI-powered similarity search** option.



7. Click **Save**.

Geutebrück Hub Security Guide

Purpose

Connected services authenticate to the Geutebrück Hub using service registrations and service tokens. Users authenticate interactively and receive short-lived sessions and access tokens.

Administrator Accounts

- Create a dedicated administrator account during installation.
- Use a strong, unique password and keep the number of administrators to a minimum.

Authentication And Authorization

- User access is controlled by Geutebrück Hub permissions and roles.
- Apply least privilege: Grant only the permissions required for the user's role.
- Regularly review user groups, roles, and administrator membership.

- Treat service tokens as sensitive credentials. Store and back them up only in accordance with approved administrative procedures.

Certificates And TLS

The Geutebrück Hub uses different certificates for various purposes:

Purpose	Use
Transport TLS	Secures HTTPS communication to the Geutebrück Hub.
Token signing	Signs access and service tokens.
Client certificate authentication	Optional mutual TLS, if enabled.

Token-Signing Certificate Rollover

Changing the token-signing certificate invalidates existing service tokens. Plan rollover as a maintenance task:

1. Install the new token-signing certificate on the Geutebrück Hub host.
2. Stop affected connected services.
3. Regenerate each service token using the product installer or the supported service-registration procedure.
4. Restart the services.
5. Verify that all services reconnect successfully.

If a service token may have been compromised, regenerate the affected service token immediately and review access to the service-registration directory.

Network Hardening

Default Geutebrück Hub endpoint:

- **Port:** 15003
- **Protocol:** HTTPS

G-Insights

Overview

System Overview

Main Features

G-Insights (G-Insights central service) is a web application that provides the following features:

- Forensic camera metadata search for persons and/or vehicles
- Forensic AI-powered similarity search based on an image or a free-text input (English, German, French, Spanish, Turkish or Arabic)
- Data insights and analytics via predefined dashboards featuring charts based on camera metadata of a selected channel

The system stores structured camera metadata, selected best-shot images, and semantic embeddings in separate technical stores. It does not store full raw video streams inside its core search databases. Video data is retrieved from G-Core.

G-Insights is intended to be used only for post-facto forensic search and analysis and lacks real-time alarm capabilities.

Functional Role of AI in Scope

Our AI-powered similarity search utilizes SigLIP2 (Sigmoid Language-Image Pre-training), an open-source vision-language model developed by Google Research (google/siglip2-so400m-patch16-384). SigLIP2 processes visual assets and text queries simultaneously, enabling highly accurate, multilingual, and context-aware image retrieval without relying on manual tagging.

To enable the system to perform semantic similarity search, SigLIP2 is used in G-Insights to transform:

- Best-shot images into image embeddings
- Text queries into text embeddings

SigLIP2 is not used here as a generative model, chatbot, automated decision writer, or autonomous case-resolution component.

What semantic space means:

- The model turns each image and each search prompt into a point in a very large mathematical map.
- Items with similar meaning end up close together.
- Items with different meanings end up farther apart.

Examples:

- A white truck should land closer to images of white trucks than to images of people.
- A person in blue trousers should land closer to matching person images than to unrelated vehicles.

That is why the system can support text-to-image and image-to-image search without a rules table for every possible phrase.

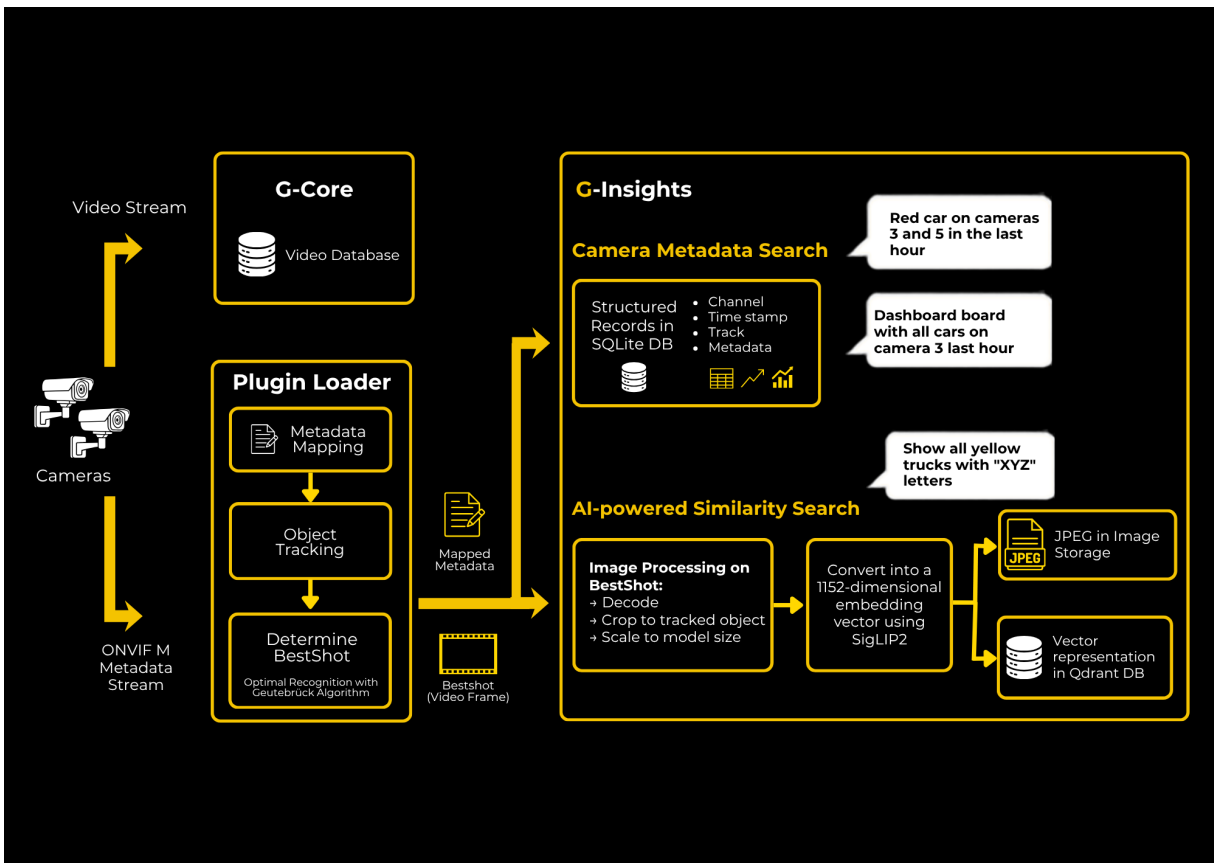
Storage Layout

G-Insights uses three logically distinct storage layers:

Storage Layer	Function	Main Data Type
SQLite	Camera object metadata	Object metadata such as timestamps, tracks, channel IDs, color attributes etc.
Qdrant	Semantic vectorindex	Text/Image embeddings and searchable payloadmetadata
Flat-file image storage	Best-shot image archive	JPEG best-shot images

Data Flow

Cameras send video streams and metadata streams. The video data is stored in the G-Core database. The ONVIF M metadata streams are processed in the Plugin Loader.



Bestshot Generation

A metadata mapping is done and an object tracking. For information on metadata mapping, see the PDF document [ONVIF Metadata Mapping](#).

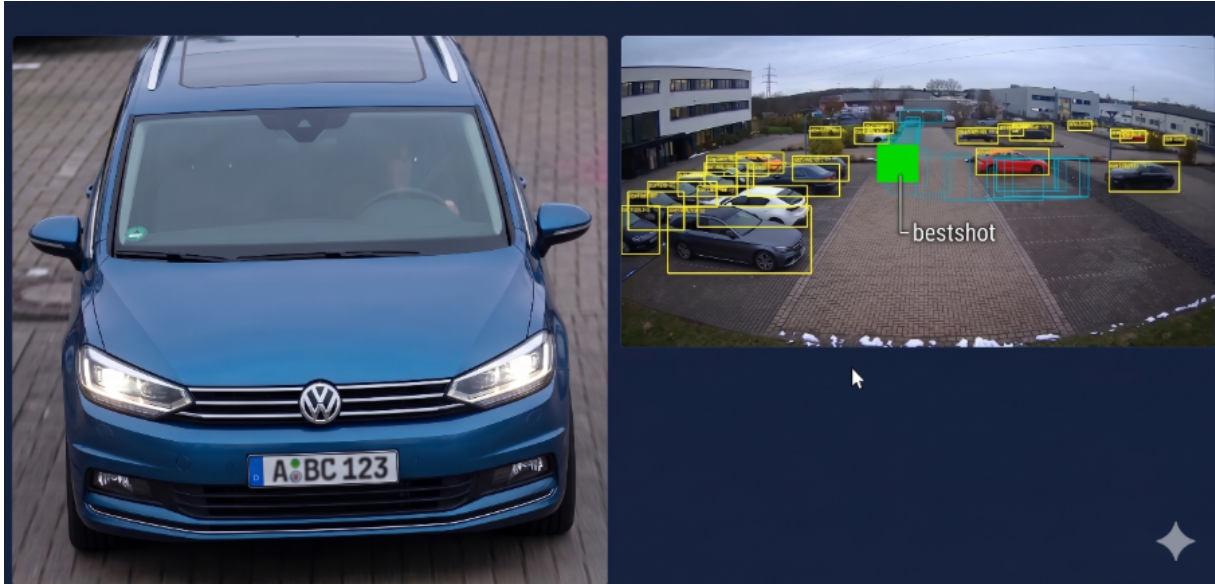
The object tracking determines a bestshot based on the object detection of the camera. Note that this is not the bestshot generated by the camera. The bestshot is the video frame that delivers optimal object recognition of an object.

The following figure illustrates the principle of best-shot generation.

- The right panel displays the full field of view, where all detected objects are outlined with yellow bounding boxes.
- For the object of interest, the tracking history is visualized via a sequence of blue bounding boxes.
- The green box defines the selected "bestshot" frame.
- The corresponding cropped best-shot image is presented on the left. This image clearly demonstrates optimal object recognition: the vehicle is cap-

tured at a track position close to the camera, maximizing resolution and providing a frontal perspective that ensures legible license plate recognition.

The resulting mapped metadata and bestshot are both forwarded to G-Insights.



Path

G-Insights has a camera metadata path and an AI-powered similarity path.

Camera metadata path:

The camera metadata path processes ONVIF M camera metadata sent via the camera's metadata stream and stores structured records in SQLite. These records include channel context, object timing, object tracking information, and other searchable forensic fields.

This path supports structured questions such as:

- Which objects appeared on a given channel/camera
- Within what time interval

AI-powered similarity path:

When AI-powered similarity search is enabled and a best-shot is available, a second processing path runs in parallel.

The system extracts a selected best-shot image that is

- decoded
- cropped to the tracked object

- scaled to the model input size
- converted into an 1152-dimensional embedding vector using SigLIP2

The system stores:

- The resulting JPEG in flat-file image storage
- The vector representation in Qdrant database

This means that the Qdrant database is populated from selected best-shot images of persons and/or vehicles, not from every raw video frame.

What This Means

In the AI-powered similarity search, only persons or vehicles can be found, that have previously been detected by the camera. In addition, arbitrary objects can be found that are in close proximity of a person or vehicle. For example. “A person walking with a dog” can be found by the AI-powered similarity search; “A dog wandering around on its own” cannot be found.

User Query Paths

The user-facing search behavior is easier to understand if it is split into two separate query paths.

Query Type	Primary Store	Result Type
Camera metadata search	SQLite	Structured metadata
AI-powered similarity search	Qdrant and flat-file image storage	Semantic matches plus returned JPEGs

Camera metadata search - SQLite

This is the classic structured search path.

Users ask questions such as:

- What objects were detected between two timestamps?
- Show vehicle count between two timestamps.

This path works against SQLite and returns structured records such as:

- Object metadata: object type and attributes (e.g. person with blue pullover)
- Timestamps
- Channel/Camera
- Other metadata fields if available

AI-powered similarity search - Qdrant and Image Storage

This is the semantic search path.

Users ask questions such as:

- Find images similar to this uploaded picture.
- Find a white truck with XYZ letters.
- Find a person holding a smartphone.

This path works in two stages:

1. Qdrant finds the nearest semantic matches using embeddings.
2. Flat-file image storage provides the actual JPEG images for those matching entries.

Compliance Information

G-Insights supports data privacy and responsible use of AI. In particular, G-Insights is compliant with DSGVO and EU AI act and provides the system administrator with the means to ensure compliant usage.

G-Insights is intended to be used only for post-facto forensic search and analysis, and lacks real-time alarm capabilities.

Only the administrator can activate data storage and searchability.

All critical actions are logged automatically in a tamper-proof log file secured by a blockchain.

The system contains these safeguards:

- Authenticated and permission-gated endpoints in secured hub mode
- Channel-scoped filtering so users only receive data from permitted camera sets
- Approved-model integrity checks to prevent silent model swaps

- Path-safety controls in image storage
- Retention cleanup to remove old vector-image pairs

EU AI Act Compliance & Prohibited Practices (Article 5)

To ensure safety, fairness, and alignment with European Union regulations, this platform features built-in compliance safeguards that strictly adhere to Article 5 of the EU AI Act.

What This Means

The system is legally restricted from processing inputs or generating outputs that fall into categories deemed an "unacceptable risk" by the EU. If a user prompt attempts to utilize the AI for any of the following prohibited practices, the system will automatically block the request and return a compliance error:

- **Behavioral Manipulation:** Subliminal techniques or purposeful manipulation designed to distort behavior and cause physical or psychological harm.
- **Social Scoring:** Evaluating or classifying individuals or groups over time based on social behavior or personal characteristics, leading to detrimental or unfavorable treatment.
- **Prohibited Biometric Categorization:** Deducing sensitive characteristics (e.g., political opinions, religious beliefs, race, sexual orientation) using biometric data.
- **Untargeted Scraping:** Creating or expanding facial recognition databases via untargeted scraping of CCTV footage or internet images.
- **Emotion Recognition:** Deploying systems to detect emotions in workplace or educational institution contexts (except for strict medical or safety reasons).

System Behavior

When an infraction is detected, the platform halts processing immediately. The prompt is handled in accordance with our secure compliance data policy, and a **"Request Blocked"** notification is displayed to the user.

In order to ensure that prohibited requests are not being processed, a filter chain gates AI-powered similarity search requests before the actual search executes.

The primary goal is to prevent unsafe or policyrelevant prompts from executing as unrestricted search operations. The secondary goal is to preserve businessacceptable search behavior for ordinary object and scene queries.

The filter architecture is designed to reduce the risk that a text query reaches the GenAI search engine when it requests or strongly correlates with prohibited or review-relevant content categories. The objective is not only to stop explicitly blocked wording, but also to route ambiguous cases into a controlled review state instead of treating every non-exact match as harmless.

To this end, the system checks queries in layers, starting with explicit blocked terms, then validating language handling, then comparing the prompt against a curated reference bundle of allowed and prohibited examples before deciding whether search may proceed.

Model Accountability and Governance

SigLIP2 is used to create embeddings for semantic similarity search.

Its functional role is limited to:

- Image-to-vector conversion
- Text-to-vector conversion
- Vector comparison in a shared semantic space

Deployment:

SigLIP2 is deployed as approved model assets loaded from disk at runtime.

The implementation shows:

- Loading of vision_encoder.onnx
- Loading of text_encoder.onnx
- Validation of approved assets via manifest and SHA-256 checks
- Fixed expected embedding dimension of 1152 for the approved SO400M variant

Fine-tuning and retraining status:

The current runtime does not show evidence of:

- Model fine-tuning
- Training loops
- Online learning
- Deployment-specific customer retraining

Model Limitations and Biases

Limitations:

- Short text context: text encoder is capped at **64 tokens**; longer captions/queries are truncated, losing detail.
- Optimized for short descriptive phrases, not long-form text, reasoning, or OCR-heavy content.
- Fixed visual resolution (FixRes variants) can distort aspect ratios; fine-grained details, small text, and counting are unreliable.
- Embedding-only model: no generation, no grounding/explanation of why an image matches.

Biases:

- Trained on large-scale web image-text pairs (WebLI), so it inherits Western/English-skewed and internet-culture biases despite multilingual training.
- Can reflect demographic, cultural, and stereotype associations (people, professions, attributes).
- Performance is uneven across languages and across underrepresented visual domains (e.g. non-Western scenes, medical/forensic imagery).

Security Information

The relevant security objective is that a caller must only be able to retrieve data the caller is authorized to access.

The implementation shows two layers of logical isolation.

Layer 1: authenticated and permission-gated API access

Protected endpoints require authenticated access. Sensitive operations use explicit product permissions, separating read-style operations from administrative or configuration actions.

Layer 2: channel-scoped result filtering

The search query is narrowed to the set of channels the caller is allowed to access.

For the AI-powered similarity search, the system applies the caller's allowed media-channel scope directly to the Qdrant query filter. In effect, the search result set is narrowed to the channel IDs the caller is permitted to access.

A user with access to Camera Group A only receives results for Camera Group A, even if the database also contains vectors from Camera Group B.

System Limits and Known Limitations

System Capacity and Sizing Guide

As you design and scale your system, understanding hardware limits is crucial for maintaining optimal performance.

Server Limits

A maximum number of 20 G-Core connections are recommended for use with G-Insights.

Channel Limits

System capacity is driven by the data rate (bestshots per minute) across your channels, rather than just the absolute number of cameras or detected objects (persons/vehicles).

Key Concept: Objects vs. Bestshots

In an ideal scenario, one moving object equals one track, which equals one bestshot. However, in real-world conditions (e.g., temporary occlusions, lighting changes), a camera may lose a track and restart it. This means a single object can generate multiple bestshots. Always calculate your capacity based on the actual bestshot rate. For instance, if a camera loses sight of a person for a split second (because they walked behind a pillar or turned around), it treats them as a brand-new track. One person can easily generate 3 or 4 "bestshot" images. If you are unsure about the bestshot rate for your channels, we strongly recommend that you view the bestshots in your camera's user interface to check how often tracks are lost.

Reference Scenarios & System Limits

To make sizing easy, we categorize customer cameras into two types.

Low rate channels:

- **What it looks like:** Quiet hallways, emergency exits, back lots, or areas with an average of 0 to 3 bestshot images per minute.
- **The Limit:** We can support up to 100 channels maximum if the entire system is low-traffic. These 100 channels can be used in all G-Insights features.

Medium rate channels:

- **What it looks like:** Main lobbies, busy turnstiles, main entrances, or areas with an average of 5 to 20 bestshot images per minute.

- **The Limit:** We can support up to 50 channels maximum for camera metadata search and analytics, thereof 30 channels for AI-powered similarity search.

The following table gives more details:

Metric / Limit	Low Rate	Medium Rate
Average frequency	0 – 3 bestshots / minute / channel	5 – 20 bestshots / minute / channel
Peak frequency (1-min window)	Up to 8 bestshots /minute / channel	Up to 40 bestshots / minute / channel
Maximum G-Insights channels	100 channels	See the "Mix & Match" Rule
Maximum metadata search and analytics channels	Included in the maximum of 100	50 channels
Maximum AI-powered similarity search channels	Included in the maximum of 100	30 channels (subset of the 50 channels above)

The "Mix & Match" Rule (How to combine them)

If your system has a mix of quiet and busy cameras, use this rule of thumb: **1 Medium rate Camera = 2 Low rate Cameras.**

Note that there is an hourly storage limit of a maximum of 36,000 bestshots / hour (shared across all AI-powered similarity search channels).

- **Example A (maximum low rate):** 100 low rate cameras + 0 medium rate cameras = Perfect
- **Example B (The 50/50 Mix):** 50 low rate cameras + 25 medium rate cameras = Perfect
 - Keep in mind that a maximum of 36,000 bestshots / hour can be stored for the AI-powered similarity search. This means, you can activate all 25 medium rate channels OR all 50 low rate channels for AI-powered similarity search.
- **Example C (maximum medium rate):** 0 low rate cameras + 50 medium rate cameras = Perfect

The "High-Traffic" Scenario: When to Scale Up

Our standard rules apply to low and medium frequency. For high-frequency scenarios—such as a major airport terminal, a stadium entrance during event rush hour, or a busy multi-lane highway intersection—the bestshot rate easily exceeds 40+

bestshots per minute. High-frequency environments will quickly overload standard configurations. In these cases, the hardware must be carefully scaled up.

General Limitations

- Finding a person or vehicle in G-Insights requires correct object detection and classification by the cameras in use.
- The size of a person or vehicle in the video depends on the field-of-view and the perspective of the camera.
- Weather conditions such as heavy rain or snow may affect the detection accuracy.
- Lighting conditions influence detection accuracy and correctness of metadata color attributes.
- A single object can generate multiple search results. For instance, when the camera tracking generates multiple tracks or when a person or vehicle is temporarily obscured by another object.

Data Storage and Retention Time

After installation, per default, no data is stored by G-Insights.

In the **Media Channels** tab of the **G-Insights Settings**, channels can be selected for use in G-Insights. To activate data storage so that the search and analytics features can be used, select the channels for use in the camera metadata search and analytics features, and/or in the AI-powered similarity search feature.

After activation, the data is stored during the configured retention time which is 30 days by default.

 **When similarity search is first activated, the system requires a brief initialization period to load the necessary AI models. As a result, users may experience a temporary, one-time delay during the very first search execution. Subsequent searches will perform at standard speeds.**

You can configure the retention time in the file `c:\-programdata\geutebrueck\ginsights\appsettings.machine.json` by setting the respective parameters for

- **Camera metadata:** `Workers.MetadataRetention` (format DD:mm:ss.SSS)
- **AI-powered similarity search:** `GenAIRetention.RetentionDays`

Example

You can find an example in the file `C:/-`

`pro-`

`gram-`

`data/geutebrueck/ginsights/appsettings.machine.json.template`

.

The configured retention time must not exceed the retention time configured for video storage in G-Set.

When the drive becomes too full, the system automatically deletes the oldest metadata and image/vector pairs until space returns to the safe range.



IMPORTANT: Dedicated Metadata Partition: Reserve the partition configured for the SQLite database exclusively for metadata storage. Storing other files on this drive—even temporarily—can cause the partition to fill up and result in critical system failure.

For the AI-powered similarity search data (vectors and bestshot images), the implementation uses a high-watermark / low-watermark deletion service.

The deletion sequence is:

1. Check disk usage of the similarity search storage drive.
2. Start cleanup when the configured high watermark is exceeded.
3. Identify the oldest vector entries.
4. Delete vectors first.
5. Delete corresponding image files second.
6. Continue until usage falls below the low watermark.

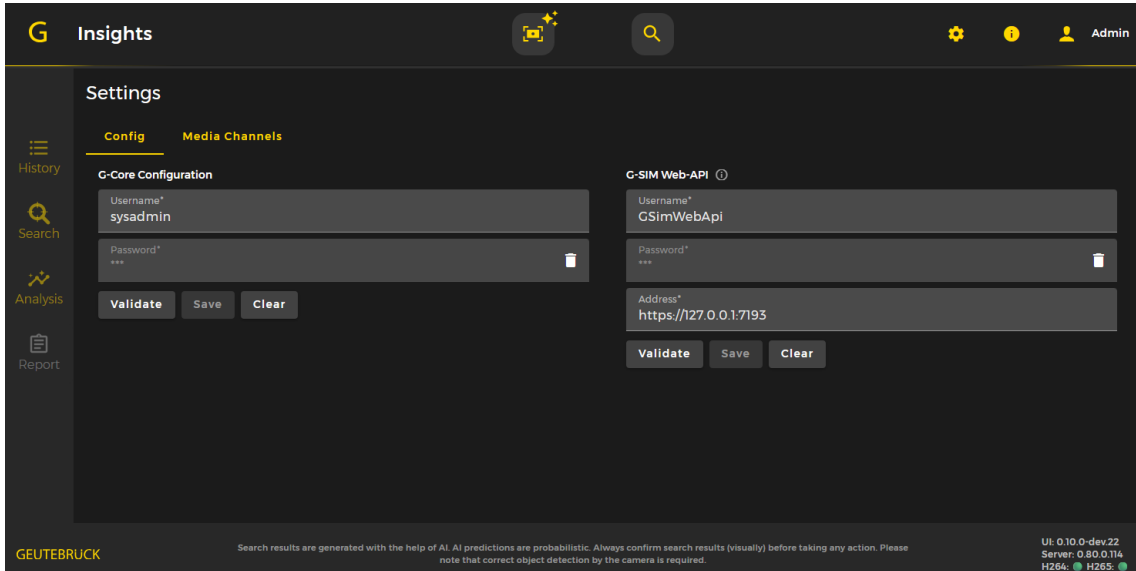
G-Insights Settings

Set up the G-Insights settings for G-Core and, optionally, for G-SIM.

1. Open Geutebrück Hub via the desktop icon and go to **Settings > G-Insights** or click the  icon in the G-Insights toolbar. The G-Insights **Settings** page opens.

 **The G-Insights settings are only visible if you have the Edit G-Insights Settings permission and G-Insights is connected.**

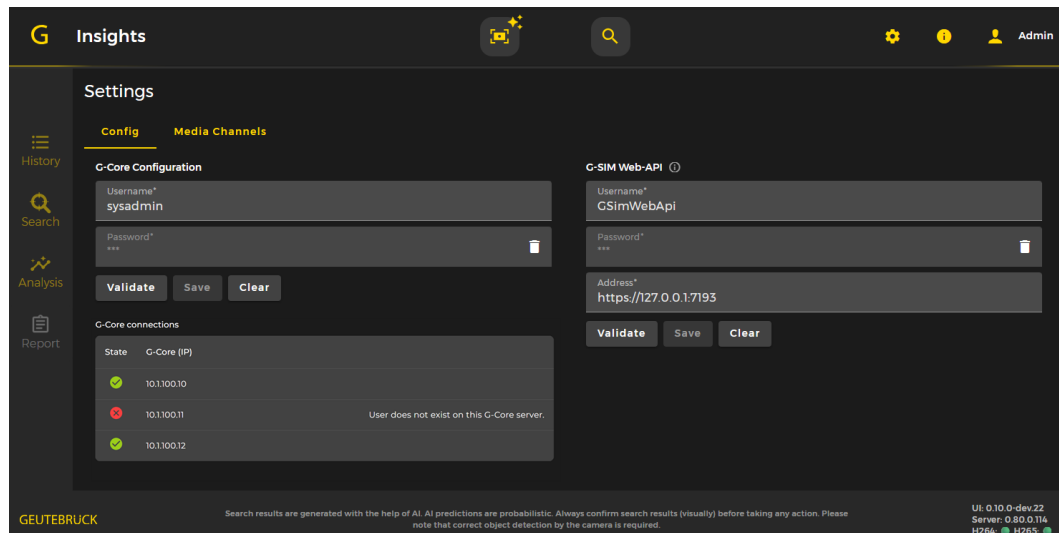
2. Go to the **Config** tab.



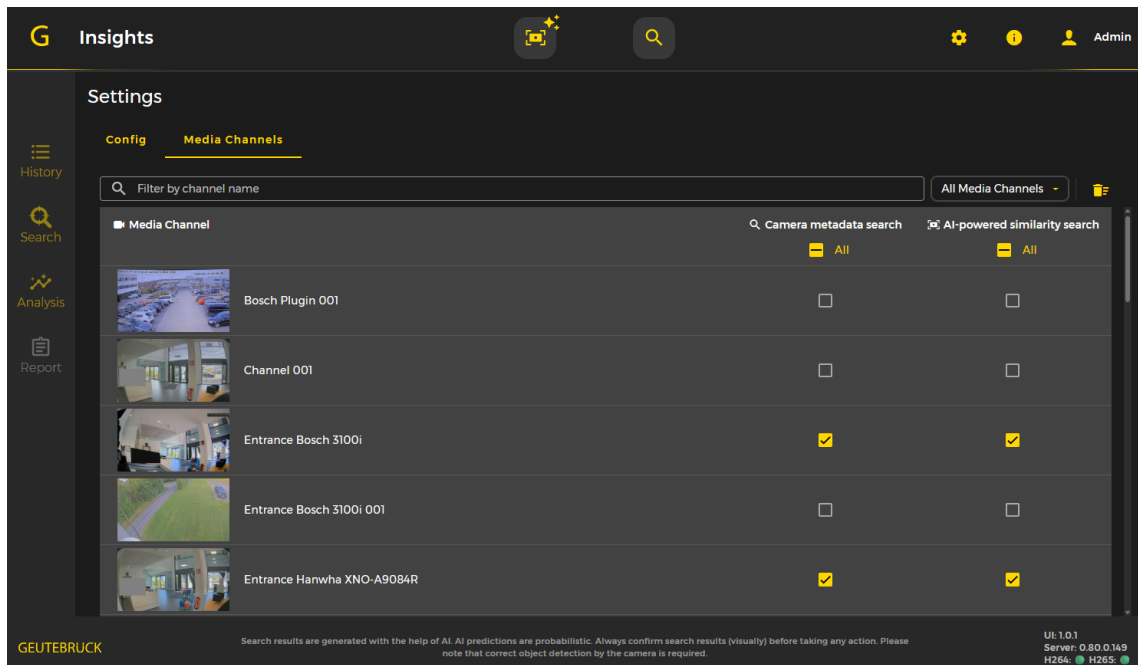
The screenshot shows the 'G Insights' settings page with the 'Config' tab selected. The page is divided into two main sections: 'G-Core Configuration' and 'G-SIM Web-API'. Each section contains input fields for 'Username', 'Password', and 'Address', along with 'Validate', 'Save', and 'Clear' buttons. The 'G-Core Configuration' section has a trash icon next to the password field. The 'G-SIM Web-API' section also has a trash icon next to the password field. The 'Address' field in the 'G-SIM Web-API' section contains the value 'https://127.0.0.1:7193'. The page footer includes the 'GEUTEBRÜCK' logo, a disclaimer about AI search results, and version information: 'UI: 0.10.0-dev22, Server: 0.80.0.114, H26A, H265'.

3. G-Core Configuration (required):
 - a. Enter the **Username** and **Password** of G-Core.

 **All G-Core systems that you want to use in G-Insights must have a user with an identical username and password. Enter this username and password. These can be the default login details `sysadmin` and `masterkey`.**
 - b. Click **Validate**, to verify in which G-Core systems the specified user exists. The **G-Core connections** list appears, displaying all G-Core servers connected to the Geutebrück Hub and indicating whether the specified user exists.



- c. Click **Save** to save the G-Core configuration.
4. G-SIM Configuration (optional):
 - a. In the **Username** and **Password** fields, enter the username and password of the G-SIM user with the G-SIM Web API privilege (see **Set Up G-SIM (Optional)**).
 - b. In the **Host** field, enter the IP address and port of the G-SIM Web API (`https://<localhost or ip address>:7193`).
 - c. Click **Validate**, to verify the connection to the G-SIM Web API. If the connection is successful, a green check mark is displayed.
 - d. Click **Save** to save the G-SIM configuration.
5. Go to the **Media Channels** tab.
6. In the media channel list, enable the **Camera metadata search** option for the media channels you want to use in G-Insights. If you use AI-powered similarity search, also enable the **AI-powered similarity search** option.



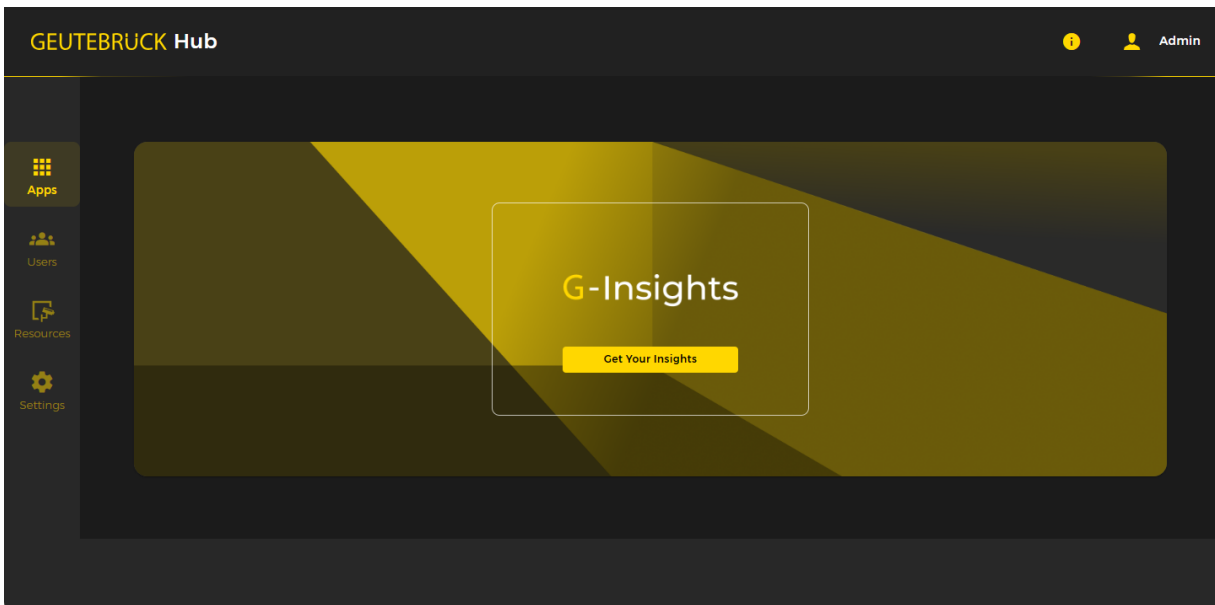
7. Click Save.

Using G-Insights

Open G-Insights

Open the Geutebrück Hub. On the **Apps** page, click the **Get Your Insights** button.

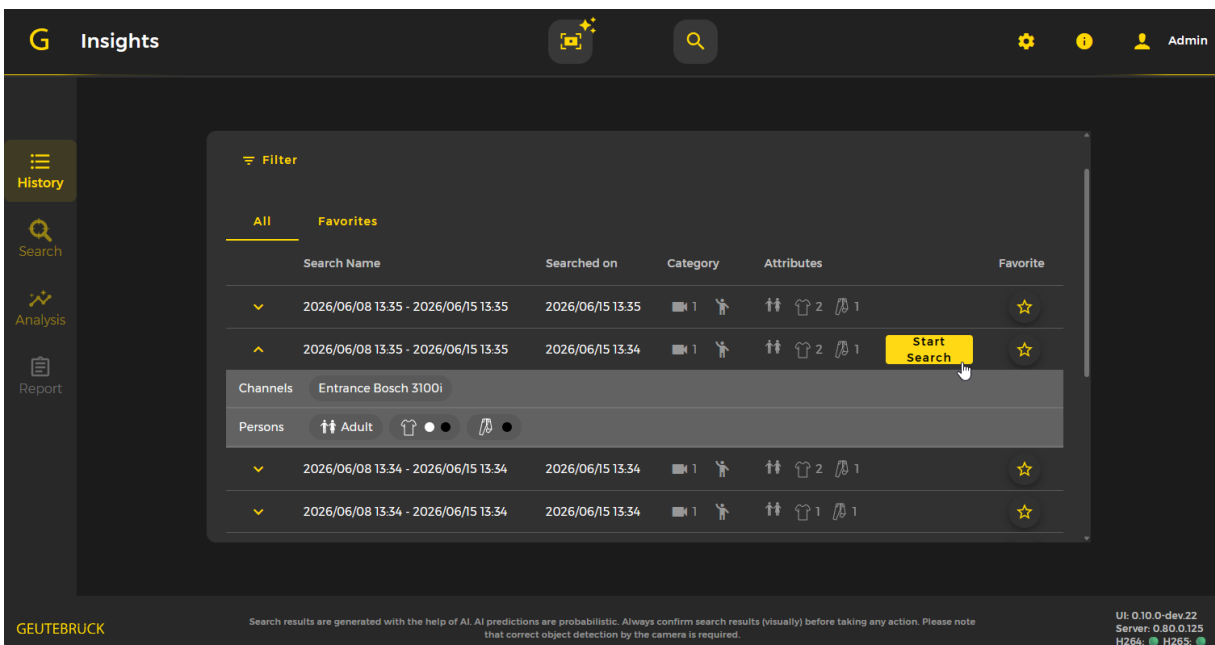
i You only see the G-Insights app if you have the required permissions.



History

The **History** page lists your last 100 search entries from the camera metadata search.

- Hover your mouse over the row of a search entry and click the **Start Search** button, to start the search again.
- Click the  icon to save the search entry in your **Favorites** list.

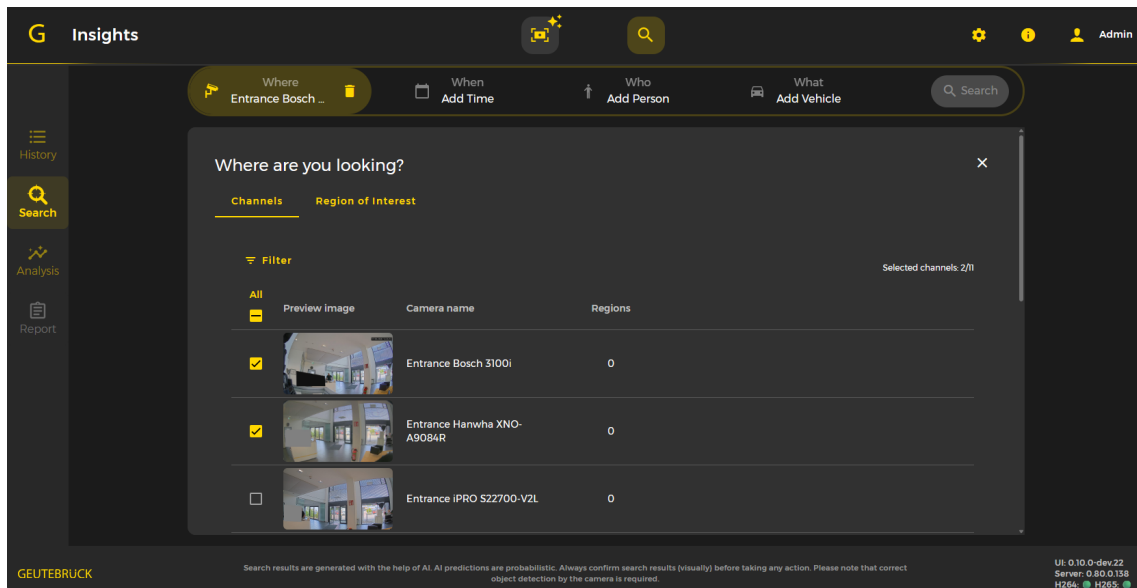


Search

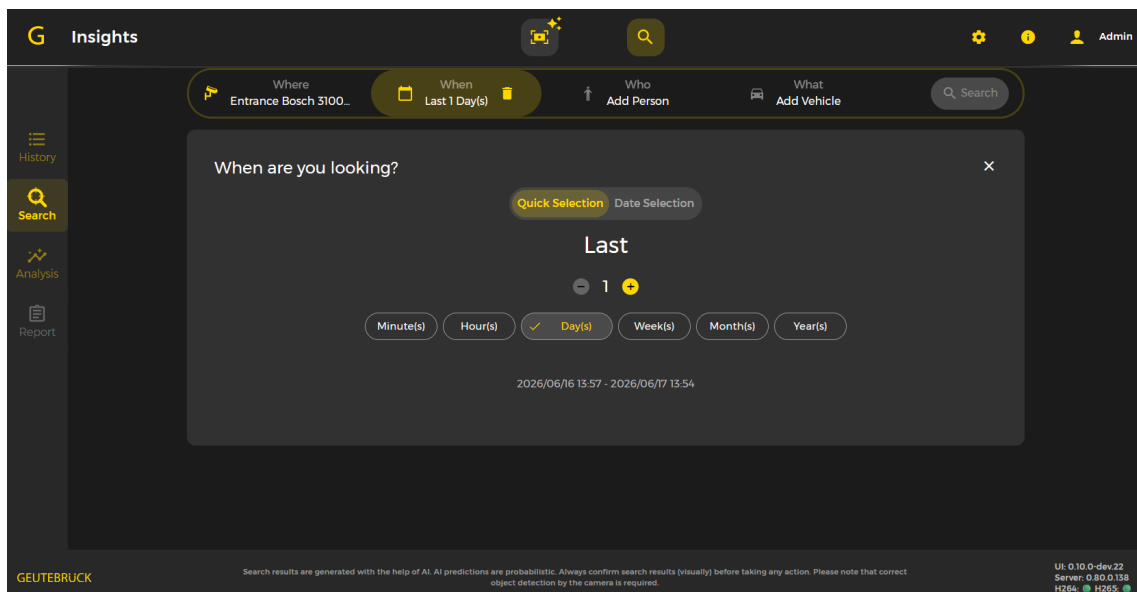
Camera Metadata Search

You can search using the camera metadata search.

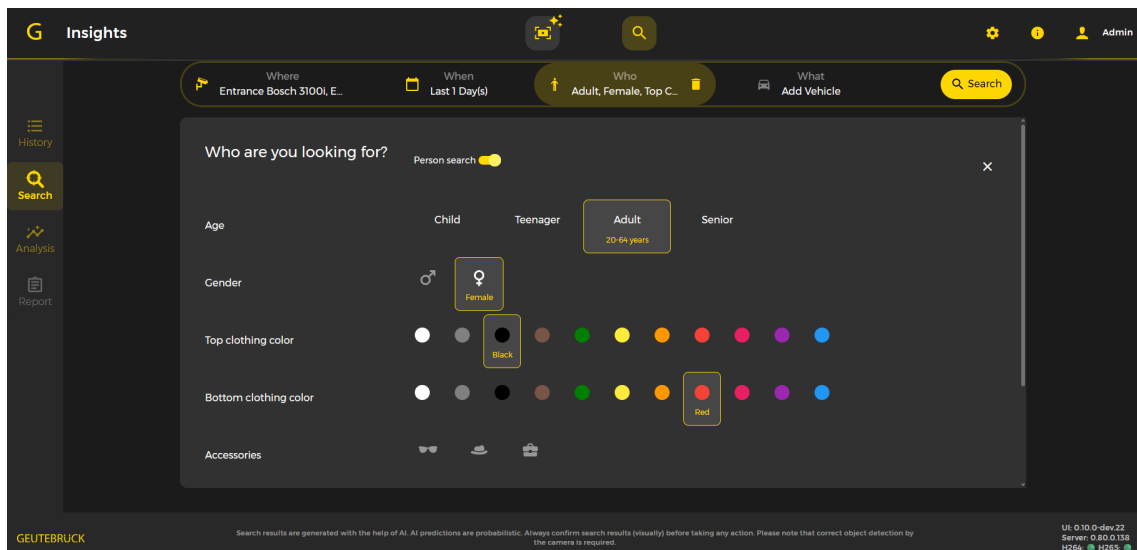
1. Click the  icon in the toolbar. The **Camera metadata search** page opens.
2. On the **Where** tab, select the media channels you want to use for your search. In the **Region of Interest** tab, you can optionally mark an area of interest for a selected camera.



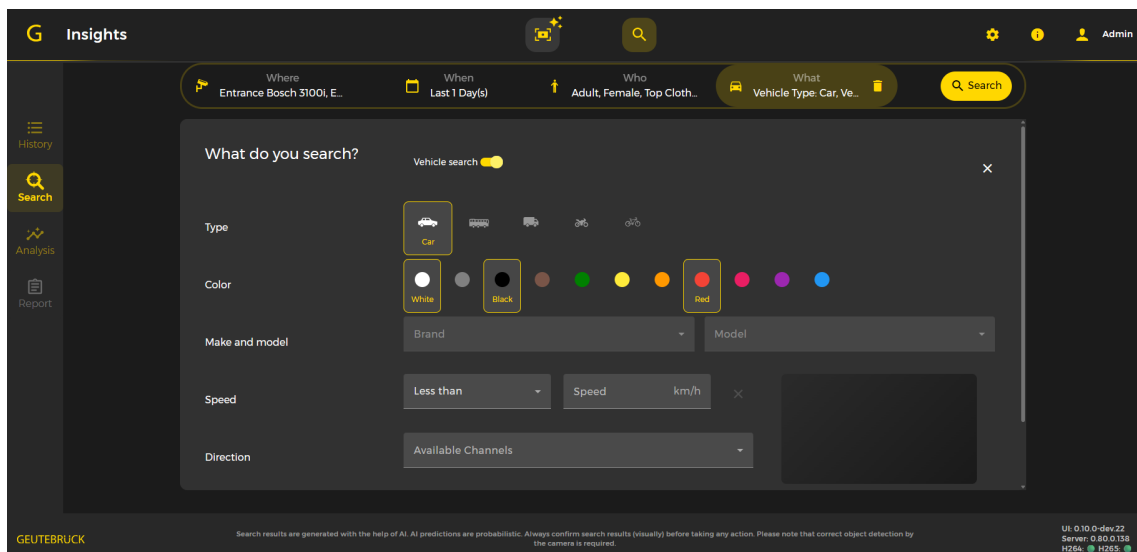
3. On the **When** tab, select the time range you want to search within.



- On the **Who** tab, enable the **Person search** slider if you want to search for persons, and select the person attributes.



- On the **What** tab, enable the **Vehicle search** slider if you want to search for vehicles, and select the vehicle attributes.



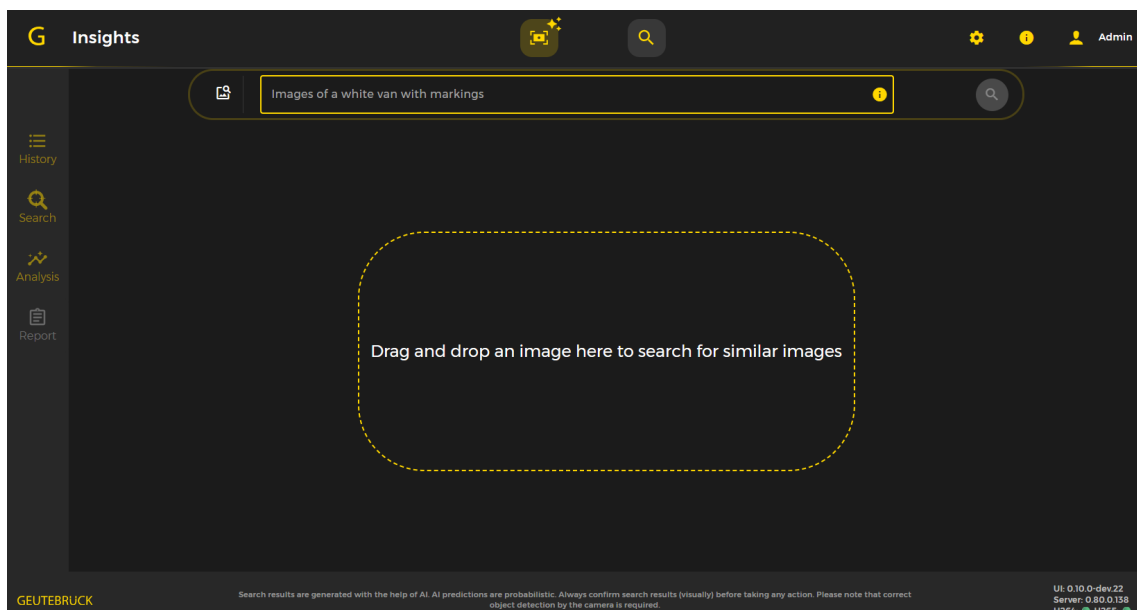
6. Click  **Search**. The search results are displayed (see **Search Results**).

The search entry is added to the **Search** menu, and your search entry is saved in the **History**.

AI-Powered Similarity Search

You can search using the AI-powered similarity search.

1. Click the  icon in the toolbar. The **AI powered similarity search** page opens.



- Click the  icon or drag an image into the drag-and-drop field to search for a similar image.
- Enter your search prompt in the text field. Click the  icon to get help in writing your prompt.
- Click the  **Search**. The search results are displayed (see **Search Results**).

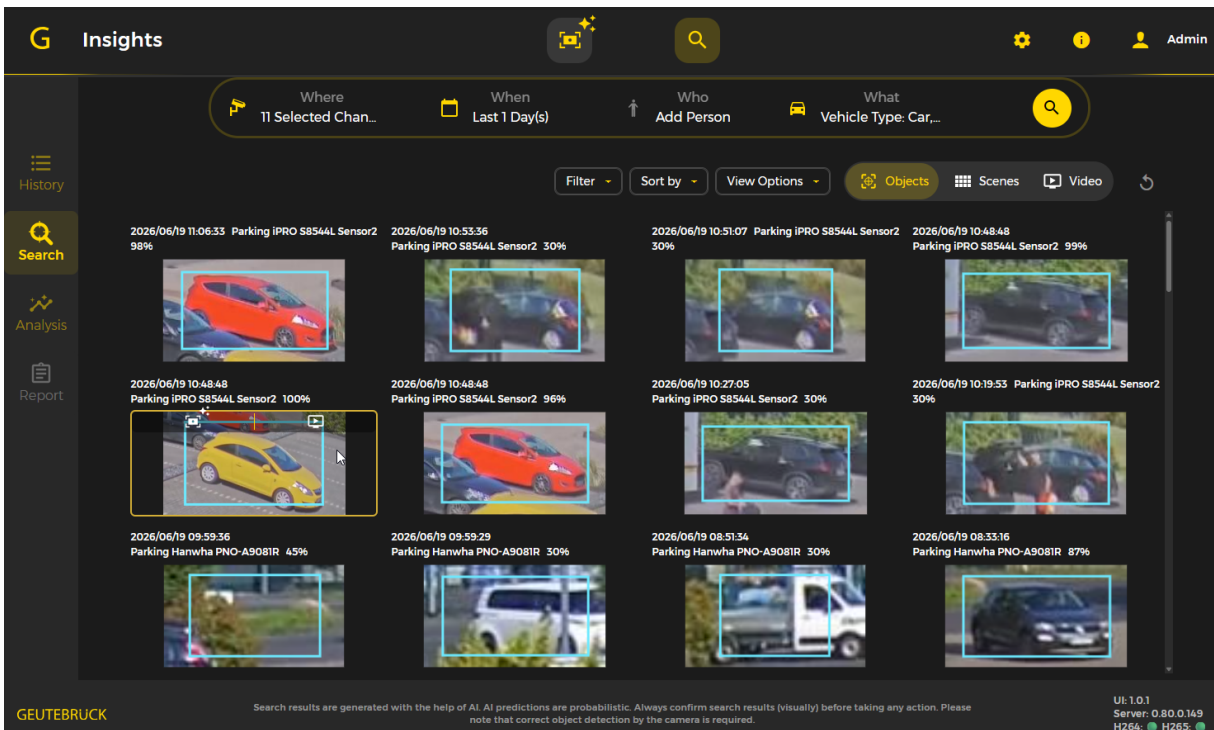
Search Results

The search results page displays thumbnails of all objects found that match your search.

You can filter the search results by likelihood, time and channels, and switch between the object view and scene view.

You can perform additional actions on an found object:

- Click the  icon of a thumbnail to start the AI-powered similarity search for the object.
- Click the  icon of a thumbnail to open the viewer and play the video of the object.



Insights

Where: T1 Selected Chan... When: Last 1 Day(s) Who: Add Person What: Vehicle Type: Car...

Filter Sort by View Options Objects Scenes Video

Timestamp	Sensor	Confidence
2026/06/19 11:06:33	Parking IPRO S8544L Sensor2	98%
2026/06/19 10:53:36	Parking IPRO S8544L Sensor2	30%
2026/06/19 10:51:07	Parking IPRO S8544L Sensor2	30%
2026/06/19 10:48:48	Parking IPRO S8544L Sensor2	99%
2026/06/19 10:48:48	Parking IPRO S8544L Sensor2	100%
2026/06/19 10:48:48	Parking IPRO S8544L Sensor2	96%
2026/06/19 10:27:05	Parking IPRO S8544L Sensor2	30%
2026/06/19 10:19:53	Parking IPRO S8544L Sensor2	30%
2026/06/19 09:59:36	Parking Hanwha PNO-A9081R	45%
2026/06/19 09:59:29	Parking Hanwha PNO-A9081R	30%
2026/06/19 08:51:34	Parking Hanwha PNO-A9081R	30%
2026/06/19 08:33:16	Parking Hanwha PNO-A9081R	87%

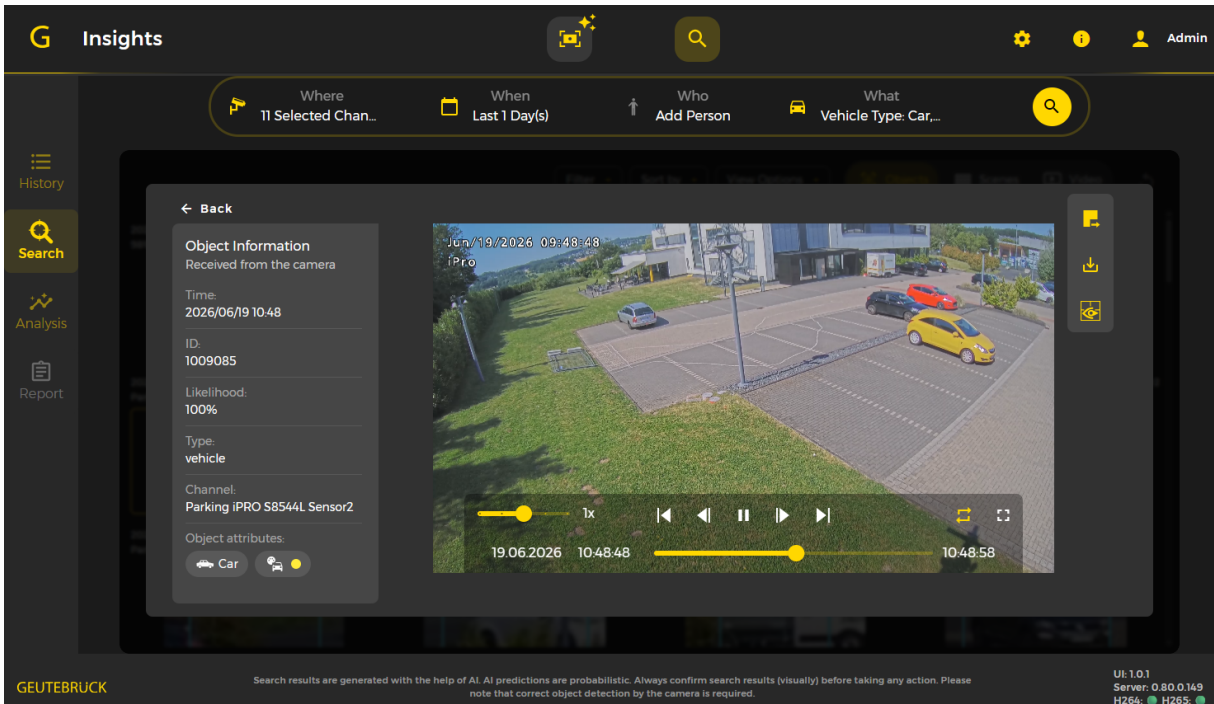
GEUTEBRUCK

Search results are generated with the help of AI. AI predictions are probabilistic. Always confirm search results (visually) before taking any action. Please note that correct object detection by the camera is required.

UI: 1.0.1
Server: 0.80.0.149
H264: H265:

In the viewer, you can perform additional actions:

-  Save Video
-  Save as Image
-  Open in G-SIM (For more information on how open G-Insights in G-SIM, see the G-SIM documentation.)

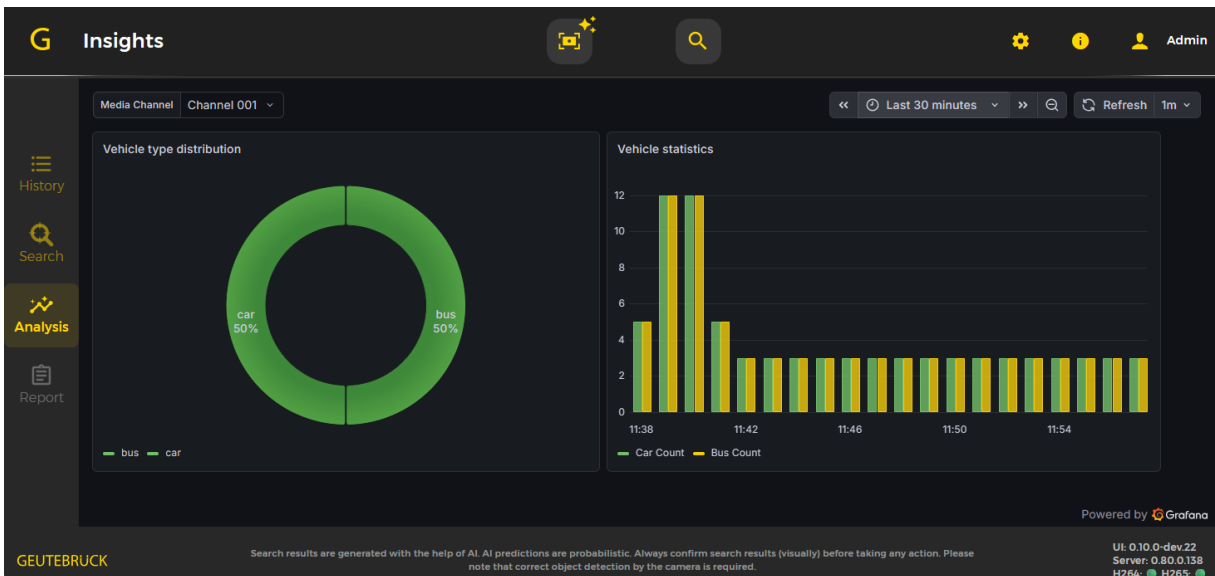


Analysis

The **Analysis** menu includes the **People Board** page and **Vehicle Board** page. On these dashboards, you can view data on the people and vehicles detected by the available cameras in G-Insights.

You can customize what data is displayed:

- Select the media channel whose data you want to view from the **Media Channel** drop-down list.
- Select the time period for which you want to view data.
- For more actions, open the context menu via the  icon of a data field.



FAQ and Troubleshooting

Hardware

- You don't have the specified NVIDIA graphics card? No problem, camera metadata search does not require a GPU.
- The application is too slow? Check if your server meets the minimum hardware requirements.

Data Flow

How is the data flow in simple terms? G-Insights turns camera output into three linked storage layers. SQLite database stores the camera metadata. Qdrant vector database stores AI embeddings for semantic search. Flat image storage holds the actual best-shot JPEG files that are returned with similarity-search results.

Security / RBAC

How is your data kept secure? In secured hub-connected deployments, user access is enforced in two steps: first the user must be authenticated and authorized for the API, and then the search/query layer restricts results to the camera channels that user is allowed to access.

Supported Languages

The user interface can be used in English, German, French or Spanish. Simply set your browser's language accordingly.

AI-powered similarity search can process free-text inputs in English, German, French, Spanish, Turkish or Arabic.

AI Model Accountability

How about responsible AI? SigLIP2 is used as a fixed out-of-the-box embedding model, not as a fine-tuned customer model. It maps text and images into the same semantic space so the system can perform semantic search. The code exhibits its strong model-integrity controls.

Search Results in Camera Metadata Search

You don't find what you are searching? This might have various reasons:

- Note that the quality of the search results depends on the quality of the metadata sent by your cameras. Check your camera configuration.
- The user interface displays tips to help you find a solution.

Recommendations:

- Search for car, instead of red car.
- Search for person, instead of man with backpack.
- Increase the search time range.
- Use the AI-powered similarity search.

Search Results in AI-Powered Similarity Search

You don't find what you are searching for? This might have various reasons:

In the AI-powered similarity search, only persons or vehicles can be found, that have previously been detected by the camera. In addition, arbitrary objects can be found that are in close proximity of a person or vehicle. For example. "A person walking with a dog" can be found by the AI-powered similarity search; "A dog wandering around on its own" cannot be found.

Recommendations:

- Try out our prompting tips:
 - Avoid single words:
 - Prompt "man sitting on chair", instead of "man".
 - Context helps the AI to retrieve better matching results.
 - Describe the context:
 - Prompt "person putting a phone in a bag", instead of "phone".
 - Only objects close to a person or vehicle are retrievable by AI.
 - Omit the location and time:
 - Prompt "black Audi A6" instead of "black Audi A6 yesterday in the main parking lot."
 - You can filter your search results by camera and time after clicking "Search."
- Use English as prompting language.
- Use the camera metadata search.
- If you still get no or too few results, check your camera configuration.

G-Insights Security Guide

Geutebrück Hub Trust And Service Token

G-Insights authenticates to the Geutebrück Hub using a service registration and a service token. The service token is created during the G-Insights installation or as part of the supported service registration process.

Default destination location:

- **Data:** G-Insights service registration
- **Default location:** `C:\ProgramData\Geutebrueck\G-Insights`

Certificates And HTTPS

Default operation user interface endpoint by opening via it the Geutebrück Hub:

- **Port:** 15003
- **Protocol:** HTTPS
- **Purpose:** G-Insights operation user interface

Local Data Protection

G-Insights stores forensic data, images, and vector data locally. These files can contain personal data or derived information and must be protected accordingly.

Default data locations:

- **Camera metadata database:** `C:\ProgramData\Geutebrueck\G-Insights`
- **AI-powered similarity image storage:** `C:\ProgramData\Geutebrueck\GenAI\Images`
- **AI-powered similarity vector database:** `C:\ProgramData\Geutebrueck\GenAI\Database`

Grafana Dashboards

G-Insights can provide Grafana dashboards through the authenticated G-Insights user interface.

Default local Grafana endpoint:

- **Port:** 3000
- **Protocol:** HTTP on loopback
- **Purpose:** Embedded Grafana backend

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