macula®

PROFESSIONAL ADMINISTRATION GUIDE

Version 1.27.0

5 March 2024

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

Document Title

Macula-Professional-Administration-Guide-v1.27.0.docx

Document Revision

Date	Revision	Description	Author
7-Oct-22	1.22.0	Macula v1.22.0 Release	keong@gsfcorp.com
3-Mar-23	1.23.0	Macula v1.23.0 Release	keong@gsfcorp.com
7-Jul-23	1.24.0	Macula v1.24.0 Release	keong@gsfcorp.com
7-Sep-23	1.25.0	Macula v1.25.0 Release	keong@gsfcorp.com
14-Nov-23	1.26.0	Macula v1.26.0 Release	keong@gsfcorp.com
5-Mar-24	1.27.0	Macula v1.27.0 Release	keong@gsfcorp.com

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Table of Contents

Table of Contents 2
1 Software Purpose and Use Cases 5
1.1 Hardware Requirements 6
1.2 Prerequisites 8
1.3 Getting Started 10
1.4 Installation of Macula Professional 11
1.5 Initialization and Remote Upgrade 16
1.6 Software Update and Uninstall 19
1.7 Start & Stop Server Service 26
2 License Activation 27
2.1 Online Activation 29
2.2 Offline Activation 31
2.3 Activation Management 35
3 Macula Console Login 39
3.1 About Product 43
3.2 Database Import 44
3.3 Configuration Backup 47
3.4 Setup Wizard 54
3.5 Interface Overview: Management Application 66
3.6 Conventions and Keyboard Shortcuts 75
4 Server Settings 78
4.1 Watchdog 81
4.2 Storage 84
4.3 Server Policies 95
4.4 Security 105
4.5 Two-Factor Authentication 113
4.6 Third Party Authentication Providers 117
5 Devices and Channels 121
5.1 Add Devices Using Autodiscovery 122
5.2 Add Devices Manually 130
5.3 Manage Devices and Device Groups 140
5.4 Configure Channels 151
5.5 Channel Settings 157
5.6 Bulk Edit for Devices and Channels 181

6 Recording Profiles, Schedules, and Configurations 184
6.1 Assign Recording Configurations 193
7 Add Users and User Groups 196
7.1 Active Directory and LDAP User Import 204
7.2 Permissions and Membership 209
7.3 Anonymous User 215
8 Streaming Server Configuration 218
8.1 Streaming Server User Interface 221
8.2 Mobile Application for Streaming Server 227
8.3 RTSP Streaming Server 246
9 Event and Action Overview 250
9.1 Rules 252
9.2 Add Rules 253
9.3 Default Events 264
9.4 Add Events 267
9.5 Defaults Actions 287
9.6 Add Actions 289
9.7 Understanding Conditions 310
9.8 Delay Timers 313
9.9 Create Schedules 315
9.10 Counters, Indicators and Variables 321
9.11 Tags and Subjects 329
9.12 ONVIF Generic Events 335
10 Other Resources and Functionality 341
10.1 Webpages and CrossLink Channels 342
10.2 Layout Templates 351
10.3 Shared Layouts 353
10.4 Maps 355
10.5 User Buttons 365
10.6 Visual Groups 368
10.7 Live Podcasts 371
10.8 Data Sources and Data Channels 374
10.9 Dewarp For Fisheye Cameras 390
10.10 Audio 392
10.11 Reports 394
10.12 Manage Mail Servers 403

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.13 Manage GSM Modems....407
10.14 Quick Access....412
11 External Services....414
11.1 Access Control....417
11.2 Gallagher....425
11.3 Inner Range Integriti....436
11.4 Camio....443
11.5 External Metadata....451
11.6 OPC Client....454
11.7 MQTT Clients....458
11.8 Modbus....463
12 Health Monitoring....466
12.1 Audit....478
13 Tools and Wizards....491
13.1 Problem Report Wizard....492
13.2 Archive Backup Wizard....497
13.3 Renderer Test Utility....502

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

1 Software Purpose and Use Cases

Macula software products can be used for any type of surveillance system: they offer a wide and flexible choice of components and license types to suit anyone from home users to corporate customers. Different product editions can be selected depending on the application area and available resources.

Macula Professional

Macula Professional is a new-generation piece of VMS software from GSF, which offers a fast and scalable stand-alone multiple-server solution that truly answers your company's security needs. Proven to be high-quality and reliable and having a 64-bit version, adding an even more intuitive user interface and better functionality, as well as a long list of add-ons.

Cross-functional and modern, Macula Professional supports over 3500 cameras and other network devices from major producers. The software is designed for surveillance systems with 96 or fewer cameras and also allows hybrid solutions. Looking for a complete enterprise-level solution? We suggest that you refer to the Macula Enterprise version of the software.

Macula Enterprise

Macula Enterprise is a complete surveillance ecosystem solution for enterprises of any size, including those distributed across multiple sites. This version of the software, Macula Enterprise, not only offers 64-bit speed and all the necessary tools for setting up an absolute situational alertness system aimed at responding quickly to events, as well as introducing a central server governance hierarchy of all the components.

This is one of the most comprehensive enterprise-level VMS solutions on the market, featuring interactive maps linked to alarms; an advanced event and action manager; analytics tools; video wall support and other impressive components you will definitely appreciate. To ensure the safety of your data, the software also offers archive replication, advanced system health monitoring and failover clustering mechanism, all of which reduce the disruption of your video surveillance recordings to zero. All this, as well as the various possibilities for customization and GSF flawless technical support, makes Macula Enterprise a video surveillance solution you can count on.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

1.1 Hardware Requirements

The table below details the **minimum** recommended **hardware sets** for Macula software. Please note that these specific processor models are given only as examples and are not compulsory: you can use different CPU provided that it has the same number of threads and its performance is analogous.

Calculations are given for two major configuration examples: all streams in D1 or FullHD resolution; of course, intermediate and mixed cases may also exist. Please contact GSF representatives if you require help with choosing hardware.

<table>
<tr><th colspan="6">HARDWARE RECOMMENDATION TABLE</th></tr>
<tr><td colspan="3">Installation specifications</td><td colspan="3">Recommended hardware per usage scenario.</td></tr>
<tr><th>Video Stream</th><th>Number of cameras</th><th>Motion Detector</th><th>Server only</th><th>Monitor*** only</th><th>Server + Monitor***</th></tr>
<tr><td rowspan="6">D1
30fps</td><td rowspan="3">Up to 9</td><td>None or camera-side*</td><td rowspan="2">CPU: Intel G1840; RAM 4GB</td><td rowspan="3">CPU: Intel G4500; RAM 4GB</td><td>CPU: Intel i3-6300; RAM 8GB</td></tr>
<tr><td>Software HP**</td><td rowspan="3">CPU: Intel i5-6600; RAM 8GB</td></tr>
<tr><td>Software HA**</td><td rowspan="3">CPU: Intel G4500; Ram 4GB</td></tr>
<tr><td rowspan="3">Up to 16</td><td>None or camera-side*</td><td rowspan="3">CPU: Intel i3-6300; RAM 4GB</td></tr>
<tr><td>Software HP**</td></tr>
<tr><td>Software HA**</td><td>CPU: Intel i3-6300; RAM 8GB</td></tr>
<tr><td rowspan="6">FullHD
30fps</td><td rowspan="3">Up to 9</td><td>None or camera-side*</td><td>CPU: Intel G1840; RAM 4GB</td><td rowspan="3">CPU: Intel i5-6600; RAM 8GB</td></tr>
<tr><td>Software HP**</td><td>CPU: Intel G4500; RAM 4GB</td></tr>
<tr><td>Software HA**</td><td>CPU: Intel i5-6600; RAM 8GB</td><td rowspan="3">CPU: Intel i7-6700; RAM 8GB</td></tr>
<tr><td rowspan="3">Up to 16</td><td>None or camera-side*</td><td>CPU: Intel G4500; RAM 4GB</td><td rowspan="3">CPU: Intel i7-6700; RAM 8GB</td></tr>
<tr><td>Software HP**</td><td>CPU: Intel i3-6300; RAM 8GB</td></tr>
<tr><td>Software HA**</td><td>CPU: Intel i7-6700; RAM 8GB</td><td>CPU: Intel i7-5930K; RAM 16GB</td></tr>
</table>

DDR4/DD5 RAM is strongly recommended!

- *Please refer to the list of Macula supported cameras for camera-side motion detector support
- **High Performance/High Accuracy mode
- ***System must provide:

- DirectX 10 support
- Graphics card with at least 256MB memory
- Latest graphics driver version

For workstations, onboard video memory should be at least 256MB per display, and the recommended minimum is 512MB per display.

For **Video Analytics** (VA): 1x physical core 3GHz+ and 1GB RAM per video channel. CPU **must** support AVX/AVX2.

For **Macula Enterprise servers** without any camera assignment (**management only**) you can use a stable but low-spec machine with high-speed OS medium with at least 4 cores (8 threads). Example: Intel i3-10320 with 16 GB DDR4 and NVMe SSD. Virtual machines are supported but make sure to allocate enough cores. If your Macula Enterprise server will assume any additional load (video channels, in the first place) and/or the number of simultaneous client connections is large (hundred or hundreds of connections), please consult with support@gsfcorp.com to get tips for your server hardware.

1.2 Prerequisites

There are a number of requirements for the Macula host system:

- Microsoft Windows operating system (10, 11, Server 2016, Server 2019, Server 2022), real or virtual machine
- both .NET Framework 3.5 SP1 and 4.x installed (the latest version should come with OS updates)
- for Windows Server operating systems, make sure the Desktop Experience feature is installed
- Windows Media Features must be installed (via Windows Features), it is missing by default in Windows N editions
- all Windows updates should be installed (especially, this is critical for Windows 10 and newer editions and for pending updates)
- ports for remote connections should be enabled through the firewalls (default ports are 60554 for Macula Monitor and Macula Console and 8080 for the Macula Streaming Server and external services)
- disable HTTP traffic analysis in the antivirus settings (especially ESET) to ensure the correct work of external services (LPR, FR, and other external video analytics modules)
- installation and recording directories should be added to antivirus exception list so that they are not scanned or interfered with in any other manner
- indexing and defragmentation services must be disabled for the storage locations
- for software analytics requirements, see the corresponding section of the VCA/VA manual (provided as a separate document)
- for Macula Monitor application, DirectX 10+ is required along with the latest stable graphics card drivers
- for Macula Monitor, display resolution of 1280x720 pixels or higher is recommended

For Windows Server 2016 and 2019, specify the Server with Desktop Experience option as part of the OS installation. Prior versions of Windows Server allow you to install this feature post installation.

If you use a server with a clean Windows installation, make sure to install **all available Windows updates before** starting the software installation. Component deficiency (framework components, redistributable etc.) may lead to unexpected issues in software operation.

If you are using Windows 10 N or KN (special edition without media technologies), make sure to install Windows 10 Media Feature Pack in order to ensure Macula operation. Without media features, Macula will not work. You will find the media feature pack online, provided by Microsoft.

In order to enable GPU usage for video analytics, please install **NVIDIA CUDA toolkit redistributable** package, which is NOT a part of the Macula installation. Please request it from GSF representative or support@gsfcorp.com.

For recording, the following recommendations apply:

- for 48+ channels and/or >20MB/s total recorded stream, RAID 5/6/10 with high speed hardware controller is strongly advisable

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

- defragmentation and indexing must be disabled for all storages
- every recording location, regardless of its type, must have 10-15% of free space, not used by Macula or any other software
- recording to the system disk is strongly not recommended
- antivirus software or any other scanners should be disabled for the storage locations
- no third-party VMS should be recording to the same location as Macula
- for NAS, make sure to disable the Recycle Bin feature, so that the erased files are actually deleted and not just moved to trash folder
- after adding the channels for recording, check the disk load (disk queue)
- disable read cache for RAID controllers

⚠ High disk queue may result in gaps in the recordings, freezing client during archive playback, etc. Minimize the disk queue to avoid system performance issues.

Antivirus **scanning**, **defragmentation** and **indexing** being enabled for Macula files may result in dramatically decreased write speed, recording disturbances and, occasionally, database corruption. We strongly recommend that you make sure that storage locations are not affected by these processes.

⚠ GSF is **not responsible** for software failures and/or footage loss caused by underlying OS and/or hardware issues. It is the responsibility of the systems administrator to configure the server and provide maintenance, unless otherwise agreed (e.g., if server hardware has been shipped by GSF).

1.3 Getting Started

Before starting the installation, make sure that:

- you have downloaded the correct software package
- you have acquired the corresponding valid **license** key
- the host operating system is stable (functioning correctly) and has all the **updates and drivers** installed
- server **hardware matches** the project **requirements**, taking into account all used features and planned post-deployment modifications
- host system retains all the features and configuration required for software operation

⚠ We strongly advise that you keep the software versions (e.g., 1.**x**.x) and subversions (e.g., 1.2.**x**) across your system match exactly. Software build numbers (e.g., 1.2.0.**xxxxx**) may differ slightly in case you are using 64-bit and 32-bit editions.

💡 If you are not sure about what server hardware to choose, do not hesitate to use GSF provided hardware calculators and/or contact GSF representative for an accurate estimation.

We advise installing and activating the software on the ultimate server assembly, as extensive subsequent hardware changes are likely to cause software license activation failure. If this happens, undo these changes, if possible, or contact product support to find a solution.

Macula is installed as a Windows service so please make sure that the Windows user you are logged in as has sufficient privileges; otherwise, software may not be installed correctly. Note that there is no option to install and run the software in application mode.

The following topics will guide you through the installation process, as well as providing details on product configuration. If you are using a GSF product for the first time, we strongly advise you to carefully read and follow the instructions in this manual and related documentation.

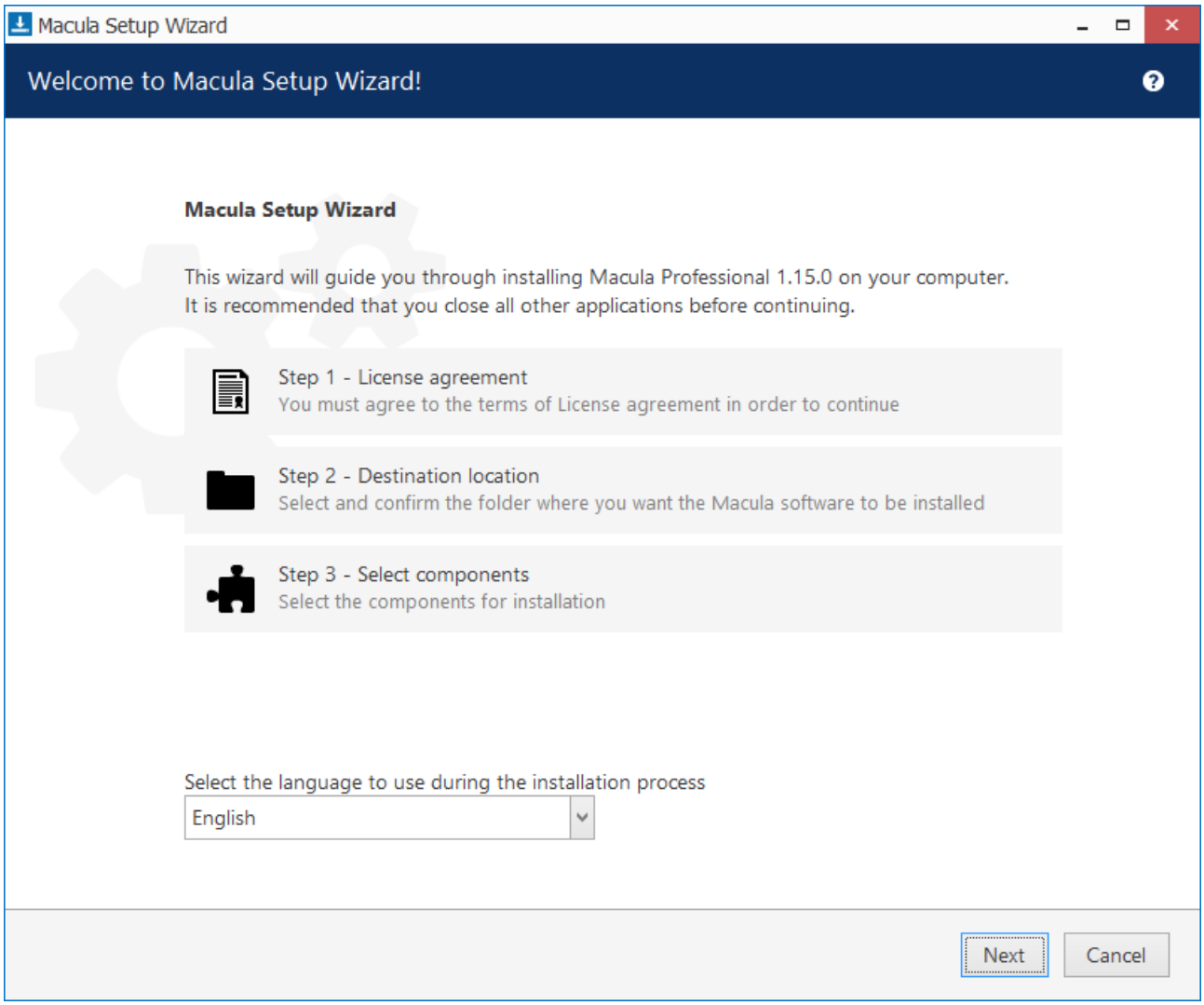
⚠ GSF is **not responsible** for software failures and/or footage loss caused by underlying OS and/or hardware issues. It is the responsibility of the systems administrator to configure the server and provide maintenance, unless otherwise agreed (e.g., if server hardware has been shipped by GSF).

1.4 Installation of Macula Professional

Start the installation process by double-clicking on the Macula Professional executable package file. The setup wizard will guide you through the installation process, providing available installation-time options depending on the chosen software package. Note that, depending on your Windows UAC configuration, you may have to confirm and/or provide administrative credentials.

We strongly advise that you stop all running third-party applications, as well as stopping antivirus scanning and Windows (and any other) updates during this phase, as these may interfere with the process and result in corrupt installation, which may cause unexpected behavior and hard-to-track issues during further software operation.

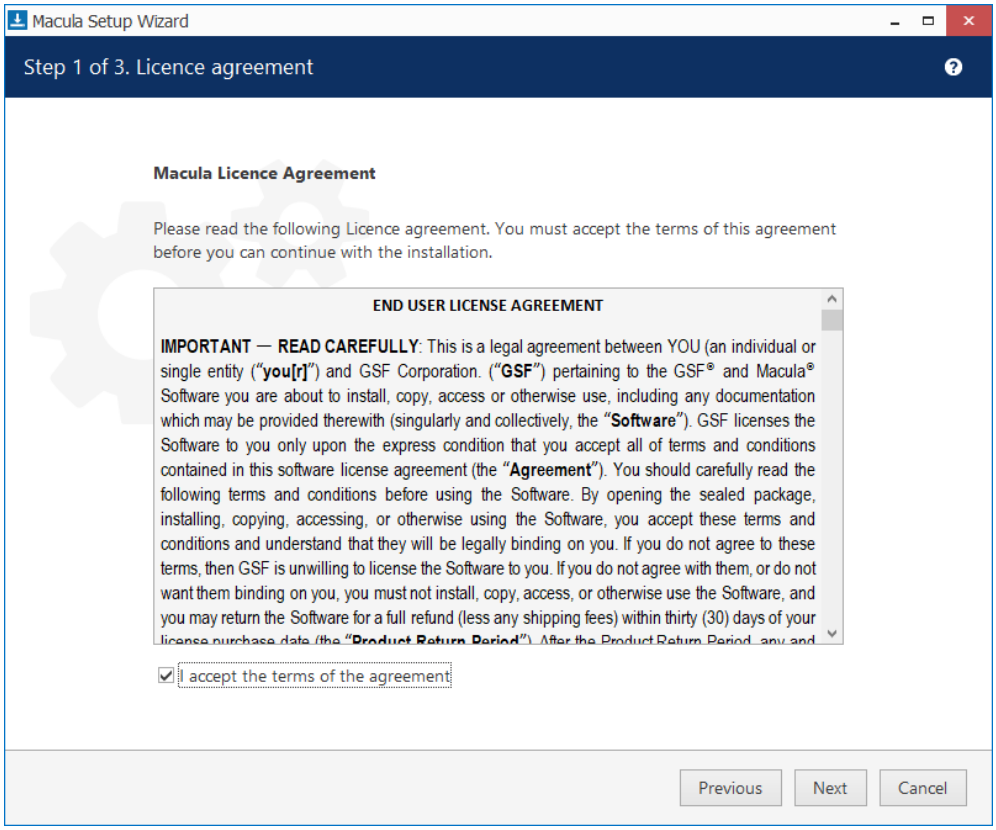
The installation wizard displays an overview of the process; also, you are able to select the installation language here. You will be prompted to select the Macula Professional interface language later.



Step 1

Carefully read the Macula license agreement: you must agree to all parts of the given document in order to proceed. If you agree, select *I agree...* in order to continue; otherwise, terminate software installation. If

you have any questions regarding the contents of the present license agreement, please contact sales@gsfcorp.com.



Step 2

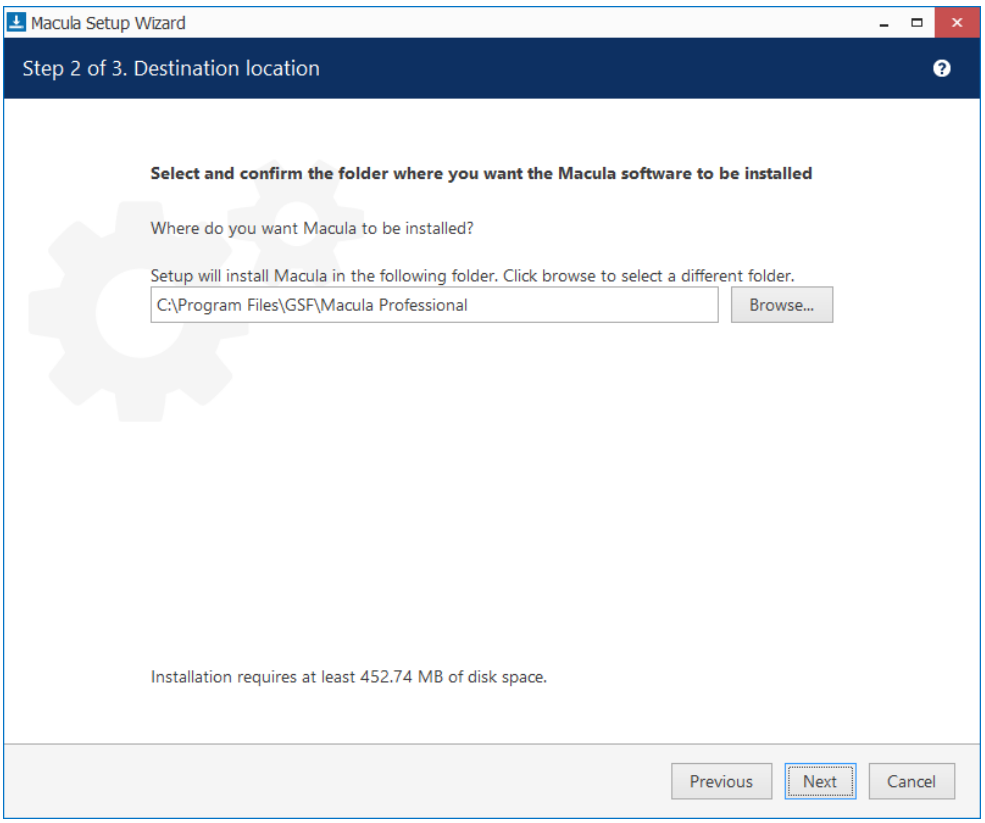
Select the destination folder you want the software to be installed in. By default, Macula Professional is installed in:

32-bit: *C:\Program Files (x86)\GSF\Macula Professional*

64-bit: *C:\Program Files\GSF\Macula Professional*

If you are re-installing Macula Professional and previously selected a non-default location, make sure to select the same destination directory, or, alternatively, completely uninstall previous Macula Professional version. If unsure about this, ask for GSF technical support team assistance. A full description of the software upgrade procedure is available in the corresponding section of the Macula administration manual.

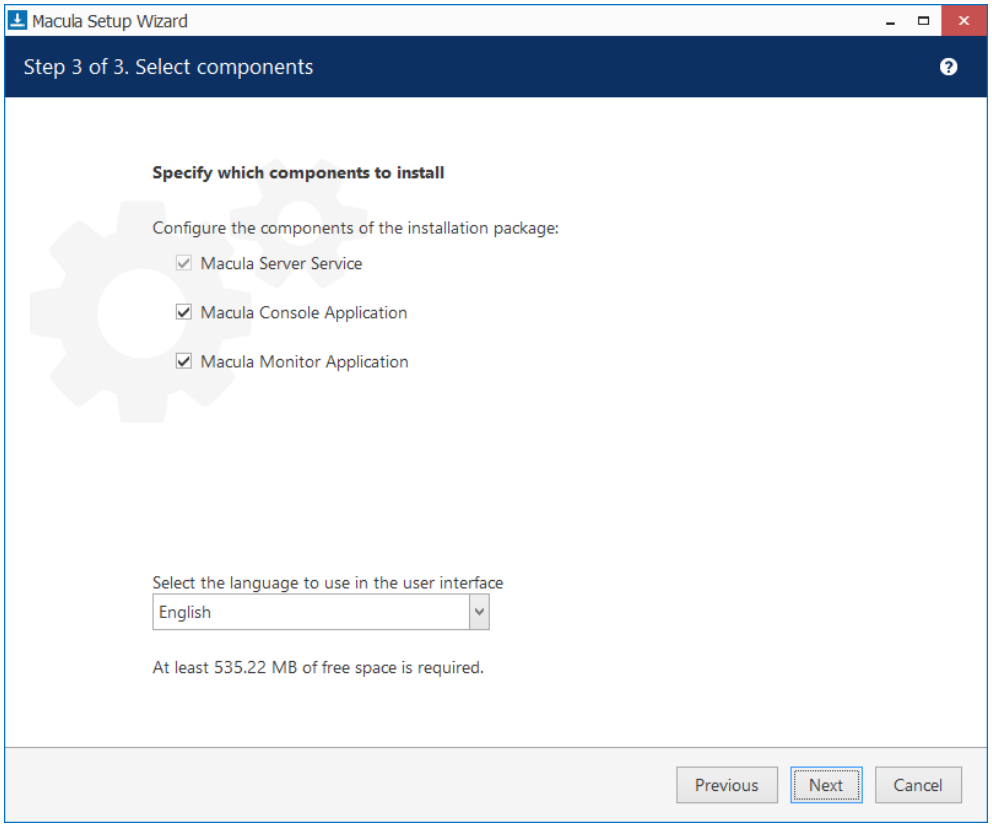
The setup wizard estimates how much disk space will be required. Make sure you have enough free space on the target disk. Note that low system disk space will dramatically decrease system performance and affect overall system stability.



Step 3

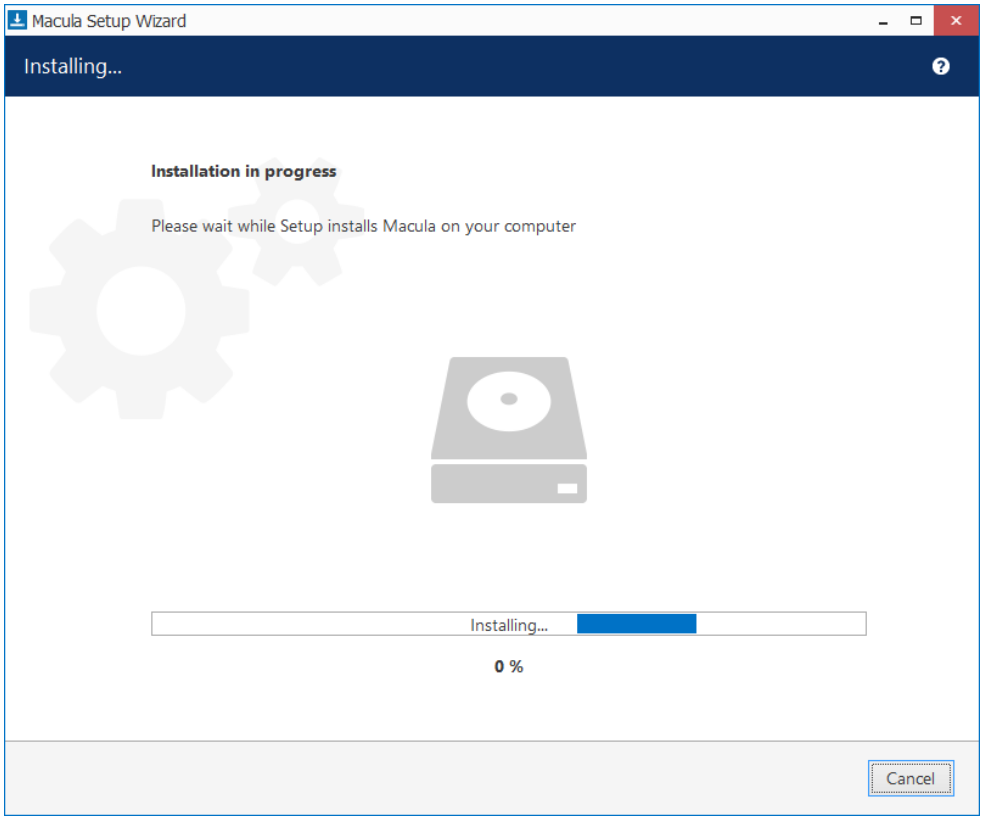
Some components are optional and so you can choose not to install them. The main Macula Professional parts are obligatory and cannot be deselected (by default, these options are selected and grayed out).

If not chosen at this stage, Macula Monitor can be installed separately later.

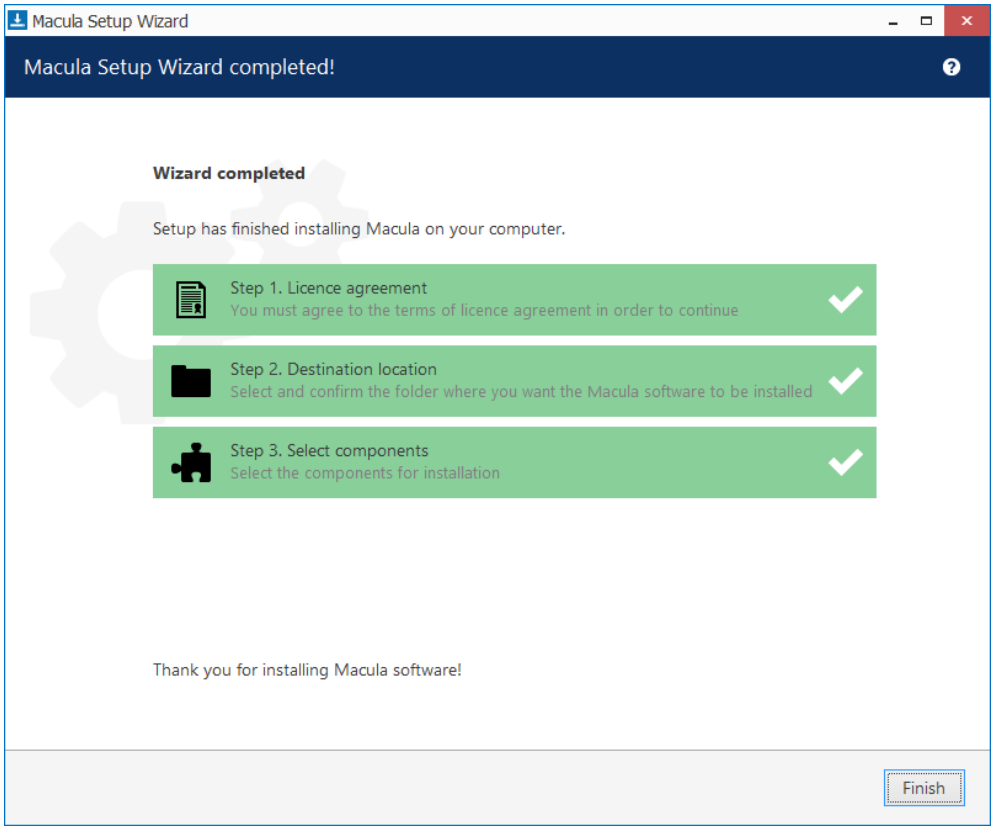


Macula® Professional Administration Guide

If you are ready to proceed, click *Next* to begin the installation. Depending on selected components and host system condition, the process may take some time to complete, so please be patient.



Upon completion, the setup wizard will show you an installation summary. If all the steps have been fulfilled successfully, simply click *Finish* to close the wizard.



After the installation has been completed, there are a few more steps necessary for you to begin using the software:

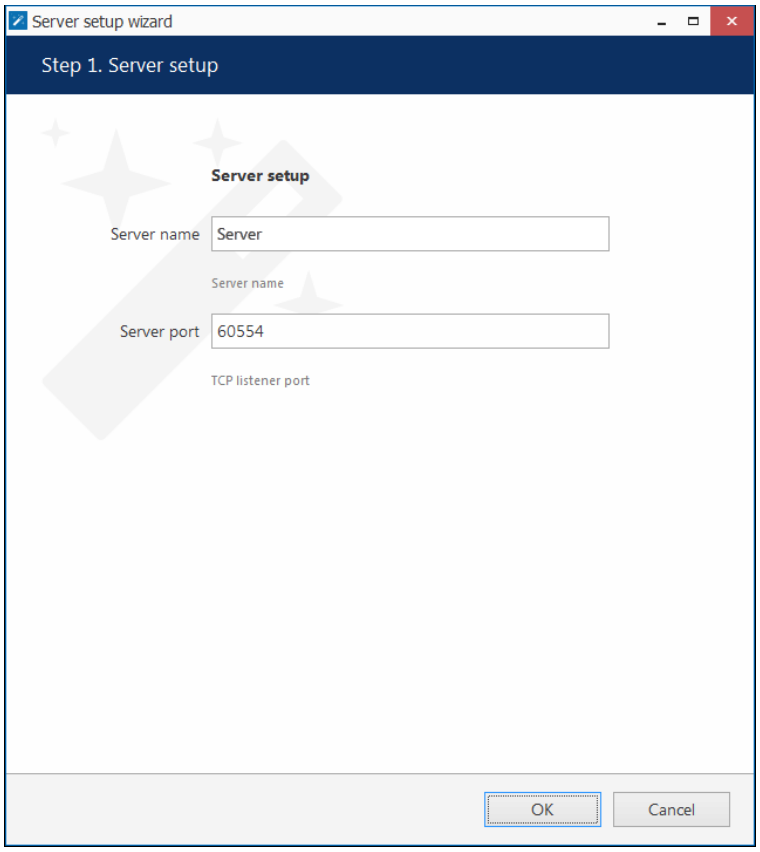
- apply server initialization settings via *Server Setup Wizard* - it will pop up automatically after the installation in case you are doing a clean or a new installation
- activate the software - if it is not activated, the wizard will also pop up automatically
- after you run the console for the first time, you will be offered to complete the *Setup Wizard* to start the deployment, following the recommended configuration steps

1.5 Initialization and Remote Upgrade

Initialization of Macula Professional Server

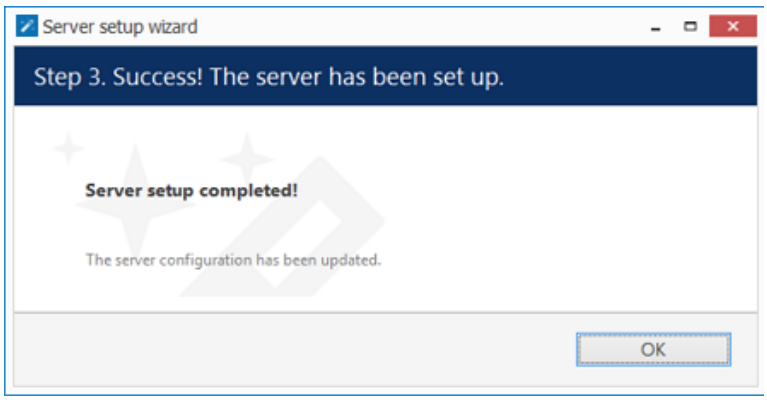
After completing the installation wizard, you will be offered to enter server setup. The settings selected during server setup can be changed later at any time via Server Setup Wizard, which will be available via your Start menu.

This step is **mandatory**; you will be unable to connect to your server and configure it if it has not been initialized. It is necessary to initialize the server even if you are planning to restore its configuration using the Server Backup and Restore Wizard later.



Setting	Description	Default Value
Server name	User defined server title	Server Title or last used title
Server port	TCP port for incoming remote Client connections	60554

Note that the port defined here will be used to retrieve the server data via local Macula Monitor and Macula Console connections. You will need to define the external (Internet) port for your Macula Professional via Macula Console in order to be able to receive video streams from remote Macula Monitor connections.

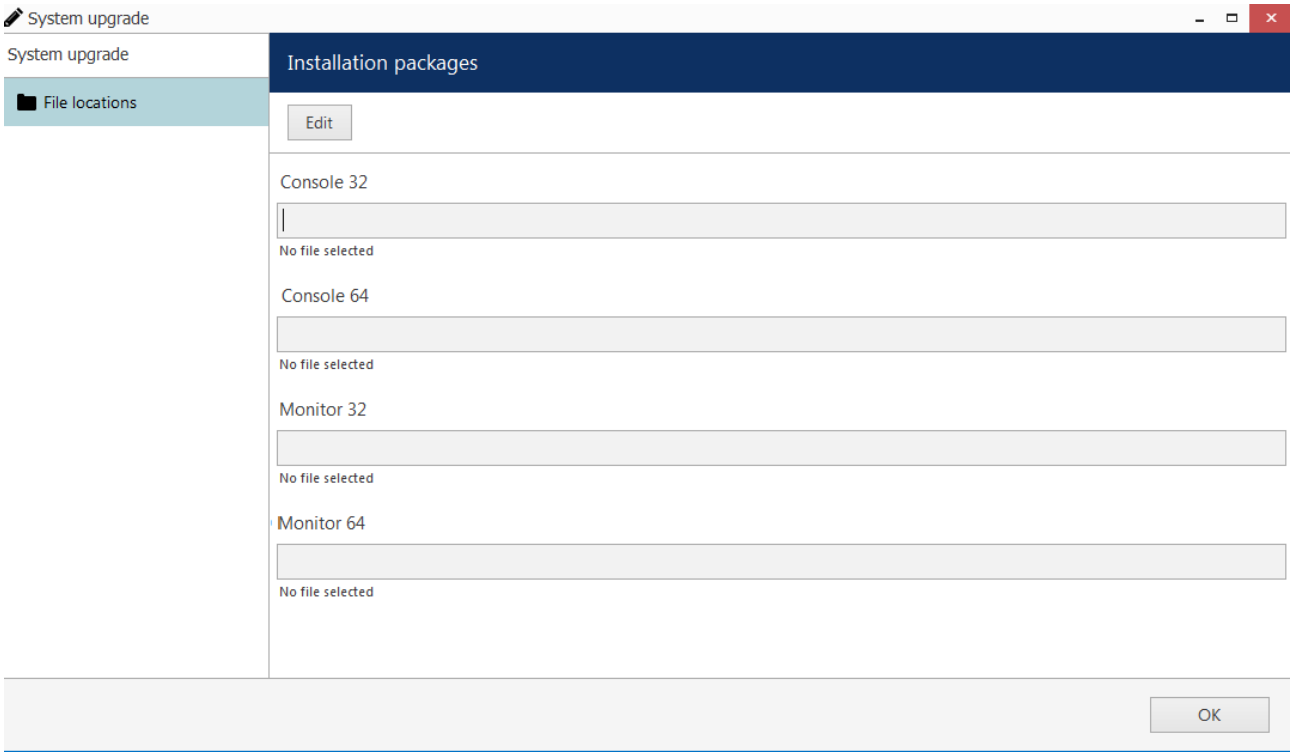


Remote Upgrade

Starting from software version 1.10.0, it is possible to apply remote upgrade to Macula Console and Macula Monitor components from the Macula Professional server. This feature allows you to deploy remote client machines once and then easily handle the upgrades from any place, keeping the whole system up to date with little effort.

Once you have upgraded the Macula Professional server to a newer version, you can then put the installation packages of the same version onto the Macula Professional server computer. The idea is that you first define the location of the executable files and then remote Macula Monitor and Macula Console applications receive an update notification. The locations must be on the Macula Professional server machine, even if you are accessing the server from a remote Macula Console. The installation itself is initiated from the remote client side.

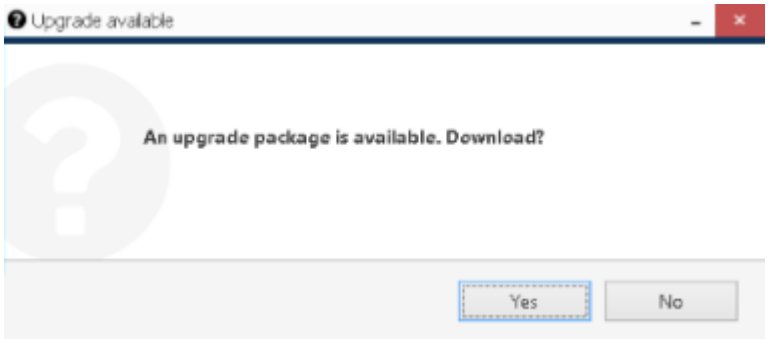
To access the remote upgrade feature, open your Macula Console application, click the main application menu button in the upper-right-hand corner and choose the *System upgrade* option. The *System upgrade* dialog box will appear.



Here, you have four entries - for 32- and 64-bit editions of Macula Console and Macula Monitor applications. These installation files can be downloaded from https://gsfcorp.com/downloads. Specify the path to each file and click OK to save.

Now, if a remote Macula Console or Macula Monitor application of an older version is used to connect to this server, it will receive a notification about the available upgrade. The notifications can be disabled in the application settings.

So, if Macula Console or Macula Monitor detects that an upgrade is available, it will offer you to download it straight away. If your network connection allows it, click OK to agree and download the upgrade package.



The upgrade package will be downloaded using your default Web browser and saved on your local computer. You can start its installation at any time, provided that your Windows user has enough privileges to run the installation. After the installation, just start the application as usual.

1.6 Software Update and Uninstall

This topic provides guidelines on the installation management use cases.

We recommend that you keep the software version up to date, as new versions include new features, various improvements and optimizations, as well as the latest bug fixes.

> ⚠ We strongly advise that you keep the software versions (e.g., 1.**x**.x) and subversions (e.g., 1.2.**x**) across your system match exactly. Software build numbers (e.g., 1.2.0.**xxxxx**) may differ slightly in case you are using 64-bit and 32-bit editions.

> ⚠ Before starting the upgrade/uninstall procedure, ensure that all Macula processes have been terminated and that Macula files are not in use: this is necessary in order to upgrade all files to the newer versions. This includes any Macula processes or related applications that are running, and also any third-party applications that have access to Macula files, e.g., antivirus scanners, third-party integrations, etc. Macula processes can be found via Task Manager ->Details tab: these start with *VMS*, e.g., *VMSServer.exe*.
> If the processes are not stopped, or if other applications are still interfering with the process, you may be asked for a **reboot**: in that case, please restart your server machine afterwards to complete the action. This will not affect the overall process quality.

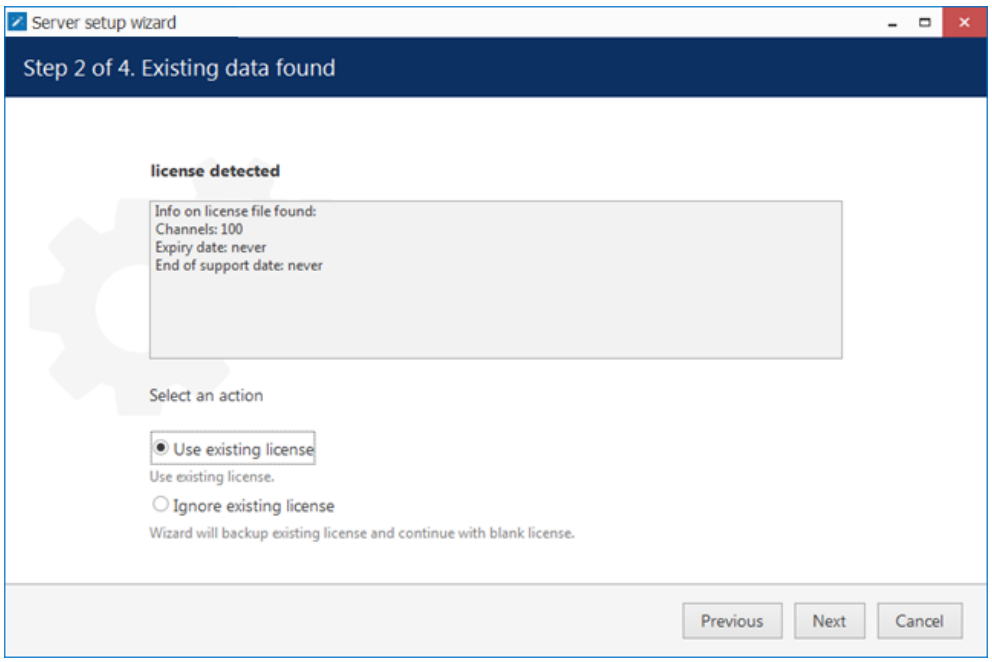
Upgrade Software

This section describes manual software update (newer version installation on top of the older one) by running the installation **locally**. For remote upgrades, see the corresponding section of this document.

Before starting the software upgrade:

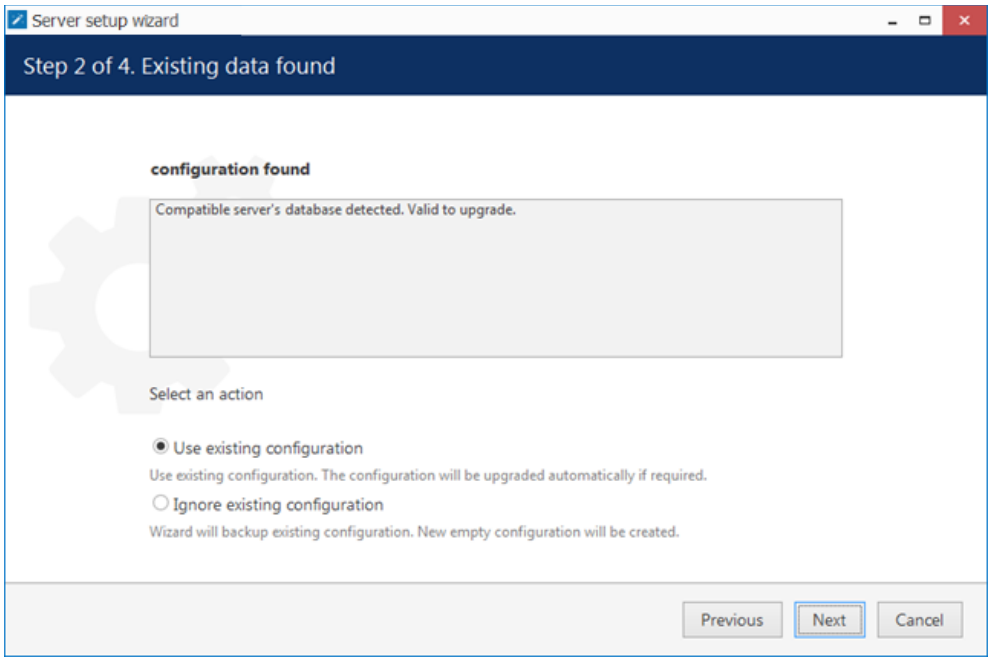
1. Make sure there are no other running installations and that the operating system is not in the middle of installing updates. If Windows updates are pending, apply them, then restart the computer (if required), and start the Macula upgrade.
2. Verify that the operating system is stable and is running normally (check system logs, overall health) - these must be no "blue screens", unexpected shutdowns, slowdowns etc. (Normally, we recommend that you regularly run such system checkups, not only before upgrade).
3. Ensure stable power and connectivity (the latter is essential if you are connected via RDP).
4. See if there are any special requirements or recommendations from GSF regarding the target version. Usually, these are either mentioned on the download page, or provided alongside the download links in case the new version was recommended and sent by our engineers.
5. Check your software license subscription, and renew it, if necessary: the subscription must not run out before the target version release date. You can check the software release date by right-clicking the installation file > *Properties* > *Digital signatures* > see timestamp. The license information is available via license manager, *Macula Activation Wizard*.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



If you launch a newer version installation package of the same kind as the already installed Macula edition, you will be given the option to **upgrade** the product. It is not possible to install another type of package on top of the existing one, e.g., Macula Recording Server on top of Macula S: if you wish to change the server type, uninstall the old software package first.

Press *Next* to go through the steps and complete the wizard, which is very much alike the installation wizard. At each step, read all the information displayed and press *Next* until finished.



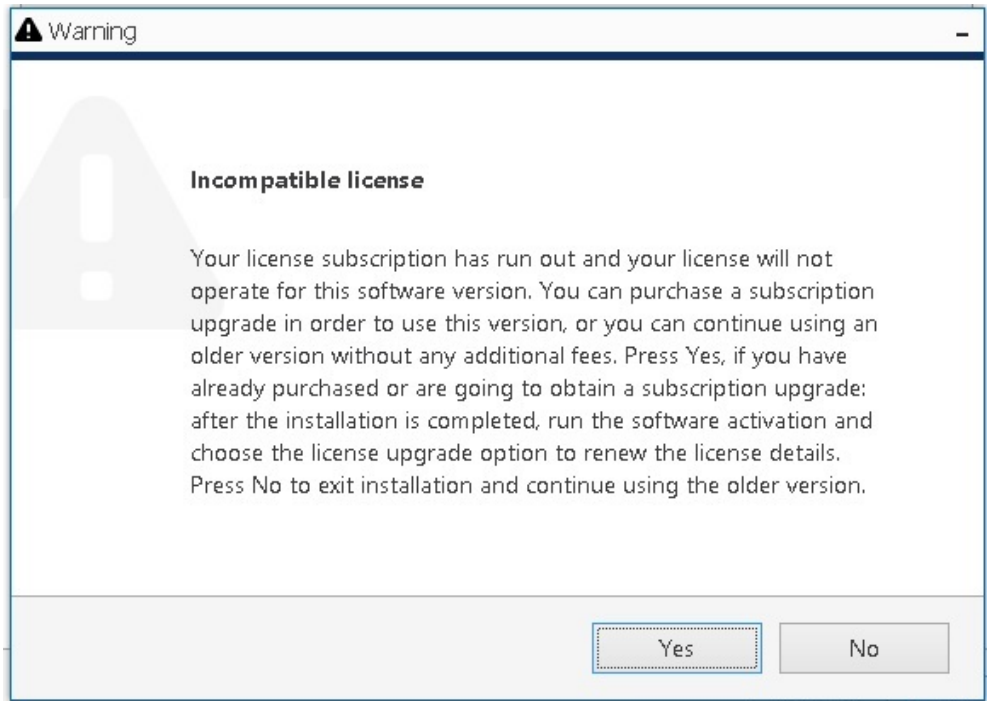
If you want a clean installation, choose to ignore the existing **configuration**: the current database will not be used and will be replaced with an empty one, as if you were installing the software from scratch. Otherwise, leave the wizard to use the existing configuration. In either case, the old database is not actually

removed but is saved as a backup, so you will be able to load it anytime later via Backup and Restore Wizard.

In case the installation wizard detects your **license subscription** has run out, you will get a **warning** about license compatibility. By default, the initial subscription will allow for version upgrades during 2 years, starting from the license activation date. Hence, if the target upgrade version is newer, this warning will pop up.

- If you have already acquired a subscription upgrade, proceed with the installation, then run the license manager and upgrade your license in either online or offline mode
- Otherwise, cease the installation and choose another software version that was released before the license subscription ran out (or continue using the existing version)

You can contact our sales department via support@gsfcorp.com to learn about the license subscription options and price offers.

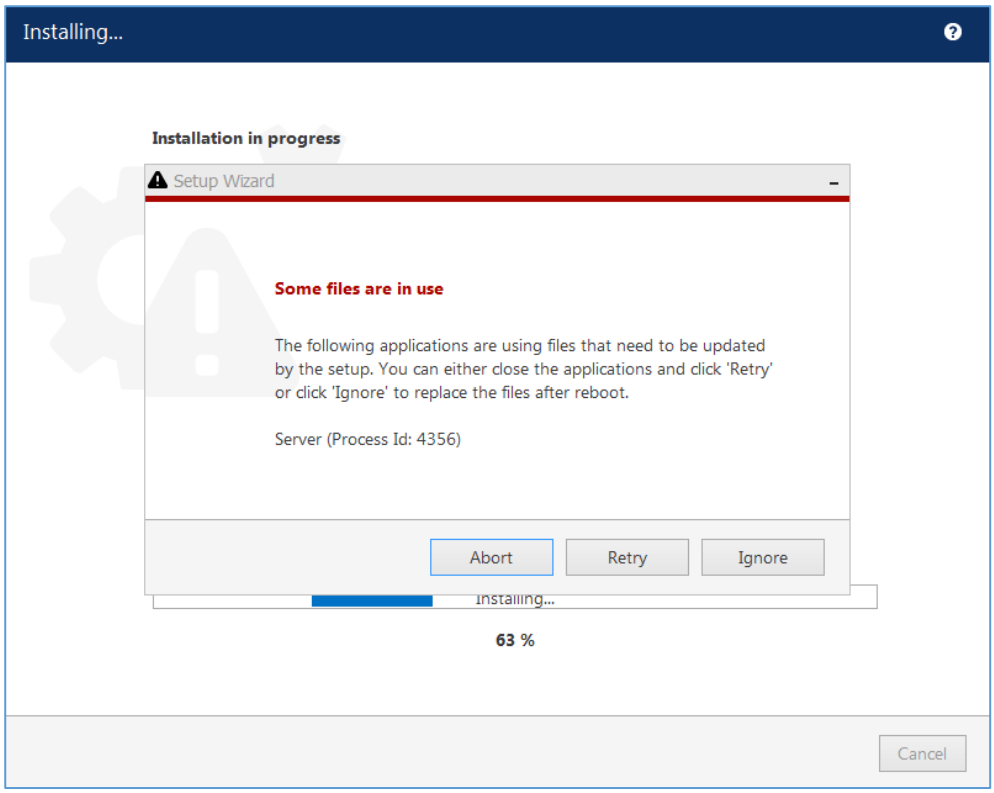


If you proceed with the upgrade but do not provide a valid license after the installation is complete, the software will not operate. Therefore, do not proceed with the upgrade until you have renewed the subscription.

To verify the software release date against your license subscription expiration date, right-click the installation file > choose *Properties* > go to the *Digital Signatures* tab and check the timestamp.

If some of the files cannot be upgraded because they are in use, you will get a corresponding warning.

- Choose *Ignore* to proceed with the installation: reboot may be required afterwards but it is safe to select this option, esp. if the processes are from Macula; or
- Stop the listed applications/services and click *Retry* to continue installing the software, or
- Click *Abort* to roll back the installation (the process will be cancelled and you will get a corresponding error in the wizard's dialog box).



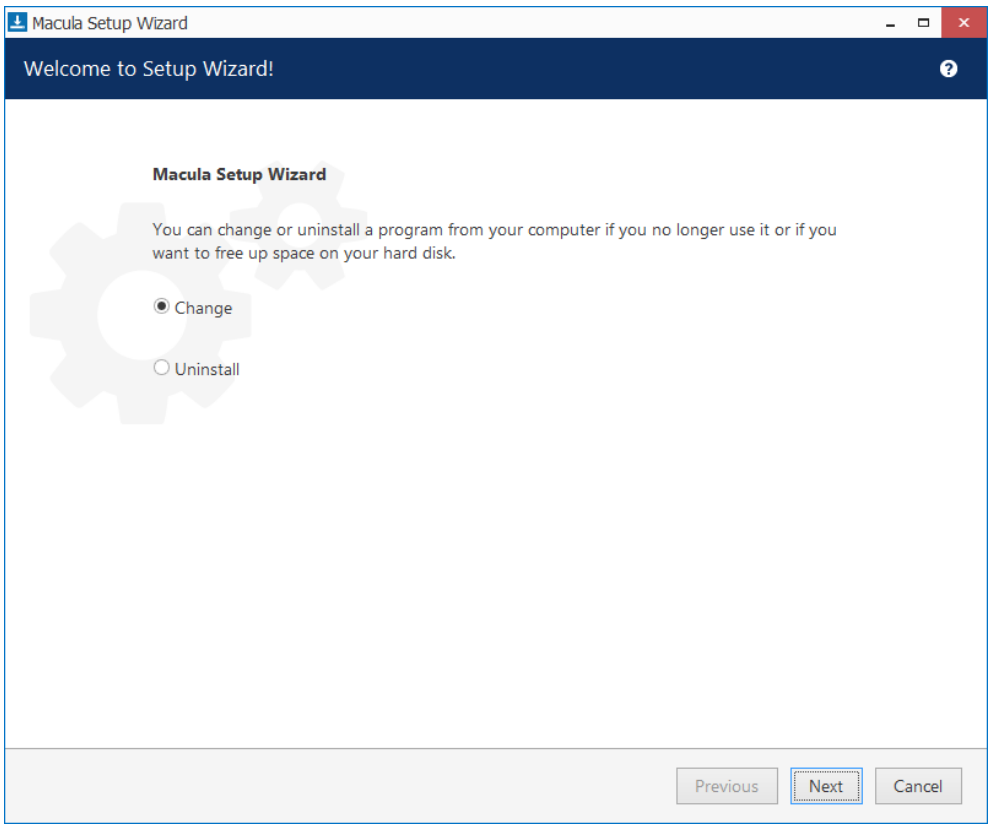
Uninstall/Change Software

Software can be uninstalled in two ways:

1. From Windows Control Panel
2. By launching the same package that was used for installation

In either case, you have a choice between changing and uninstalling the product.

> ⚠ Before making any changes to the installation, make sure to close and stop all software services and applications. If processes are not stopped, some of the software components may not be removed or replaced during the installation process.
>
> In order to check this, open Windows Task Manager, select '*Show processes from all users*' and make sure there are no processes starting with 'VMS...'. If there are any, stop them manually and then proceed with the installation changes.

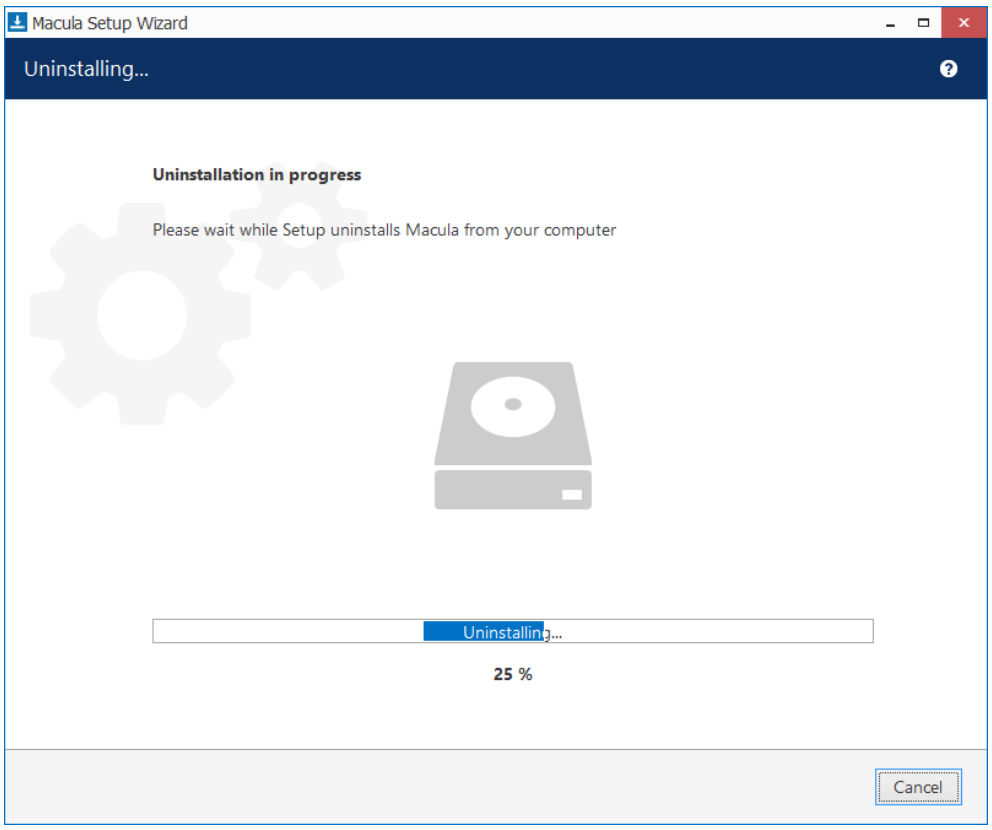


Select *Change* if you wish to re-install or add software components. The process will be similar to the initial installation.

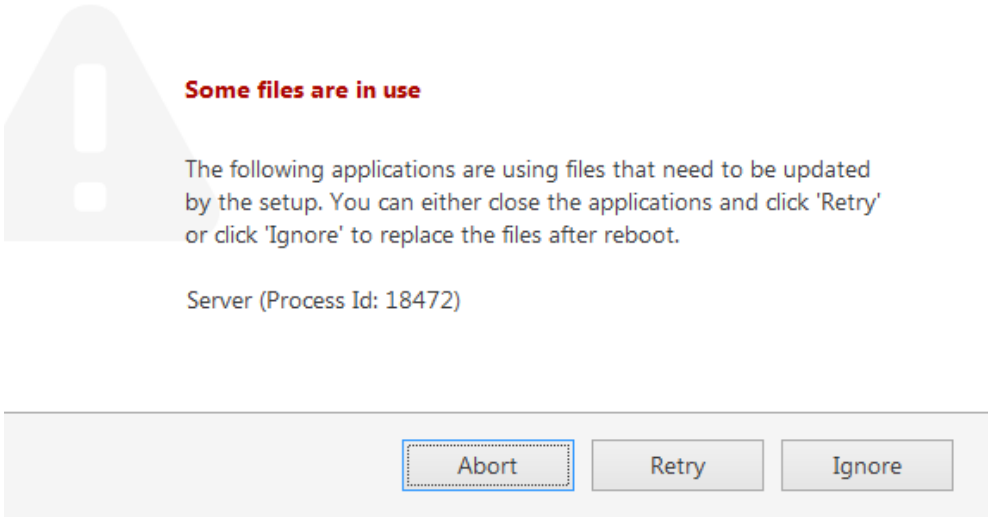
Select *Uninstall* to remove all software components. You will be asked if you wish to keep the configuration and the current license; the following common use cases apply:

- keep the license and remove the configuration if you wish to re-configure everything from scratch after re-installation (e.g., in event of a corrupt database or having to move the server to a different system);
- keep both if you are going to clean install the software;
- remove both if you do not intend to use the software on this machine anymore.

Press *Next* to proceed with the uninstallation process. Note that you may have to confirm these changes if UAC has been turned ON.



If you did not stop the Macula server before starting the uninstall process or if some third-party software (e.g., antivirus) has locked Macula files, you will get a warning.



In this case:

- choose **Abort** to cancel the uninstall process
- stop the processes manually yourself and then click **Retry**
- click **Ignore** to let the wizard handle the files automatically (recommended)

Generally, if you see that the process mentioned in the warning is Macula **own process**, simply choose the **Ignore** option and let the wizard do the job.

When the wizard finishes removing software components, hit *Finish* to exit.

Clean Install

Sometimes it is necessary to install software anew, i.e., to change software bit version, and also in event of major software-related troubles.

> You can perform clean install yourself if you are already familiar with the software. If you are doing it for the first time, we recommend that the procedure is supervised by a GSF support engineer so that you learn how to do this quickly and effectively, avoiding possible mistakes.

> Although software upgrade is not possible with different bit versions, you can migrate your installation to a different bit version by performing a clean install.

To perform a clean installation, it is crucial to make sure that no Macula software processes are running, whether explicitly or in the background. Follow these steps:

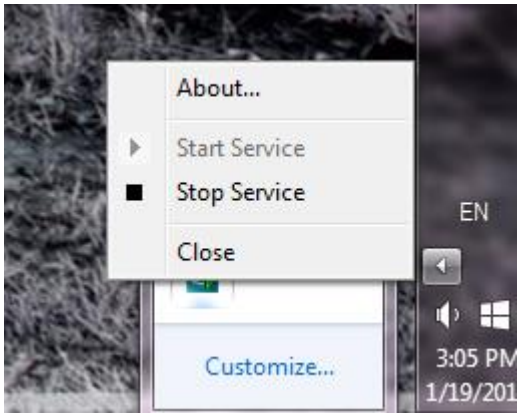
1. Stop all Macula software services and/or applications;
2. Open Windows Task Manager, click *'Show processes from all users'* and check that there are no processes starting with 'VMS...'; if there are any, stop them;
3. Uninstall software as described above, keeping your license and configuration;
4. Install [new] software version, carefully following all steps and recommendations;
5. Start software and check if the desired change has been carried out.

1.7 Start & Stop Server Service

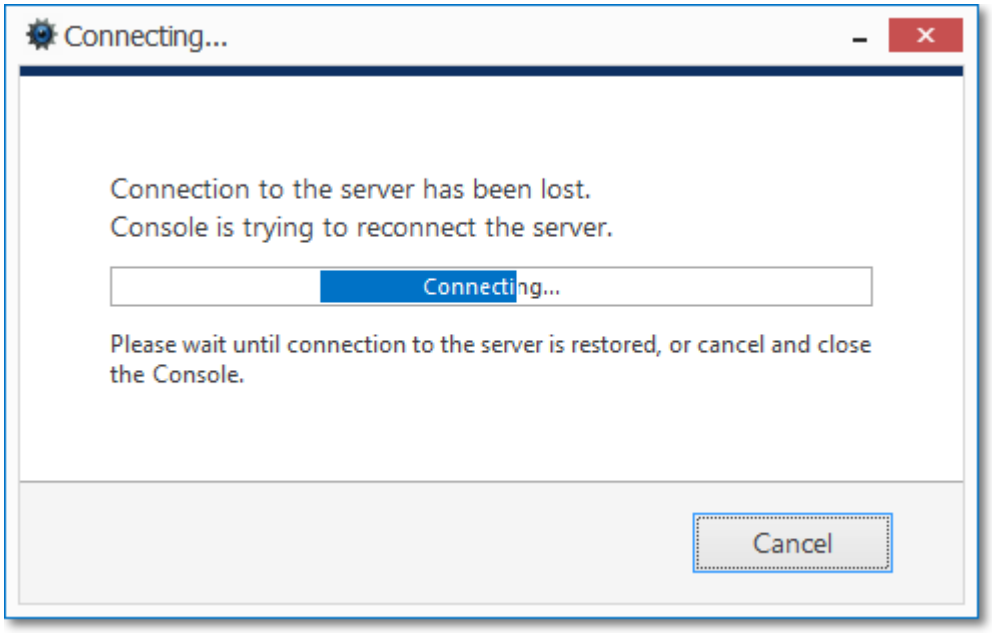
After software installation (except for the Macula Console or Macula Monitor only installations), two components are registered as **Windows services**: Macula Server service and the accompanying Watchdog service. Both these services are set to automatic start meaning that they will be launched straight after Windows start-up regardless of whether any user is logged in or not.

By default, the server will run in silent service mode, i.e., without any status indication other than that in the Windows Services management console; from there, both services can be stopped, started and restarted.

Double-click the server shortcut on your desktop to launch the system tray shell for the server: the server icon will appear in the system tray, allowing you to start and stop the service by right-clicking it and selecting your desired option. Macula Watchdog service runs silently in background as an auxiliary service and has no user interface except for the settings' dialog box in Macula Console.



If the server service is stopped while Macula Console connections are active, the wait-for-server-connection window will appear on top of Macula Console, disabling any input. The same thing will happen if there are any problems with server connectivity. It will automatically disappear when the server is online again; alternatively, you can click Close to exit Macula Console at this point and open it manually later.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

2 License Activation

In order to use the product, a **valid license** is required. Any of these licenses can be activated using this wizard; note that license activation choice will differ depending on the installation package you have selected.

For the standalone server edition, Macula Professional, the license is applied to that specific server. Client applications do not require a license to operate.

For Macula Enterprise system, the license is applied to the Macula Global server (central management server) only; Macula Recording Server machines do not require a license to operate because they cannot operate independently. Client applications do not require a license to operate.

Each server only accepts one Macula license key, no matter how many and which features it includes. Each Macula license key can only be applied on one machine.

License Types

Each license includes a certain number of channels. Traditionally, these are **video channels** (normally, one video source equals to one license), and then there are special channels with **advanced functionality**. Macula features (video walls, maps, redundancy, etc.) do not require any additional feature licenses.

License types:

- **video** channels: regular video channels.
- **VA** - embedded video analytics (embedded, generic VA engine)
- specialized VA (embedded, different engine types)
- CrossLink - interactive channels
    - **CrossLink Basic**: interactive web applications (webpages)
    - **CrossLink Advanced**: interactive remote applications (workstations)
- advanced device integrations (Leica, CrossWalk, etc.)
- **data channels.**

Also, each Macula license contains 1 (one) generic video analytics channel free of charge.

For detailed information on Macula license options, please contact our sales via https://gsfcorp.com/about/contact.html

The Macula server controls the total number of the channels of each type in the system. For Macula Enterprise systems, you must apply the license onto the Macula Global server (the central management server), and then you are free to allocate and move the channels across the Macula Recording Server servers. The Macula Global server will keep track of all license channels used throughout the system.

The server tracks the license channels using the following logic:

- video channels: one license channel is used for each channel that is created when you create a device of any model (except for CrossLinks).
- VA: VA licenses are separated from video channel licenses and do not include them. You should purchase VA channels on top of the regular video channels. You are free to enable VA for any video

channel, as long as the total number of enabled video analytics does not exceed the VA number in the license.
- CrossLinks:
  - CrossLink Basic: one Basic license channel allows you to create one Webpage or one device of the CrossLink Basic model
  - CrossLink Advanced: one Advanced license channel allows you to create one Webpage or one device of any CrossLink model
- advanced integrations: each special integration (e.g., Leica) channel allows you to create a device of the corresponding type.
- data channels: one data channel license is required to create one data channel. Databases are unlocked automatically (DBs do not operate without a data channel).

License Activation

Once you have installed the software and entered the server initialisation settings, the activation wizard will appear. If it does not, or if you have rebooted the server computer after completing the installation, simply run the **activation manager** in one of the following ways:

- from the Windows Start Menu, under folder, or
- by typing *Activation Wizard* in the search field, or
- by right-clicking the server tray icon and selecting *About* > *Manage license* (server tray icon appears only after you run the Macula Server shortcut from your Desktop or Start menu), or
- when connected to localhost via Macula Console, go to the main menu > *About* > *Manage license*.

The license manager will only pop up automatically after the initial installation. If you wish to apply license upgrades at any time, including the after-software-upgrade, run the license manager manually as described above.

It is advisable to run hardware stability tests and finalise server hardware configuration before the license activation, as subsequent hardware changes may cause activation related issues. Approximately up to 30% of the initial hardware components can be replaced without losing the activation.

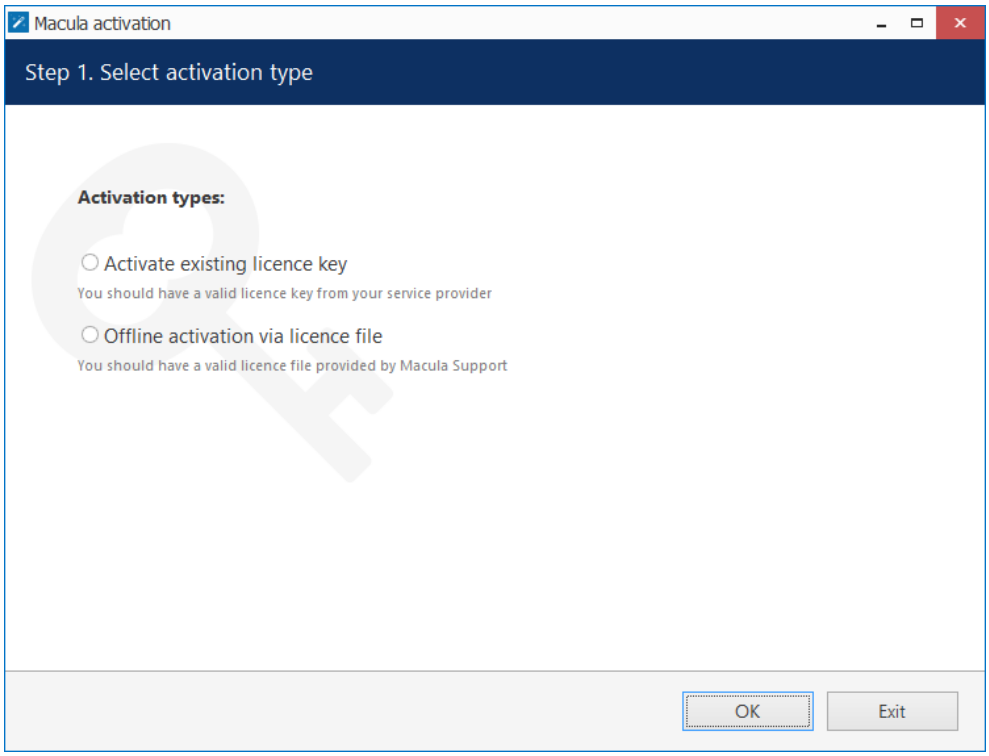
Subtopics here describe every type of license activation in details.

Licensing is mandatory for Macula Professional and Macula Enterprise software packages. Macula Recording Server does not require a license as it is not an independent component but rather operates under a Macula Enterprise server only.

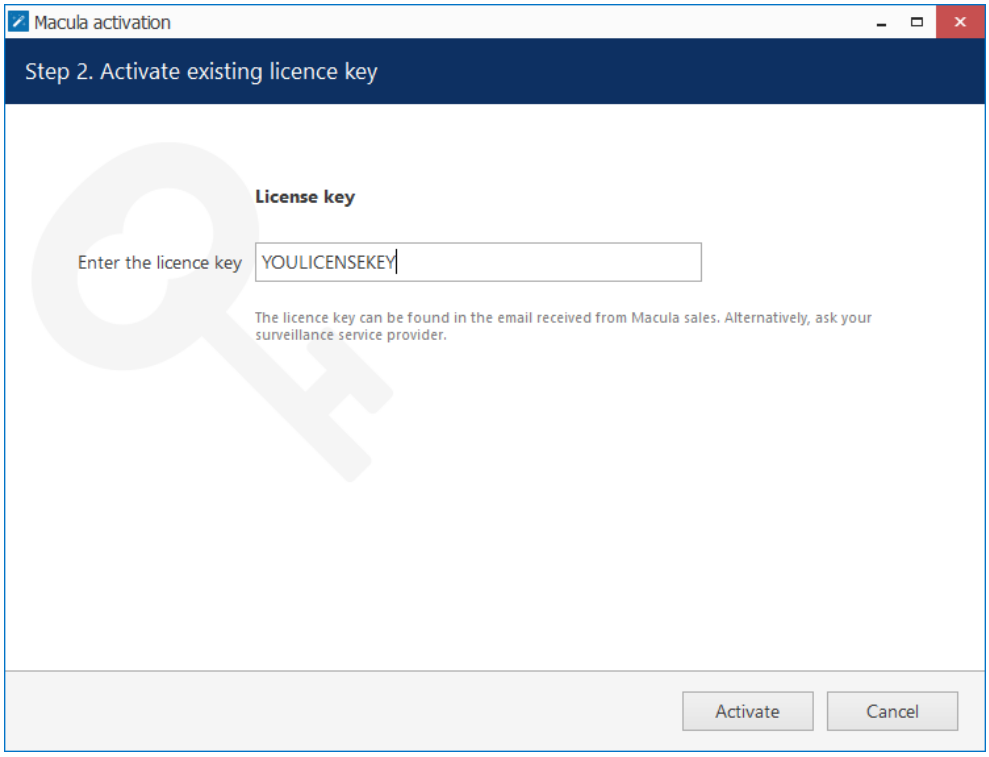
Virtualized environment is supported starting from software version 1.13.0. If you experience any issues with the license activation, kindly contact our support engineers by emailing support@gsfcorp.com.

2.1 Online Activation

If your server has Internet connection available, you can choose online activation mode. The software will automatically connect to the activation server and register your pre-purchased license.



Enter your product license key and hit *Activate*. If your key is incorrect, the wizard will notify you with a red *X* sign next to the key field: if this happens, double-check the key you have typed, looking out for mistyped characters and superfluous spaces at the start or end.



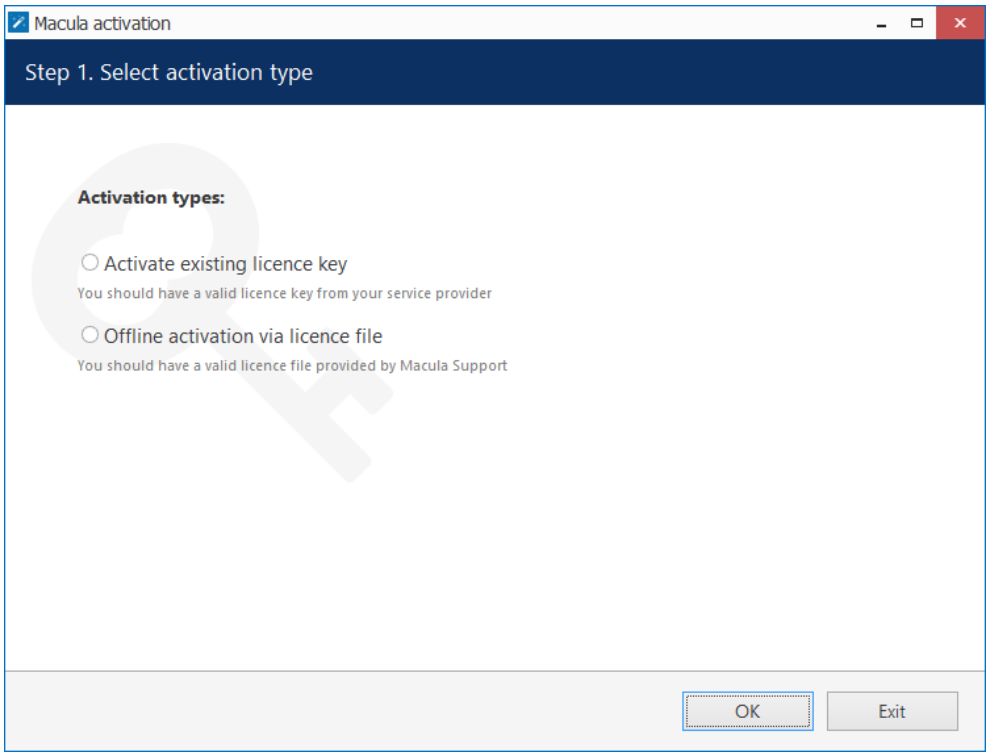
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

When you have entered a valid license key, the wizard will activate your software. If you have decided to go with a different activation option, click *Cancel* to return to the activation type selection step.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

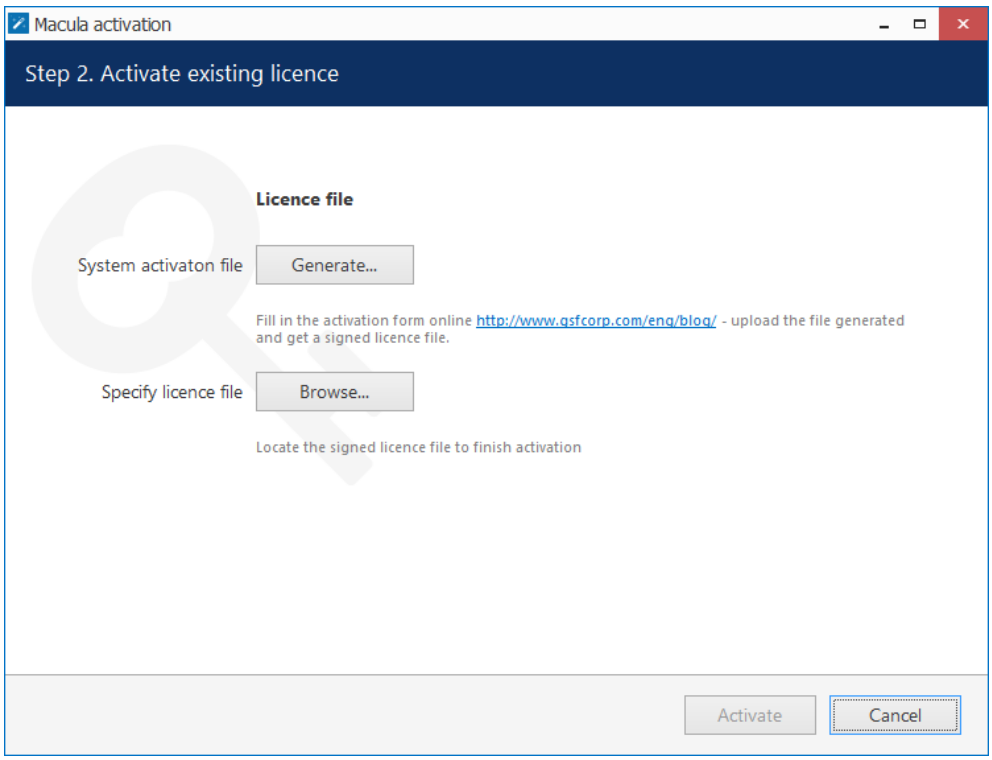
2.2 Offline Activation

If there is no Internet connection for security reasons and/or server disposition particularities, choose the *Offline Activation* type.

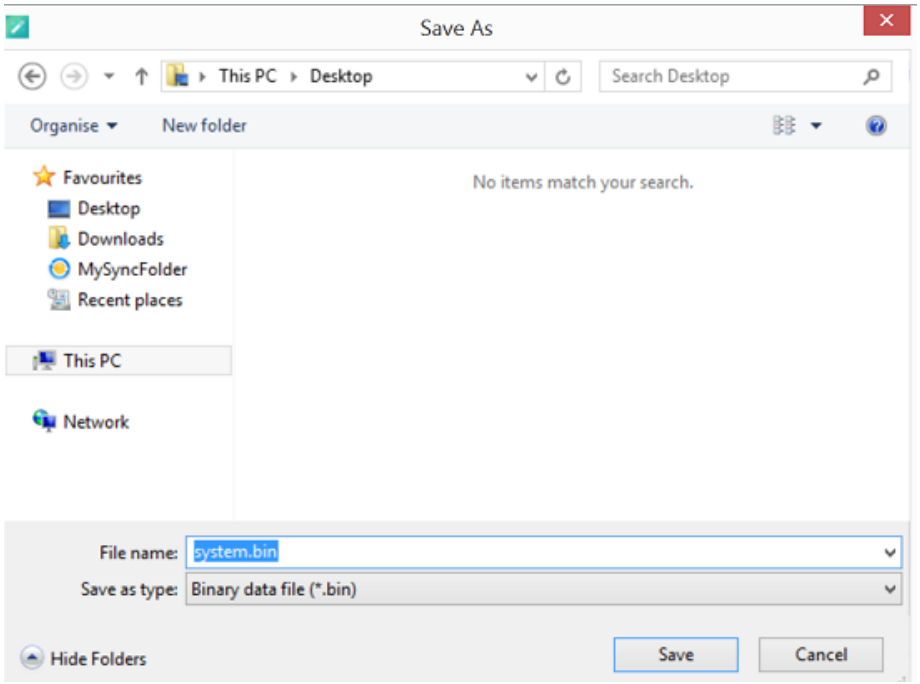


This mode consists of three steps:

- generate the activation file on the target server
- go to the online activation system at http://app.gsfcorp.com/macula/activation/ and fill in the form
- apply provided license file to your system



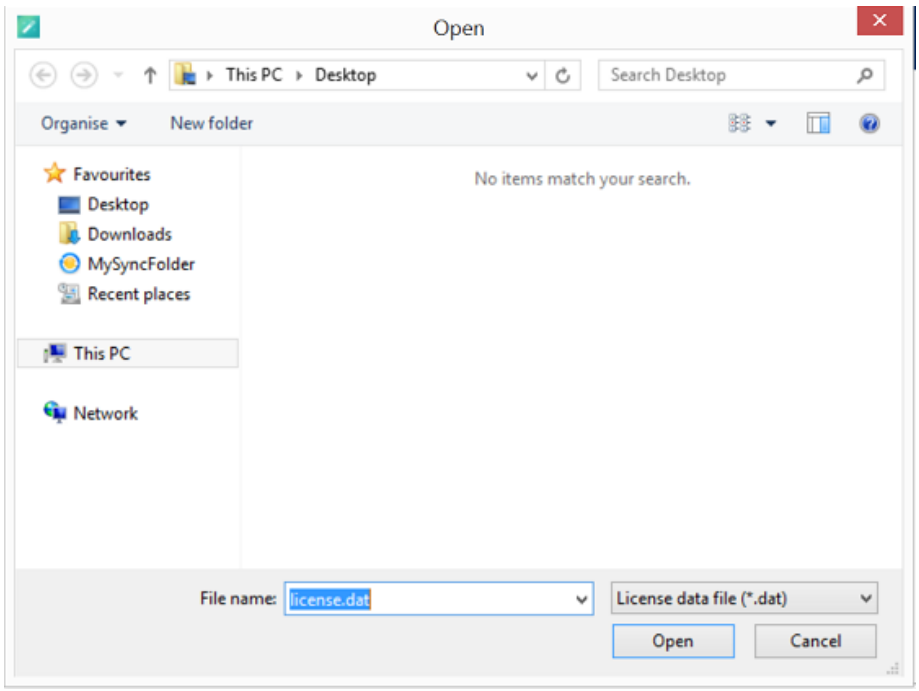
Click *Generate* to create the activation file; choose a location and save it. The default file name is *system.bin* and we do not recommend changing it.



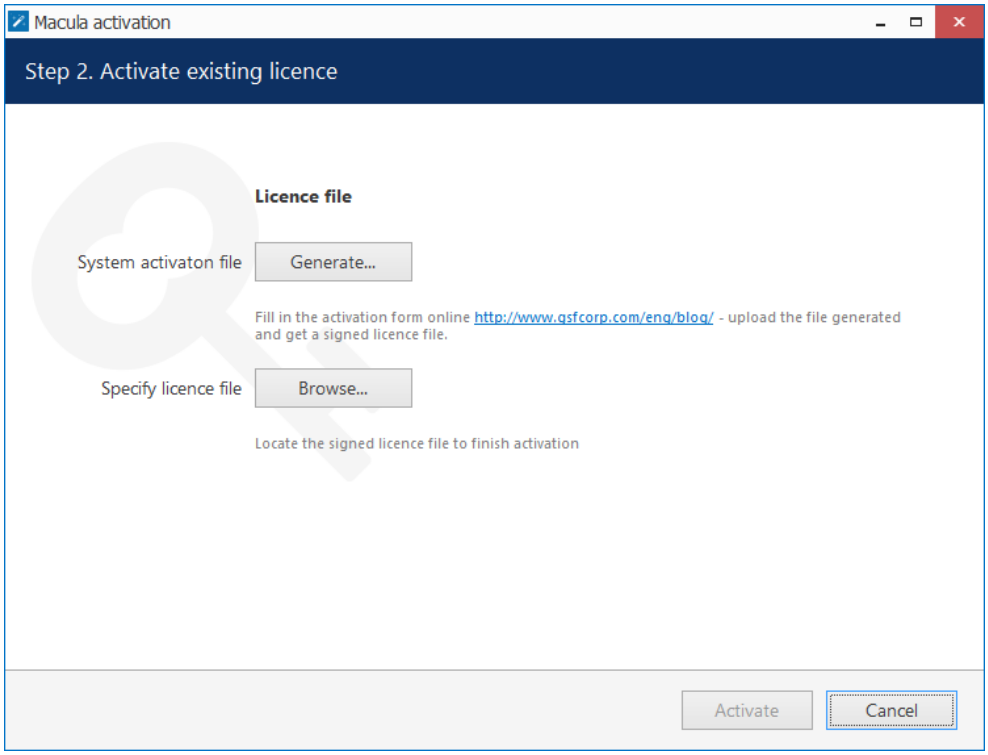
Next, copy this binary file to any other computer that has Internet access, then go to the online form available at http://app.gsfcorp.com/macula/activation/, fill in the required fields and upload the file. The activation system will process your file and allow you to download a license file. This license file will be unique and will only be valid on the same machine from which the original *system.bin* file comes.

You can close the activation wizard after creating the activation file and reopen it later to apply the license file. Click *Browse* to locate it and open the *license.dat* file provided by the activation system.

Macula® Professional Administration Guide



The validated license.dat file will be loaded, allowing you to finish the registration process.



Click *Activate* to apply the license file. If the license is valid, you will see an activation success confirmation with the following details:

- product type
- license key
- license key expiration date, if applicable
- support subscription expiration date
- allowed channel amount

The license information will be stored on your server. However, you may wish to save a snapshot of this screen for your future reference, so that this information will be accessible in case of server OS or hardware failure.

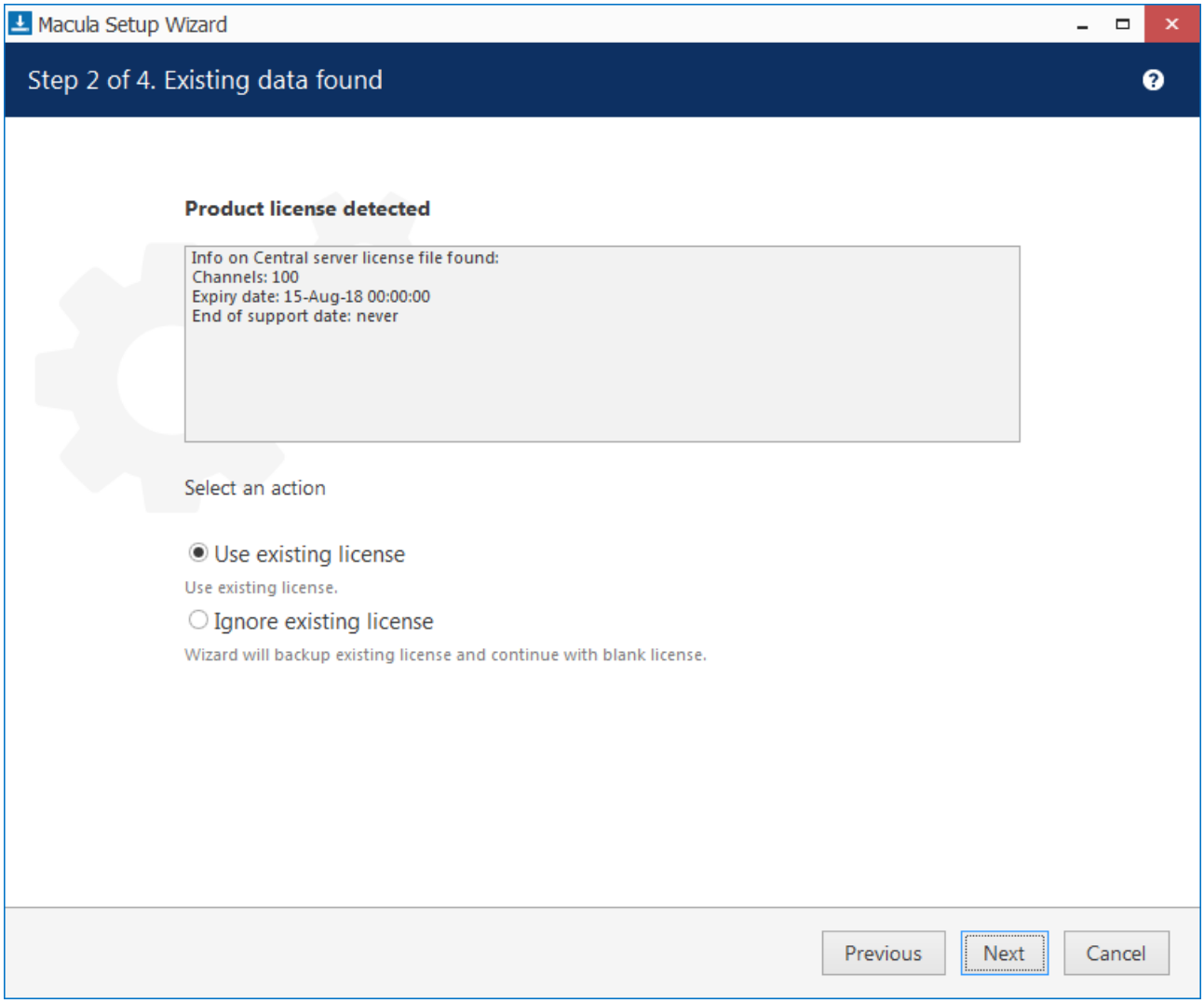
Finally, click *Done* to exit the activation wizard or click *Start Quick Setup Wizard* to proceed with server configuration.

2.3 Activation Management

When a server already has a license key installed, you can retrieve that information in two ways:

- right-click server icon in the system tray and select *About*. The dialog box will contain basic information about the product version and license type
- run the *Macula Registration & Activation* from the Start menu

To start the wizard, go to *Start -> All Apps -> Macula -> Macula Registration & Activation* (in Windows 7 and older versions, use *Start -> All Programs -> software installation folder -> Tools -> Macula Registration & Activation*); alternatively, use Search to locate the Activation Wizard in the programs menu.

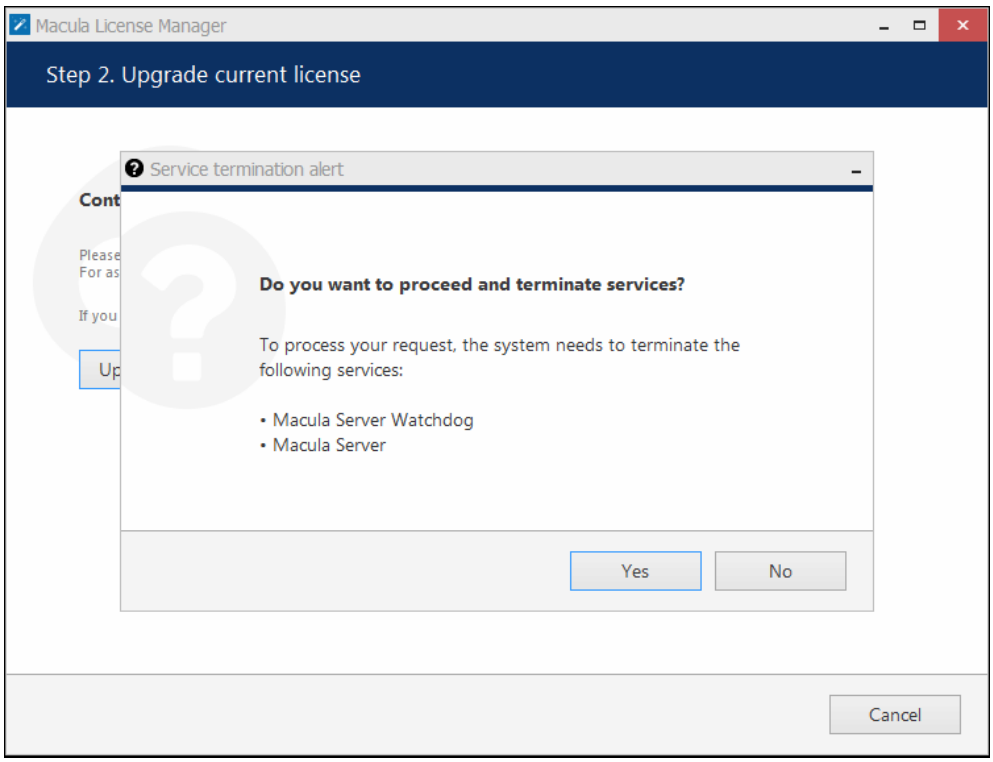


The wizard will display a summary about the currently installed license key and show the available management options.

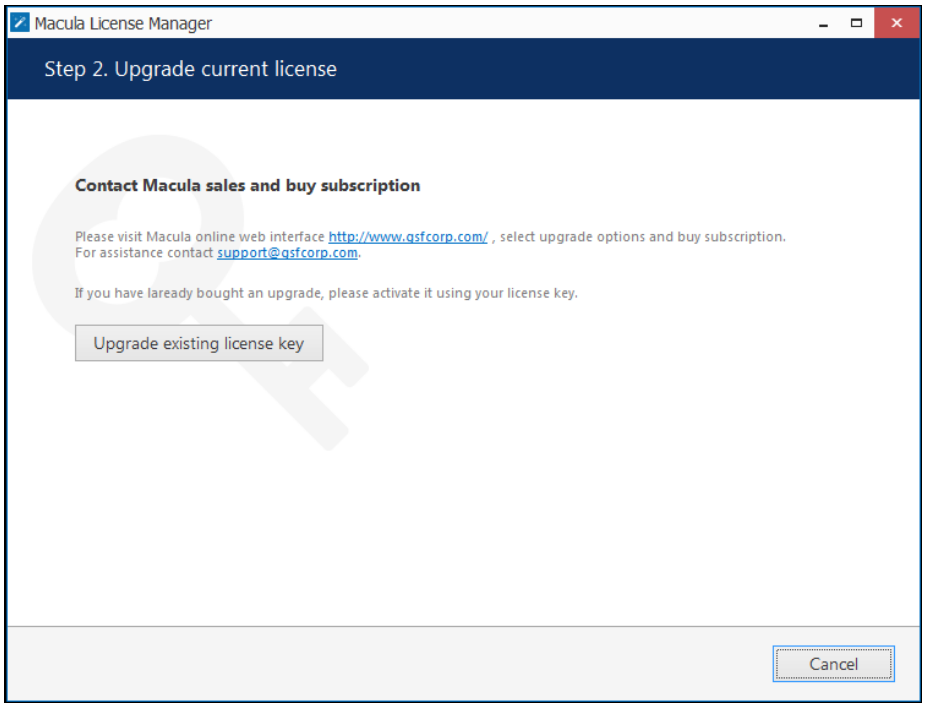
Online license upgrade

License upgrade is available for the license keys purchased earlier. Note that all the software processes (both applications and services) must be stopped in order for the license to be applied correctly.

For upgrade acquisition details and assistance, please contact sales@gsfcorp.com.



All software processes must be stopped in order to apply license related changes



After acquiring the upgrade from GSF, click *Upgrade Existing License Key* to enter it. Your license information will be synchronized with the activation server and you will be presented a license summary. Click *Cancel* to return to the beginning of the wizard.

Offline license upgrade

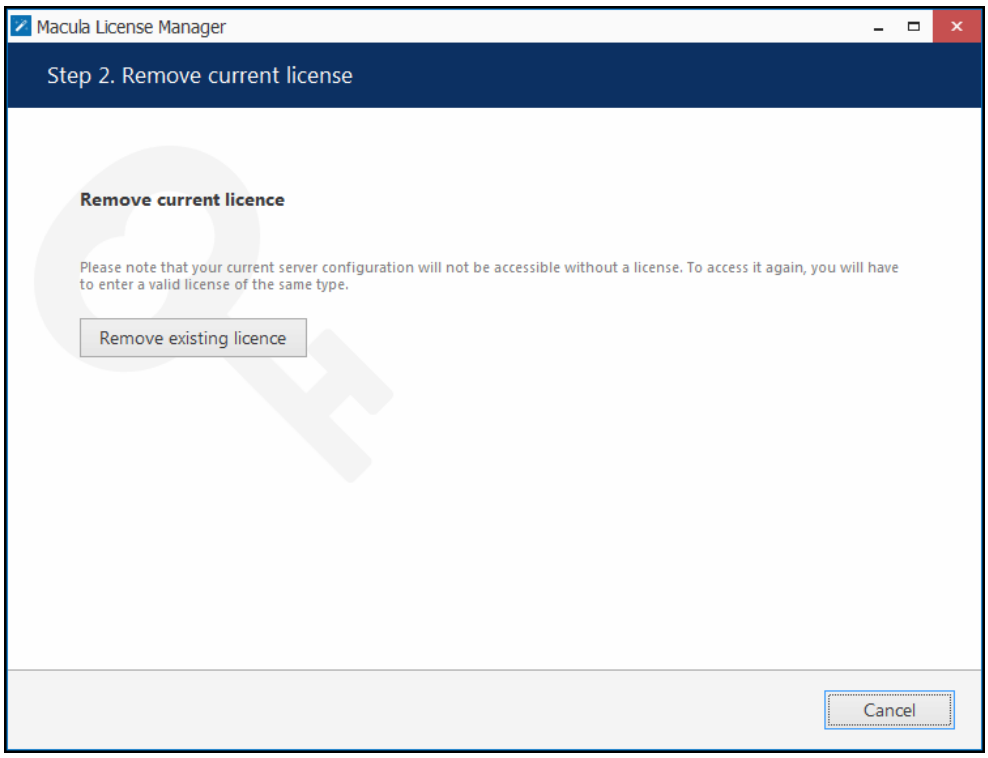
Offline license upgrade essentially the same as the offline license activation process: the same steps should be taken to retrieve the new license file.

- generate activation file on the target server
- go to the online activation system at http://app.gsfcorp.com/macula/activation/ and fill in the form
- apply provided license file to your system

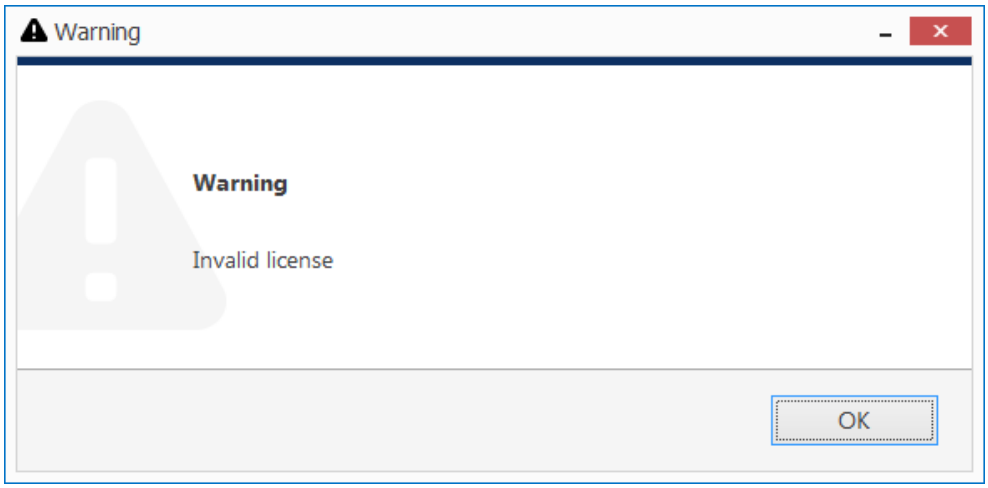
Click *Cancel* to return to the beginning of the wizard.

Remove license

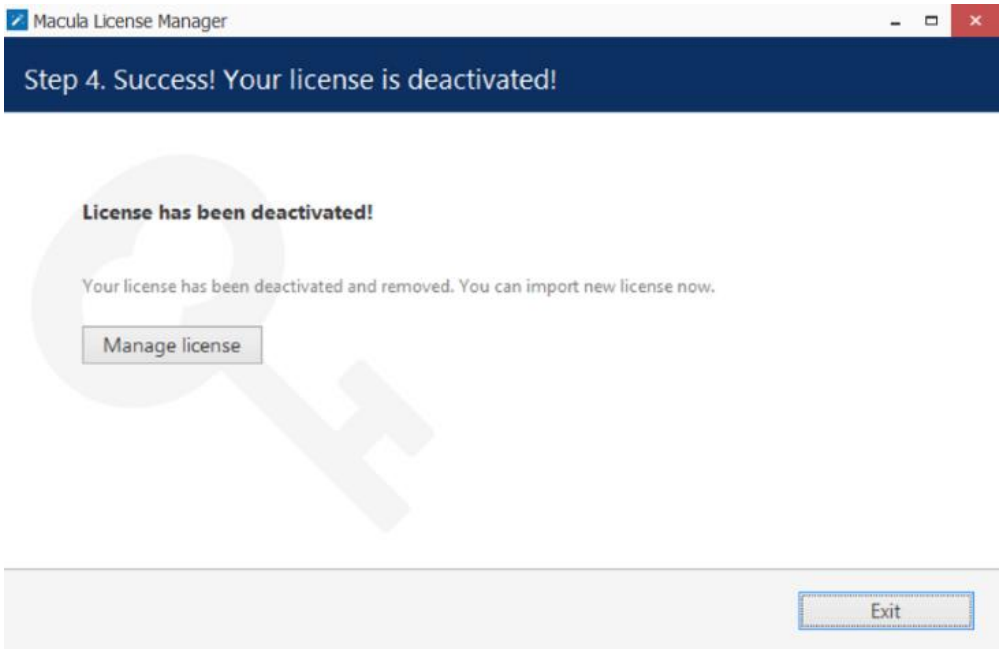
Select *Remove License* if you wish to completely delete all the license information from the server.



Click *Deactivate Existing License* to confirm deletion of the currently installed license. Note that you will be unable to log into Macula Console to access your current server configuration without a valid license of the same type; Macula Monitor applications will also not connect to such a server. In order to use the server again, you will have to enter the license again - either the same or a new one.



Alternatively, press *Cancel* to return to the wizard start page. If you are not sure about the deactivation, consult GSF technical support.



After license deactivation, you will be offered the chance to go back to license management in order to enter a new software license.

3 Macula Console Login

All server configuration is conducted through a dedicated interface - the Macula Console management application. The management interface has been intentionally separated from the Macula Monitor application in order to concentrate all administrative utilities in one place and also to conceal the unnecessary menus from the Macula Monitor operator. Applications are totally independent from each other and can be or not be installed on the same machine. Macula Console for a single installation management can be installed on one or more computers, depending on the system administrator's needs.

> It is implied that Macula Enterprise installations are handled through the **central server** by logging into the target central server locally or remotely via Macula Console. **Recording servers** can be also reached via Macula Console but it is not possible to change their settings directly.

Run Macula Console application by double-clicking the Macula Console shortcut from the desktop or Start menu.

To log in, simply enter your Macula Global server's local or remote address (IP or host name), TCP port and user information. If you have logged into different servers from this Macula Console instance in the past, the Macula Console login dialog box will have a drop-down list in the *Server* field.

> If your server has default TCP port configured (which is 60554), you do not need to specify it when connecting: simply type the IP or hostname of the server to connect to. However, if the server TCP port has been altered, you need to specify the port explicitly, making the connection address look as follows:
>
> <address>:<port>, e.g., *192.168.1.77:60555* or *localhost:60887*
>
> Server TCP port can be changed via Macula Server Setup Wizard.

Note that, if you already have pre-configured user accounts, the user must have corresponding permissions in order to connect.

Macula Console can be launched **multiple times** if you need to control multiple different servers simultaneously, e.g., if you need to configure Macula Global and check Macula Recording Server configuration directly at the same time. In general, you only need to connect to your Macula Global server machine directly once for all configuration routines. Direct Macula Recording Server login is usually required for monitoring and audit purposes.

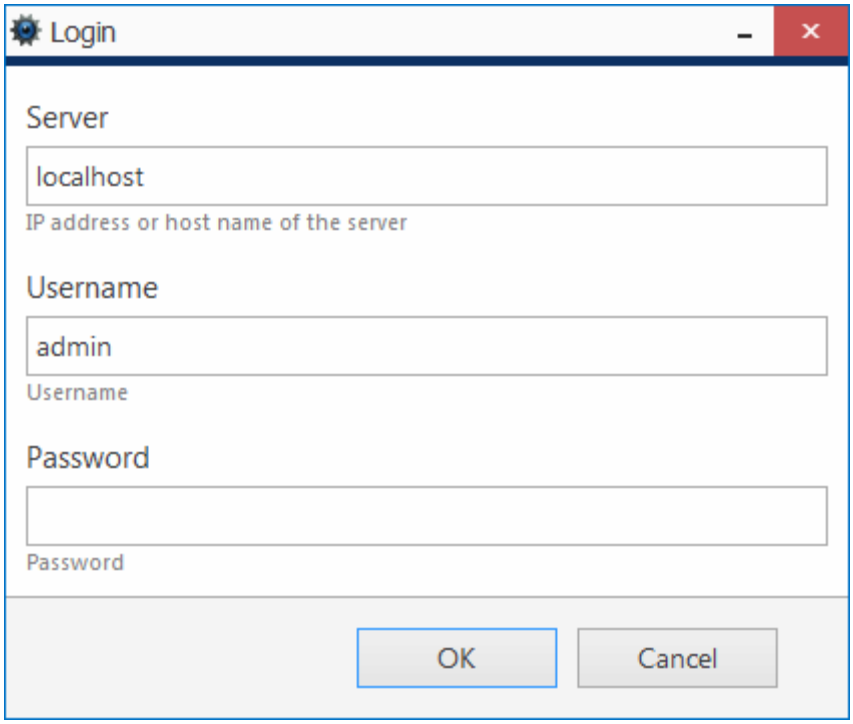
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

First-Time Login

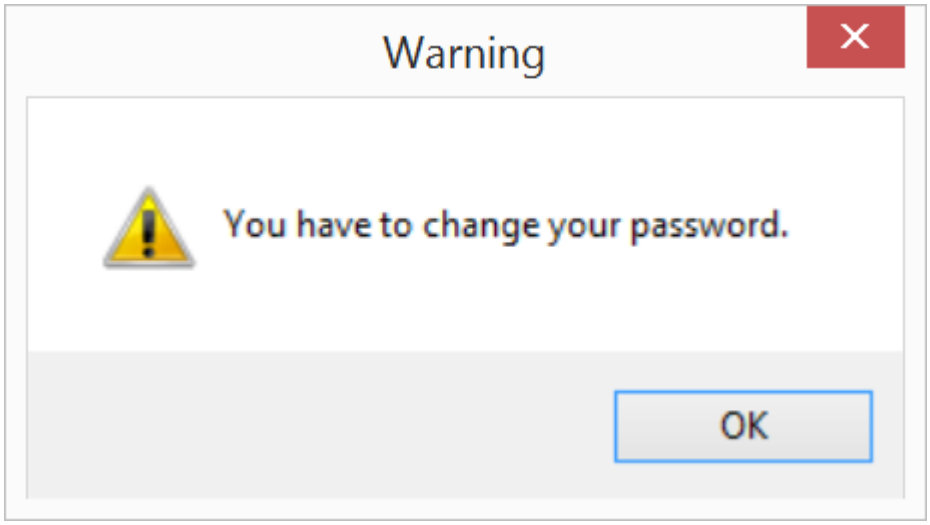
When logging in for the first time, use the default combination of user name and password**:** admin/[empty]. You will be asked to change the password to a more secure one immediately afterwards.

> The **default username and password** for the new installation is **admin/[empty]**.

If you are refused a connection, make sure that the server is running and accessible over the network. (For more detailed information about what to do, please refer to the Troubleshooting section of this document: it is constantly updated with most common cases).



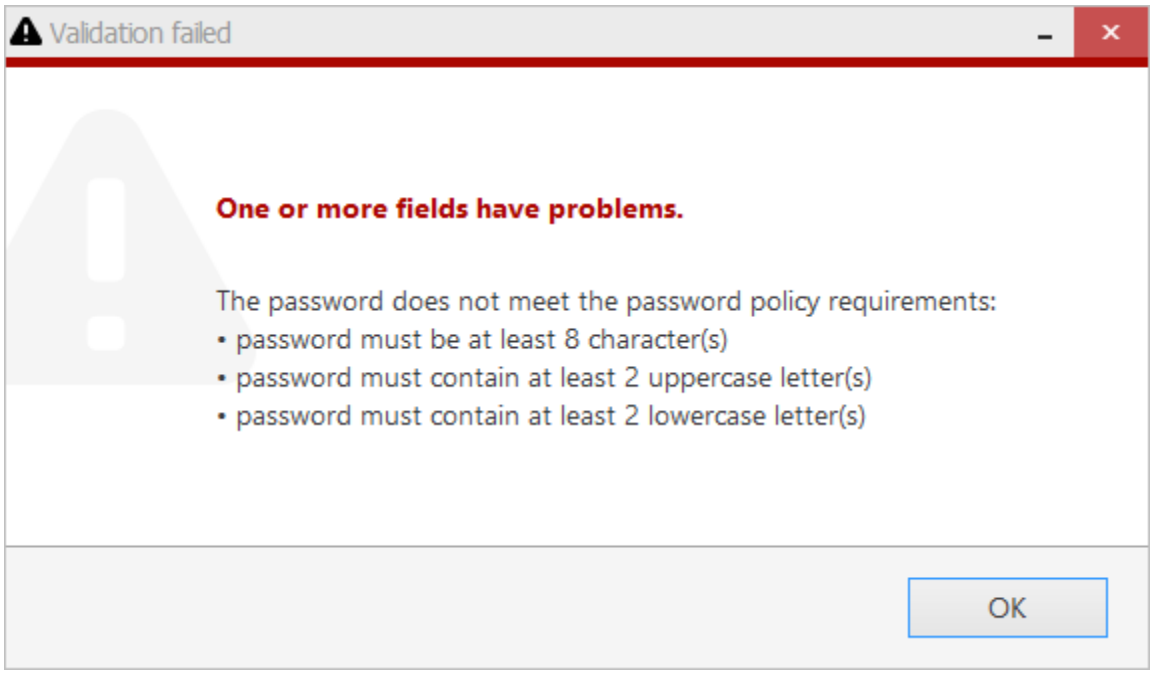
After logging in for the first time with default username and password, you will be reminded to change your password. For security reasons, we strongly recommend that you do so at once.



You will be given the option to change the password using an additional dialog box. To change the password, enter your old password (initial, default password is empty so just leave the field empty),

then enter your new administrative password for the current server, enter it for the second time to confirm, then click *OK to save.*

> The new password must **comply with server policies**, by default these are: minimum 8 characters total length, including at least 2 lowercase and 2 uppercase letters.



After you are done with password update, you will be given the opportunity to fill in the initial server settings using the quick Setup Wizard. We recommend that for optimum first-time configuration you follow the steps in the wizard.

Two-Factor Authentication Login

Starting from the version 1.21, Macula supports 2FA for Macula Console. You can use it to log into the Macula Global system and or individual Macula Recording Server servers.

This application supports two-factor authentication as an additional security measure for the user login. It does not eliminate the necessity to enter the user password; instead, it serves as an additional security layer.

If the target server has two-factor authentication (2FA) policy enabled, you will be asked to confirm your identity by requesting and entering a code. Depending on the server configuration, the code may be requested by email or by SMS.

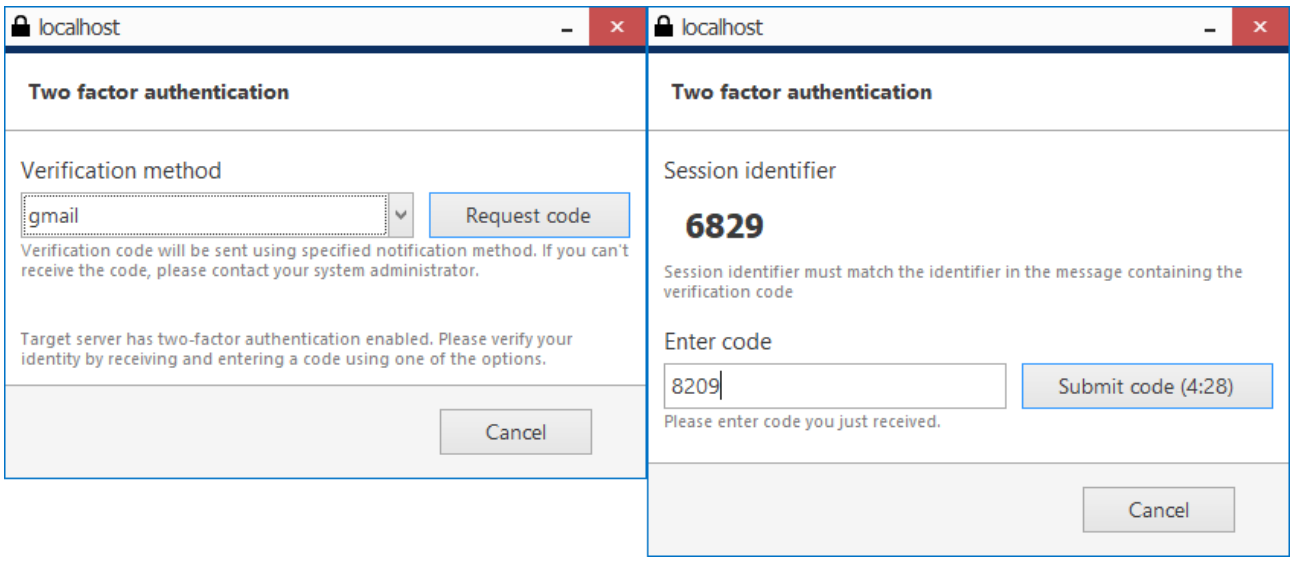
> 2FA is configured by your Macula server administrator, so if you have any issues with requesting, receiving, or entering the code, contact the person who maintains the target Macula server. Provide the server administrator with your valid email and full phone number.

> The 2FA settings affect all users and all clients by default; the system administrator can set up exceptions for localhost connections and also for individual users.

Macula® Professional Administration Guide

The login procedure with 2FA is as follows:

- an additional dialog box pops up upon the server connection attempt
- choose one of the provided verification methods and click *Request code*
- in the next dialog, you will see a session ID and an empty box
- check your email or phone (or other provided verification source) for an email with the same session ID (for example, marked as #6708 here) and copy the code from the message body (1234 here)
- click *Submit code*: if everything is OK, you will be logged in

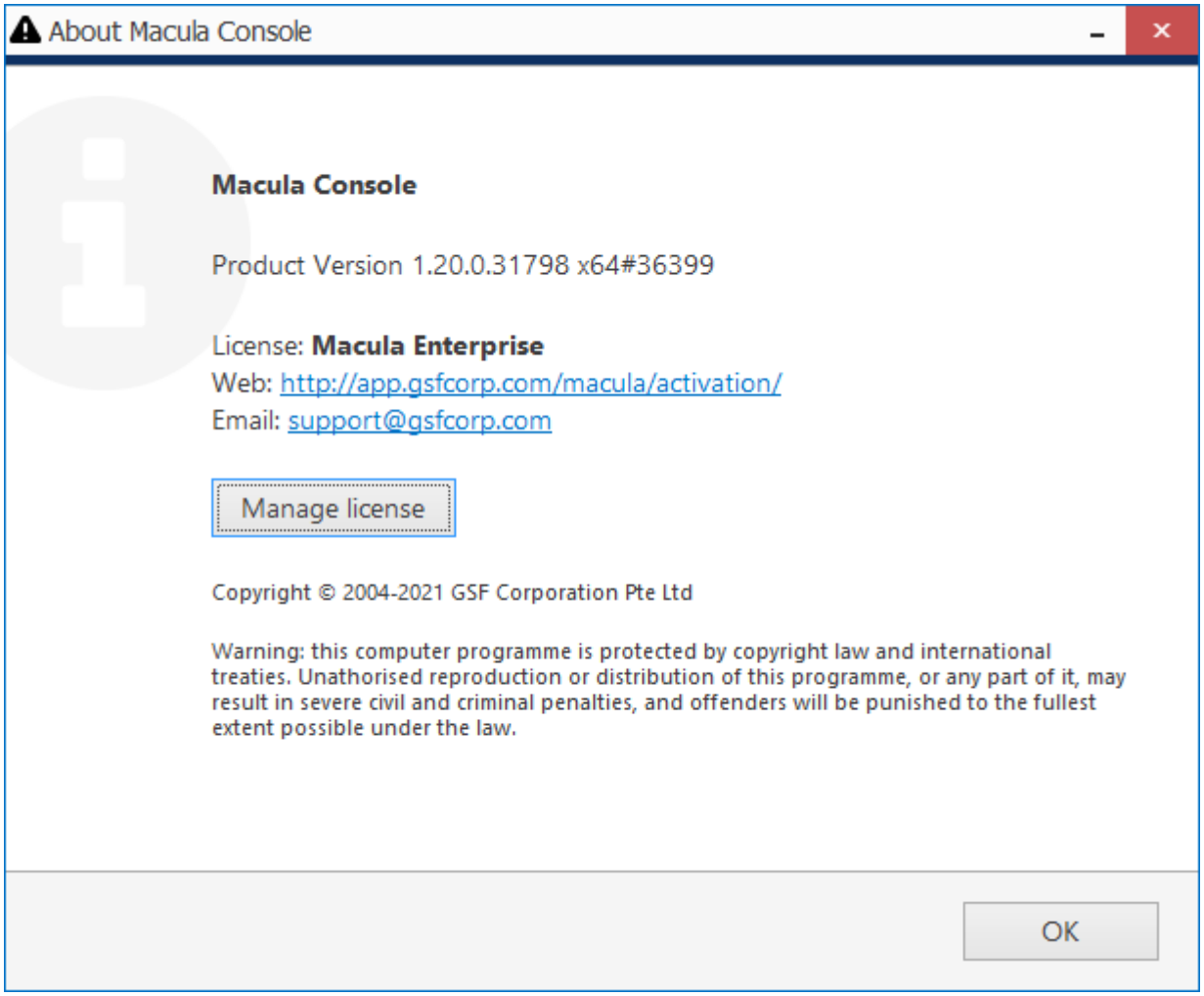


© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

3.1 About Product

Information about the currently running product can be viewed from the local computer in three ways:

- right-click the system tray icon and select *About* (if there is no tray icon, launch server shortcut to run the tray shell);
- from Macula Console, click the Application menu icon on the navigation panel and choose *About;*
- from Macula Monitor, go to the main menu, click Help and select *About*.



If you are connected to your Macula server locally (via *localhost*), the *About* window will allow you to open the activation manager from here (except for Macula Monitor). For remote connections, this option will be grayed out.

3.2 Database Import

You can use an existing Macula database to import resources into any other Macula installation. This feature allows you to **migrate** the server configuration 1-to-1 or **reuse** the configuration of devices and channels, user profiles, maps, recording calendars, etc., to speed up the site configuration.

Prerequisites

The database may come from any server and/or software edition, but it must contain no more than one server in its configuration. If you wish to import from a Macula Enterprise database, create a copy of it for backup, then remove all recording servers from its configuration first (move the devices to the Macula Enterprise server first if you need to preserve them), and use the single-server version for resource import.

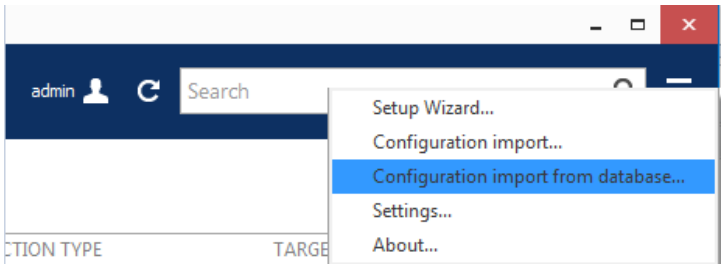
⚠ It is only possible to import the data from single-server databases.

Possible scenarios for this feature may be as follows:

- combine many Macula Professional servers into a single Macula Enterprise installation
- transfer configuration from one Macula Professional server to another

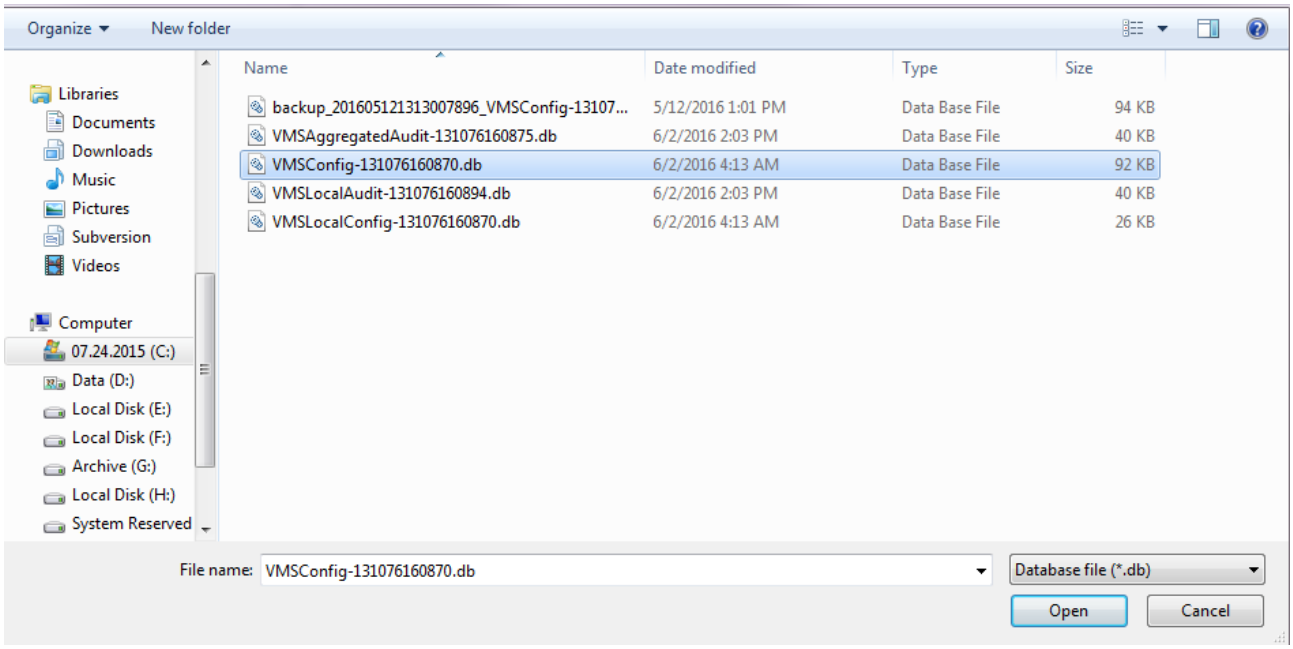
The database you need to take for future import is named *VMSConfig-xxxxxxxxxxxx.db* and it is located in the ProgramData directory.

💡 By default, all Macula databases are located in the following directories:
- C:\ProgramData\GSF Corporation Pte Ltd\Macula Professional - for the Macula Professional product edition
- C:\ProgramData\GSF Corporation Pte Ltd\Macula Enterprise - for the Macula Enterprise product edition
- C:\ProgramData\GSF Corporation Pte Ltd\Macula Enterprise Recording Server - for the Macula Enterprise Recording Server component of a Macula Enterprise installation

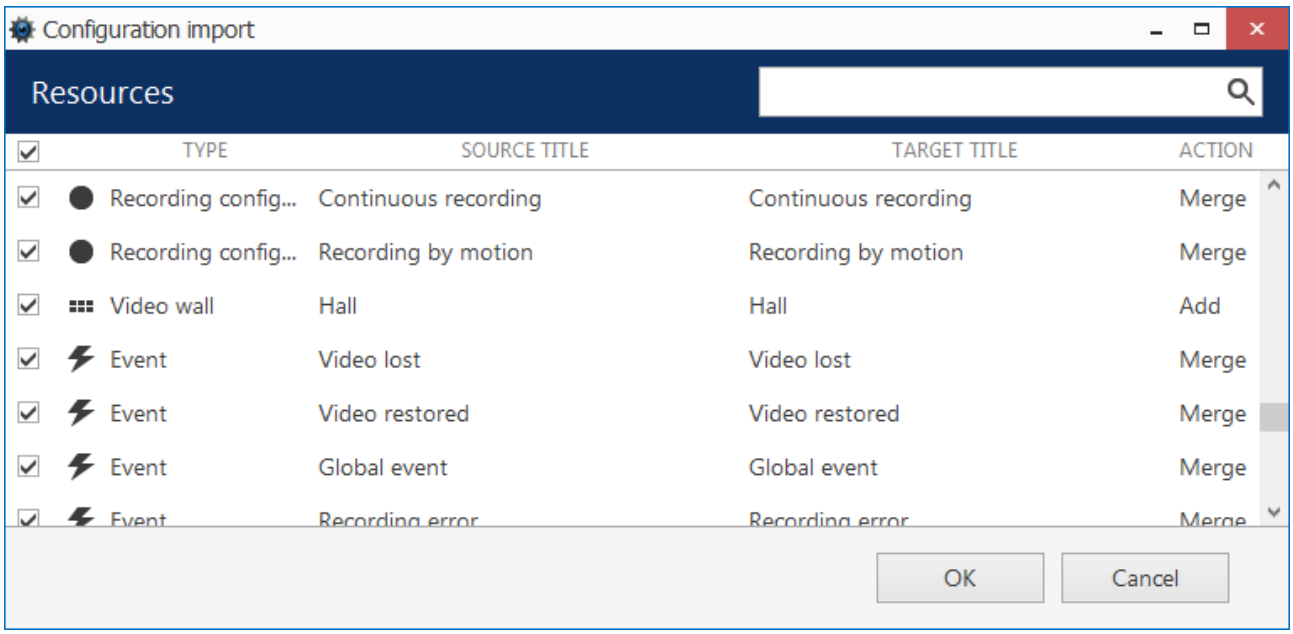


To start data import, press the application menu button in the upper-right-hand corner of the Macula Console window and choose the *Configuration import from a database* option.

From the standard Windows Explorer *Open File* dialog box, locate the target *VMSConfig-xxxxxxxxxxxx.db* file and open it.



The resource selection dialog box will appear. Choose the items to be imported using checkmarks in the left column; use the search field in the upper right corner to filter the items by type or by any other text field. In case the imported entities already exist on the host server (e.g., built-in recording profiles), their import action will be *Merge*; otherwise, the action will be marked as *Add*. When resources are merged, their permissions are merged as well. All types of resources can be imported.

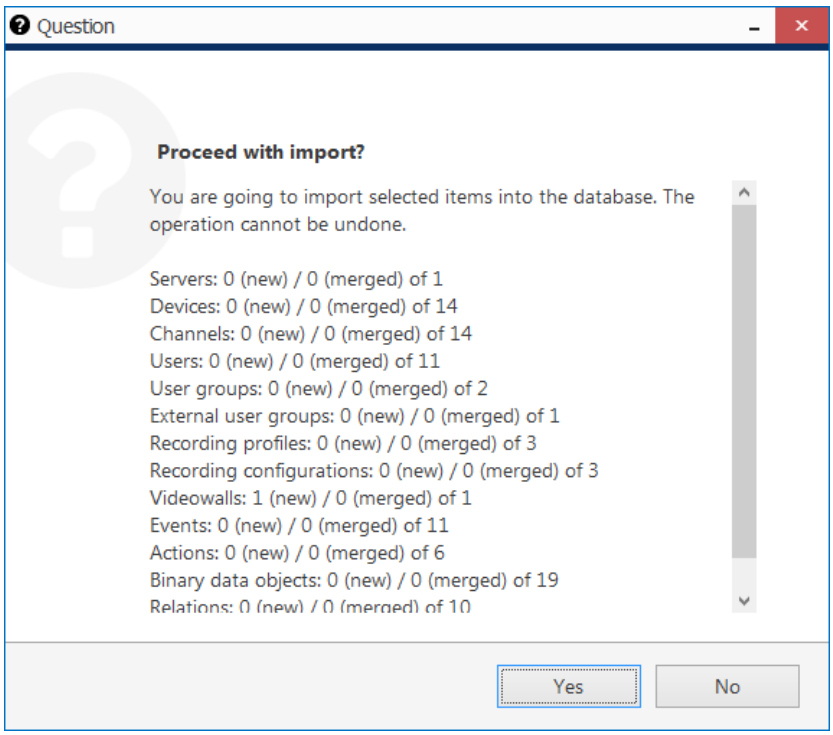


When you have finished with resource selection, click *OK* to proceed.

> ⚠ **Important**: this action cannot be undone. Before confirming, make sure to review all the changes you wish to apply.

Before applying all the changes, review your import summary and click *OK* to confirm and finish the import.

Macula® Professional Administration Guide



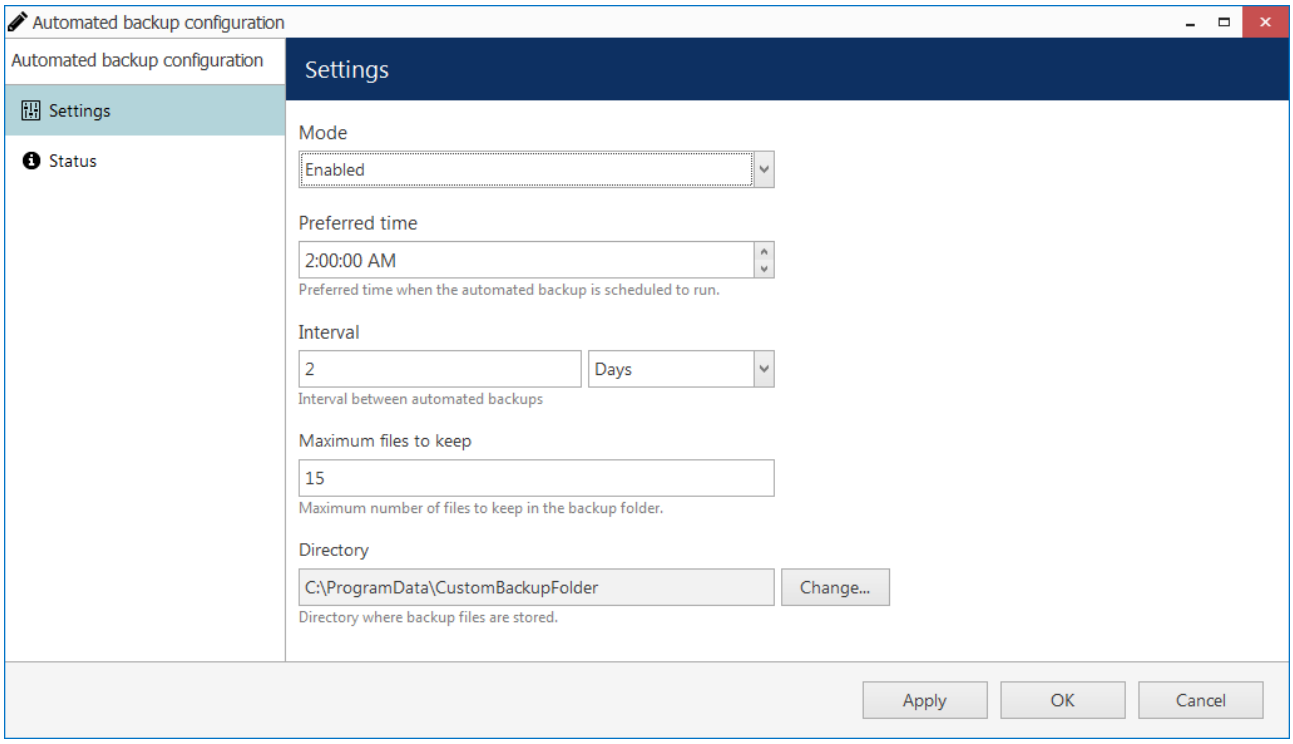
All selected items will be added to the server configuration immediately and you will be able to work with them normally.

3.3 Configuration Backup

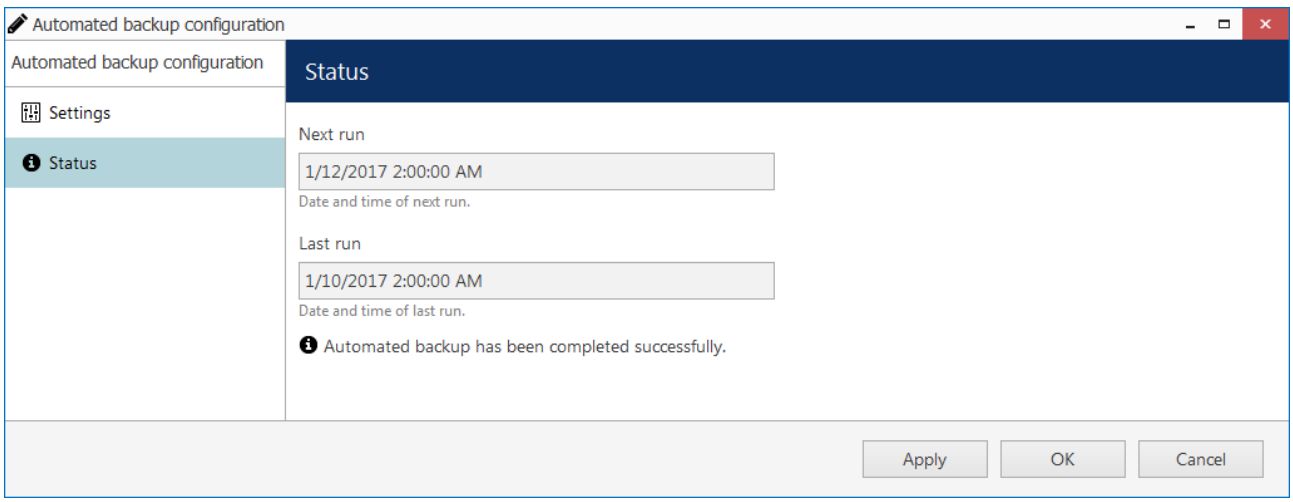
Server configuration is a time-consuming process and it is wise to save a copy of your Macula database after certain changes so that you have something to start the server with in case the main database becomes corrupt because of a hard disk failure or some other reason. Macula provides several options for database backup and we strongly recommend that you create configuration restore points to save the trouble of re-configuring the server from scratch.

Automatic Backup

Automated configuration backup allows you to save your Macula database based on a schedule. To access the settings via Macula Console, click the application menu button in the upper-right-hand corner and choose *Automated backup configuration*.



Automated backup is enabled by default with the following settings: a restore point is created every two days at 2AM, with a maximum of 15 files to be kept. You can either leave the default settings, including the default location, or define your own backup time and frequency in the *Settings* tab.

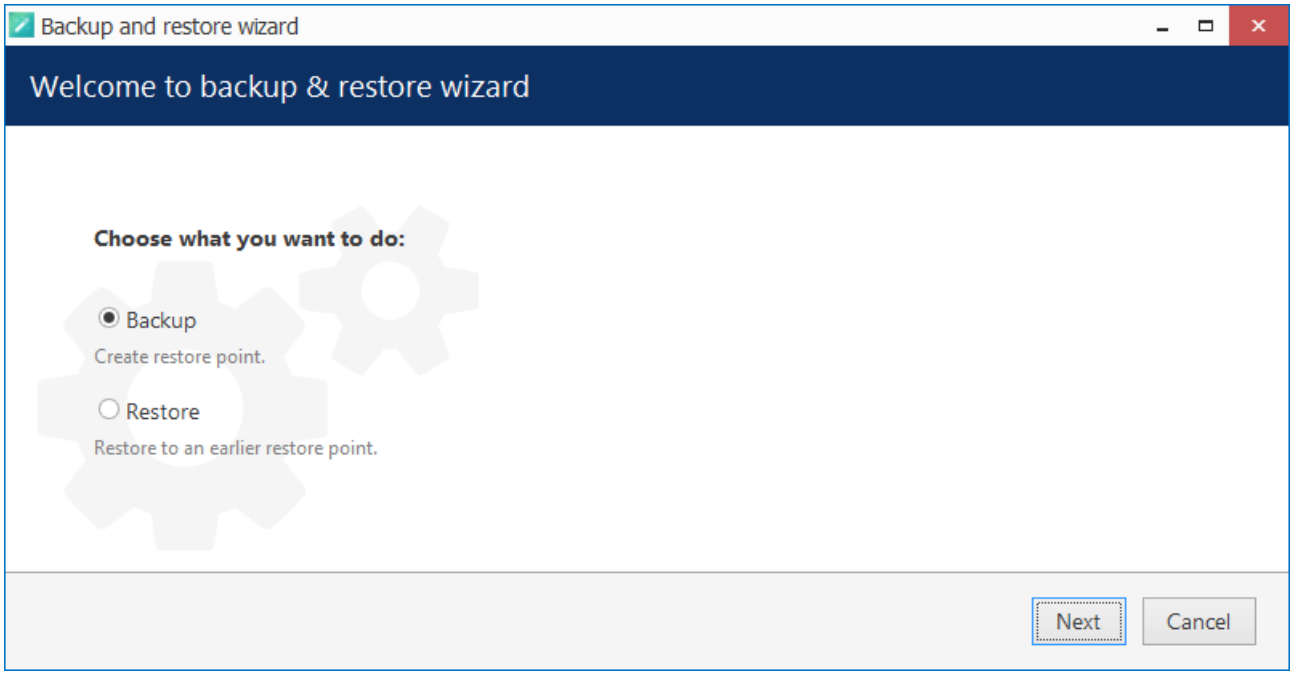


In the *Status* tab, you can see the date of the last backup attempt and the next scheduled backup time.

Backup and Restore Wizard

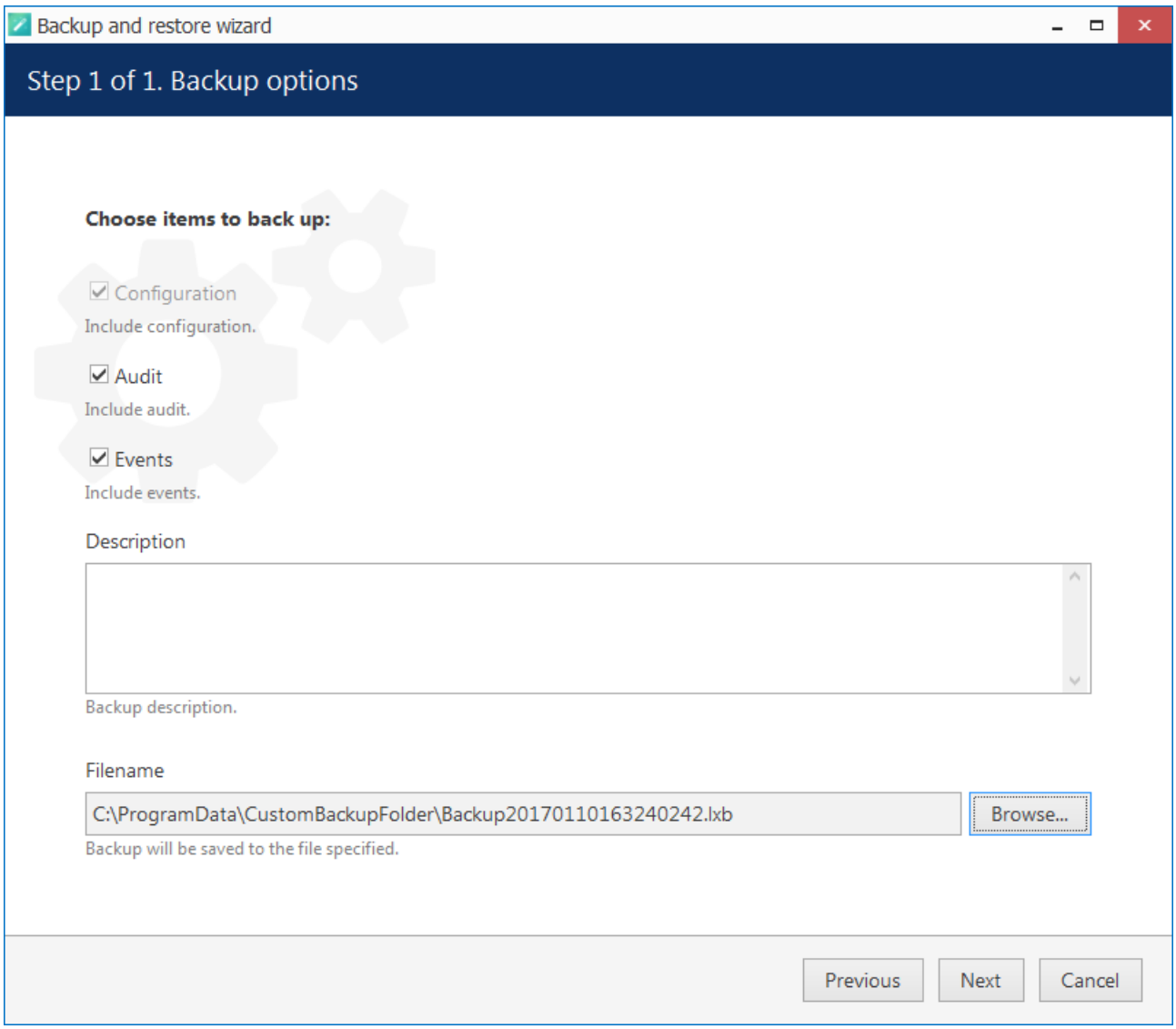
Additionally to the automated backup, it is possible to create a configuration restore point manually at any time. The same wizard provides an opportunity to start the Macula with an earlier database version.

Run the Backup and restore wizard from your Windows Start menu: *Start -> All Apps ->* Macula *-> Macula Server Backup and Restore Wizard*. In Windows 7 and older versions, use *Start -> All Programs ->* software installation folder *-> Tools -> Macula Server Backup and Restore Wizard*; alternatively, use Cortana/Search to locate the wizard in the programs menu.

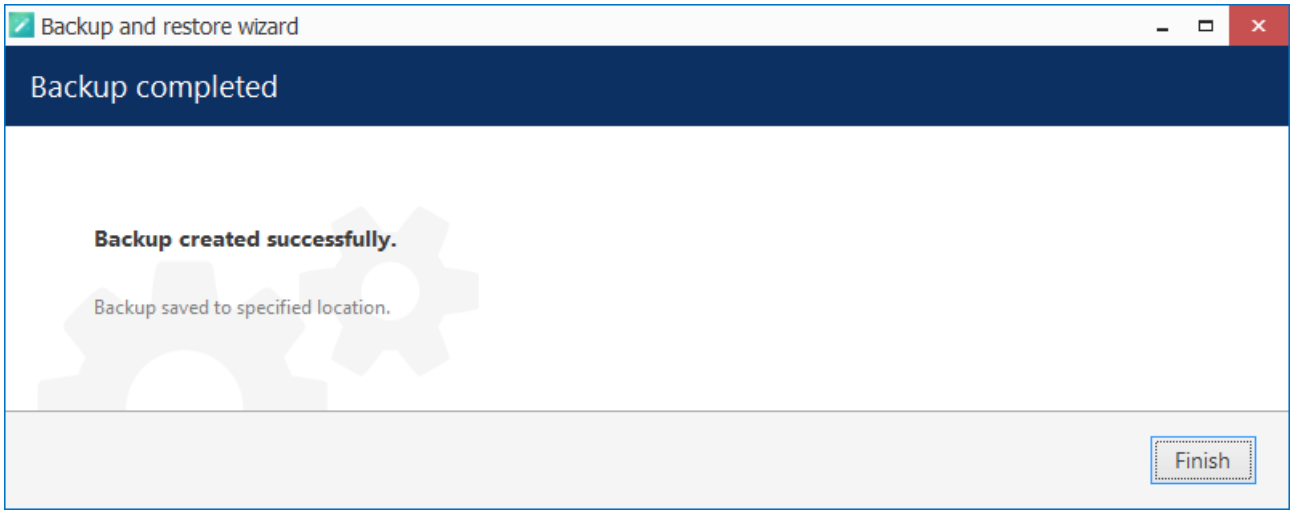


Create Backup

Choose the first option to back up the database contents to serve as a restore point and click Next.



Here, you can choose the information to be saved and also add a custom description for your future reference. You can either use the default destination folder or choose a custom one, even located on a different disk or a network drive.

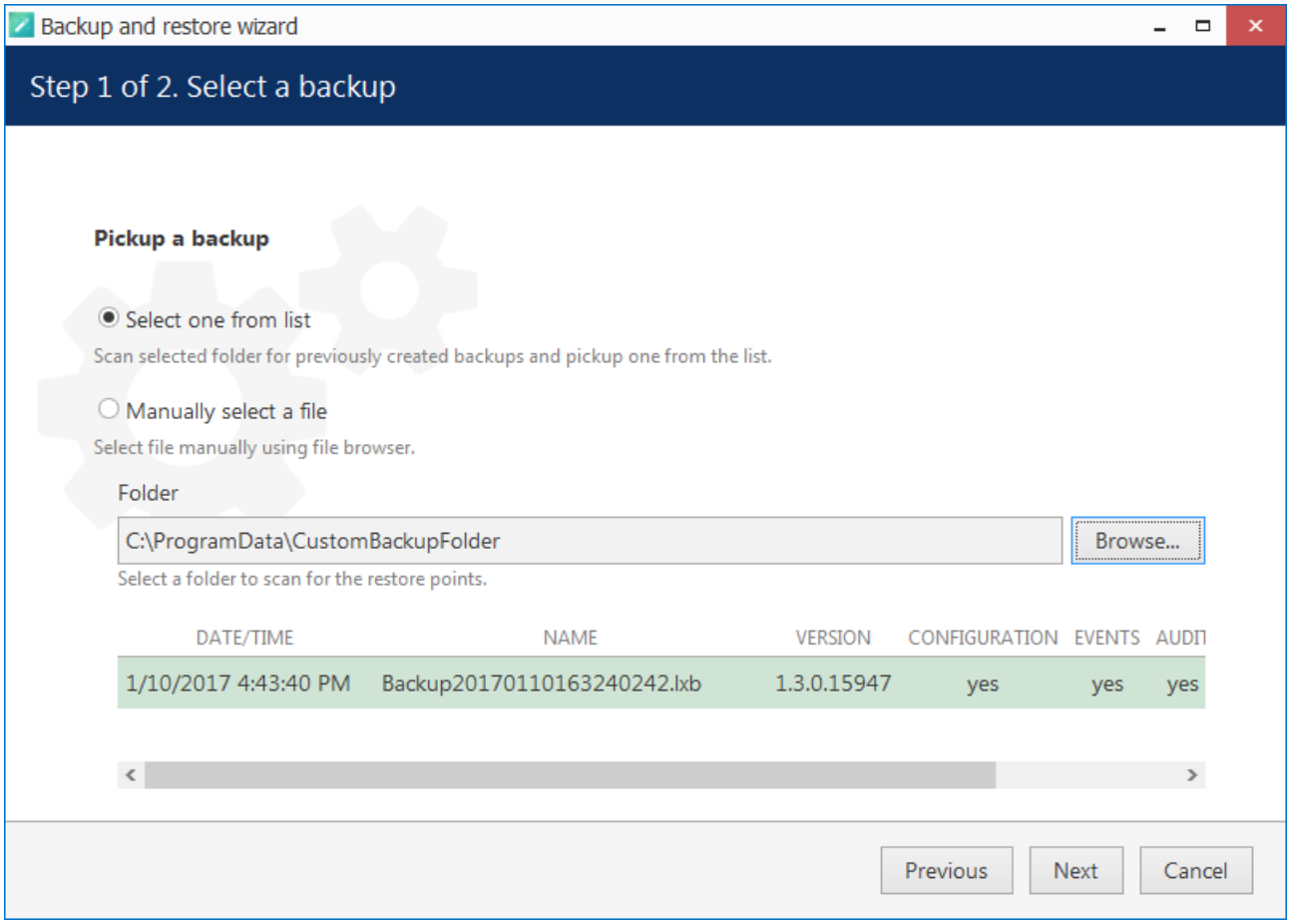


The wizard will create the backup and display a success message. Click *Finish* to exit.

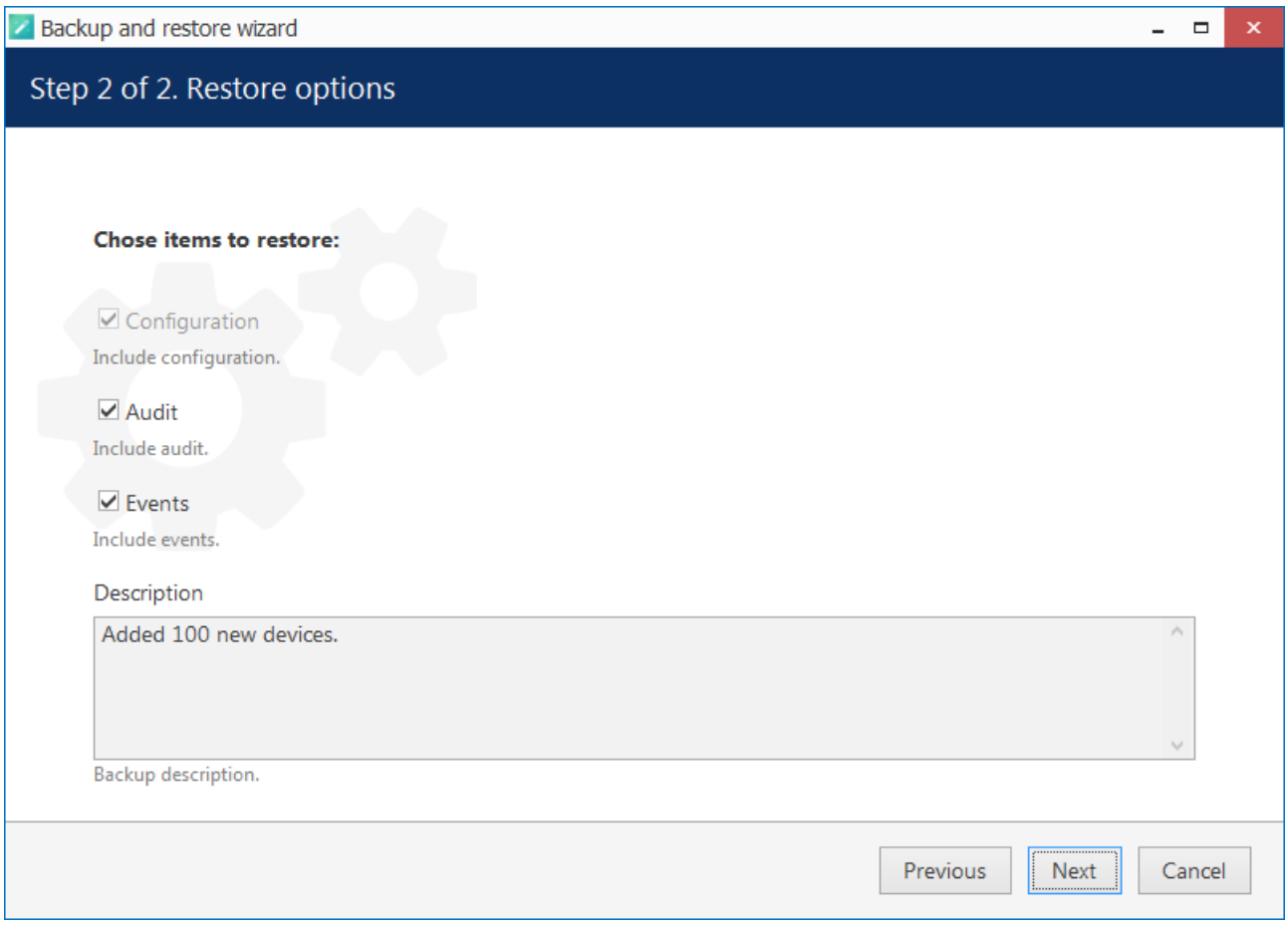
Restore to an Earlier Database Version

Choose this option if you wish to start the Macula server with a database from an earlier time instead of the current configuration.

> ⚠ If you have a clean Macula installation and wish to restore its configuration from an earlier point, make sure to initialize the server using the Server Setup Wizard, which usually pops up automatically after the installation is completed and is available via Start menu. (There is no need to do this if you upgraded the software to a newer version so that it already has been initialized earlier).



Here, you have two options: select a backup file from the list or manually locate the necessary *.lxb file. In either case, make sure you have chosen the right backup to be used and then click *Next*.



Make sure you have chosen a suitable database to be restored by reviewing the items and using your earlier comments as a reference. Click *Next* when ready.

On this additional step for Macula Global, you will be able to choose to **reset** the Macula Recording Server configuration.

How to choose the right option?

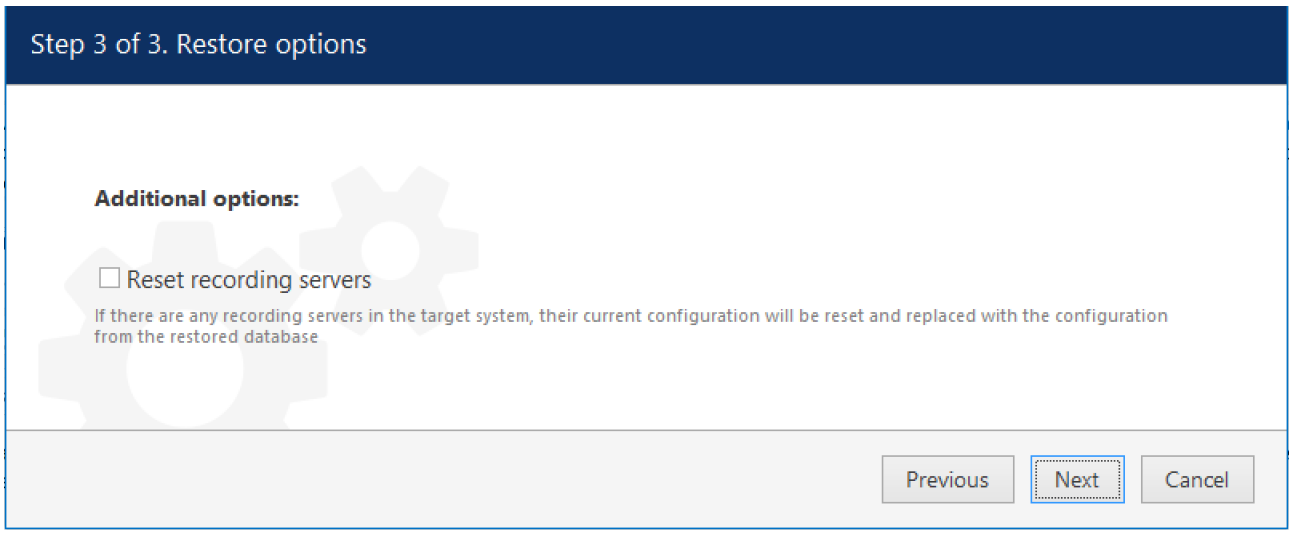
- If you are just restoring the Macula Global server database (e.g., after the central server version rollback), you do not need to reset the recording servers because their configuration is actually the same (just the DB version is incompatible).
- If you are using a much earlier database backup that certainly has a different Macula Recording Server configuration, then you need to include the reset.

⚠ Recording server reset is usually necessary if the remote server configuration is invalid (corrupt or different from the target DB contents).

If you choose to reset all recording servers at this point, it will take some time for them to re-synchronize (remove and then accept the restored configuration), which may result in some downtime. On slow connections with a lot of remote servers the downtime may be significant.

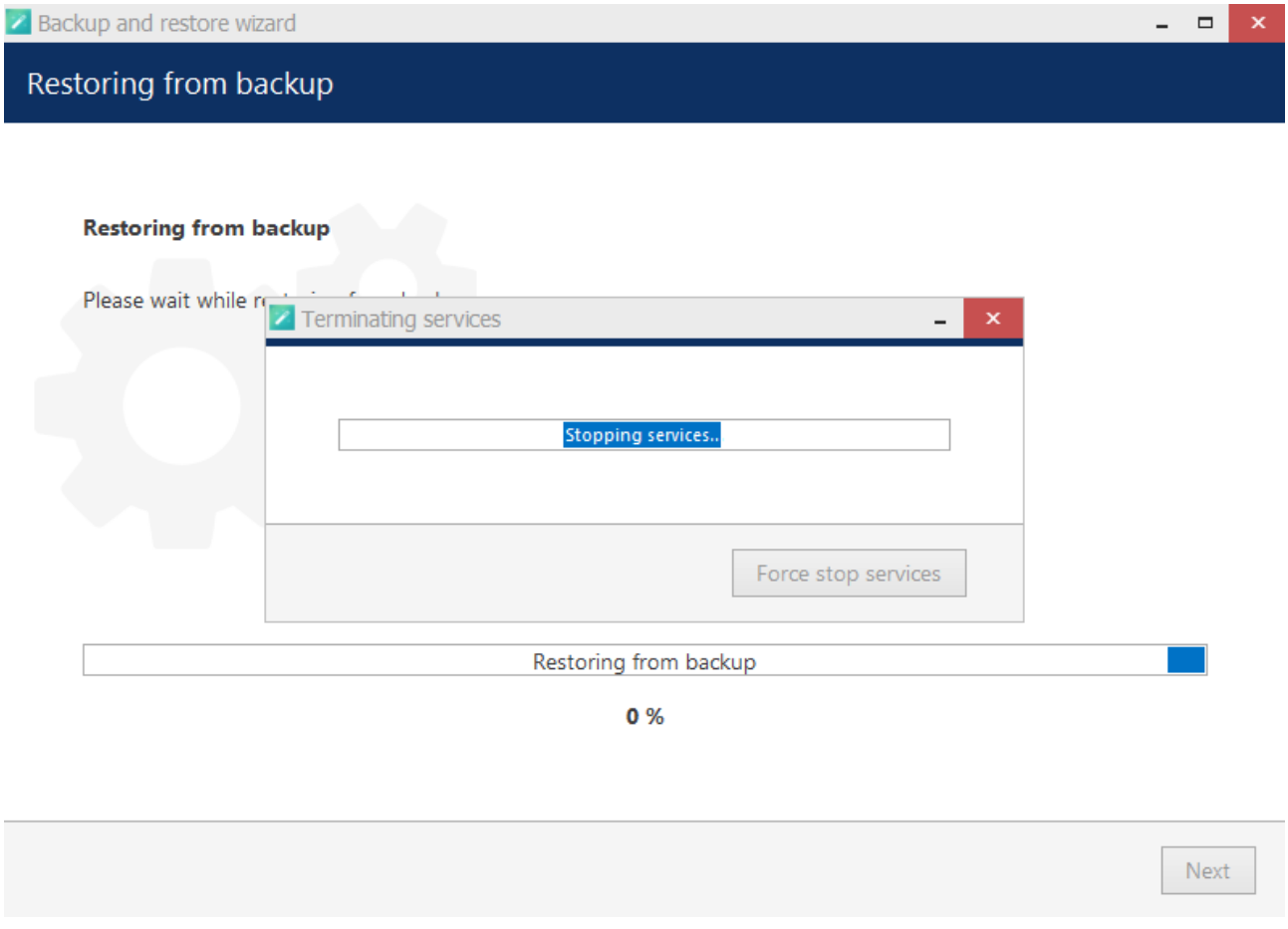
If you have many recording servers on a slow connection, we recommend that you do NOT reset them at this point. These servers will continue to operate with their current configuration but their status in the *Monitoring* section may turn to *Not synchronized*. In that case, initiate the re-synchronization manually later via %console% main menu > System upgrade > select server > Re-synchronize configuration.

This option is disabled by default to decrease the potential downtime.



When you click *Next*, you will see additional details about the recording server reset, which will help you choose the correct option for your system before proceeding - and give you a chance to re-consider. Carefully estimate the need for the reset before initiating the restore procedure!

> A database from a newer software version cannot be used for this. Older database versions can be used without issues.



Then, the wizard will ask you to stop the Macula services and start restoring the database after your confirmation.

> ⚠ Caution! This is an irreversible operation. Do not abort the process or shut down the server machine during the process.

If nothing interferes with the restore process and the backup file is intact, you will receive a success message after the wizard finishes restoring your Macula server configuration. Server service will be automatically started with the restored database. If you chose to reset the recording server configuration, all Macula Recording Server instances will receive the restored configuration as well.

3.4 Setup Wizard

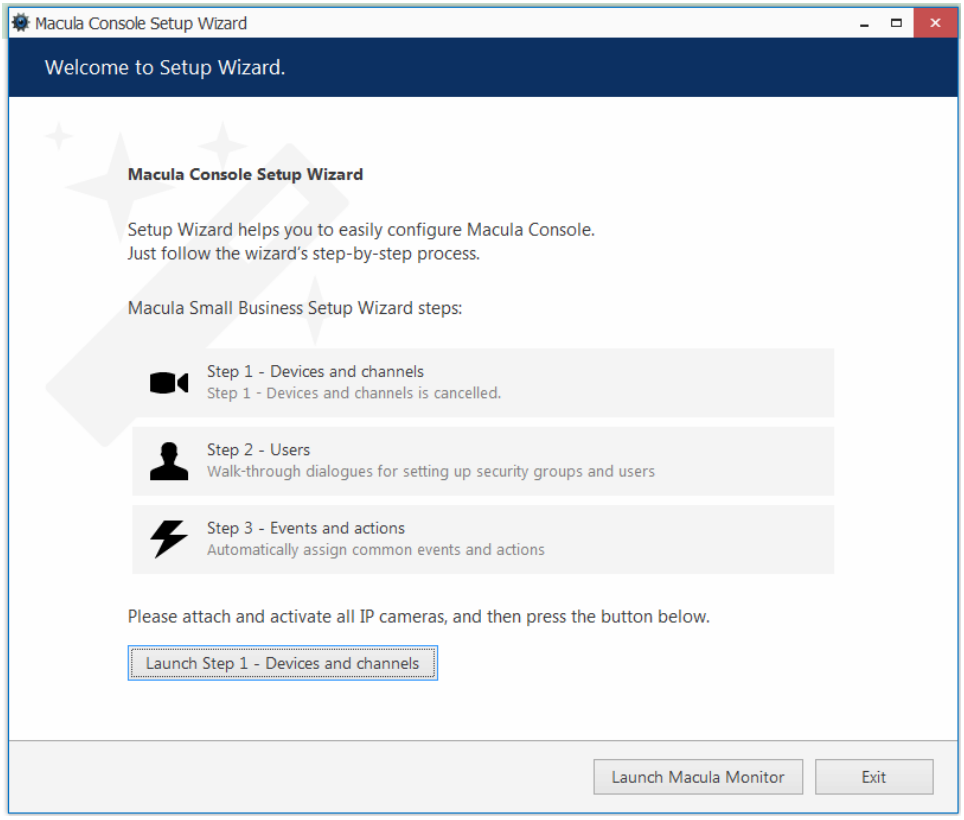
The Macula Console Setup Wizard is automatically started after product installation and activation is complete. You can skip the wizard at this point and launch it later anytime from the Macula Console upper-right-hand corner menu:

Setup Wizard will show you the process summary and guide you through the steps to configure the installation. To proceed with each next step, simply click the button below the step list; to exit the wizard prematurely, press either *Exit* or *Launch Macula Monitor* button in the bottom-left-hand corner.

Setup wizard for Macula consists of just one step that covers devices and channels; setup wizard for Macula Professional includes three steps, which are devices& channels, users and basic events & actions. Make sure you connect all devices (IP cameras and/or other video sources) before launching the wizard: it will automatically scan the network for available video sources.

Step 1: Devices and Channels

This step will allow you to automatically search and add cameras and other video source devices into your server configuration. Press the *Launch Step 1* button to begin.



Scan Parameters

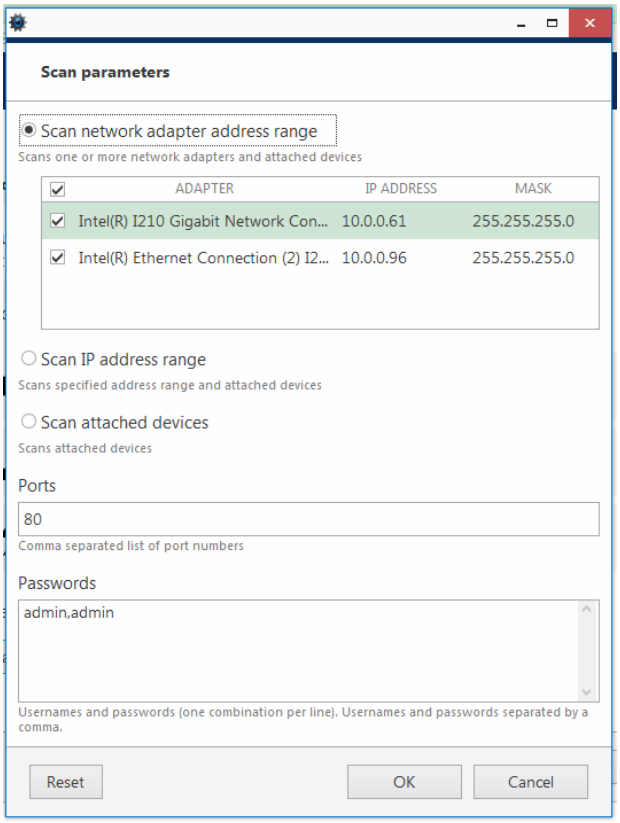
First, select scan mode; the following options are available:

- scan IP address range: specify a continuous LAN segment to be scanned
- scan network adapter address range: select one or more network interfaces to be fully scanned
- scan attached devices: the local hardware system will be scanned for capture boards and Direct Show video sources

If you have chosen to search for IP video sources, you should review additional connection settings and change or update them, if required:

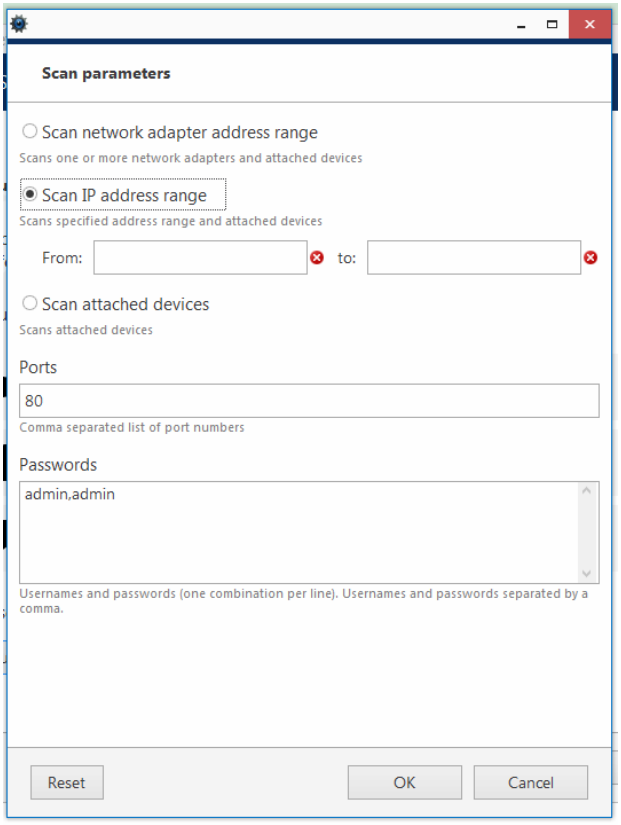
- ports: HTTP ports, comma separated
- user credentials: pairs of comma-separated user names and passwords, one pair per line

Use the *Reset* button below to discard all changes and start entering scan parameters again. When you are ready, press *OK* button below to begin scanning.

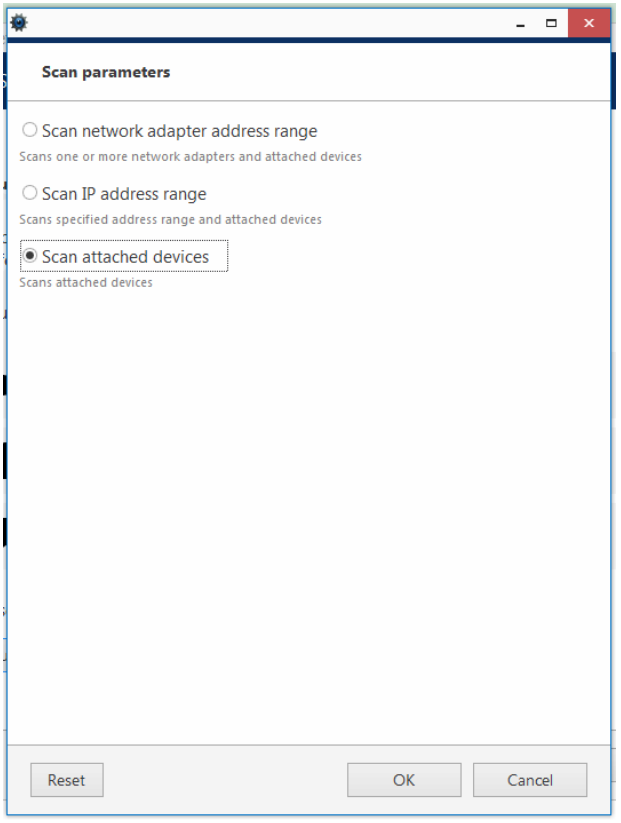


Scan network adapter address range

Macula® Professional Administration Guide



Scan IP address range



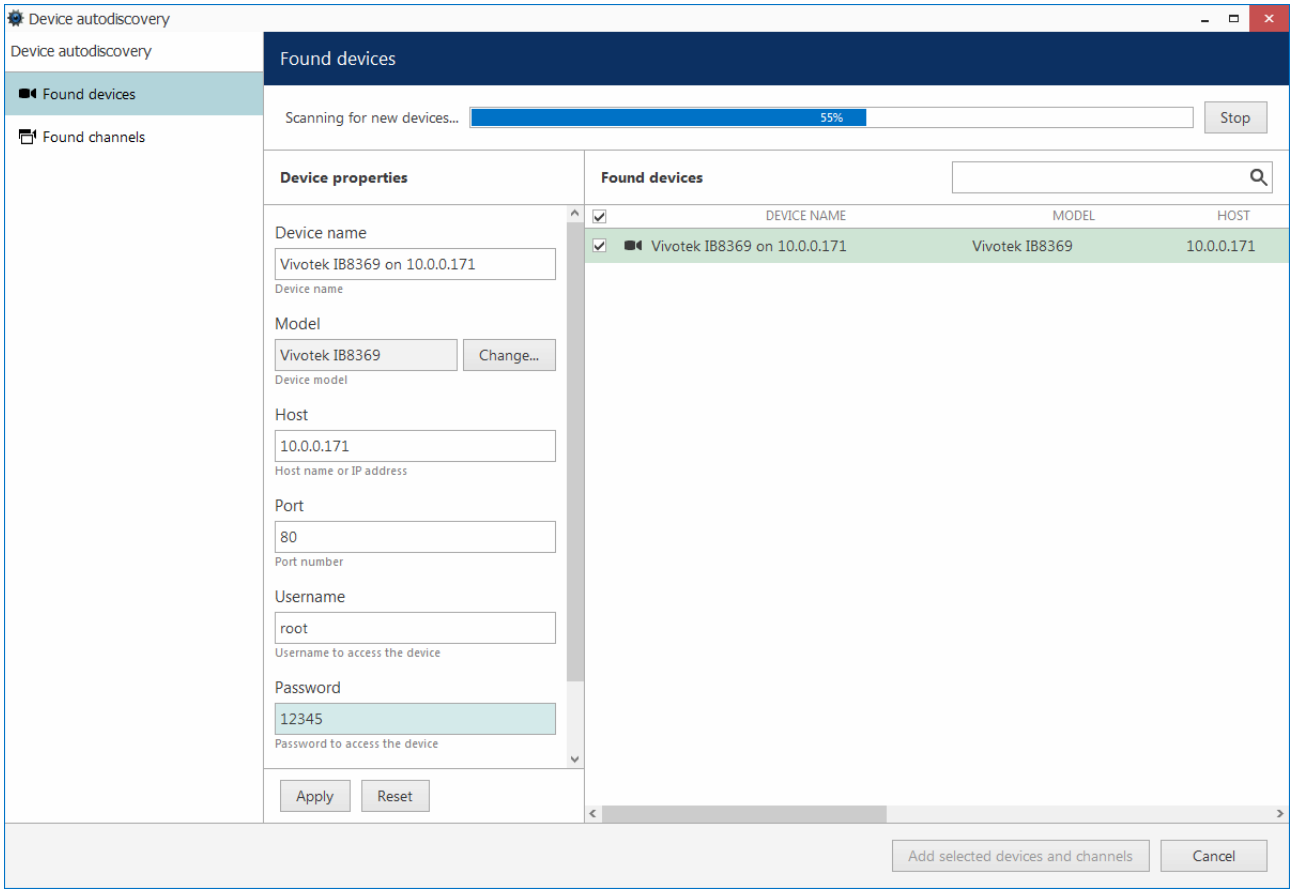
Scan attached devices

Device Autodiscovery

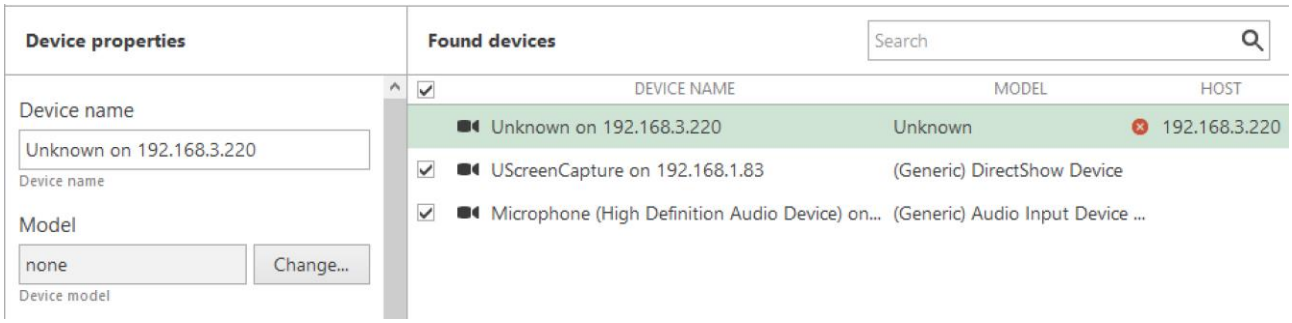
After scanning has been completed, you will be taken to the Device Autodiscovery dialog box, which will allow you to review the found devices and their channels, and enter/modify related settings. Use the *Search* field in the upper-right-hand corner to find a specific device by name, model, IP, port or hardware ID (for IP devices, ID includes MAC address).

> There are two types of selection in the item list: **checkboxes** and color highlight. Checkboxes are used to choose the items to be added to server configuration after you close the dialog box; **highlighted** items are subject to immediate properties changes. Use *CTRL+click* or *Shift+click* to select all or several items at once to change their settings.

Click a device in the item list to load its settings into the *Device Properties* window. Note that some settings may be missing for some of the automatically found devices; this depends mostly on device and whether user data was correctly provided. In such cases, simply fill in the missing data manually and click the *Apply* button below to save the configuration changes.



If device is not integrated with the software (native support), it may be detected as generic type (e.g., ONVIF). If you think some devices have not been discovered, check if they have different HTTP ports; also, try adding them manually.



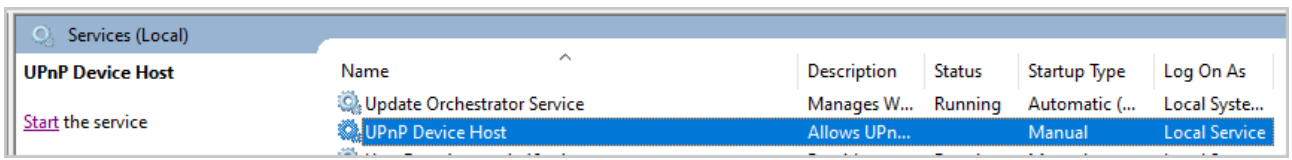
If the device cannot be matched with a model in the list and it also does not respond as generic ONVIF, it may be discovered as *Unknown*; in that case, try settings its model manually to the closest one (from the *Suggested models*), or try Generic RTSP and specify an RTSP URL in the channel settings. This may happen to devices that are not listed as an exact model and are also old enough not to support ONVIF Profile S.

Setting	Description	Default value
Device name	User-defined video source name	Autodetected model + IP, empty if not detected
Model	Device manufacturer and model, or generic type	Autodetected vendor and model, empty if not detected
Host	Device IP address	Autodetected
Port	Device HTTP port	Autodetected
Username	Device user credentials; note that you have to provide administrative profile credentials in order to be able to change device settings via software interface	Appropriate username from provided list or autodetected
Password	Device user password	Appropriate password from provided list or autodetected

Make sure you select all the devices you wish to add by putting a checkmark next to them. Devices with missing configuration (model and/or IP) are unchecked by default and will not be added to active server configuration.

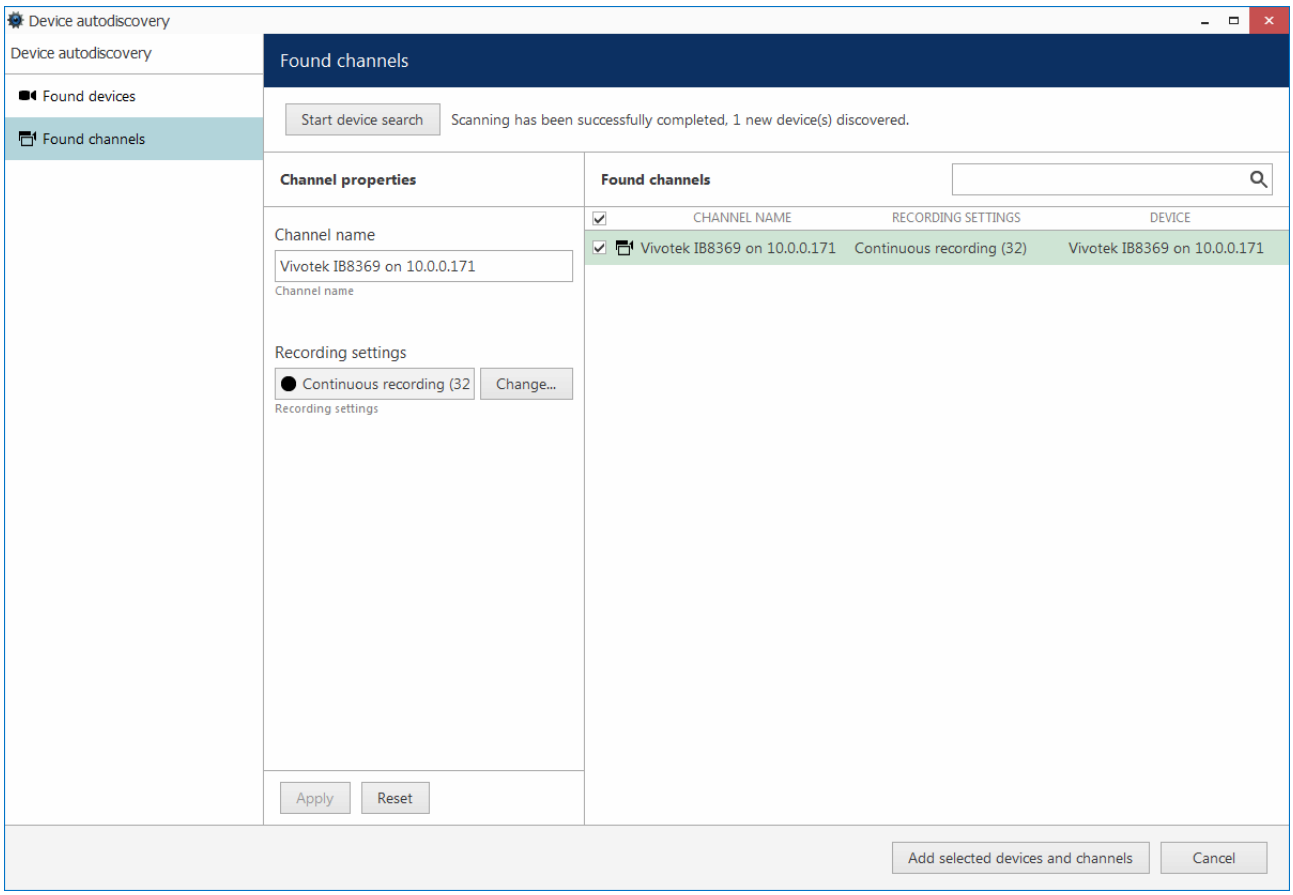
⚠ If the autodiscovery **does not find any cameras** or all of them are Generic ONVIF instead of proper models:

- check models
- check IPs and passwords and ports
- make sure that the UPnP Device Host service is functioning properly on your system.



Switch to *Channels* tab to review the detected video channels of the discovered devices: this is particularly important if you are using multichannel devices, e.g., capture boards and encoders. Use the *Search* field in the upper-right-hand corner to find specific channels by name or device name.

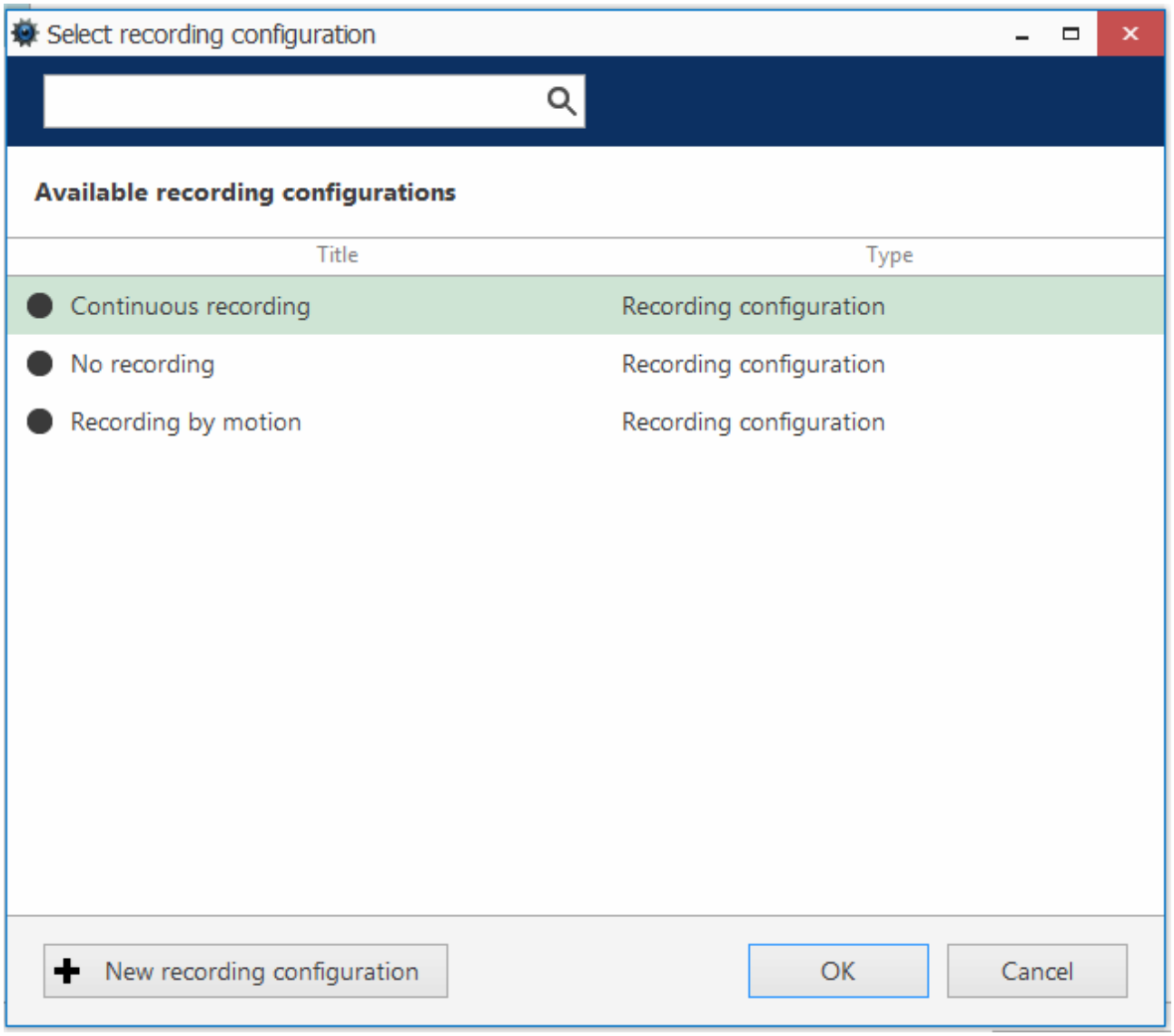
Macula® Professional Administration Guide



Here you can edit the channel name and assign recording configuration. By default, recording is enabled for all channels: click the *Change* button near *Recording settings* to manage recording profiles and assign them to your channels. To add a new recording profile, click the *+ New recording configuration* button below; you can find more details about recording profiles in the corresponding section. Click *OK* to save and return back to devices and channels; click *Apply* to save configuration changes.

⚠ After changing the channel recording configuration, do not forget to click *Apply*, otherwise the changes will not take effect.

💡 Recording configuration here is assigned to the main streams of the target channels. In order to set up substream recording, please go to channel configuration.



Click the *Start device search* button above at any time to restart device discovery.

> ⚠ All previously discovered devices and all configuration changes will be discarded if you restart camera autodiscovery.

When you have finished with configuration, click *Add selected devices and channels* to go back to the wizard.

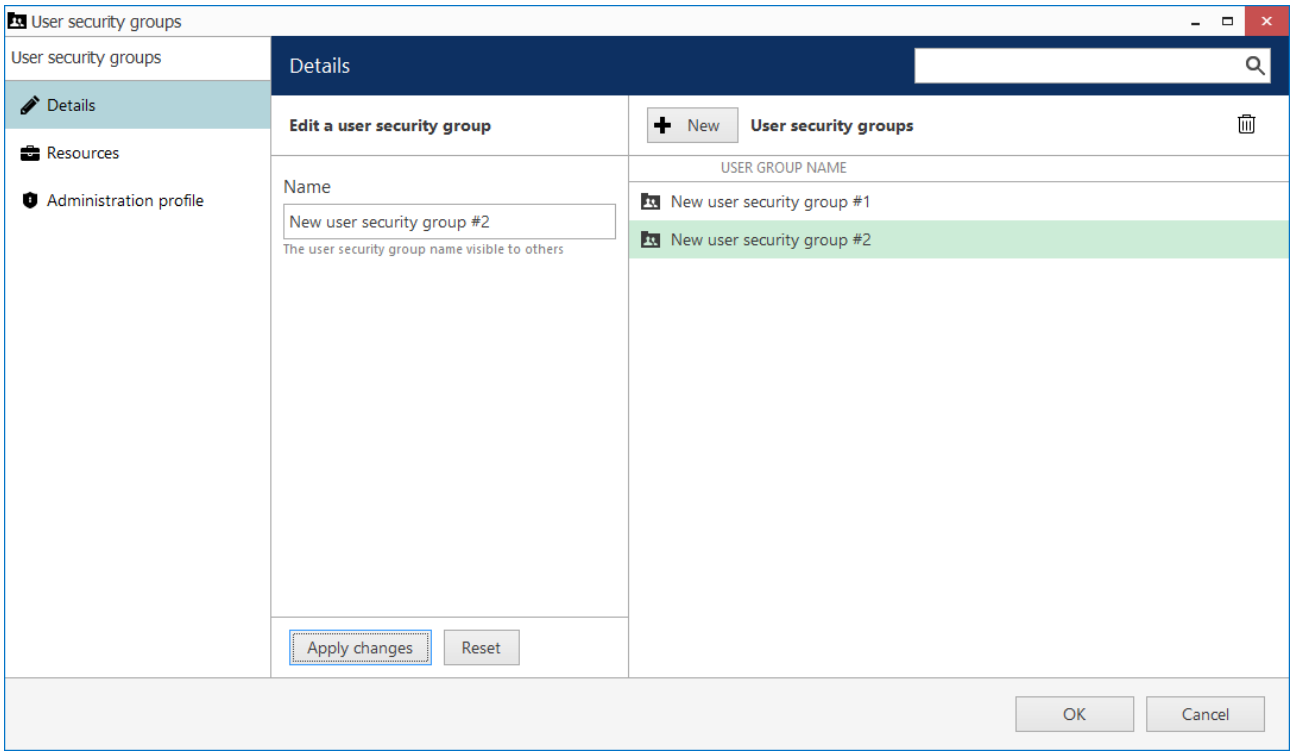
Step 2: Users and User Groups

Macula Professional users can press the Launch Step 2 button to proceed with *Users*. This step will allow you to add users and user groups and give them permissions for the devices and channels added earlier.

> 💡 The built-in Administrator user account and built-in Administrators group are root users with access to absolutely all the available resources. As a result, resources choice is unavailable for the Administrators group, and it is also impossible to add Administrator user to any other group.
> Any users added as members to the built-in Administrators group will have the same full authority as root users.

User Groups

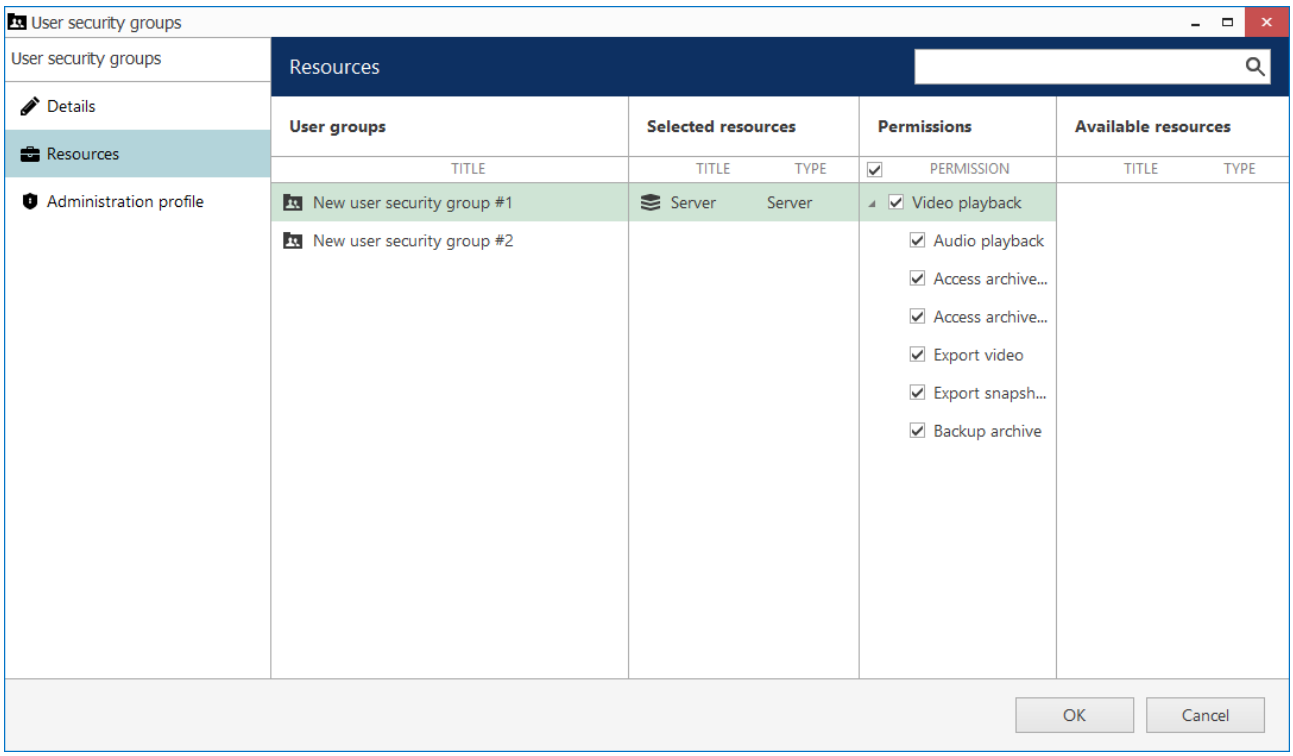
First, decide whether you want to create user groups or work with a non-systemized array of user accounts. For large systems with complex user structure, groups are strongly recommended for reasons of improved manageability. Choose *No* to proceed with plain user management at once; otherwise, you will be offered the chance to create user groups and distribute existing resources between them. Note that the Setup Wizard interface offers simplified settings for user groups at this point; later, you will be able to create nested groups via the corresponding Macula Console section.



Enter a name for the first user group and then click the *Create* button below: newly created group will appear in the item list on the right. By default, the last modified group stays opened for changes. Correct group name, if necessary and then click *Apply changes*, or click *Reset* to discard the latest changes and revert to the most recently saved state (the same thing will happen if you select a different item for editing).

To create more groups, click the + *New* button on the upper panel and proceed in the same way as on the first iteration. Use the Recycle bin icon button recycle bin icon to delete selected group(s) (hold CTRL or Shift to select multiple items).

Switch to the *Resources* tab to assign the permissions for this user group. Available resources at this point include servers, devices and channels.



Choose the group name in the first column to manage its resources. To add a resource, pick at least one permission for it and it will be automatically moved to the *Selected resources* list. To remove a resource, uncheck all its permissions - either manually or using the *Clear* button below. Note that double-clicking resources does not work here as one or multiple different permissions must be specified.

When you have finished, click *OK* to proceed with user accounts.

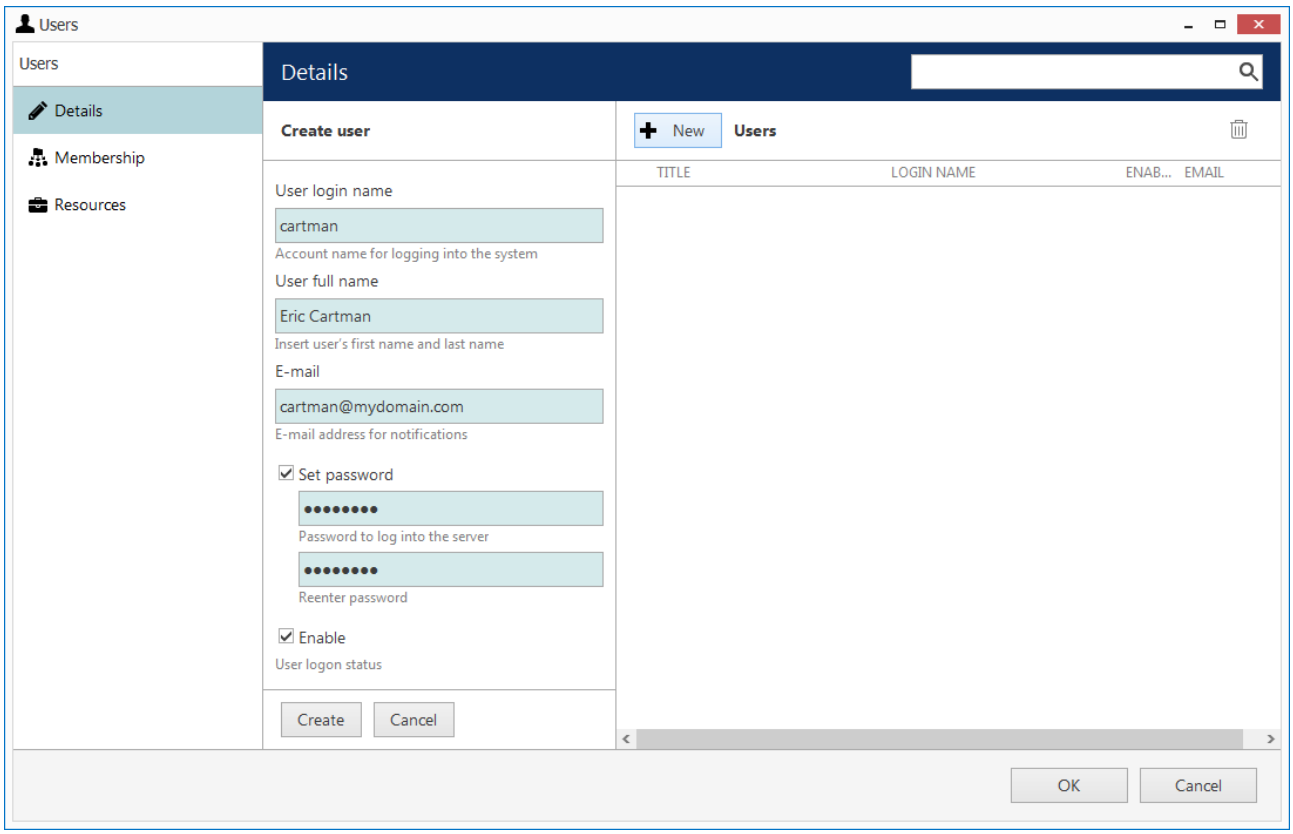
Users

To create the first user, simply fill in their details and then click *Create* below. By default, the most recently modified user will stay open for changes; correct user details, if necessary and then click *Apply changes*, or click *Reset* to discard the most recent changes and revert to the latest saved state (the same thing will happen if you select a different item for editing). Note that you do not have to re-enter the password when editing - only activate *Set password* if you wish to re-define it.

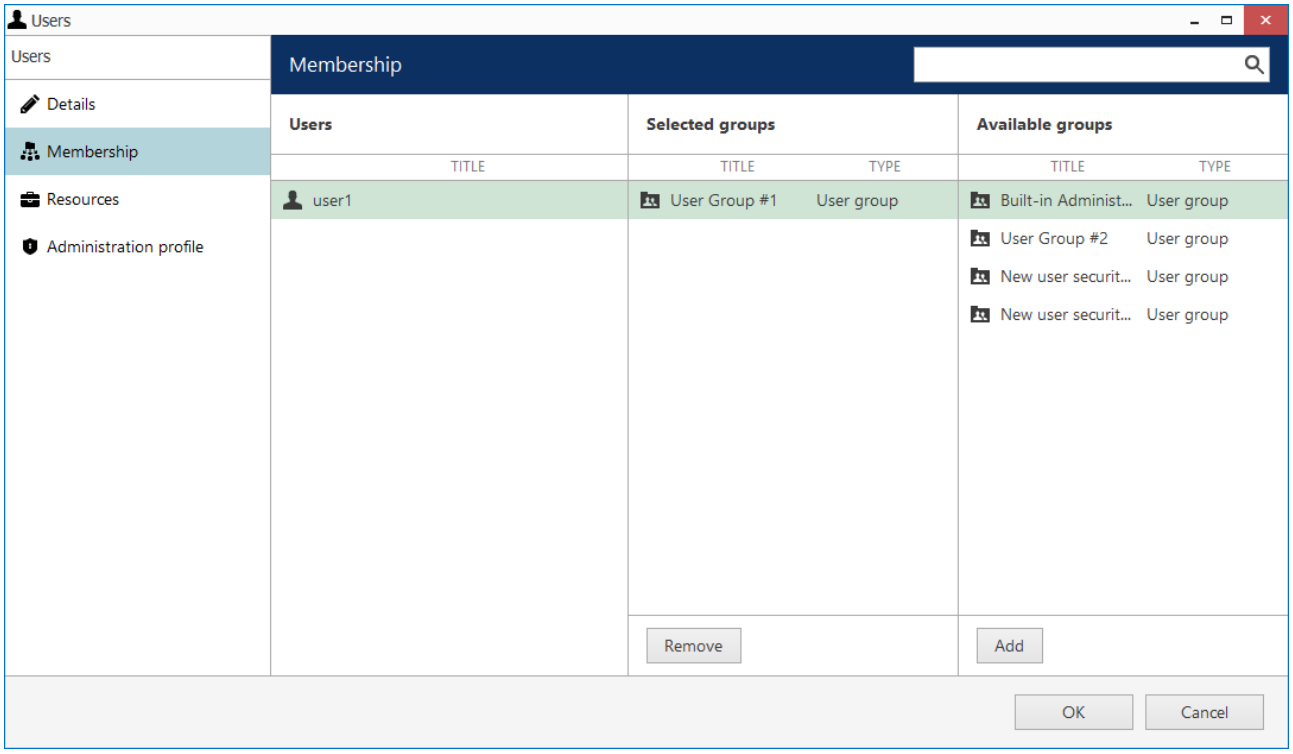
To add more users, press the + *New button* on the upper panel and proceed in the same way as described previously. Use the Recycle bin icon button recycle bin icon to delete selected user(s) (hold CTRL or Shift to select multiple items).

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



On the *Details* tab, the following user properties are available (all fields are required): login, full user name, email address, password and status. Passwords must be entered twice - this is a security precaution to avoid typos. Every user is enabled by default meaning that the target account is active and can be used for server logon; disable user accounts you wish to suspend while keeping all user-related information and resource permissions.



On the *Membership* tab, select groups for the specified users to become members of: move groups by double-clicking them or by using the *Add/Remove* buttons below.

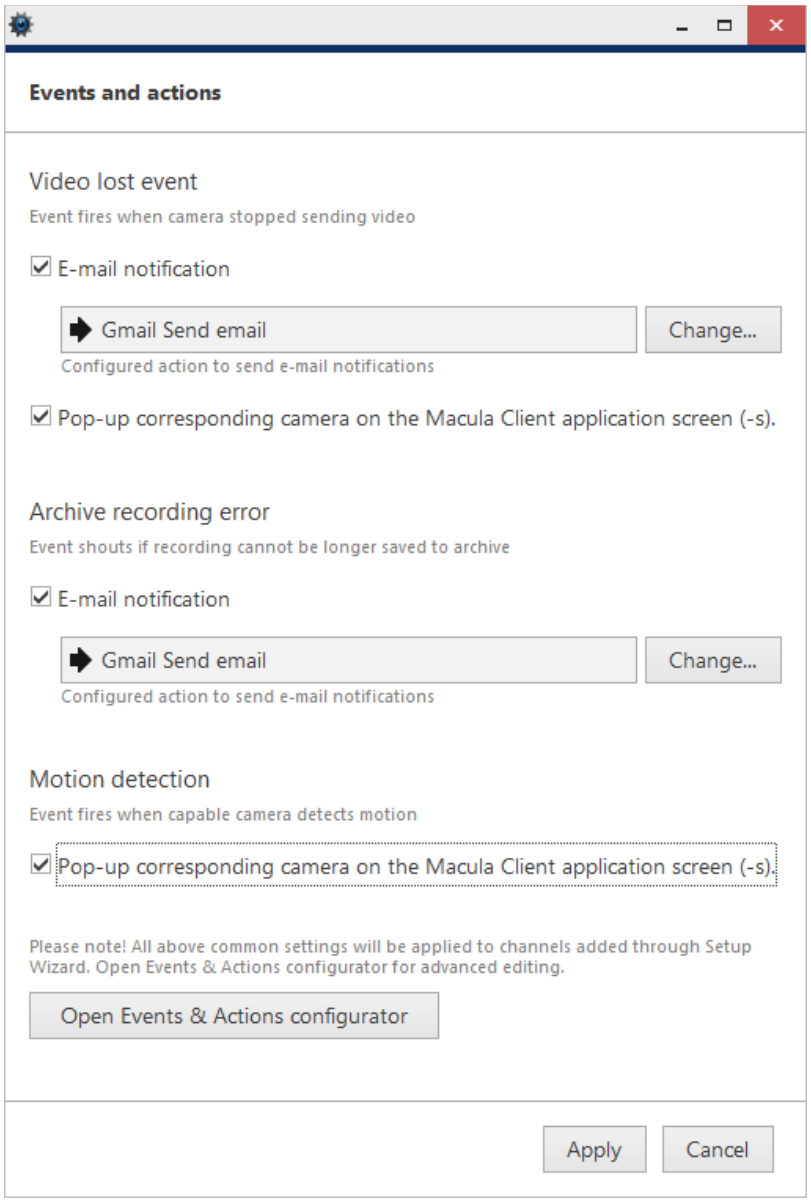
Switch to the *Resources* tab to add individual resource permissions. This can be used both for group members and for users not belonging to any of the groups; individual permissions will not be removed if the user is excluded from the group.

To add a resource, pick at least one permission for it and it will then automatically be moved to the *Selected* resources list. To remove a resource, uncheck all its permissions - either manually or using the *Clear* button below. Note that double-clicking resources does not work here as one or multiple different permissions must be specified.

When you have finished, click *OK* to save and go back to the main wizard window.

Step 3: Events and Actions

On the last step, basic alarm and action management is introduced. Press the *Launch* Step 3 button to open the dialog box.



Note that all the settings here apply solely to the channels discovered on the previous step; if you have configured other devices prior to launching this wizard, they will **not** receive the current event & action

settings - launch the *Event & Action Configurator* to set up rules for other devices. You can also use *E&A Configurator* if you wish to add other (advanced) types of alarms and/or actions.

When you are finished with all steps, you have the following options:

- **Restart wizard**: start the wizard again to set up more resources
- **Launch Macula Monitor**: open Macula Monitor application (will close the wizard)
- **Done**: close the wizard and proceed to Macula Console

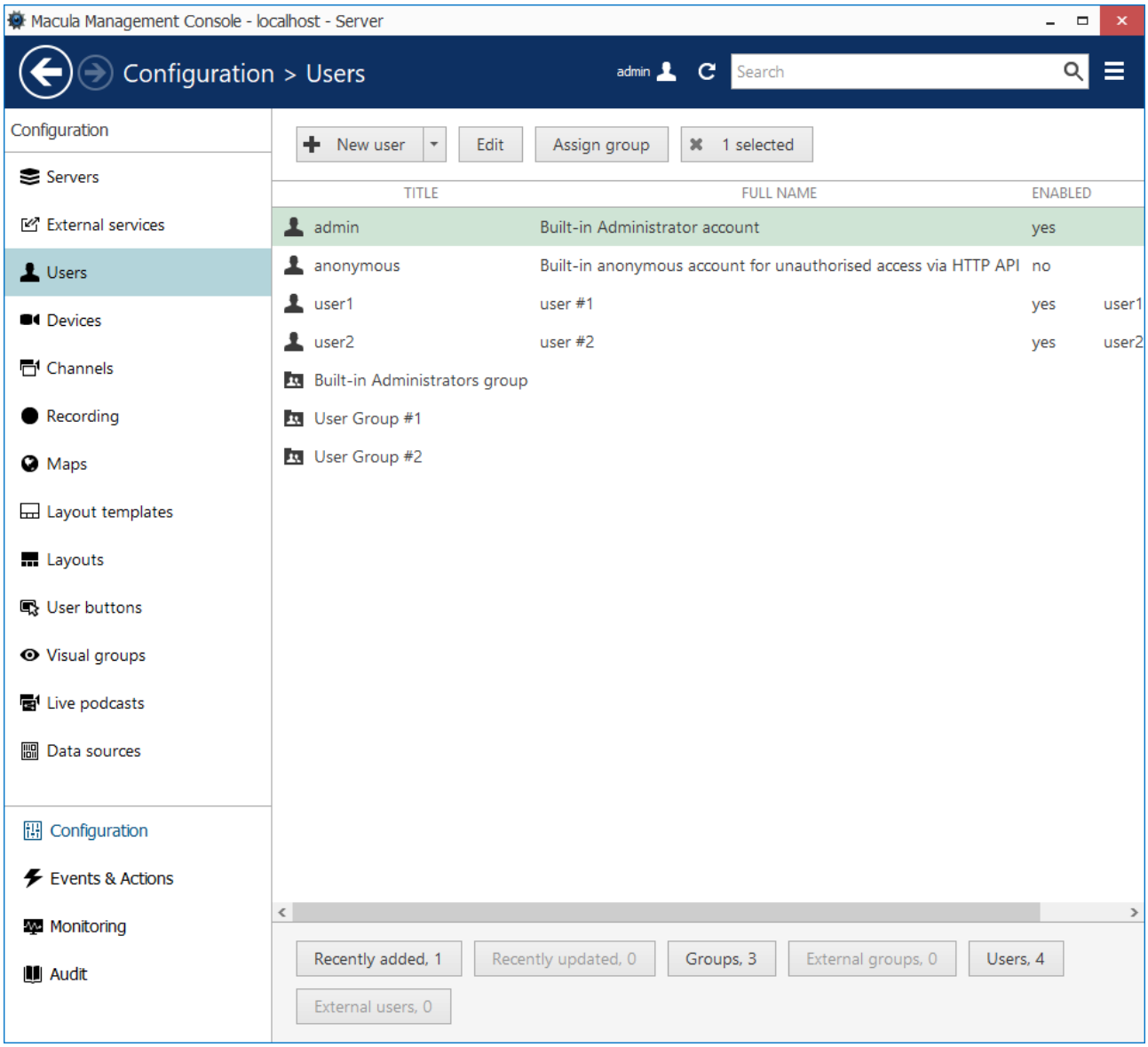
You can run this Setup Wizard again at any time via your Macula Console application menu in the upper right corner.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

3.5 Interface Overview: Management Application

Macula Console is a straightforward graphics user interface tool with access to all possible server settings. To ensure comfortable and easy navigation, it is important that you become acquainted with its structure before starting to use it.

Note that Macula Console appearance slightly depends on your software package and license limitations. Nevertheless, its logic always remains the same. Those sections, which are unavailable due to license restrictions, will be grayed out but still listed to get you acquainted with all available features. You can hide those features via Macula Console settings or upgrade your Macula server to a superior version.



Navigation Panel

The blue panel on top serves as navigation bar and its usage is similar to that of Windows Explorer. Here are its main components (from left to right):

- *Left* and *Right* arrows enable navigation through your browsing history and allow you to switch between previous and next locations; you can also use Backspace on your keyboard to go back
- Your current location is displayed right next to these arrows
- If you are in the Organizations view, an *Exit* button will appear
- Currently logged in User account button with options to view user profile, switch servers*, or to log out
- *Refresh* button - reloads current item list
- *Search* field - only items matching the search criteria will be displayed in the list

*The option to switch servers is hidden by default and can be enabled via application menu.

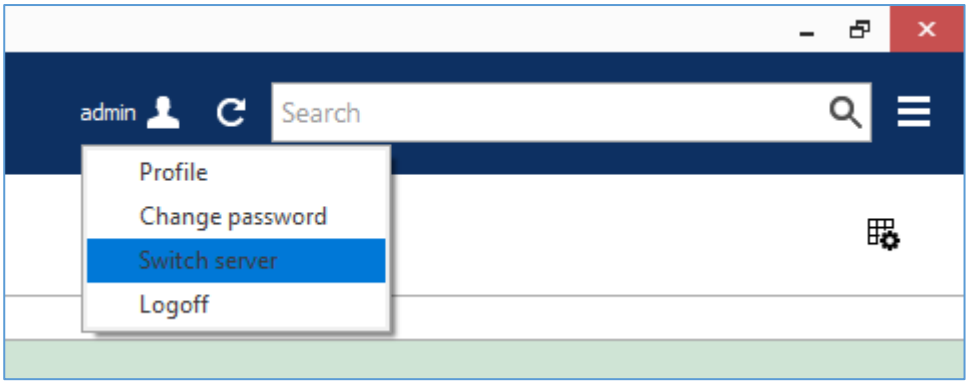
Application Menu

- Application menu button in the upper-right-hand corner gives you the following launches the options:
- launch the Setup Wizard
- import the configuration from an XML file
- import the configuration from another GSF Macula server database
- change Macula Console settings
- enable cybersecurity checks
- set up automatic configuration backup
- remotely upgrade system components
- open the software documentation
- open the About section

User Menu

This menu offers the following options:

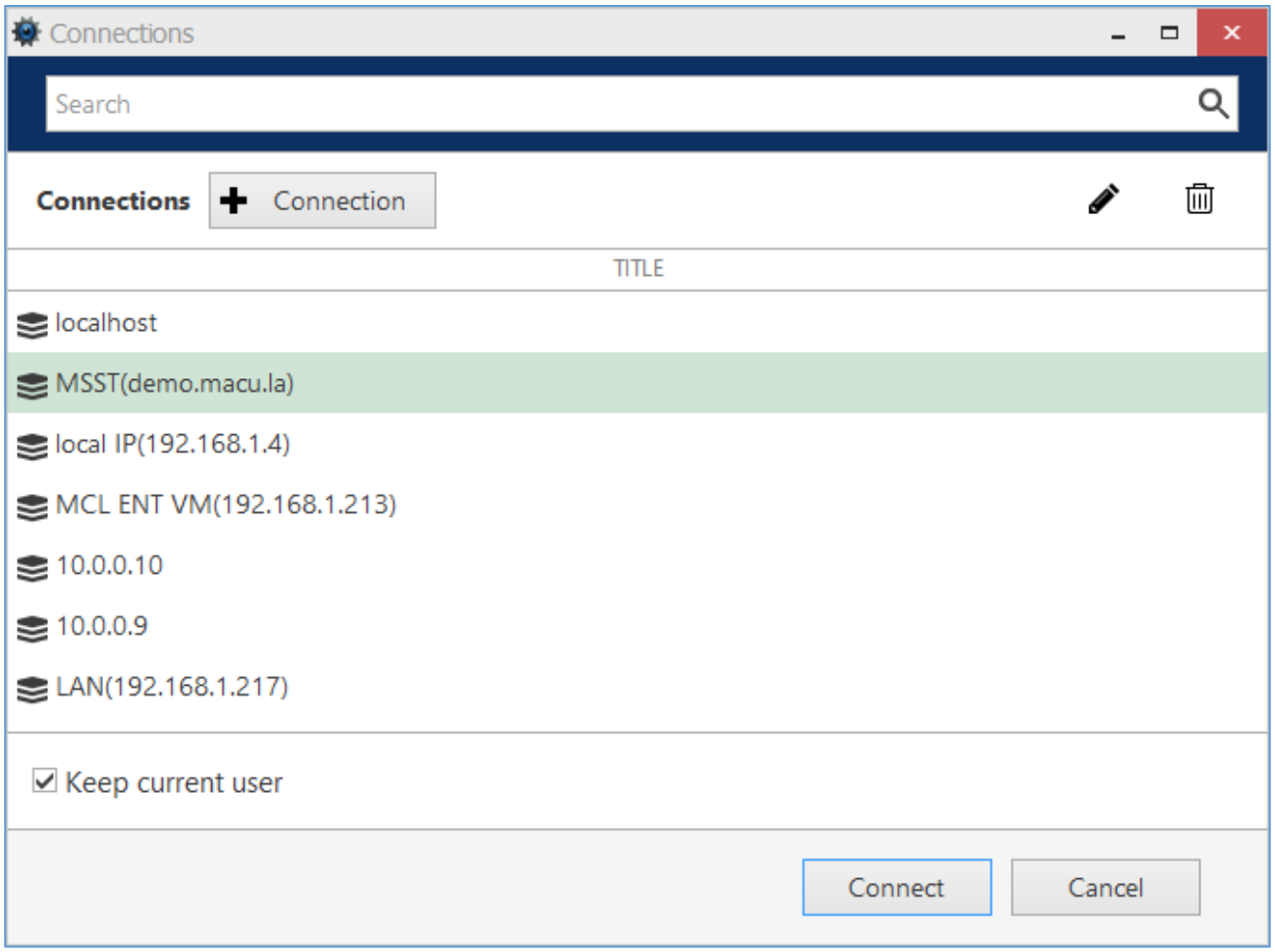
- View current user profile and adjust their settings, if necessary
- Quickly change the password for the current user (will not open the user profile dialog)
- Switch server: if enabled in the application menu, this option allows quick switching between different servers with the same user account
- Log off and return to the initial Macula Console login interface



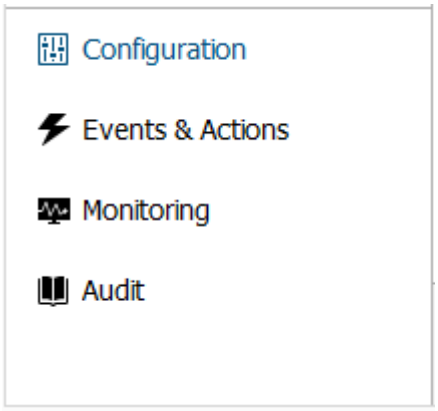
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

The **server switching** option allows you to pre-configure a list of servers and then switch between them with a single click. This feature is useful for engineers who maintain multiple locations/customers, and for Macula Enterprise system engineers to quickly switch between Macula Enterprise and servers.



Sections



The bottom left panel allows you to switch between the four main Macula Console sections: Configuration, Events & Actions, Monitoring and Audit. The contents of the components panel on the left will change depending on the selected section. If the Macula Console windows is resized, the sections will be reduced to icons.

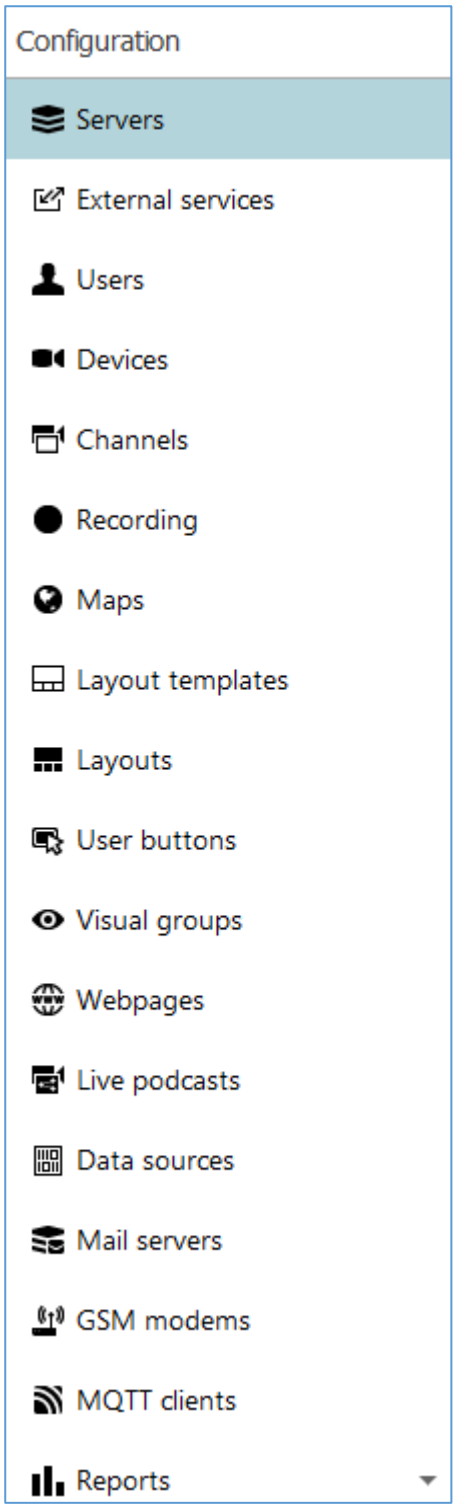
Components

The panel on the left will display the list of all available configuration components based on the selected section. As a result of license limitations, some of the items may be grayed out or unavailable. The list below shows maximum available items by category:

- **Configuration:** setup for the server components
  - Servers, Networks, External services, Failover clusters, Users, Devices, Channels, Recording, Maps, Layout templates, Layouts, Video walls, User buttons, Visual groups, Webpages, Live podcasts, Data sources, Data channels, Mail servers, GSM modems, MQTT clients, Reports, Access control, Quick access, Schedules, Organizations
- **Events & Actions:** configuration of automated scenarios
  - Rules, Events, Actions, Global events, Conditions, Counters, OPC, Indicators, Variables, Tags, Subjects
- **Monitoring:** live component status
  - Servers, Devices, Channels, Streams, Archive statistics, Storages, User sessions, Video walls, External services, Reports, Access control, OPC, Indicators
- **Audit:** log of server events and user actions
  - Servers, Users, and Problems

This document further describes the purpose and usage of each category in details.

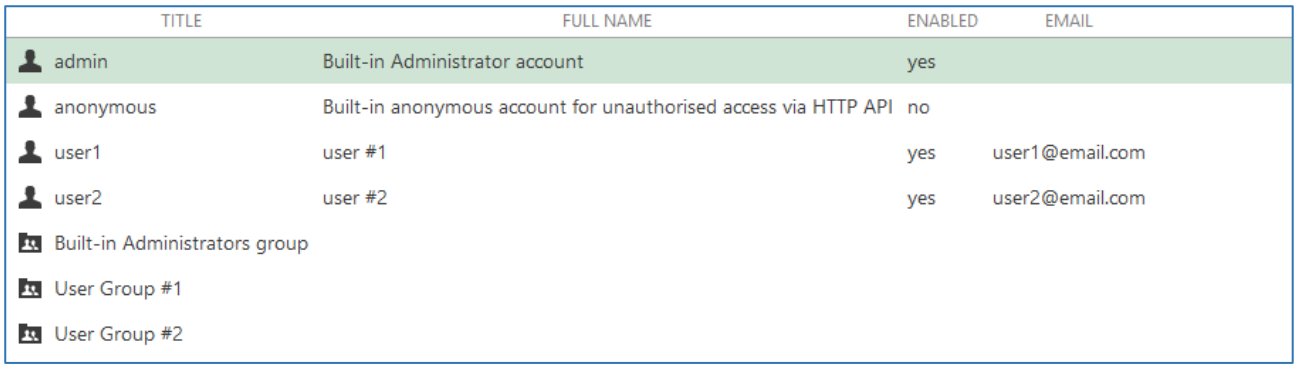
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



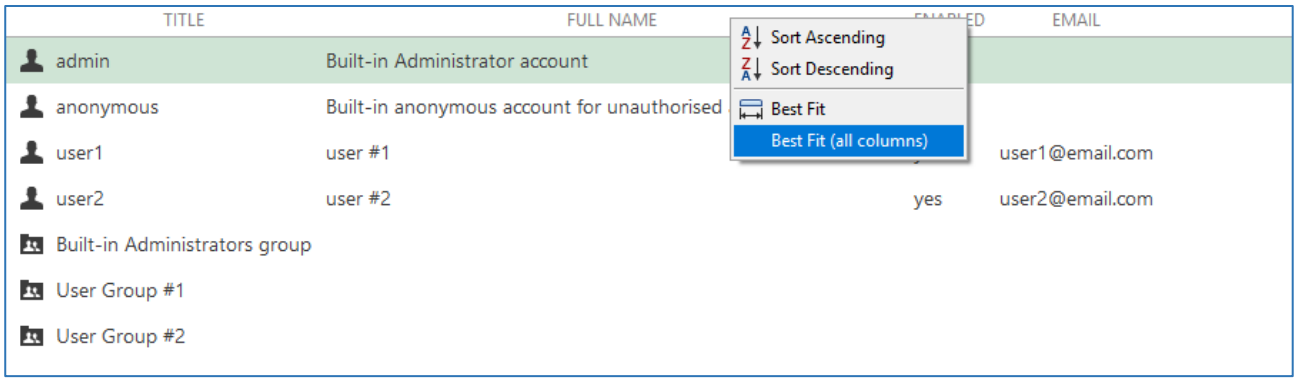
Item List

The main part of the Macula Console window displays items in the selected category depending on the search and/or item filters. You can select one or more items at once using the *Shift* or *CTRL* button.

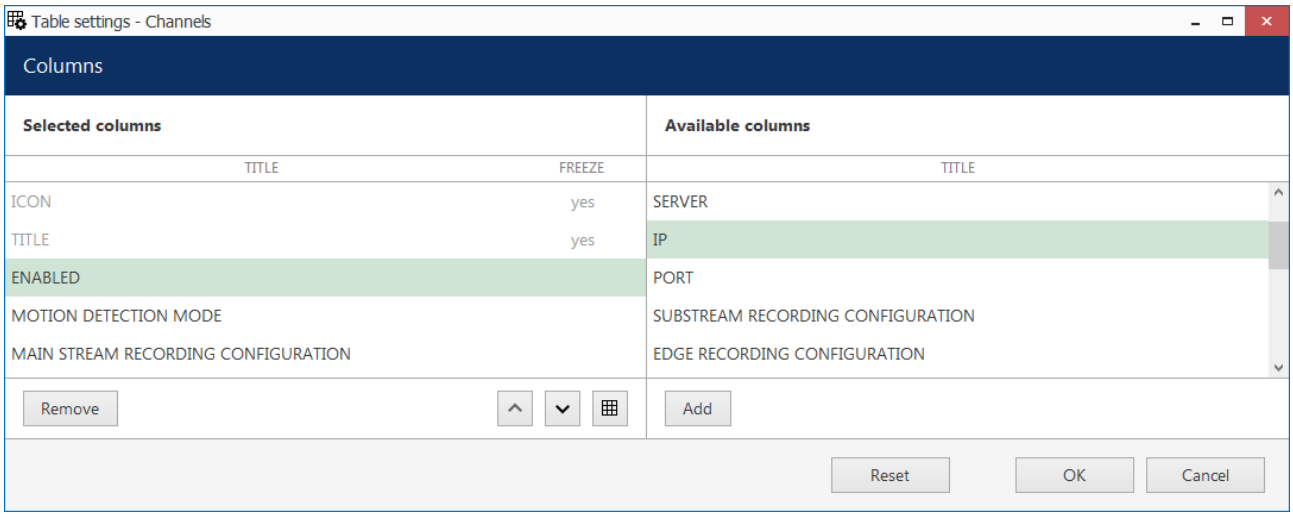
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Click any column title to use is as a sorting basis for the whole item list; the little arrow near the column title indicates that it is currently being used for arrangement - either ▲ ascending or ▼ descending. Right-click item list header for sorting options and column fit settings. The Best fit option will assign automatic size to all columns based on their name width. You can change column **width** simply by dragging their boundaries in the header row: these adjustments will be remembered and restored after you go to other sections, or close and re-open the Macula Console application.



For each category, it is possible to **define the set of columns** to be displayed, and **freeze** one or several leftmost columns for convenient horizontal scrolling. To do this, click the grid icon in the upper right corner just below the application menu (the rightmost button in the upper panel). An additional window will pop up, allowing you to define the column layout.



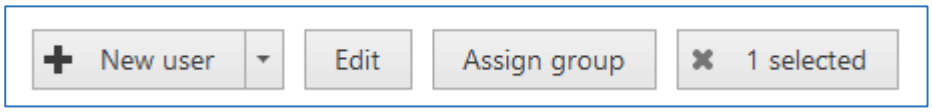
One the left, you will see the currently displayed details. On the right, there will be all available columns.

- Use the *Add* and *Remove* buttons, or simply **double-click** items to move them from left to right and vice versa to select and deselect them.

- Use the *Up* and *Down* arrows to sort your selected columns on the left side.
- The grid button next to these arrows allows you to **freeze/unfreeze** the leftmost columns (i.e., those on top of the list). These will stick to the left window side as you scroll the table horizontally. You can freeze as many columns as you like, but only the ones on the far left side. For the columns in the middle of the list, this button will be grayed out (inactive).
- To discard all changes and **restore** the default (application original) list of columns, click the Reset button.

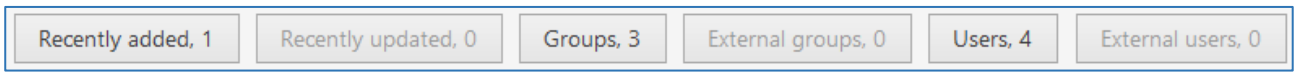
When done adjusting the table layout, click *OK*. Your new column configuration will appear: adjust the width of the newly appeared details, as desired.

Item Actions



The panel above the item list displays the available actions, if applicable. Usually, the buttons here will allow you to create a new item, edit or delete existing ones, create or edit contiguous items, etc.

Item Filters



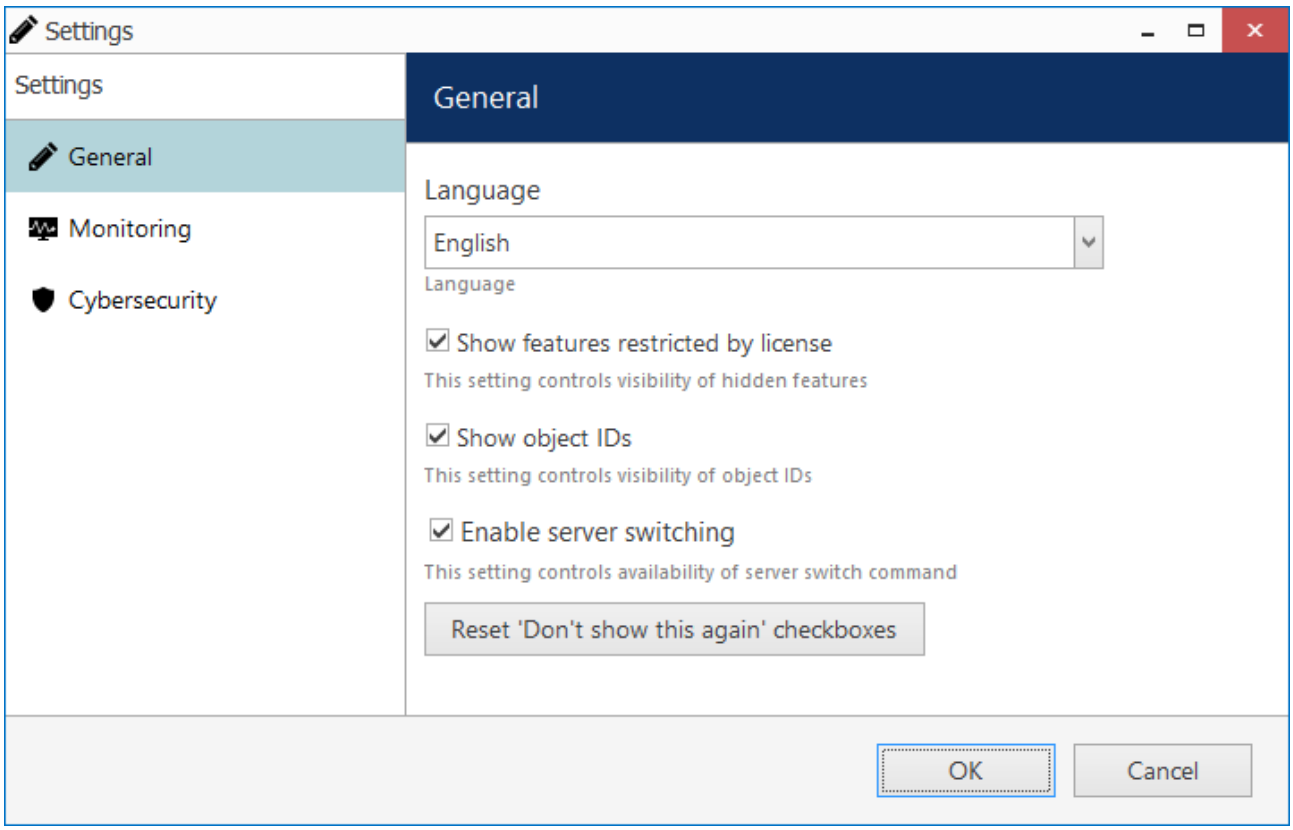
The bottom panel contains miscellaneous item filters, such as: recently added and updated, corresponding groups etc. Click any of the filters to apply them; use the *X* button to reset and display the full item list.

Application Settings

To change Macula Console application settings, go to the main application menu in the upper-right-hand corner and choose *Settings*. The preferences here only affect the current Macula Console instance, no matter to which server it connects. The interface language setting also affects the Macula Monitor application installed on the same machine.

For your convenience, the settings have been grouped into several tabs.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Here, it is possible to:

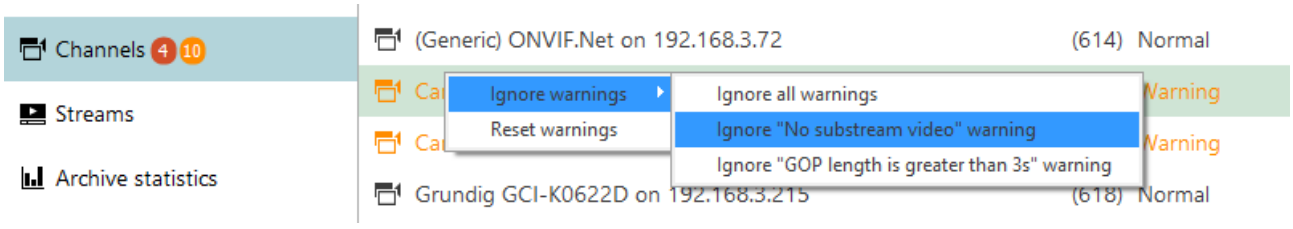
- change application **language** (by default, the language chosen during installation is used)
- show or hide software features restricted by license
- show or hide **object identifiers** (internal object IDs mostly necessary for addressing GSF Macula entities via HTTP API)
- show or hide Organizations
- enable quick server switching
- reset all *Don't show this again* checkboxes, which have been set so far

Monitoring

This section contains settings related to the *Monitoring* section of Macula Console, namely:

- auto refresh interval in seconds for the *Monitoring* section dashboards (set 0 to disable autorefresh)
- show or hide monitoring warnings (critical errors will always be showed, only warning level info can be turned off)
- reset monitoring section warnings, which have been cancelled (set to be ignored) so far

See the Monitoring section documentation for more information about warnings.



Cybersecurity

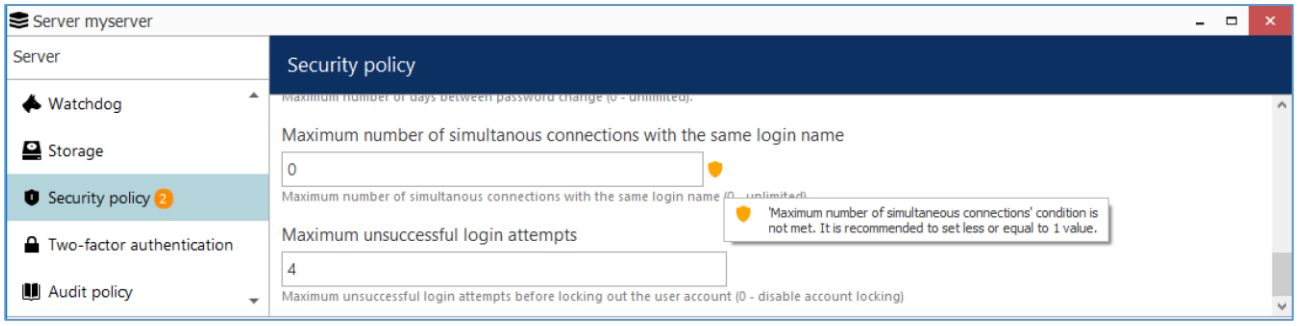
The following setting is related to cybersecurity:

- show cybersecurity warnings

Cybersecurity warnings are different from those in the *Monitoring* section. Security warnings are displayed as shields in the server and channel settings, indicating that the related setting does not match the defined security level. See below for more information about warnings.

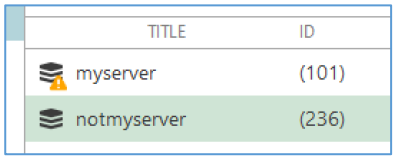
Errors and Warnings

The Macula Console application will sometimes warn you about certain misconfigurations. For example, when the entered setting value is out of range, invalid, or incoherent with the system settings in some way, you will see a corresponding **mark** next to the preference.



The following marks are used:

- **security** shield indicates that the setting value does not meet the current cybersecurity level preference
- number of issues shows how many **warnings** (orange) or **errors** (red) are in the current category
- an X icon is used to mark a completely invalid value (e.g., the field cannot be empty)
- other kinds of red or orange marks on top of the item icons, or text color



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

3.6 Conventions and Keyboard Shortcuts

Mouse Gestures

Double-click an item containing more entities (e.g., any group): opens item contents in the same window

Double-click a **non-expandable** item (e.g., server, user): opens entity configuration dialog box

CTRL+click or **Shift+click**: select multiple items in a list

Right-click on a text field: standard text edit menu

Right-click on a text field when creating an action: standard text edit plus text macros

Keyboard Shortcuts

Backspace: browse one step back in Macula Console

Alt+F4: close Macula Console

CTRL+A: select all items

Visual Elements

General

New item (click drop-down arrow to see available options)

Remove item(s)

Deselect item(s)

Unacceptable filed value, hover mouse cursor for more information

More information about the item, click to view the details

Refresh item list

Search

Macula Console sections

Configuration

Events & Actions

Health monitoring

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Audit log

Management

Network (server connection), connection settings

Server

Server group

External service

External service group

Failover cluster

Software Watchdog

Storage

Resources (all or any type)

User account/session

User group

General details

Members of the current item

Current item membership in other groups

User and user group permissions for target item

Device

Device group

Channel

Channel group

Recording profile (core recording settings)

Recording schedule (recording itinerary based on core recording settings)

Recording configuration (recording interface assignable to channels)

Motion detector

Layout Template

Layout

Layout group

Map

Video wall

User button

Visual group

Shared channel

Audit Journal (software log)

Set (period etc.)

Event & Action schedules

Events & Actions

Rules

Events

Actions

Global events

Conditions

Mail servers

Action delay timers

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

4 Server Settings

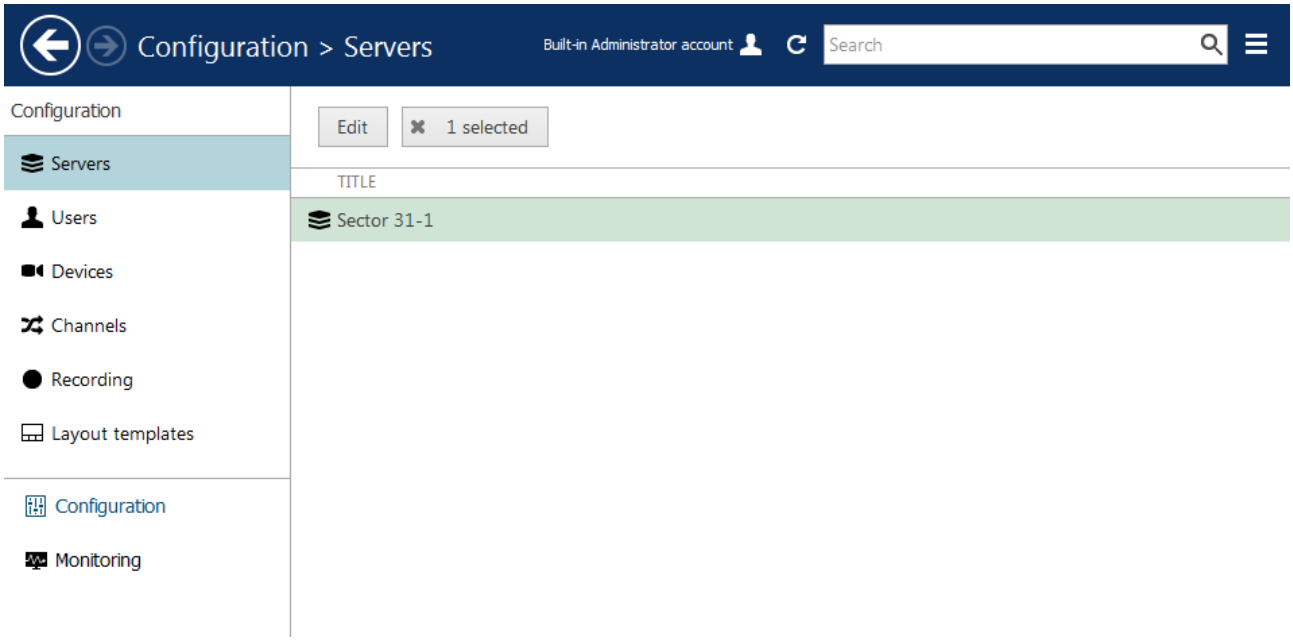
All the changes in the server configuration are done via Macula Console application. The settings are immediately saved and stored in an **encrypted internal database**, which guarantees that your server configuration cannot be accessed without entering a valid username and password.

> ⚠ Server database encryption is automatic, meaning that you do not need to enabled it explicitly, and is available starting from the software version 1.8.0.

This topic describes available server settings.

General

In order to access Macula Professional server settings via Macula Console, select Configuration section and then choose Servers components from the menu on the left.

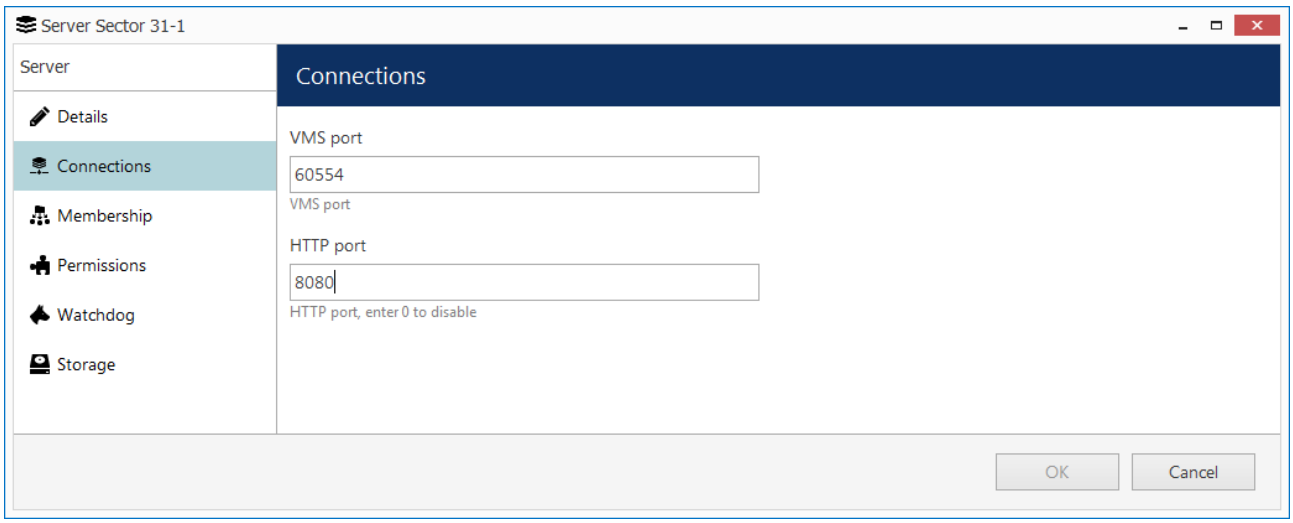


Double-click server or click the *Edit* button on the upper panel to access server configuration dialog box.

Details

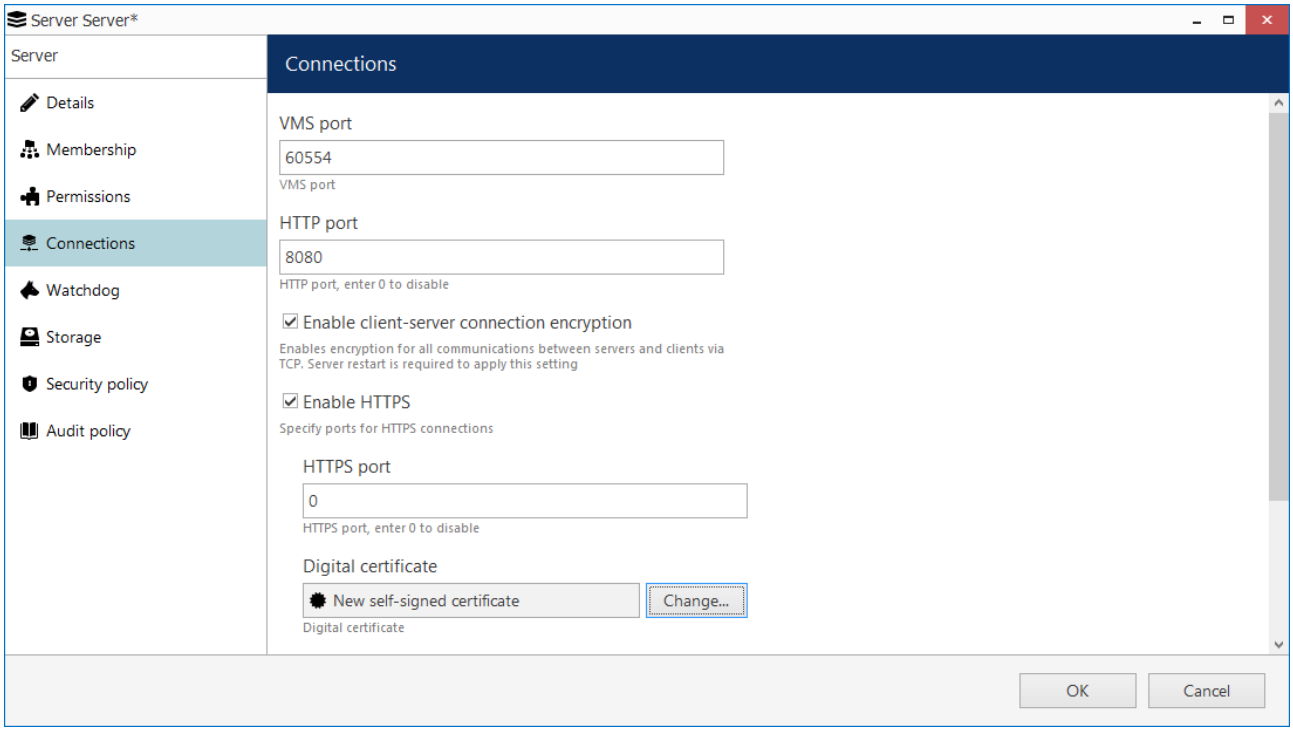
On the *Details* tab, you can change the server **name**: it will appear everywhere in Macula Console and in the connected Macula Monitor applications, including Web clients.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Connections

The *Connections* tab allows you to define **ports** for Macula Monitor and Macula Streaming Server connection; the default ports are **60554** for Macula Monitor and **8080** for Macula Streaming Server (HTTP). Note that, in case you plan to access your Macula server from the Internet, the ports must be properly forwarded on your router according to your desired topology and allowed through the firewall. Details on the port forwarding setup can be found in your router operation guide.



Here, you can **enable encryption** for client-server connections and also for HTTP connections (by default, it is disabled).

Server-client encryption setting affects all TCP traffic, i.e.:

- Macula Console connections to the Macula server
- Macula Monitor connections to the server

When you change the server-client encryption setting, all currently connected clients - both Macula Console and Macula Monitor applications - will be disconnected so that the encryption settings can be applied correctly. They will re-connect back shortly provided that they support encryption, too - make sure to upgrade them so that their version matches server version.

> ⚠ Connection encryption is supported starting from software version **1.8.0**. If your system has remote Macula Console and/or Macula Monitor applications of older versions, these will be **unable to connect** to a server that has encryption enabled; therefore, first make sure to **upgrade all the clients** and only then enable encryption on the server side.

To enable **HTTPS** (HTTP over TLS), mark the corresponding setting and then:

- specify HTTPS port (different from HTTP)
- add a digital certificate

You can either use your own valid **digital certificate** or generate one right in the software. In the latter case, the certificate will be self-signed and you will need to add it as trusted when connecting from the mobile app and from your Web browser(s).

> ⚠ If you are using your own CA certificates, create a .pem file with your certificate chain as described here: https://www.digicert.com/ssl-support/pem-ssl-creation.htm
>
> This is necessary for the certificate to be recognized correctly by all HTTP clients - Web browsers and Macula mobile applications. If you simply apply your CA certificate in Macula Console, there is a chance it is not recognized because some applications require the entire certificate chain.
>
> Then, apply the .pem file as the certificate together with your key when the importing certificate into Macula Console.

Also, if you are going to use SNMP traps in your Event & Action scenarios, here you can define server's **SNMP community** name and **SNMP port** for incoming and outgoing messages. Community will be used by the SNMP manager to send requests; SNMP port will serve for both incoming and outgoing messages (supported incoming messages are third-party SNMP manager requests, **not** external SNMP traps!). Leave both values zeroed to disable this functionality.

4.1 Watchdog

General

Server Watchdog is an integral part of the server core. It protects the software from certain types of failures by automatically attempting to restart the server.

Watchdog operates based on the software and system overall health monitoring; default trigger values have been selected on the grounds of our analysis of extensive tests run on systems of different configuration and stability level.

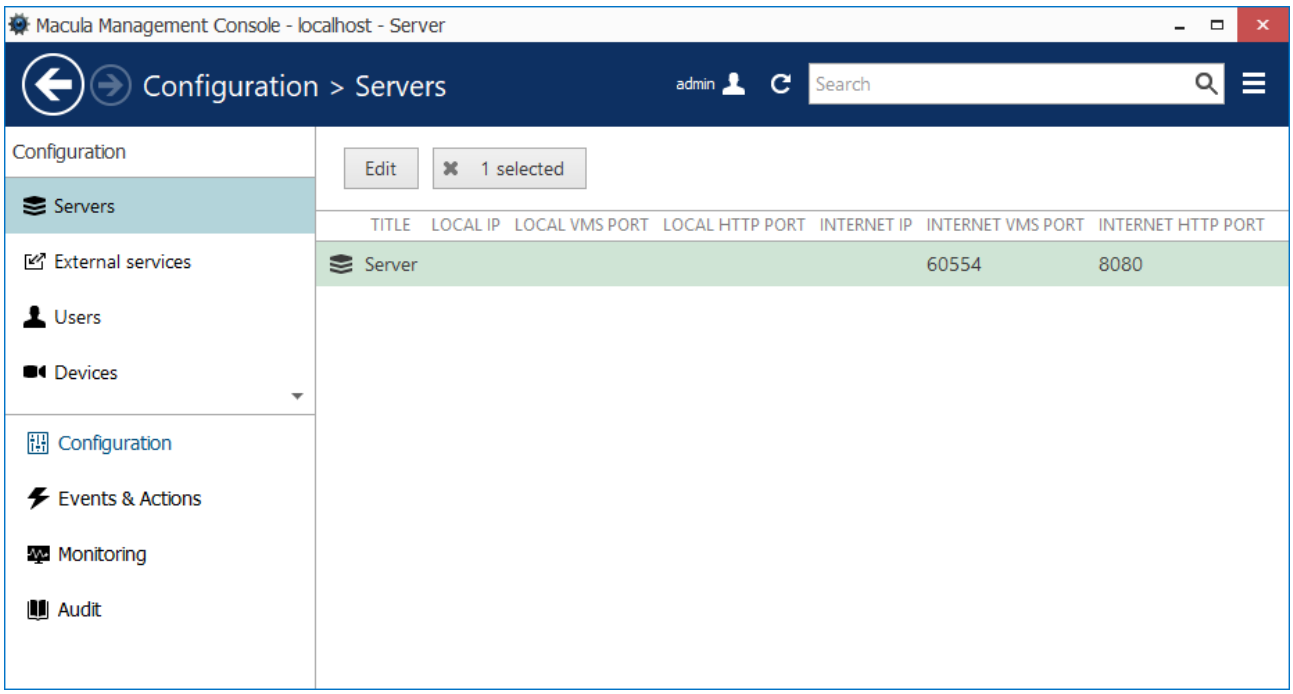
Although it is possible to disable the Server Watchdog service, we strongly advise against doing so, as the principal role of Watchdog is to keep the software operation as stable as possible in the given circumstances.

Watchdog operation can be tracked by messages in the Windows Application log and in the software Audit log. If you do experience frequent disturbances such as software restarts or server rebooting, this will be an indication of some serious issue related to the software, operating system and/or underlying hardware. In such a situation, the best course of action is to:

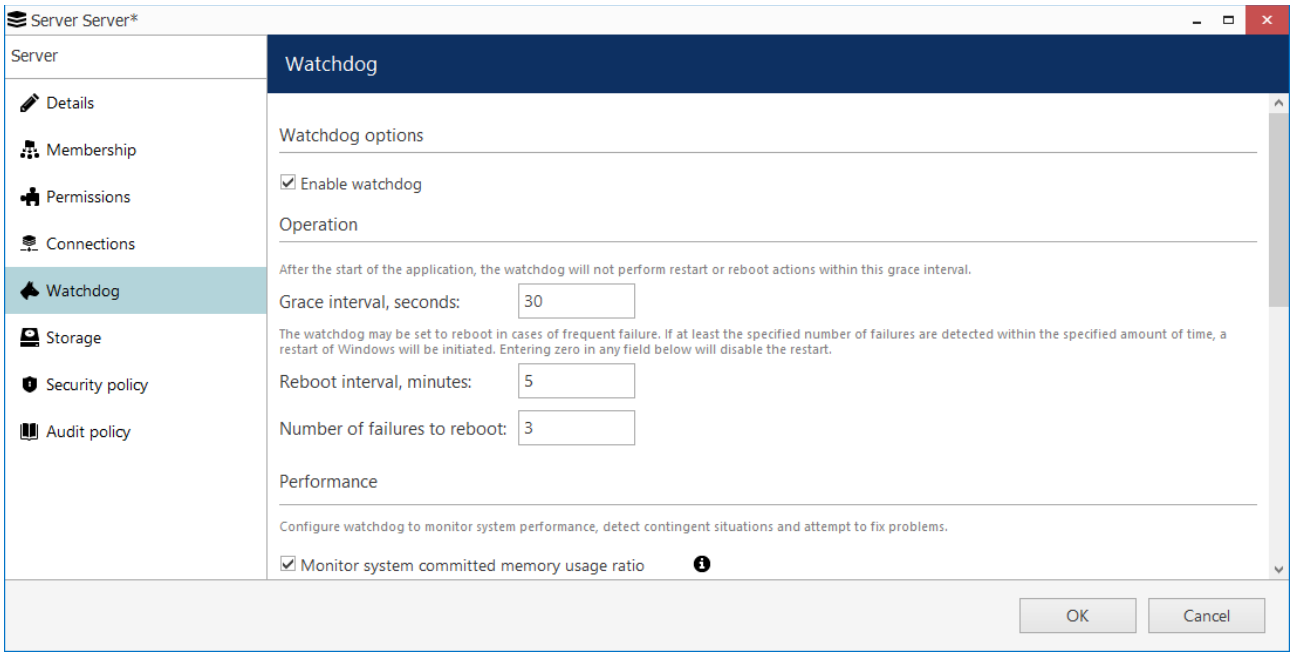
- carefully read the messages in the Windows Application Log, as these may already contain some indication of why Watchdog was triggered;
- refer to the relevant topic in the Troubleshooting section of this manual to read about typical causes of such cases;
- send a Problem Report from the faulty server, providing as much information as possible about the issue;
- consult the GSF technical support team directly via support@gsfcorp.com.

Configuration

Watchdog operation can be configured for each server independently. To access Watchdog settings, in Macula Console select *Configuration* in the bottom left menu and select *Servers* from the list on the left, then double-click the desired server or simply click *Edit* button on the top panel for the pre-selected server.



In the Server dialog box, select Watchdog from the left menu.



The table below contains a detailed explanation of Watchdog settings. Please note that, for most cases, **default and near-default settings are recommended**; it is advisable that you consult with GSF support if for some reason you plan to make extensive changes to these settings. Click the information icon next to each setting to read more about them.

Setting	Description	Default Value
Enable Watchdog	Enables Watchdog operation for the target server	Enabled
Grace Interval, seconds	Time interval in seconds, counting from server start, during which Watchdog will not attempt to restart the software	30
Reboot Interval, minutes	Watchdog will reboot Windows if there have been a certain number (N) of software restarts (N is specified below) in the given	5

	time interval; the default for rebooting is 3 restarts in 5 minutes; setting the specified number to 0 will disable rebooting	
Number of Failures to Reboot	Watchdog will reboot Windows in case there have been N software restarts in the time interval specified above; the default for rebooting is 3 restarts in 5 minutes; setting the specified number to 0 will disable rebooting	3
System Committed Memory Usage Ratio, %	Watchdog will restart the software if the ratio of total system committed memory exceeds the specified percentage; this value is shown under Memory section of Performance tab in the Windows Task Manager	Enabled, 70%
System Pool Nonpaged Memory Usage, MB	Watchdog will restart software if the amount of system nonpaged pool memory exceeds the specified amount	Disabled
Private Memory Usage Ratio, %	Watchdog will restart software if the amount of private memory used by server process exceeds the specified value	Enabled, 45%
Virtual Memory Usage Ratio	Watchdog will restart software if the amount of virtual memory used by server process exceeds the specified ratio; ratio shows the amount of virtual memory used by server process versus maximum per-process virtual memory allowed by OS	Enabled, 90%
Enable Periodic Restart	Enables automatic software restart every N days or hours; use hours for troubleshooting purposes	Enabled
Restart interval	Choose between every N weeks, days, or hours; use hours for troubleshooting purposes	1 week
Weekday	Restrict periodic restart to specific day of the week	Sunday
Enable Periodic Restart Hours	Limit periodic restart to specific hours, e.g. only restart at night; we recommend to leave at least a 1h interval for the restarts	Disabled

Up to software version 1.22, the *System Committed Memory Usage Ratio* was equal to 70% by default. Afterwards, it has been changed to 95% for a more optimal usage of system resources.

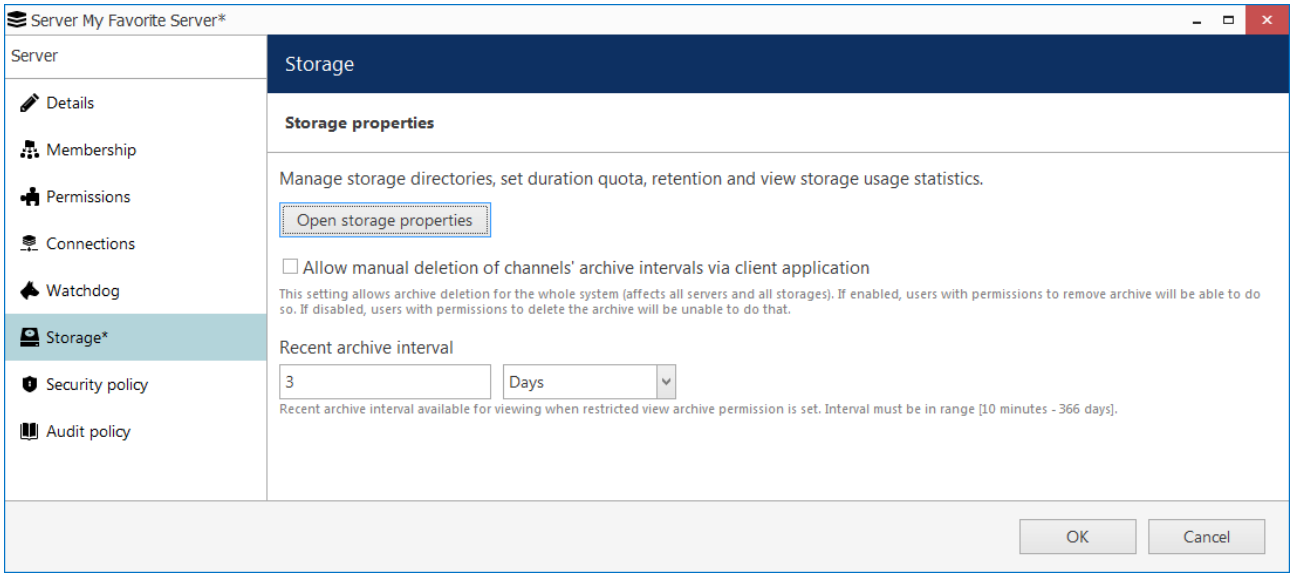
If you choose to limit the periodic restart time to specific hours or weekdays, the watchdog service will attempt to restart the main service straight away (at the very beginning of the allowed interval). If the watchdog does not succeed for some reason, it will continue to try until the end of the period, and then the next attempt will only take place when the next safe period begins. For example: if the restart is limited to 00:00-08:00 on Sundays, you should typically expect the restart at 00:01 on Sunday; if the watchdog was manually stopped before that time and started at 08:30, the following periodic restart would not happen until next Sunday at 00:01.

Macula 1.27 Update: The *Server Watchdog* now automatically monitors the *Streaming Server*, enhancing system stability and reliability. This integration ensures uninterrupted streaming and improved performance, with no additional settings required.

4.2 Storage

Server storage configuration includes storage directories, size and duration quotas, optional encryption, cleanup time settings and storage differentiation by name for further flexible allocation of the recorded streams.

To access the storage settings for the server via Macula Console, choose the *Configuration* section, select Servers from the menu on the left, double-click your target server and then click the *Storage* tab. Click the Open *storage properties* button to open the configuration dialog box.



To **save the changes** after you have finished with storage configuration, hit the *Apply* button beneath the storage settings, then hit *OK* to close the storage configuration dialog box, and then click *OK* to finally save the storage settings together with the server configuration. Pressing *Cancel* on the last step will revoke the changes in the storage configuration.

Directories

All available **local disks** will be automatically listed after the first installation (with empty configuration) and enabled for recording with default archive directories using the Default storage label. By default, system disk (C:) is not listed if other disks are available, as we strongly do not recommend recording to the system disk.

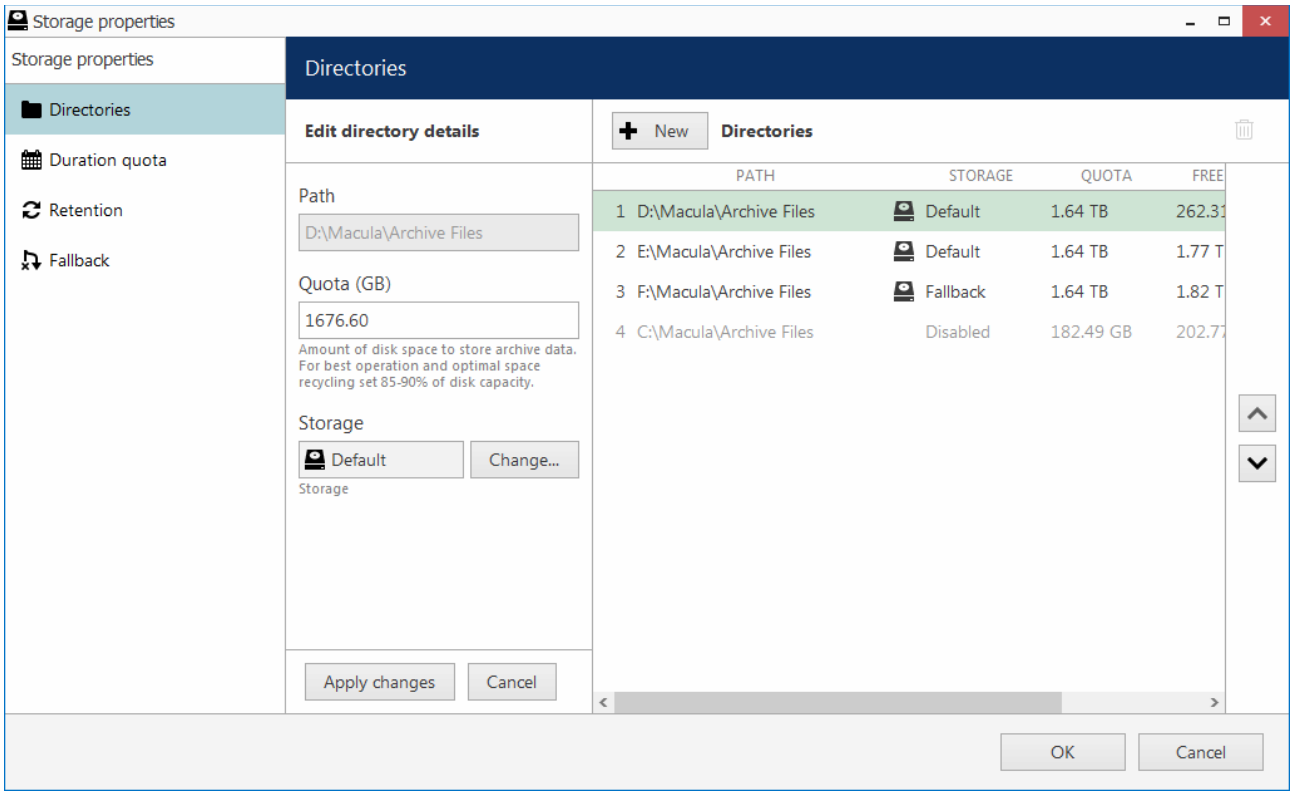
If you are upgrading, re-installing the software, restoring an earlier database configuration, or inserting new local disks into the server after the software has been installed, the local disks will not be listed automatically so you need to **add** them as **new storages**. You can also add network paths to remote storage locations.

Use UP and DOWN arrows on the right to change the disk order (priority); use the recycle bin button in the top panel to **remove** any local or network directory from the storage configuration.

> Mapped network shares that appear as drives in Windows Explorer will **not** be listed automatically because Macula operates as Windows Service and therefore is unable to access these (due to Windows API peculiarities). You are welcome to add these as network directories in storage settings.

For each storage location, the following information will be displayed:

- storage priority: determined by the item position in the list
- storage label (see description below)
- current quota size
- free space on disk (except network storages)
- total disk size (except network storages)



Each directly attached storage location will be automatically assigned a quota of 90%; each storage will have 20GB quota by default. We strongly advise that you review all the settings and make sure that all the storage locations have sufficient free space, and, if necessary, free up some space. It is recommended that every recording location has 10-15% of free space: this helps avoid fragmentation effect and also allows highly loaded software to effectively enforce recording quotas.

⚠ **Minimum quota** per each storage location for any storage type is 20GB.

We advise against recording to the **system drive** because it is often used by other processes like defragmentation and system backup, not to mention the operating system itself, and thus doing so may affect recording efficiency and stability. As a result, disk C: is not selected for recording by default.

Total size and free space on the **network storages** is not displayed here. You can check these in the Monitoring section of Macula Console, under Storages.

To change the disk quota, simply highlight the desired location for storage from the item list, then enter the quota size in GB and click *Apply changes*.

⚠ If you plan to **protect** some footage from being erased (this functionality is available via Macula Monitor application), keep in mind that **protected archive** areas will be **ignored when forcing quotas**. Make sure there is enough free space on the disk(s) and set lower quotas, if necessary.

To review and/or **un-protect** such areas, go to the *Monitoring* section of Macula Console, choose *Archive statistics* on the left, highlight one or more target channels, and press the Protected intervals button on the top panel.

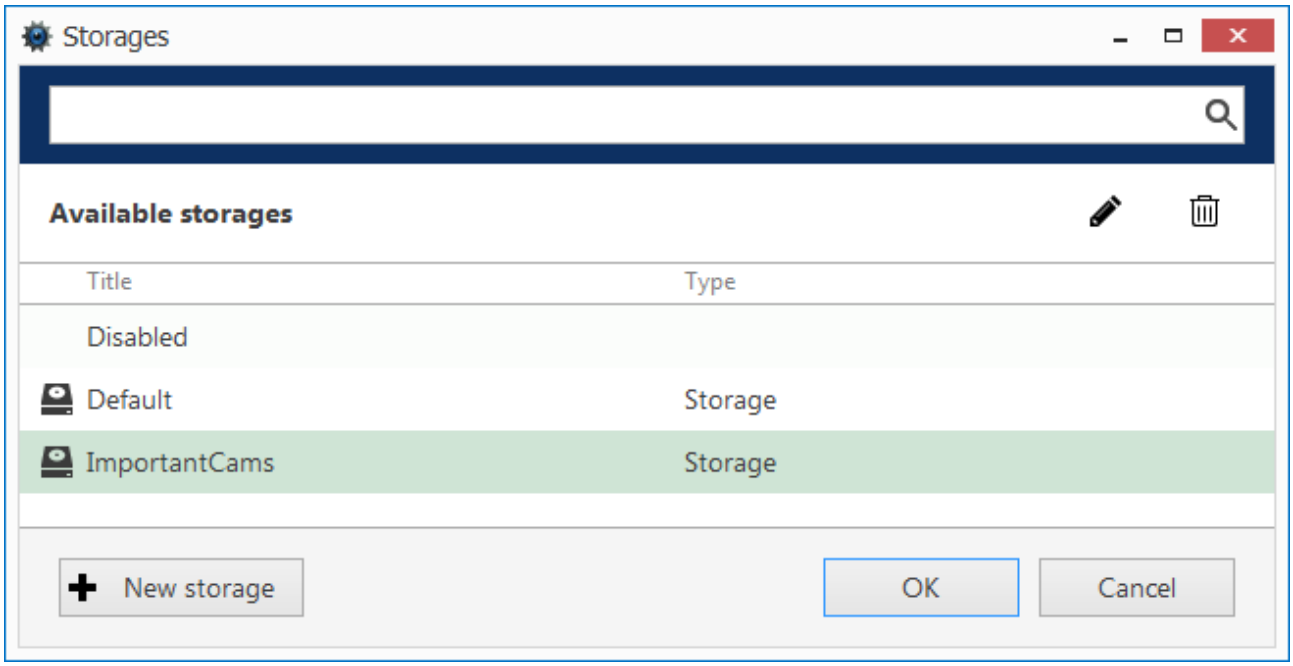
Storages

You can either use the Default storage category for all locations, or create multiple different **storage** profiles (types, names, labels). These can be used for manually distributed streaming between storage directories:

- storage directories are marked with corresponding storage tags
- each channel is assigned to a recording location

To choose a storage profile different from *Default*, select storage location from the *Directories* list and click the *Change* button.

Select one of the built-in storage profiles or create and edit a new one.



The built-in storage types are:

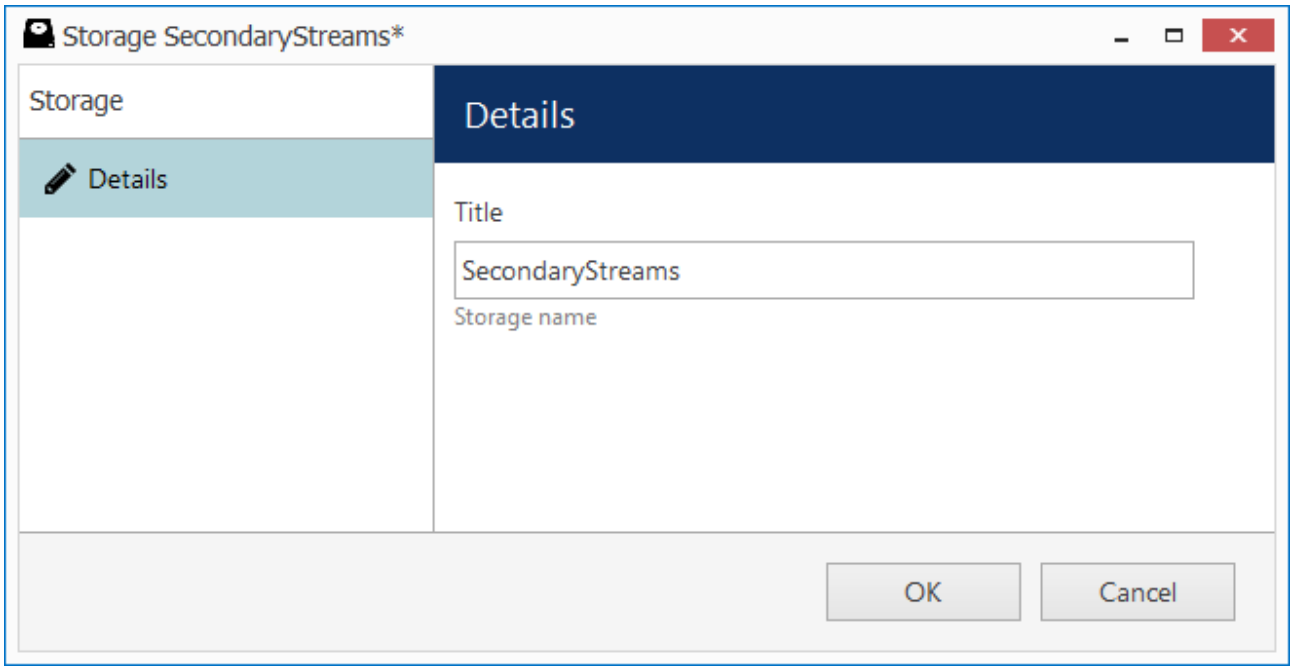
- **Disabled**: storage location will not be used
- **Default**: default storage tag
- **Fallback**: storage destination to be used if all the storage units with specified tags have failed

- **Readonly**: existing data will be available for reading and will not be erased; no new recordings will be appended to this location

These profiles cannot be edited or removed. Fallback storage settings are available in the corresponding tab of the *Storage properties*.

> Readonly storage type can be used, for example, in the following cases:
> - it is necessary to view the old data from a different Macula server when you need to insert the disks originating from another computer and you do not wish that these data are erased
> - some storage unit contains important footage that has been requested to be kept for a longer time so that the recordings are not erased over time while still allowing access to the footage

Click + *New storage* button to create a new storage profile or select an existing one and click the *Edit* button in the upper-right-hand corner to change its name.



Enter the storage profile title and click *OK* to save and exit.

The storage tag you have selected or just created will appear as selected. Click the *Apply* button below to **confirm** storage configuration settings before proceeding.

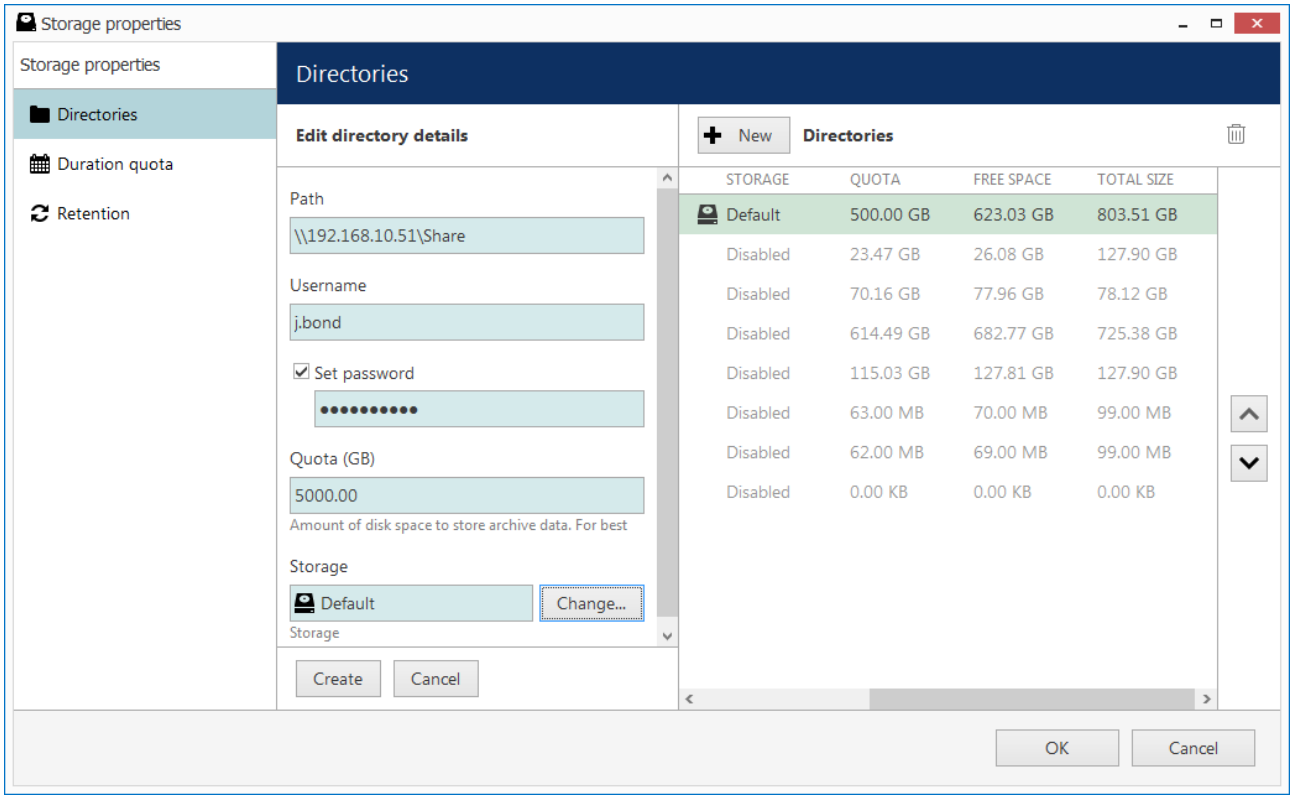
Add Storage

In order to add a new **local disk** or a **network storage** (NAS, SAN, network share), click + New button on the upper panel, select *New local directory* or *New shared directory*, and then enter the setup details.

> ⚠ If you are using a NAS, make sure to **disable** the *Recycle Bin* feature (for some NAS models, it is called *trashbox* or similar). This will ensure that the erased files (e.g., when reaching quota) are actually **deleted** permanently

Macula® Professional Administration Guide

> ⚠ If you are adding a previously encrypted storage (e.g., it has been used on another server), make sure to provide the same password. You can track the storage status in the *Monitoring* section of Macula Console, under *Storages*.



The table below details the available settings for a **shared directory**. Enter the settings for the target storage and click *Create* below: the storage will be validated immediately.

Setting	Description	Default Value
Path	Full network path to the storage directory	\\Server\Share\Macula\Archive Files
Username	User name to connect to the storage	[empty]
Password	Define storage access password, if applicable	[empty]
Quota	Maximum amount of storage in gigabytes to be used for recording; 85-90% is recommended	20GB
Storage	Storage label to be assigned to the target storage directory	Disabled

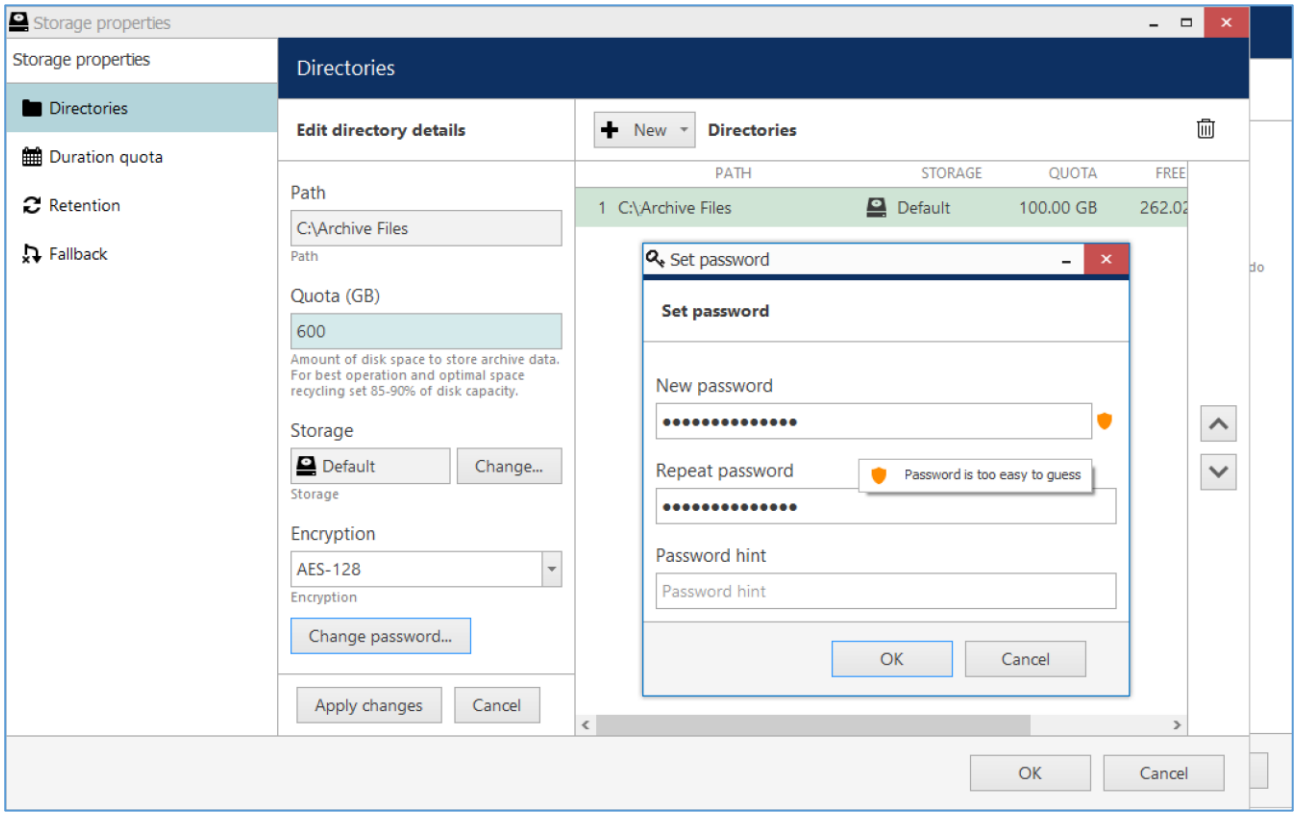
When adding a **local directory**, you are first offered to choose the disk from the list of detected ones. If there is just one disk left available, it will be chosen automatically.

Setting	Description	Default Value
Path	Full path to the archive directory	X:\Macula\Archive Files
Quota	Maximum amount of storage in gigabytes to be used for recording; 85-90% is recommended	20GB
Storage	Storage label to be assigned to the target storage directory	Disabled

Macula® Professional Administration Guide

Storage Encryption

Once you have added all the necessary storages, you can enable encryption and set a password for each storage separately.



Mark the *Enable encryption* option and specify the password you want. You can change the password at any point, and there is also an additional field that lets you add a hint that may help remembering the password in future: it will appear either as regular text or a tooltip when hovering your mouse cursor over the password prompt field.

The currently available encryption options:

- **None**: no encryption
- **AES-128** or **AES-256**: choose the one you need

When assigning a new password for the storage, make sure to remember it or store in a secure place: you will require it, should you need to access the storage contents in the following scenarios:

- when accessing the archive with the Portable Player tool
- when adding the same disk as a storage unit for another server
- when adding a disk containing archive backup as a storage unit
- if you delete the encrypted disk from the storage configuration and then add it anew

There is a field that allows you to enter a password hint, which will be displayed in these situations.

You will not be prompted for the password when accessing the archive from the Macula Monitor application connected to a server with encrypted archive: Macula server will decrypt it automatically.

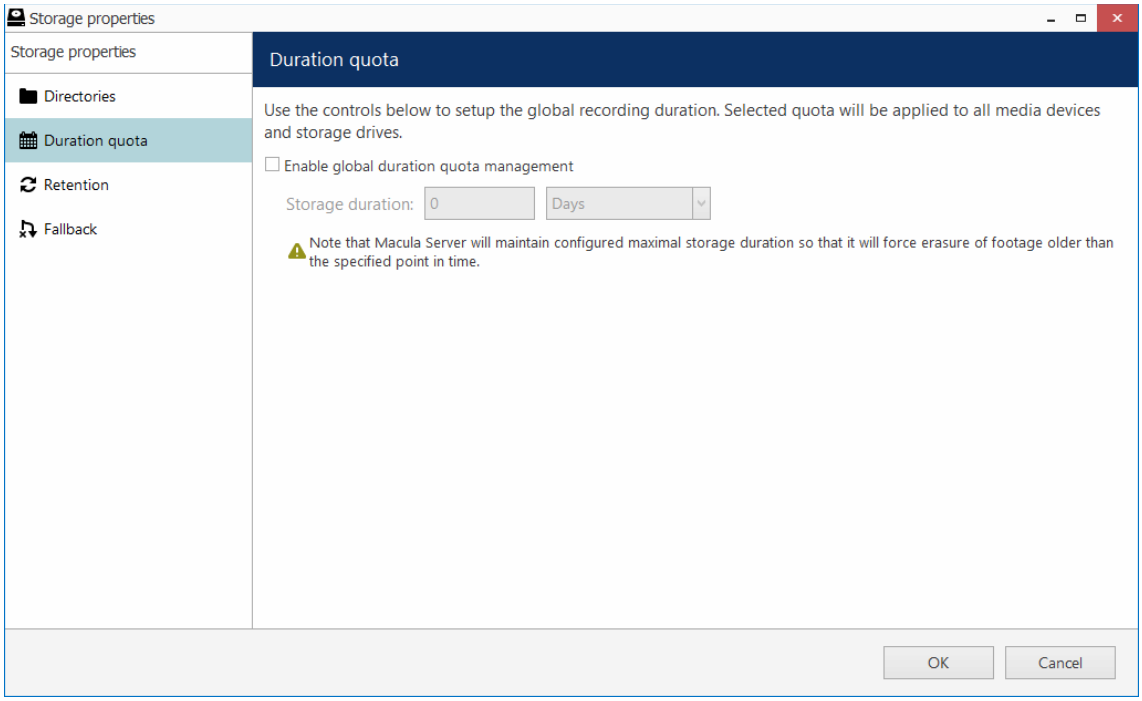
> ⚠ **There is no option to recover the password if you have forgotten it.**

Starting from the moment you set the password, all footage recorded to the target storage becomes encrypted; retroactive encryption for the previously recorded archive is not supported.

When the storage password is changed, the new password is used for encryption from then on. If storage encryption is disabled for some time and then enabled back, that part of the archive will remain unencrypted.

Duration Quota

Set the global recording duration limit for your server here: enable quota management and then enter desired number of days. All recordings older than the number of days specified will be erased.

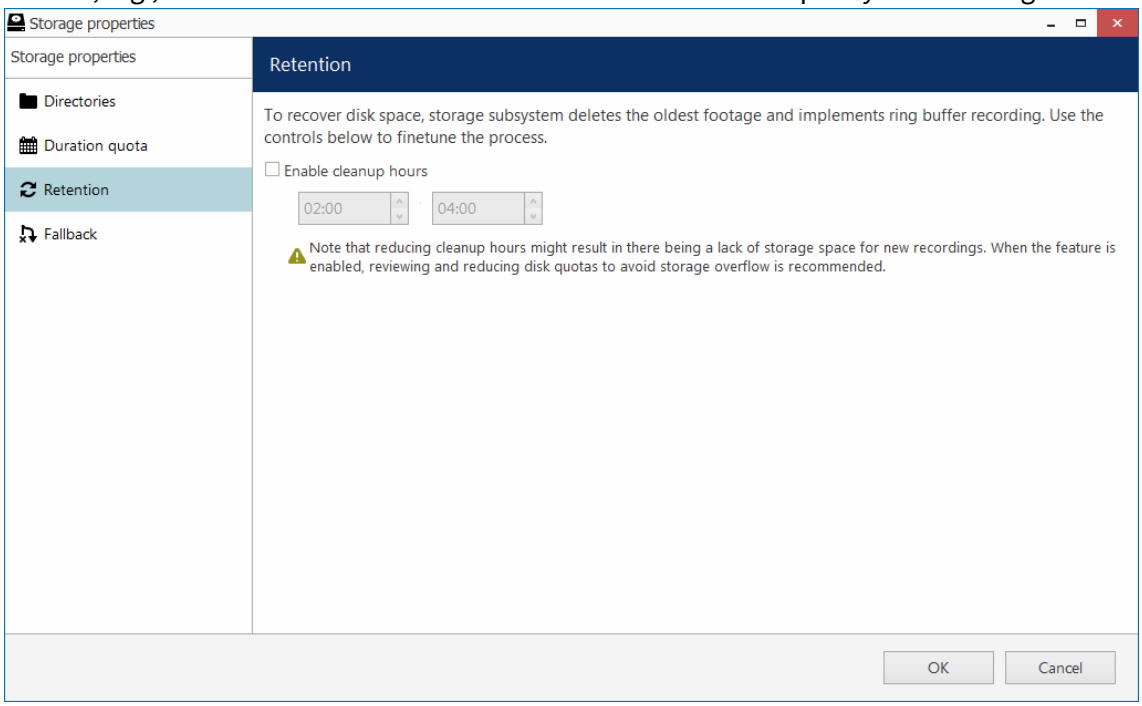


Note that the global duration quota has priority over the individual (per-channel) duration quota that is set in the Recording Configurations.

Retention

Macula® Professional Administration Guide

You can set the software erasing mechanism so that it cleans up old recordings only during specific periods of time, e.g., when the recorder is less overloaded or when the quality of recordings are less important.



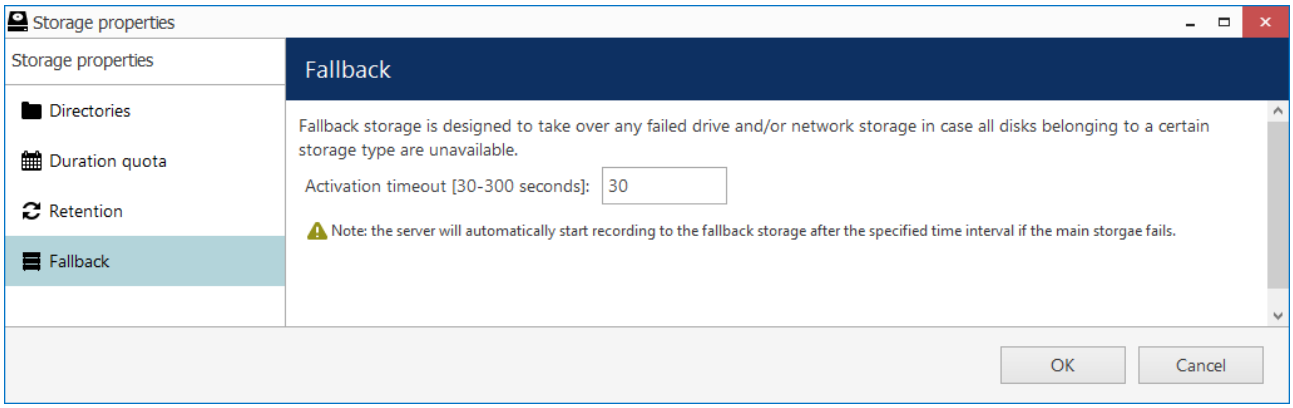
To do this, enable the cleanup hours setting and then specify the time period during which erasing is allowed.

> ⚠ This control has priority over the storage quota. Setting insufficient cleanup time may lead to storage overflow and result in partially missing recordings. We strongly recommend that you do not enable any cleanup hours' restrictions unless you absolutely know what you are doing.

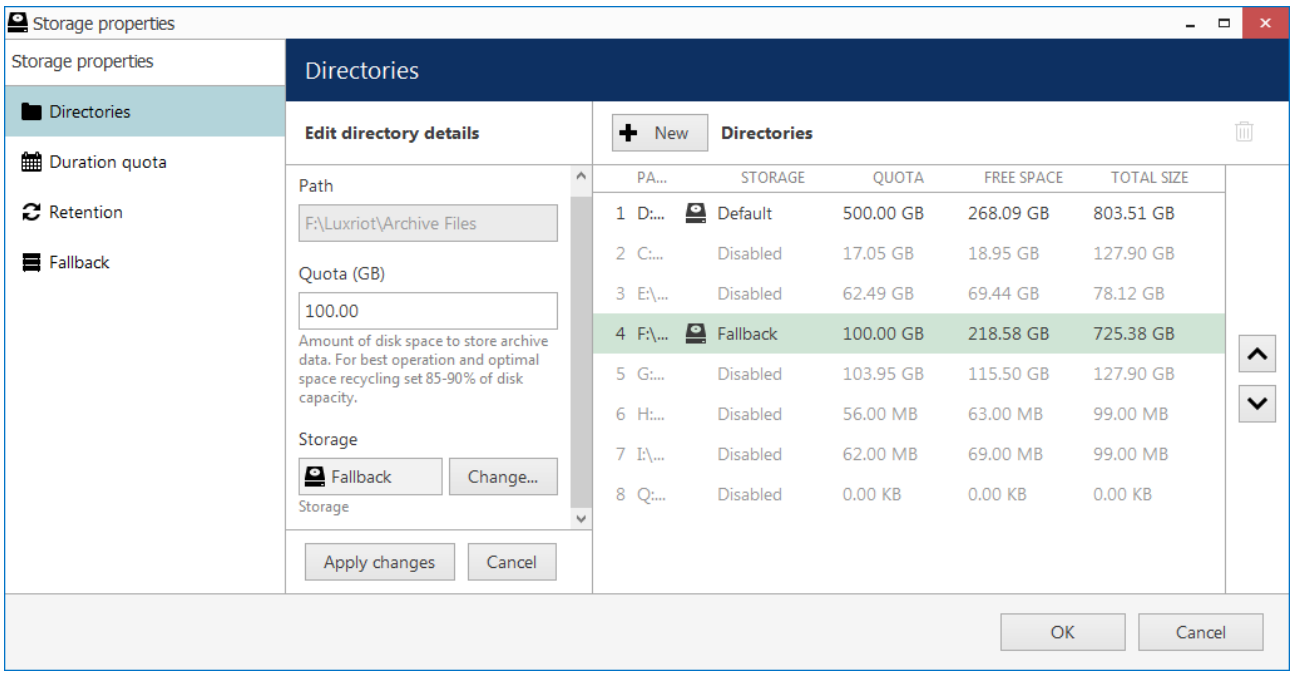
Fallback

You can dedicate a specific recording location to serve as a failover storage, called **fallback storage**. Such storage location will be used for recording only if all specified target storages of the certain type have failed.

Macula server automatically detects when a channel or channels cannot be written onto their normal destination storage and switches to the fallback storage after the specified timeout has been reached. Minimum and also default timeout is thirty seconds, and maximum is five minutes. A default system event is raised when fallback is activated.



After setting the desired timeout, switch to the *Directories* tab and specify, which storage will serve as fallback.



Usage example:

Consider a system where all main streams are recorded to the storage with the tag *Main* and all secondary streams are, in their turn, recorded to the *Substreams* storage. If either or both of these storages fail, recording will automatically proceed to the *Fallback* storage.

> ⚠ The fallback storage must be able to handle the load and have enough free space to keep the recordings until the main storage gets back online.

Server checks if the main storage is available if one of the conditions has been fulfilled:

- server has finished and closed a data file (4GB)
- the data file has not reached 4GB in size but six hours have passed
- server was restarted

In other words, the recording mechanism checks if the main storage is available every 6h OR every 4GB of recorded data OR after a restart (upon startup). If the main storage is OK, Macula server continues to record onto it; the recordings made onto the fallback storage stay there and are not transferred anywhere.

To **save the changes**, hit the *Apply* button beneath the storage settings, then hit *OK* to close the storage configuration dialog box, and then click *OK* to finally save the storage settings together with the server configuration. Pressing Cancel on the last step will revoke the changes in the storage configuration.

Archive Protection and Deletion

Outdated archive is erased automatically once any of the quotas is reached (storage or duration, server wide or individual). Oldest recordings are removed to free up some space for the newer recordings. However, there are some exceptional cases when the footage is not or may not be erased:

- storage marked as *Readonly* will not be used for writing and no data will be erased from such storages based on quotas (however, footage from such storages can be removed using selective erasing from the Macula Monitor application)
- no erasing will be conducted outside cleanup hours (by default, erasing is allowed 24/7 and this setting is recommended)
- protected archive intervals will be also ignored by the erasing mechanism until you un-protect them

Archive protection is a feature available in the Macula Monitor application, in playback mode. You can mark certain footage from being erased if it is important to keep it for longer (e.g., as evidence). To unlock the protected intervals, go to Archive statistics in the Monitoring section of Macula Console.

⚠ If there are too many protected recordings on a disk, the storage may be filled up to 100%: this may negatively affect the overall recording operation. Pay attention to the amount of free space on every storage unit in case you are using archive protection:
- set lower recording quotas so that there are always 10-15% of free space on each storage,
- un-protect the archive that no longer needs to be protected from erasing.

⚠ When you **protect a short period** of the archive (e.g., several minutes), in fact, the **whole file** containing this period is protected from erasing. Therefore, intervals adjacent to protected period will also be locked. You can verify the exact protected interval by opening Macula Console >> *Monitoring section >> Archive statistics >> Protected intervals*.

Keep this in mind when protecting too many short intervals: as all files containing them are locked, they will not be erased when forcing quotas, so you may come to a point when there is **not enough free space** on the disk. If you know you will use the archive protection feature a lot, it may be wise to set a **lower disk quota** - for example, 80% instead of 90%.

Macula Monitor application allows users with corresponding privileges to delete certain parts of the archive. This mechanism can delete recordings from storages marked as *Readonly* but cannot erase protected archive from any storage unit.

If the footage is not protected, it will be removed as outdated when the server eraser reaches one of the quotas. Also, the **unprotected** footage can be removed manually by someone who has a permission to **delete archive**. However, as such a feature may be may be regarded as a potential threat for the archive integrity, it is **disabled by default**. You can enable it in the server storage settings by marking the *Allow manual deletion* option.

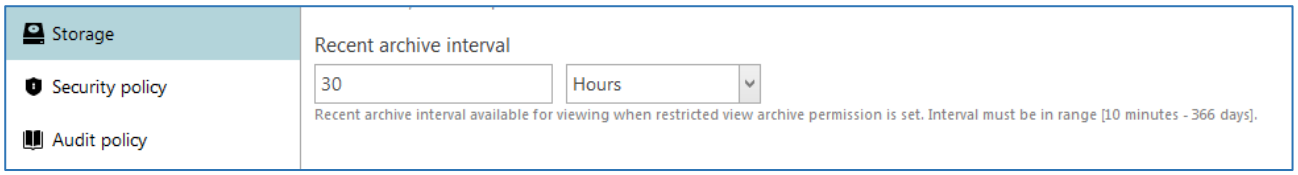
⚠ Enabling manual archive deletion will automatically enable the **admin** user to do so, as admin is a root user who has all possible privileges. The same is true for all users belonging to the *Administrators group*. If you are enabling this feature, make sure that no unauthorized personnel have access to the administrative accounts.

Time Restricted Access to Archive

There is a possibility to grant **archive access** permissions for a **limited time**: for example, for the last N days or M hours. The access permissions are a part of the channel permission set.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Here, in the server settings dialog box > *Storage* tab, you can define the allowed archive access period, starting from the present moment.



Depending on your needs, the duration can be expressed in **minutes**, **hours**, or **days**. The minimum period is 10 minutes and the maximum value is 366 days (1 year).

Example: if the recent archive interval is set to 30 minutes, all users having a Restricted video playback permission will be able to browse the last half an hour of the target channel archive in all archive playback modes of the Macula Monitor application.

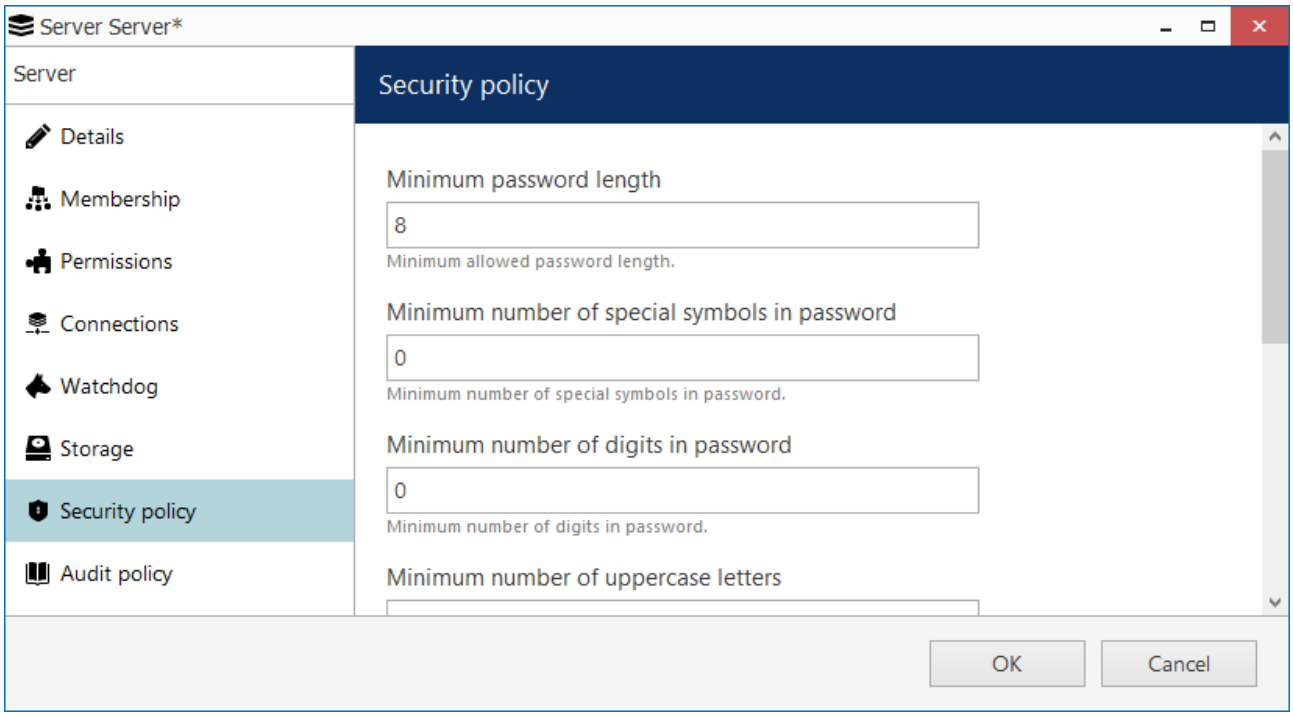
4.3 Server Policies

Macula policies are configurable sets of rules that are followed by Macula servers when handling access requests. At this point, these include security settings and external database configuration. Default values and state of the policies depend on the chosen security level.

Security Policy

Security settings related to password management, connections etc. can be defined for each server. To access server security policy settings via Macula Console, choose the *Configuration* section, select *Servers* from the menu on the left, double-click your target server and then click the *Security policy* tab.

It is recommended that, in order to enhance your system security, you do not leave the default policy settings but rather define your own, system-specific preferences.



The table below details the available settings.

Setting	Description	Default Value
Minimum password length	Minimal mandatory length of a user password	8
Minimum number of special symbols	Define how many (at least) special characters (#$%&...) must be present in a user password	2
Minimum number of digits	Define how many (at least) digits must be present in a user password	2
Minimum number of uppercase letters	Define how many (at least) UPPERCASE letters must be present in a user password	2
Minimum number of lowercase letters	Define how many (at least) lowercase letters must be present in a user password	2

Number of previous passwords to remember	Password history to be kept by the server to prevent the user from using the same password again when changing it	1
Maximum number of days between password change	Define how frequently Macula will ask users to change their password; this setting can be overridden in the user settings to make the password never expire for a specific user	0 (unlimited)
Maximum number of simultaneous connections with the same login name	Allowed number of simultaneous incoming connections from the same user account via any port (TCP/HTTP) or client app, this setting can be overridden for the specific user in the user settings; 0=unlimited	0 (unlimited)
Maximum unsuccessful login attempts*	After this number of unsuccessful login attempts the user account will be blocked (can be unlocked via user properties). Set 0 to allow unlimited attempts.	0
Disconnect disabled users**	Disconnects User from Server as soon as system marks account as disabled	Disabled (not selected)
Disconnect upon user password change**	Disconnects User from Server as soon as password change event happens	Disabled (not selected)
Disconnect if password expires**	Disconnects User from Server if user password is expired	Disabled (not selected)
Disconnect if auth token is reset**	Disconnects User from Server if authentication token was reset	Disabled (not selected)
Put user ID as an OSD watermark	Add **watermark** with the **logged-in monitor User's ID** over the all Live View and Playback viewports displaying video streams. Such a watermark allows compliance with GDPR and specific countries' local data and privacy protection regulations, making it possible to identify any data leak source recorded even by a third-party recorder (such as a phone) directly from the display. **You can't change the text** displayed in the watermark - the only option is to turn on or off the feature.	Disabled (not selected)

Password related policies are solely meant for Macula internal users and they do not affect any other user account settings (e.g., Windows users etc.). All policies are in effect for **all user accounts**, including the built-in root *admin* user account.

***To **unlock the user** account, go to the *Users* section > open the user details for editing > enable the *Active* option > save. To override the policy for a specific user, enable the *Never lock account on bad password* option in the user account details.

****** **if** the option is disabled - the user will continue with the current session, even if this particular user is already disabled.

The **maximum number of simultaneous connections** from the same user account can be re-defined for any specific user via user settings dialog box. User-specific setting has priority over global connection quota and it may be either larger or smaller than the global quota.

Example 1: global policy is set to 0, which means no imposed limitations. However, user account *admin* has his max number of connections set to 3, which means that three incoming connections with this user account are allowed at a time so that the administrator can connect via Macula Console, Macula Monitor and Macula Mobile at once for troubleshooting purposes.

> **Example 2**: global policy is set to 1, which means only one connection from each user is allowed at a time. However, user *demo* has an allowance of 30 simultaneous connections so that this account can be used for demonstration purposes.

Two-Factor Authentication

For additional security, you can turn ON **two-factor authentication** (2FA) for all client logins. When 2FA is enabled, all users who want to connect to your Macula server, will have to enter both their password and a code they receive. Thus, the users prove their identity not just by entering what they know (the password) but also what they have (the email or phone). By default, this policy affects all users; you can disable 2FA for individual users in their permissions.

> At this point, Macula 2FA supports code sending via **email** and **SMS**, and works for Macula Console and Macula Monitor login.

Terminology:

- session: an established connection between client and server once the user logs in
- code: a numeric code sent to the user's email

The following settings are available here:

Setting	Description	Default Value
Enable two-factor authentication	If selected, additional authentication will be required for server login	Disabled
Set up notification providers	Set up desired providers (using email servers or other means) that will be used for sending out authentication codes	[button]
Session expiration time	During this time period, 2FA will not be requested again if client disconnect was caused by server; after this time or after user-initiated disconnect, the user will have to use additional authentication again	1 day
Code expiration time	The time period during which the sent code will be valid, starting from the code send out moment; after this time, the user will have to request another code	00:05:00 (5 minutes)
Code generation interval	The minimum time between two consequent code requests; the user will be unable to request a code more frequently	00:00:10 (10 seconds)
Skip for localhost connection	If enabled, 2FA will not be applied to localhost connection	Enabled
Subject	Message subject line, can consist of text and macros (via right-click)	{SESSION_ID}
Body	Main message part, can consist of text and macros (via right-click)	{CODE}

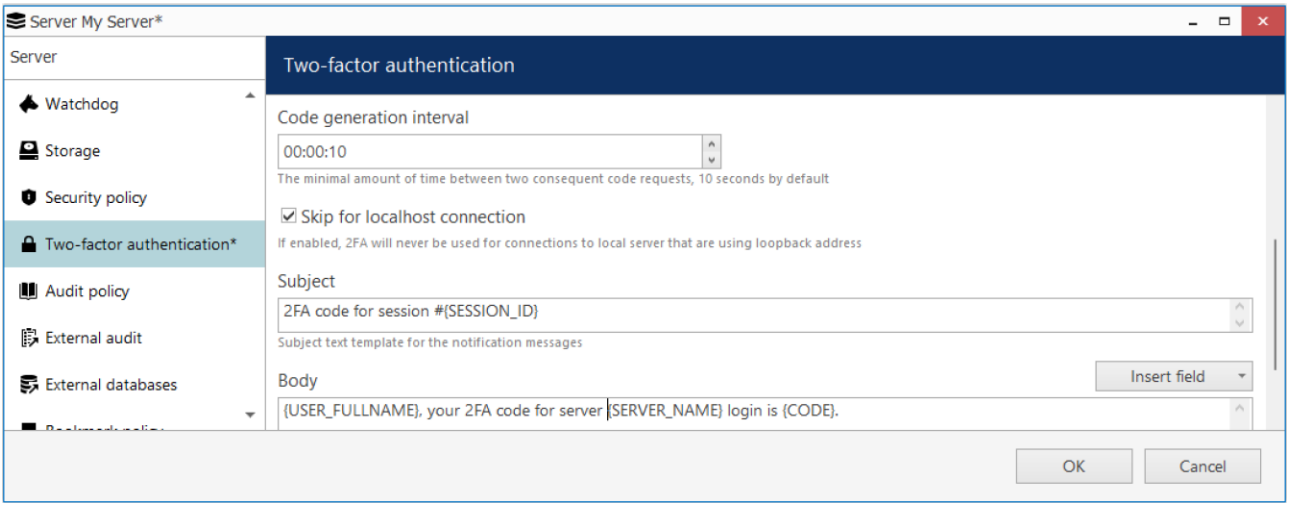
> Name your **notification providers** according to the used verification source (e.g., **Email**) so that the users understand where to look for the code.

> Write some text in addition to the session ID and the code so that:
> 1. The user understands which one is which
> 2. The email does not go to Spam

When you try enabling 2FA, you will get a **warning** that you will need to test 2FA before saving the configuration. This is necessary to ensure that all the settings are correct and 2FA actually works; otherwise, you may be unable to log into the system at some point. The 2FA verification will start when you click OK to save and close the settings window.

Settings to be verified before enabling 2FA:

- make sure you have added a valid 2FA notification provider (SMTP server)
- add a contact email for each user
- it is recommended that at least one administrative user account is allowed to log in without 2FA, or 2FA is disabled for localhost connections: this is to ensure that you can log into the system if your 2FA notification provider fails or becomes unavailable



The best approach for 2FA configuration:

- in 2FA settings, add a notification provider and adjust everything but do not enable 2FA yet, click OK to save
- make sure your email server user for notification provider is valid, and that all users have correct emails
- go to 2FA settings again and enable it, and go through the test verification

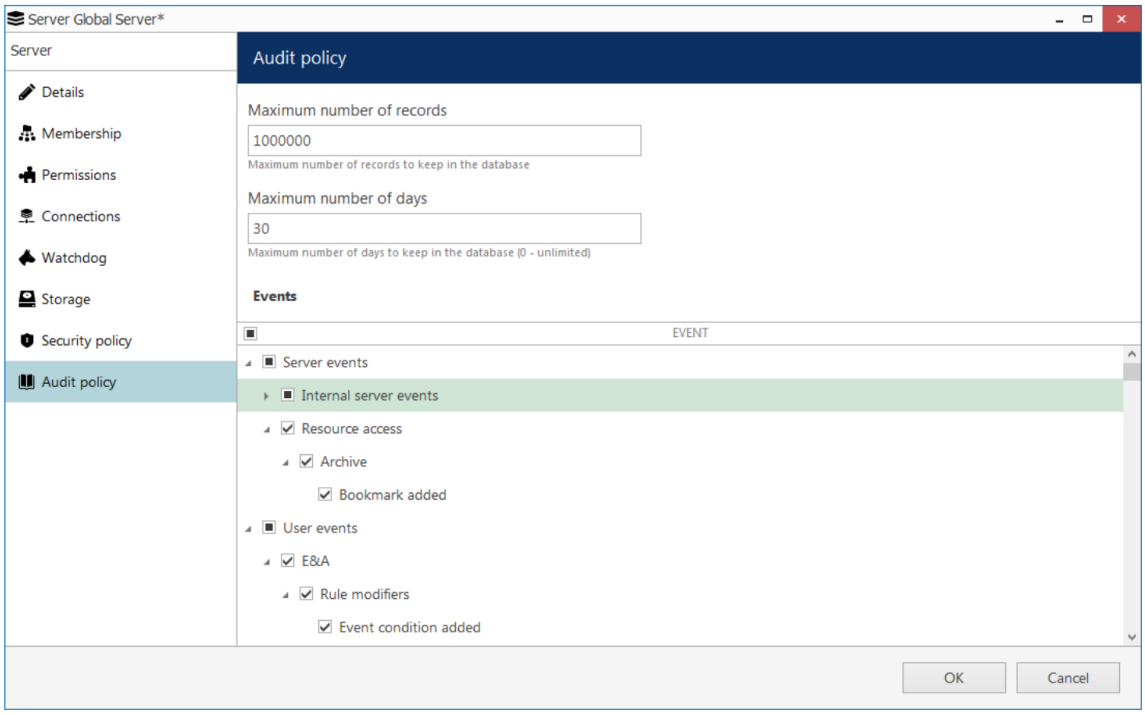
When you turn off 2FA, you will have to go through the setting verification again next time you enable it. If you make changes to the 2FA settings and enable it at once, this test verification will use the previous settings for formatting and intervals (because it basically happens before saving the settings, and these will not be saved until you pass 2FA successfully).

Two-factor authentication is also a recommended setting when you choose the highest cybersecurity level – the system will check if 2FA is enabled and remind you with a warning mark if it is not.

Audit Policy

Whenever a permission is used, a corresponding entry appears in the internal Macula audit log; internal server events are logged as well. The audit policy lets you define, which user actions and server events are recorded, as well as set the maximum size and duration of the audit log.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



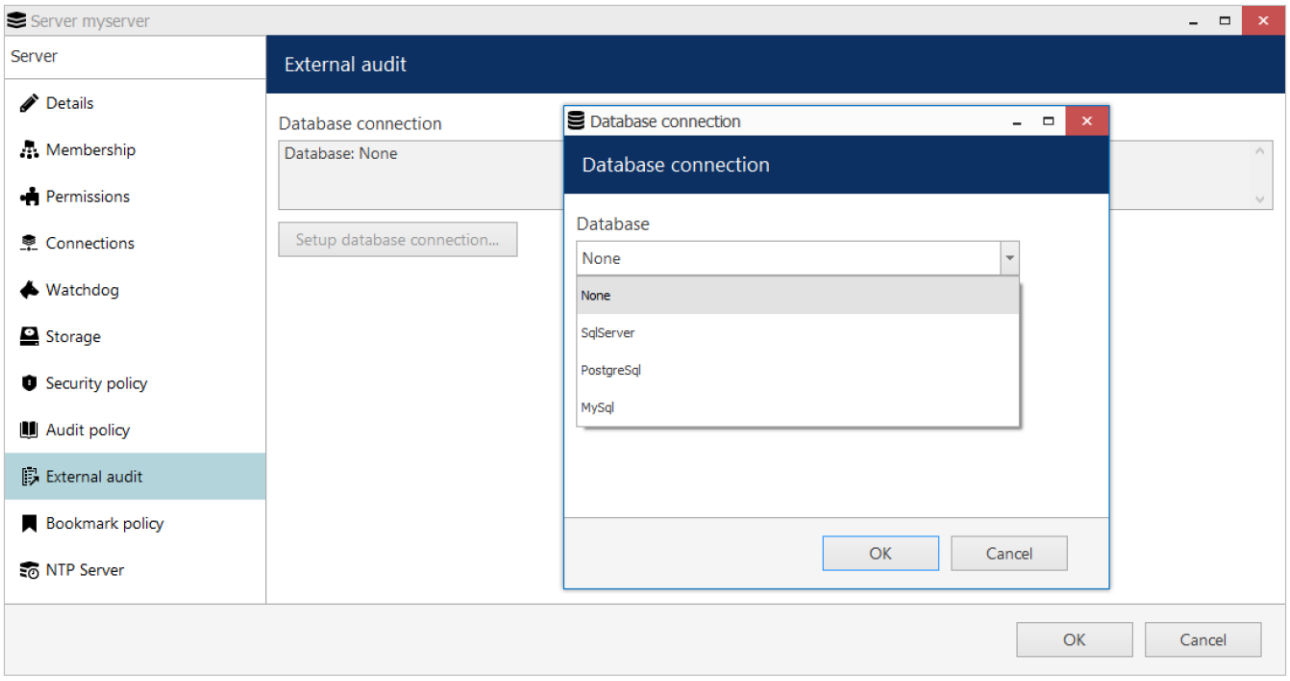
The default limit for the number of audit entries is one million and they are kept for one month; set zero days to disable the duration limitation (the quota for the number of records will still have effect). By default, all the events are audited.

External Audit

For Macula Global software edition, it is possible to set up log event storing in an **external audit database**.

The main (internal) audit log is kept always, and the external audit is a copy (addition). You cannot turn OFF the internal audit if you do not need it, but you can limit it to one or two days, and keep the external log for a longer period. The built-in database (SQLite) is OK for low and medium load; for high and extra high load, especially for lots of entries per second, an external database with extra hardware is strongly recommended.

Macula® Professional Administration Guide

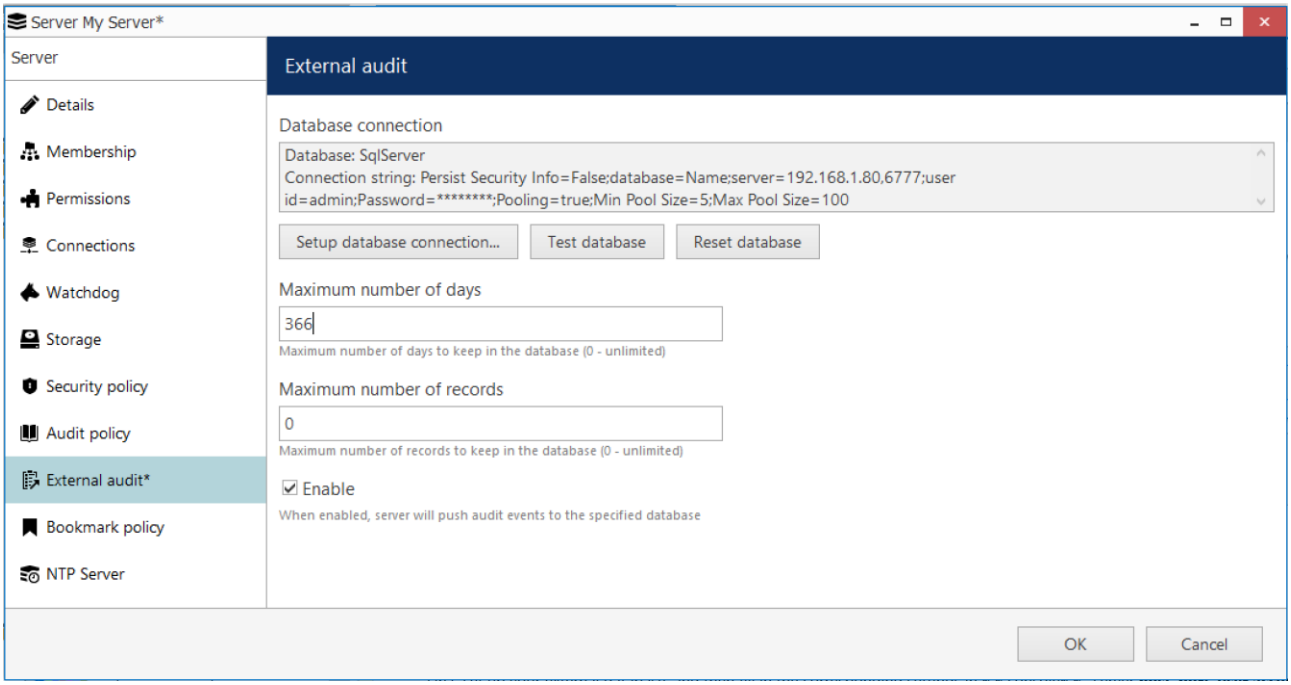


At this point, three database formats are supported:

- SQL database
- PostgreSQL
- MySQL

First, set up your external database, and then fill in the corresponding settings in Macula Console: server **host**, **port**, **user account**, and target **database name**.

> ⚠ Please consult with your database server architect to build the database server. Macula hardware recommendations do not include hardware for the external database server.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

After adding the database connection, you can **test** it to verify that the entered configuration is correct. The database **must exist** for the Macula server to connect successfully, and you cannot create a new external database from Macula Console. The connection test runs **automatically** once you have entered a new DB connection or modified the connection settings.

> ⚠ The connection **test may take some time**. You can tell by the disabled (grayed out) buttons below. If you close the server settings dialog box, the test will still run in background so you will have the result pop up after some time.

If your target database contains something else and you want to clean it, press *Reset*: all contents of the target database will be then **removed** and replaced with the tables necessary for the audit log.

Similarly, to internal audit, here you can **limit** for how long and how many records should be kept in the external audit database. Set zeroes for **unlimited** options (the number of records will be then only limited by database type).

> 💡 External databases are recommended when you need to keep larger amounts of information for much longer periods of time. The built-in database (SQLite) is OK for low and medium load; for high and extra high load, especially for lots of entries per second, an external database with extra hardware is strongly recommended.

You can prepare the database connection and leave it disabled (default mode) until you decide to **enable** the external logging. To do this, put the check mark in the corresponding checkbox.

When done, click *OK* to save the settings and close the dialog box.

Troubleshooting: if, during operation, the Macula server is **unable to write** events to the external database, you will have a **warning** (highlighted orange) in the *Monitoring* section of Macula Console, under the Servers category. Click the target Macula Global server, then click *Details* on the upper panel to see the **database connection errors**.

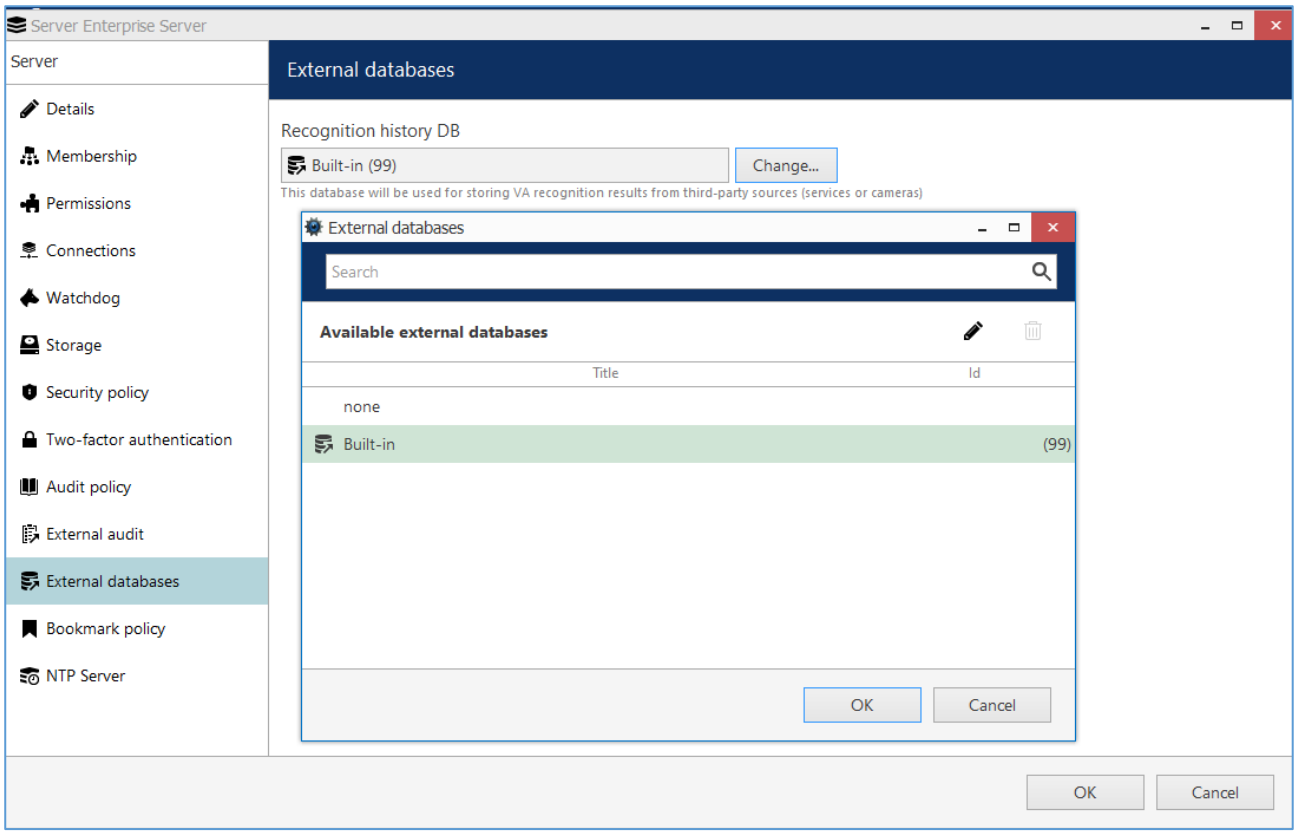
External Databases

For certain data types, you can set up separate databases in a similar manner. In the *External Databases* tab, available databases will appear.

Currently available: a separate database named *Recognition history database* can used for storing external recognition events. Without it, only metadata (bounding boxes) are stored for external recognitions (in the video archive), so you will be unable to search these events in a separate tab in Macula Monitor. If you do not use external services/cameras for LPR/FR recognition, you will not be needing this database.

> 💡 If you have made a clean installation, this DB is enabled by default. If you made an upgrade from a software version prior to 1.21, this DB is disabled.

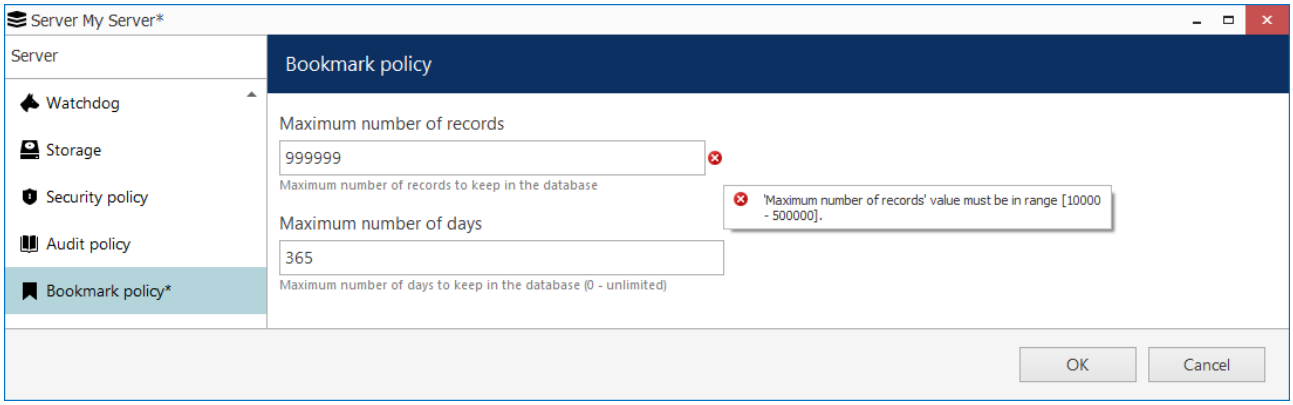
Click the *Edit* button to change the built-in database settings: limit the number of recordings and the number of days, and enable/disable the database. Click *OK* to save and then *OK* again to save and close the dialog box.



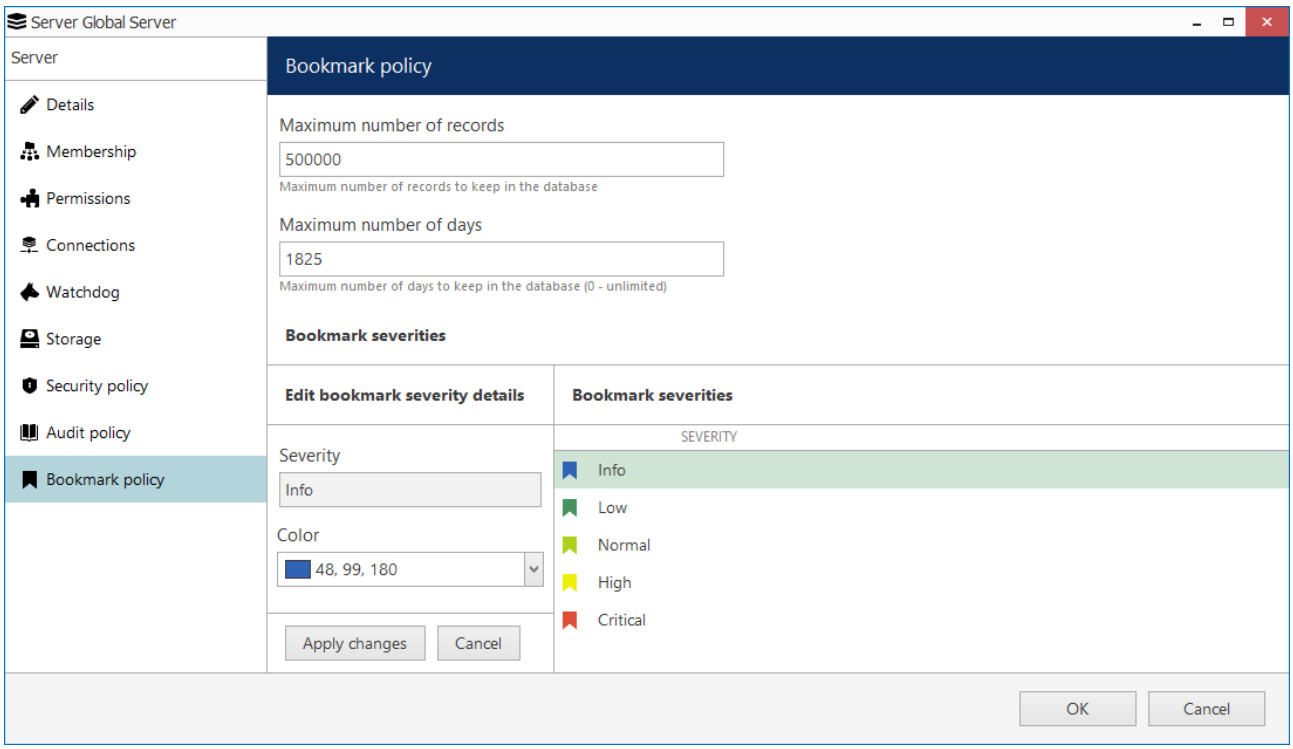
Bookmark Policy

Here, you can set limits for the bookmark database by defining its desired duration and size, and also change bookmark colors for different severity levels. The settings here affect the whole system - all servers, all channels.

The default (and also the maximum) **number of records** (items in the database) is 500000, and they are kept for 5 (five) years. Set 0 days to set unlimited **duration quota** (the items' quota will still have effect).



These limitations were introduced in the software version 1.14.1. Therefore, when you upgrade from an older version, database will be reduced in size by removing the oldest bookmarks so that their number matches the default quota (500000). If the old database contains more than 1 million items, it is truncated and compacted during the upgrade.



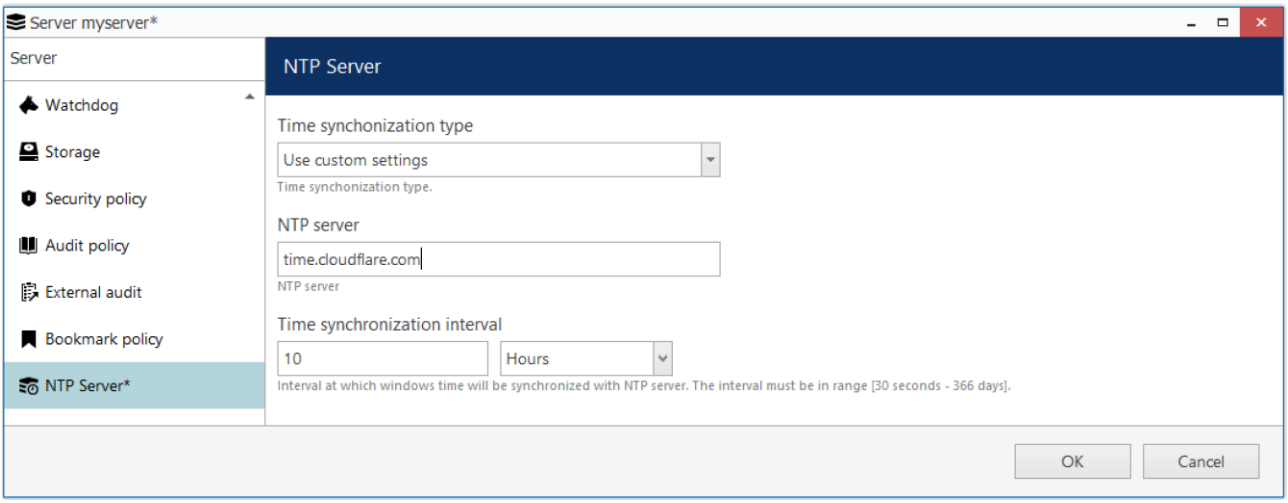
Bookmark **severity levels** were introduced in the software version 1.16.0. Prior to this version, all bookmarks were red and had no ranking; to preserve compatibility with older archive, all bookmarks from the older archive will stay red and have the highest severity, *Critical*. Here, in the policy tab, you can change the colors used for different bookmark labels. To do this, select an item in the ranking list, then choose a color using the built-in picker.

After you change the color related to a certain severity level, all bookmarks with that severity level will start using the new color. If the bookmarks are already opened somewhere (e.g., on the timeline of a Macula Monitor), simply refresh the timeline to see the new color: remove the channel from the view and add it anew. In instant playback mode, switching to live and back will do the trick.

NTP Server

Macula servers use the local machine time. Macula Console provides you with an opportunity to force **sync time** with the specified NTP server.

Essentially, this is the same as configuring the target server OS use the specified NTP server: the time server you set via Macula Console is applied to the underlying OS settings. The only difference is that you can do this remotely via Macula Console interface, without connecting via RDP or other remote control software.



The available settings here are:

- **NTP server**: the target IP or hostname of the time server, local or public
- **Time synchronization interval**: how often to sync the time, choose any desired interval from 30 seconds up to 1 year.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

4.4 Security

All Macula editions have enhanced security aimed at data protection, which includes not only advanced permission management but also encryption wherever possible. Data protection for Macula encompasses database encryption, server-to-server and server-to-clients connection encryption, password protection for the proprietary archive, as well as certain system settings and policies that increase the level of cybersecurity.

The system offers pre-configured security levels, each of which includes a certain preset of security-related features. Some of the security settings are system-wide, and some other can be adjusted for individual servers (e.g., archive encryption).

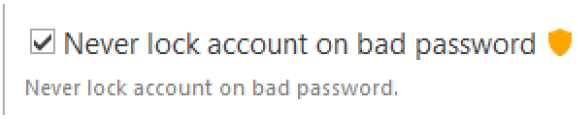
Cybersecurity Dashboard

You can access the cybersecurity dashboard via Macula Console main menu in the top right corner > *Cyber security*.

Four pre-defined **security levels** range from the lowest to the highest. You can choose any level as a basis and, either leave it is it is, or turn off individual security checks.

> ⚠ The security checks for the selected settings mean that these settings are monitored and you are warned trying to assign an inappropriate value. Enabling a certain security level does NOT change any of the related configuration parameters!

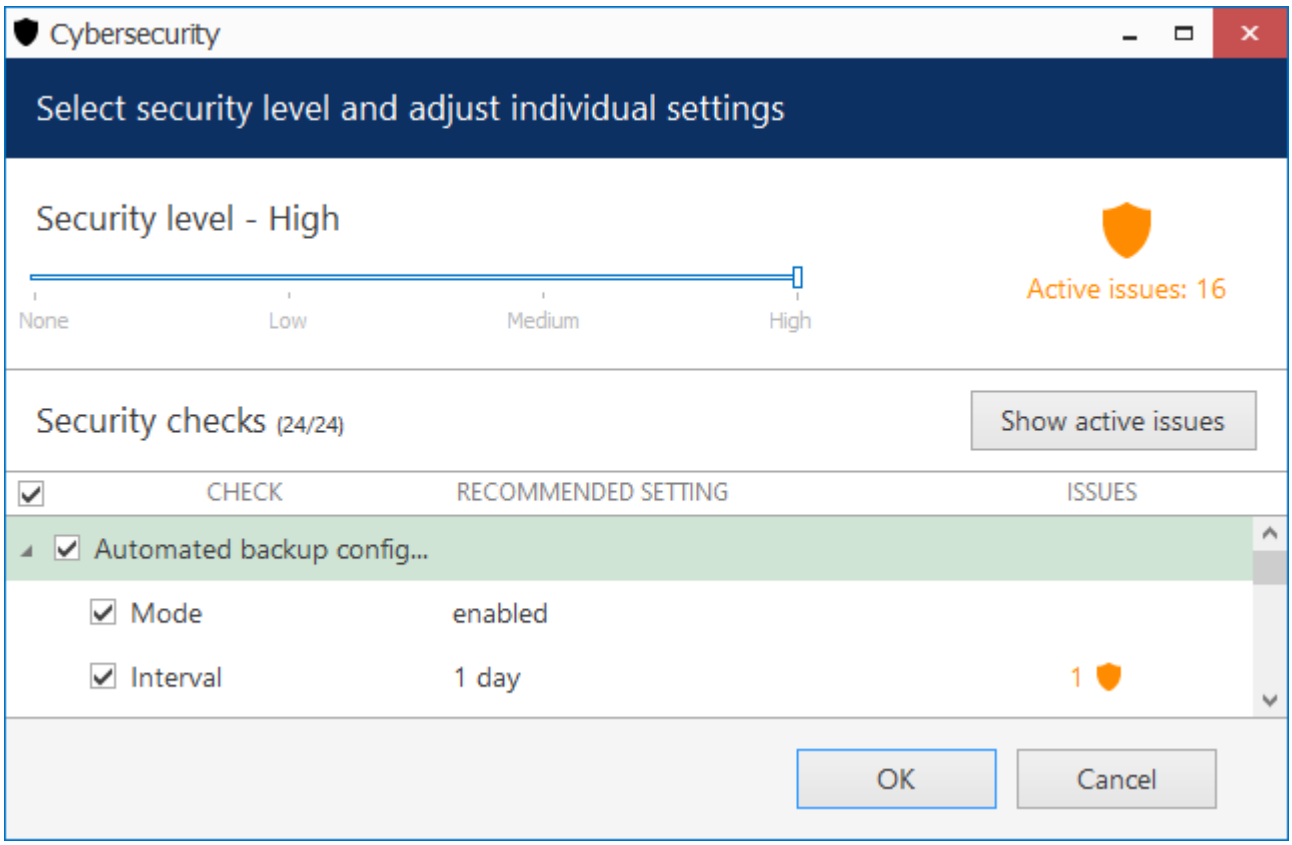
Each security check means that the related setting is tracked and you are notified if it does not meet the security requirements. For example, if the automated backup location is on the same disk as the main configuration file, the backup directory setting in the *Automated backup configuration* dialog box will have a warning shield. Thus, the **selected security level is a set of recommended security settings**, and you are free to ignore the warnings or exclude individual checks from the security profile.



Security Levels

The cybersecurity dashboard will display recommended setting values accompanied by warnings if the current preference is lower than recommended. For some of the checks, the warnings cannot be displayed: this happens if the security check is applied at a certain moment. For example, this is true for the storage and device passwords: the server cannot validate the existing password so the password complexity will be estimated on the password creation step.

Macula® Professional Administration Guide

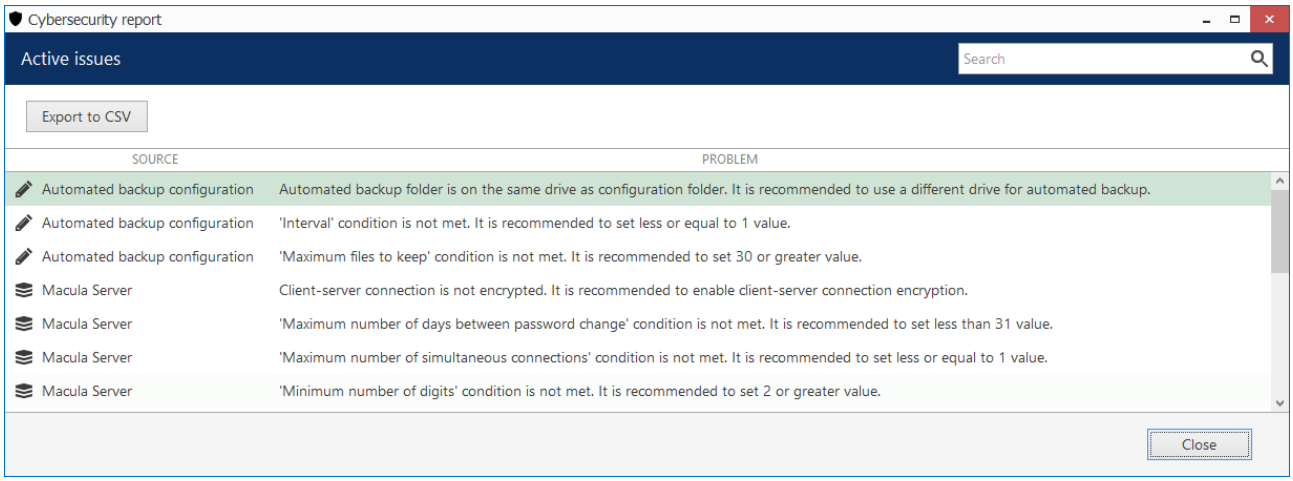


Cybersecurity levels:

- **None**: no security checks at all
- **Low**: only some password policies and server backup settings are tracked
- **Medium**: more of these settings plus user- and device-related settings
- **High**: all possible settings related to security are monitored for maximum system protection

If the security check concludes there are **issues** with the current configuration, you will be notified with an orange shield and offered to **review** the list of issues.

Click the *Show active issues* button to see the list of detected security issues and recommendations on how to get rid of them.



From here, you can save the list of active cybersecurity issues into a CSV file.

Security Checks

The following security checks are available with their corresponding recommended values for different security levels:

Category	Security check	Low	Medium	High
Automated configuration backup	Automated configuration backup mode	Enabled	Enabled	Enabled
	Automated configuration backup interval	Every 5 days	Every 2 days	Every day
	Number of config backup files to keep (max)	1 or more	15 or more	30 or more
	Backup directory is located on a different drive	-	+	+
	Databases to be backed up	-	All	All
Server security policy	Minimal user password length	6+ characters	8+ characters	12+ characters
	Minimum number of uppercase letters in the user password	1+	2+	2+
	Minimum number of lowercase letters in the user password	1+	2+	2+
	Number of previous passwords to remember	-	1+	3+
	Number of days between password changes	-	90-	30-
	Max number of simultaneous connections using the same user account	-	1	1
	Max unsuccessful login attempts before blocking the user account	-	5-	3-
	Minimum number of special symbols in the user password	-	-	1+
	Minimum number of digits in the user password	-	-	2+
Server storage	Check storage password complexity (upon setting the password)	-	+	+
	Storage encryption is enabled	-	-	+
Audit policy	All audit options related to security policy are enabled	-	+	-
Server connections	Client-server connection encryption is enabled	-	-	+
	HTTPS is enabled	-	-	+
Two-factor authentication (2FA)	2FA is enabled	-	-	+
User account	Check password complexity against server policy	-	+	+
	Lock account after N unsuccessful login attempts ("never lock on bad password" option is disabled)	-	+	+

	User password is valid for a limited time ("password never expires" option is disabled)	-	-	+
Device settings	Verify password complexity (upon entering the password)	-	+	+

Some of the security options are hard-coded so it is impossible to disable them (e.g., database encryption) and these are therefore not listed here.

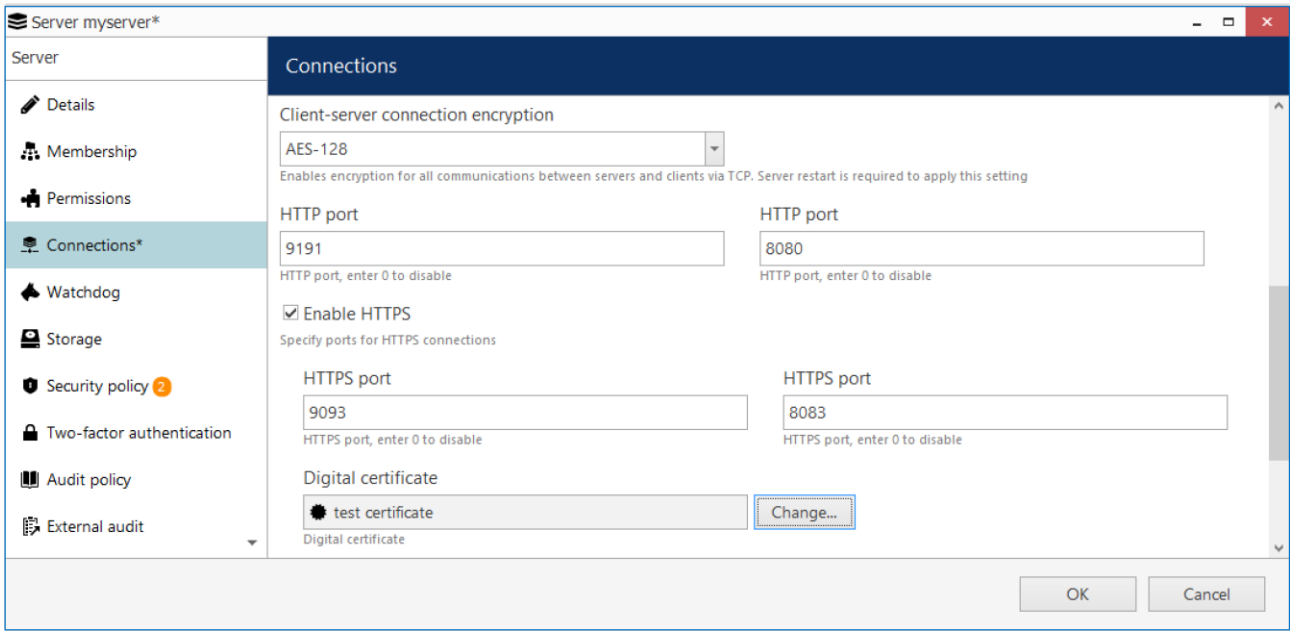
Database Encryption

Macula server uses several databases for storing the server configuration, audit logs and other software data, and all of them are encrypted by default. Once you install the software version that supports database encryption, all the databases are automatically converted to the encrypted format. There is no need to adjust any settings to enable this feature.

> Database encryption was introduced starting from the Macula version 1.8.0 and is supported in all succeeding versions.

Connection Encryption

Traffic encryption is not enabled by default, it can be turned ON in the server settings, in the *Connections* tab. There are separate settings for TCP connection encryption and HTTPS.



Client-Server Connections

This setting affects all TCP traffic between servers and clients, including server-to-server communications in Macula Global.

The currently available encryption options:

- **None**: no encryption
- **AES-128** or **AES-256**: choose the one you need

⚠ When configuring a Macula Global system that has remote servers and clients of version 1.7 or earlier, make sure to upgrade all remote components to the same version as Macula Global so that they support encrypted connections. As soon as it is done, you can safely enable encryption for TCP connections.

HTTPS

Connections from remote Web browser clients and mobile applications, as well as API connections, can also use a secure channel instead of plain HTTP.

To enable secure communications, enable HTTPS in the server settings, then specify desired HTTPS ports (different from HTTP ports) for local and internet connections, and then add the digital certificate you wish to use; you can either use your own certificate or generate a self-signed one right on this step.

⚠ If you are setting up a Macula Global system:

In addition to the setup in the central management server settings, HTTPS should be enabled for each Macula Recording Server **separately**, in the settings of the target server. The certificate, though, should be only added **once**, and then you just need to choose it from the list, when setting up HTTPS on the Macula Recording Server machines.

💡 It is recommended that you use a valid digital certificate signed by a trusted authority instead of self-signed ones. If you use a certificate generated by Macula, your browser will show you a warning.

Archive Encryption

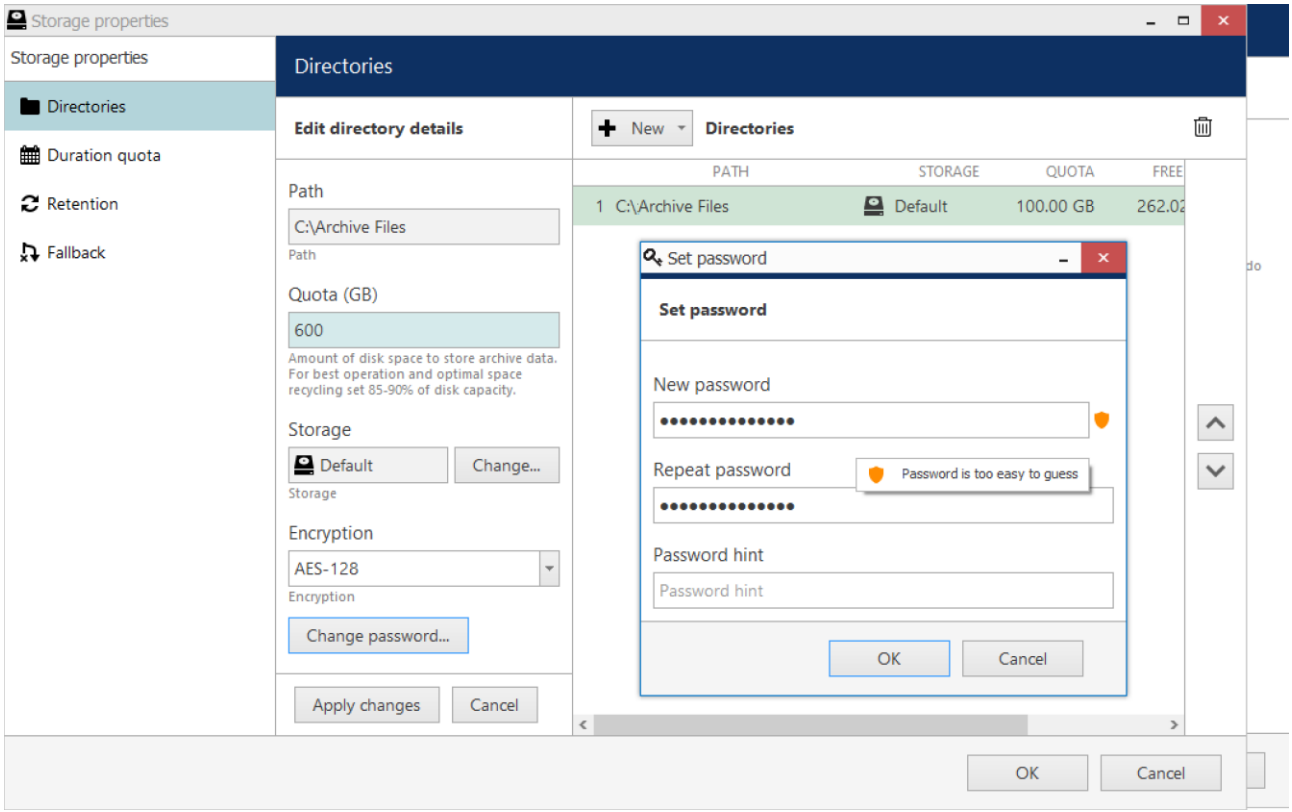
Each archive storage (local or network), as well as archive backups made through the Archive Backup Wizard, can be encrypted. You can provide a different password for every storage unit, and there is also an option to change the password at any time.

Regular Server Archive

To access the archive encryption settings in Macula Console, open the *Configuration* section, choose *Servers* on the left, then double-click the desired server to edit its settings. In the *Storage* tab, click the *Open storage properties* button.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



Click the target storage in the list on the right or add a new local or network storage unit by using the *+New* button above the storage list: its properties will appear on the left. Mark the *Enable encryption* option and specify the password you want.

The currently available encryption options:

- **None**: no encryption
- **AES-128** or **AES-256**: choose the one you need

To **save the changes**, hit the *Apply* button beneath the storage settings, then hit *OK* to close the storage configuration dialog box, and then click *OK* to finally save the storage settings together with the server configuration. Pressing *Cancel* on the last step will revoke the changes in the storage configuration.

When assigning a new password for the storage, make sure to remember it or store in a secure place: you will require it, should you need to access the storage contents in the following scenarios:

- when accessing the archive with the Portable Player tool
- when adding the same disk as a storage unit for another server
- when adding a disk with archive backup as a storage unit
- if you delete the encrypted disk from the storage configuration and then add it anew

There is a field that allows you to enter a password hint, which will be displayed in these situations.

You will not be prompted for the password when accessing the archive from the Macula Monitor application connected to a server with encrypted archive: Macula server will decrypt it automatically.

There is no option to recover the password if you have forgotten it.

Starting from the moment you set the password, all footage recorded to the target storage becomes encrypted; retroactive encryption for the previously recorded archive is not supported. If you wish to have the already recorded data to be encrypted, you can use the replication feature in Macula Global, targeting the replicas to an encrypted storage.

When the storage password is changed, the new password is used for encryption from then on. If storage encryption is disabled for some time and then enabled back, that part of the archive will remain unencrypted.

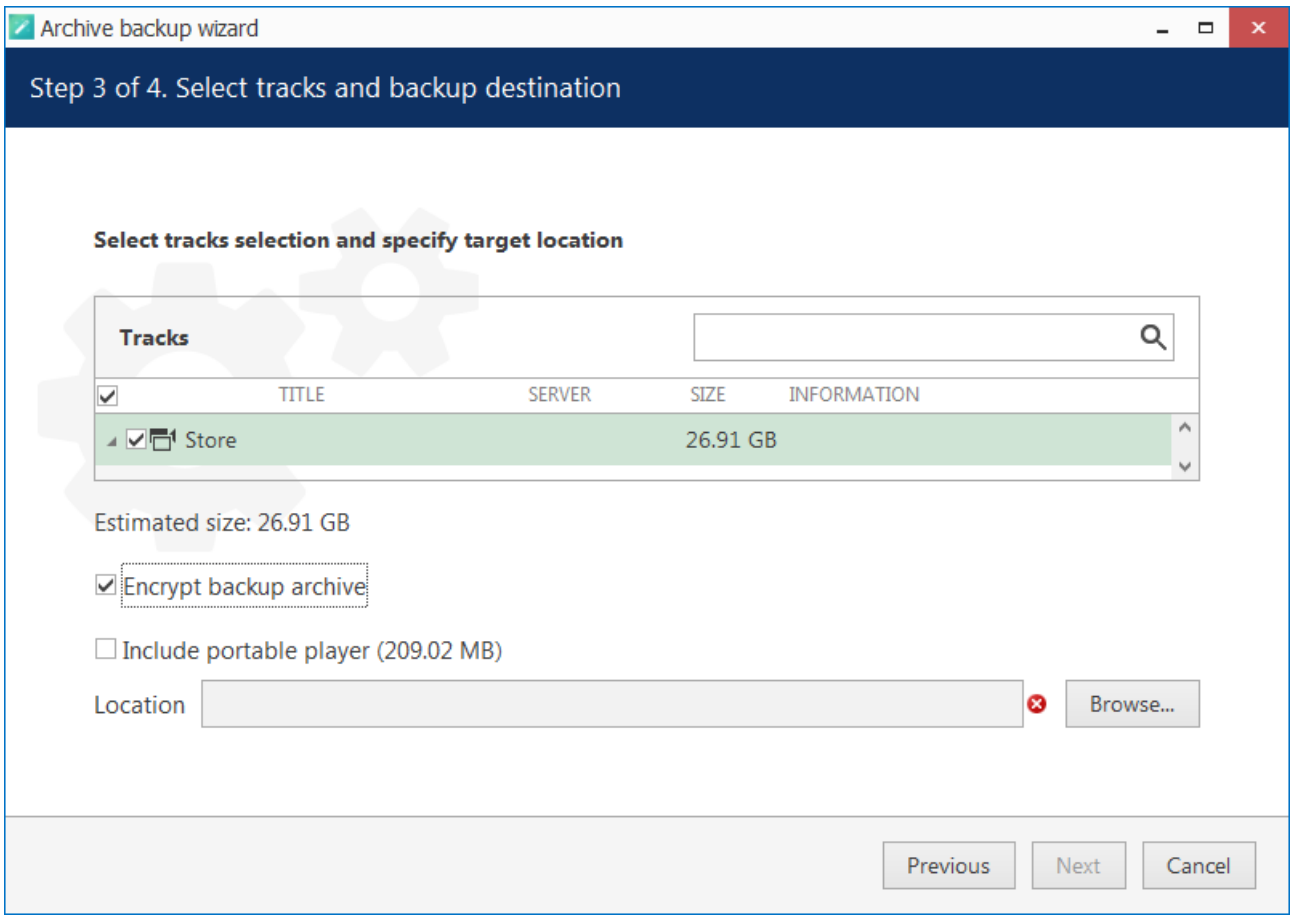
Adding an Encrypted Disk

If you wish to use a storage, which contains encrypted archive, as a new storage unit and add it to the server configuration, you will be prompted for the password. You need to provide the **password** that was used to encrypt that disk. If you have provided a password hint earlier, it will appear as a **tooltip** when hovering your mouse over the password field.

> ⚠ Do not modify the contents of encrypted disks manually, this may result in the corruption of the whole archive.

Archive Backups

The archive backup tool also provides an option to specify a password to encrypt the backup.

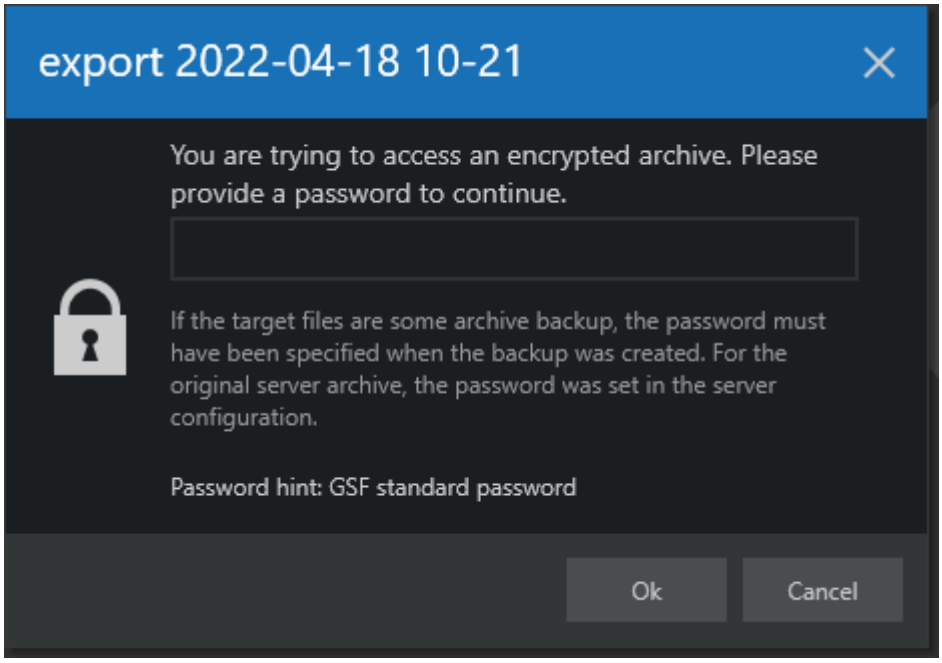


There is no difference if the backup is made from an encrypted or an unencrypted storage; the password provided at this step will be used in future for archive access, whether you read the disk contents using the Portable Player tool or add the disk as a new storage to some Macula server.

Encrypted Archive Access

When accessing an encrypted storage via Macula Monitor and Macula Mobile, the archive is decrypted automatically and provided for browsing according to the user permissions.

Should you want to access a directory that contains proprietary Macula archive or its part (backup) using Macula Portable Player tool, you will be prompted for the password.



If you have specified a hint at the point of setting the password, it will be displayed as text or as a hint when hovering your mouse over the password field.

4.5 Two-Factor Authentication

Macula servers support two-factor authentication (2FA) for the Macula Console and Macula Monitor logins. It is disabled by default, and you can turn it ON via server policies. When 2FA is enabled, all users who want to connect to your Macula server and who are not an exception, will have to enter both their password and a code they receive. Thus, the users prove their identity not just by entering what they know (the password) but also what they have (the email or phone). By default, this policy affects all users; you can disable 2FA for individual users in their permissions.

> At this point, Macula 2FA supports code sending via **email** and **SMS**, and works for Macula Console and Macula Monitor login.

Terminology:

- **session**: an established connection between client and server once the user logs in
- **code**: a numeric code sent to the user's email
- **notification provider**: an SMTP server or a GSM modem that will relay the notification

The **recommended** course of action is: first, create a notification provider, then fill in all the settings, save, and then enable and test 2FA.

2FA Settings

2FA is configured via server settings: in the *Configuration* section, choose *Servers* on the left, then double-click your server to open its properties. In case of a Macula Global system, make sure to open the central management server properties.

The following settings are available here:

Setting	Description	Default Value
Enable two-factor authentication	If selected, additional authentication will be required for server login	Disabled
Set up notification providers	Set up desired providers (using email servers or other means) that will be used for sending out authentication codes	[button]
Session expiration time	During this time period, 2FA will not be requested again if a client was disconnected by server; after this time or after user-initiated disconnect, the user will have to use additional authentication again	1 day
Code expiration time	The time period during which the sent code will be valid, starting from the code send out moment; after this time, the user will have to request another code	00:05:00 (5 minutes)

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Code generation interval	The minimum time interval between two consequent code requests; the user will be unable to request a code more frequently	00:00:10 (10 seconds)
Skip for localhost connection	If enabled, 2FA will not be applied to localhost connection	Enabled
Subject	Message subject line, can consist of text and macros (via right-click)	{SESSION_ID}
Body	Main message part, can consist of text and macros (via right-click)	{CODE}

Name your **notification providers** according to the used verification source (e.g., **Email**) so that the users understand where to look for the code.

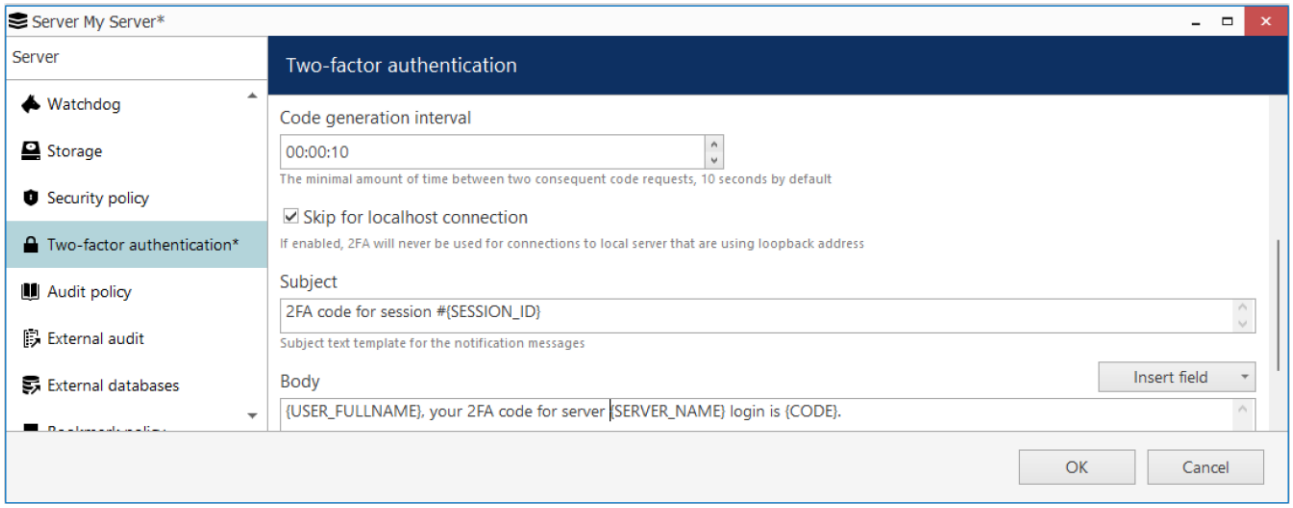
In the verification message, write some text in addition to the session ID and the code so that:
- The user understands which one is which
- The email does not go to Spam

When you try enabling 2FA, you will get a **warning** that you need to test 2FA before saving the configuration. This is necessary to ensure that all the settings are correct and 2FA actually works; otherwise, you or other user(s) may be unable to log into the system at some point. The 2FA verification will start once you click *OK* to save the settings and close the window.

Settings to be verified before enabling 2FA:

- make sure you have added a valid 2FA notification provider (SMTP server or modem)
- add a contact email/phone number for each user
- we recommend that you allow at least one administrative user account to log in without 2FA, or that you disable 2FA for localhost connections: this is to ensure that you do not lose access to the system if your 2FA notification provider fails or becomes unavailable

You can configure 2FA without enabling it, verify these settings, and then finally enable 2FA.



The best approach for 2FA configuration:

1. In 2FA settings, add a notification provider and adjust everything but do not enable 2FA yet, click *OK* to save.
2. Make sure your email server or GSM modem used as a notification provider is valid, and that all users have correct emails/phone numbers in their account properties.
3. Go to 2FA settings again and enable it, then go through the verification.

When you **turn off** 2FA, you will have to go through the setting verification again next time you enable it. If you make changes to the 2FA settings and enable it at once, this test verification will use the previous settings for formatting and intervals (because it happens before saving the settings, and these will not be saved until you pass 2FA successfully).

Two-factor authentication is a recommended setting when you choose the highest cybersecurity level - the system will check if 2FA is enabled and remind you with a warning mark if it is not.

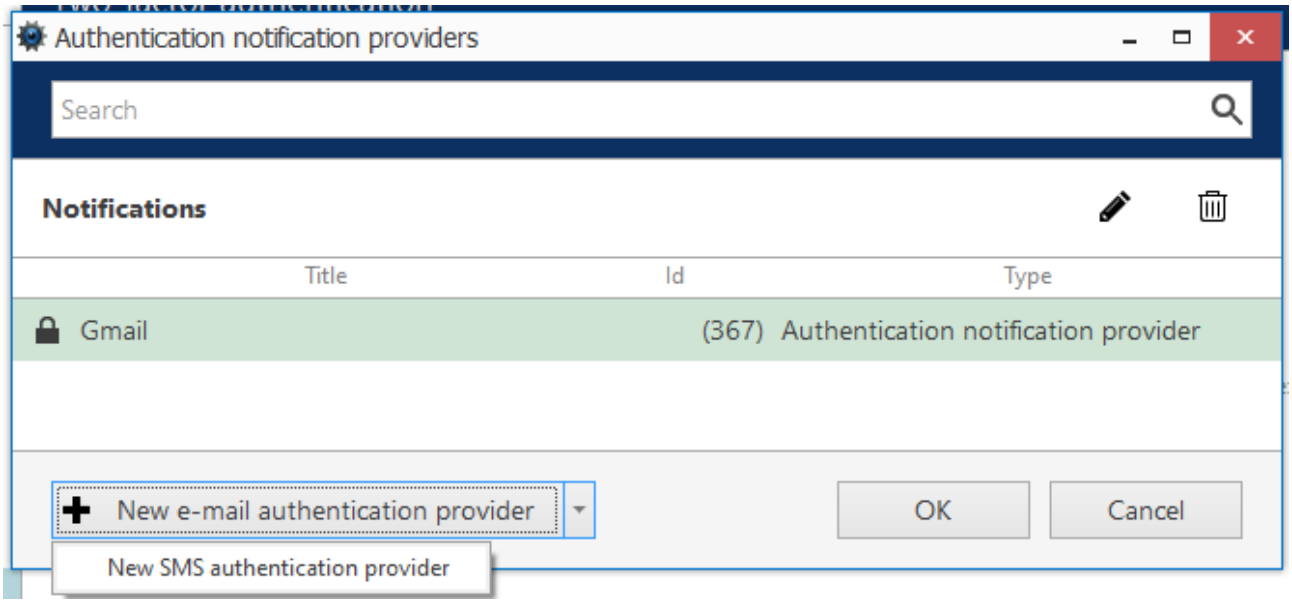
Set Up Notification Providers

You can set up one of multiple notification providers of each kind to give your users an alternative in case one of the providers does not work or is unacceptable for some reason.

To add a new notification provider, click the corresponding button in the 2FA settings. In the dialog box, you will see the list of existing providers (none exist by default). Click the *+ New..* button in the bottom or use the drop-down arrow to see all options.

For each provider, specify:

- **Title**: name that will be shown to the user (so make sure to include the communication means, e.g., Email via Office 365)
- **Mail server**: for e-mail notification providers, choose one of the pre-configured SMTP servers
- **GSM modem**: for messages, choose one of the pre-configured modems



If you have no pre-configured means of notification delivery, add them, and then return to this screen.

Click *OK* to save the provider, then click *OK* to go back to 2FA settings. All created providers will be shown to the user when they try logging in.

> Tip: if some of your notification providers do not work temporarily, add a corresponding note to the provider name. Thus, you will not have to remove it from the configuration but the users will know that they cannot use it for 2FA.

To edit an existing provider, use the pencil button on the top panel; to remove any of the items, select it and then click the *Recycle bin* button. Removed providers will be erased from the list, but the related email servers & modems will be preserved.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

4.6 Third Party Authentication Providers

Macula servers can use external authorization frameworks, such as OAuth, to facilitate user login, allowing your engineers and operators to use their existing accounts to log into Macula servers.

Currently supported authentication means:

- Google account
- Apple ID
- Microsoft account
- Okta
- custom (generic)

You can use public OAuth providers or, if your organization requires so, set up a local custom OAuth service.

> For public OAuth services to work: please reconfigure your system firewall(s) to allow browsers to connect to connect.vmsregistrationportal.com:5001 (allow HTTPS traffic to that port).

To set up user login with external authorization, follow these steps:

1. Add authentication provider(s) of your choice
2. Add user account
3. Activate the user account
4. Log in routinely
5. Repeat steps 2-4 for other users

Below, you will find a detailed description of each step.

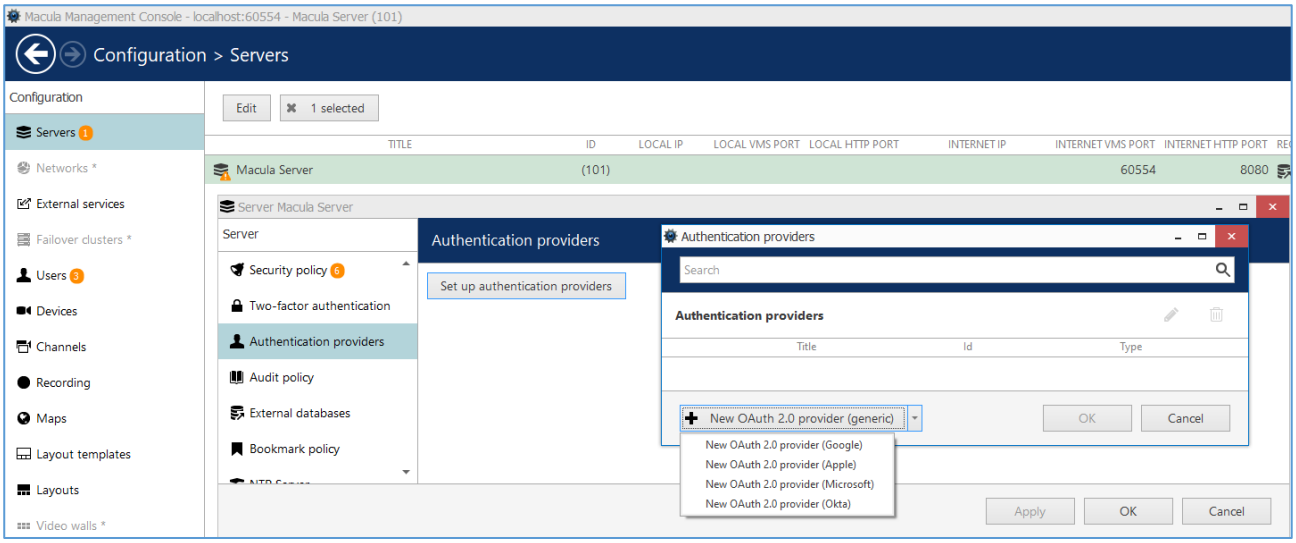
Add a New Authentication Provider

In Macula Console, go to Configuration > Servers > double-click your server (Macula Global server if you are using Macula Enterprise system) > choose the Authentication providers tab. Click the Set up authentication providers button to open the existing provider list.

Choose your desired authentication service from the drop-down list in the bottom part of the window: for example, New OAuth provider (Google) if you wish to use Google accounts.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



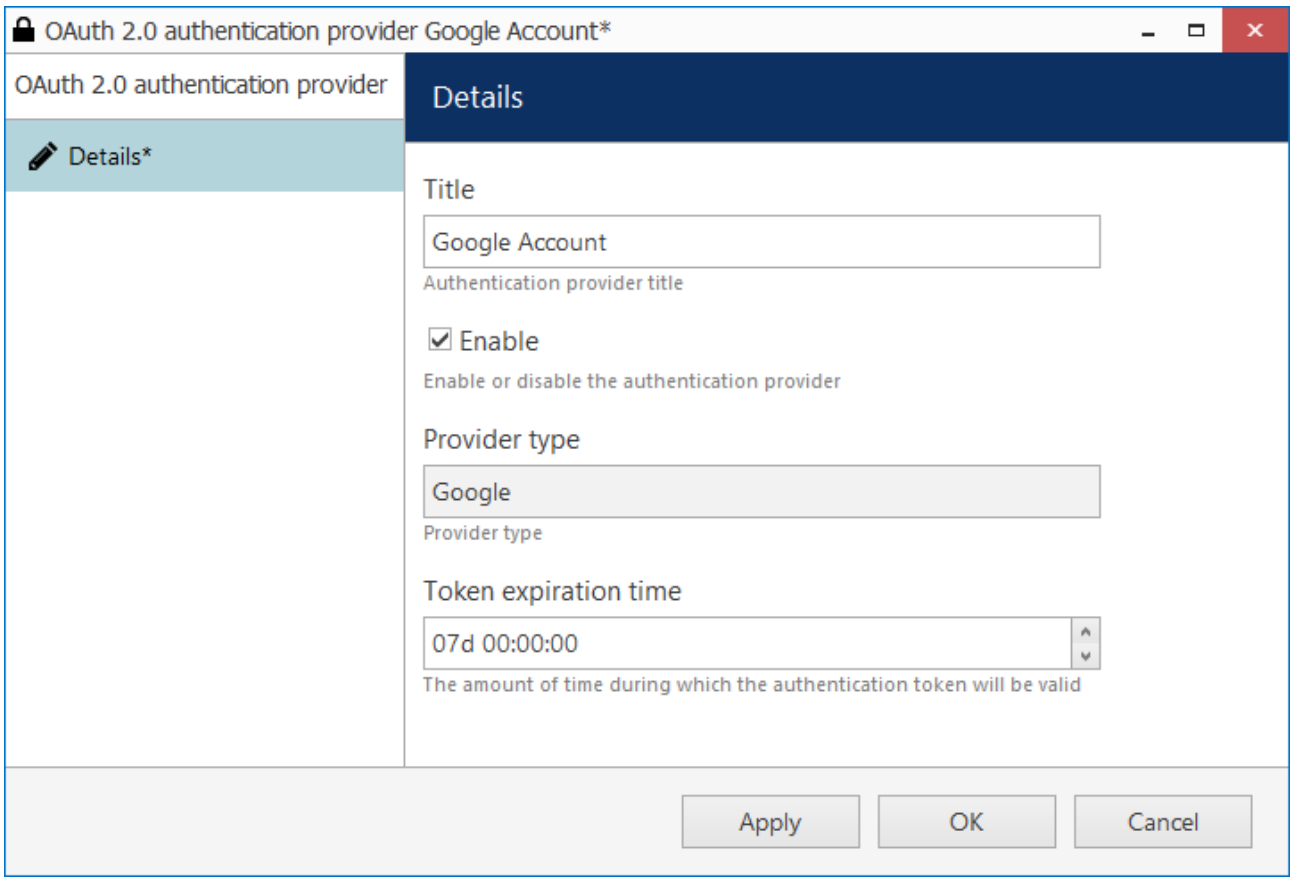
For each authentication provider, different settings are available. For Google, Microsoft, and Apple accounts, the settings are as follows:

Setting	Description	Default Value
Title	User-defined provider name that will be shown	Google
Enable	Enable or disable current authentication provider (use this option to temporarily disable the provider if you do not to remove it)	Enabled
Provider type	[Automatic field]	[Automatic field]
Token expiration time	Time interval, during which the user will not have to enter their password again (session length)	7 days (7d00:00:00)

The token expiration time defines how frequently the users will have to log in again. You may want to set the session expiration time equal to the operators' shift.

For Okta and other (generic) authentication types you must provide additional settings and fill in all the suggested fields. You can retrieve these from the administrator who configured the authentication server.

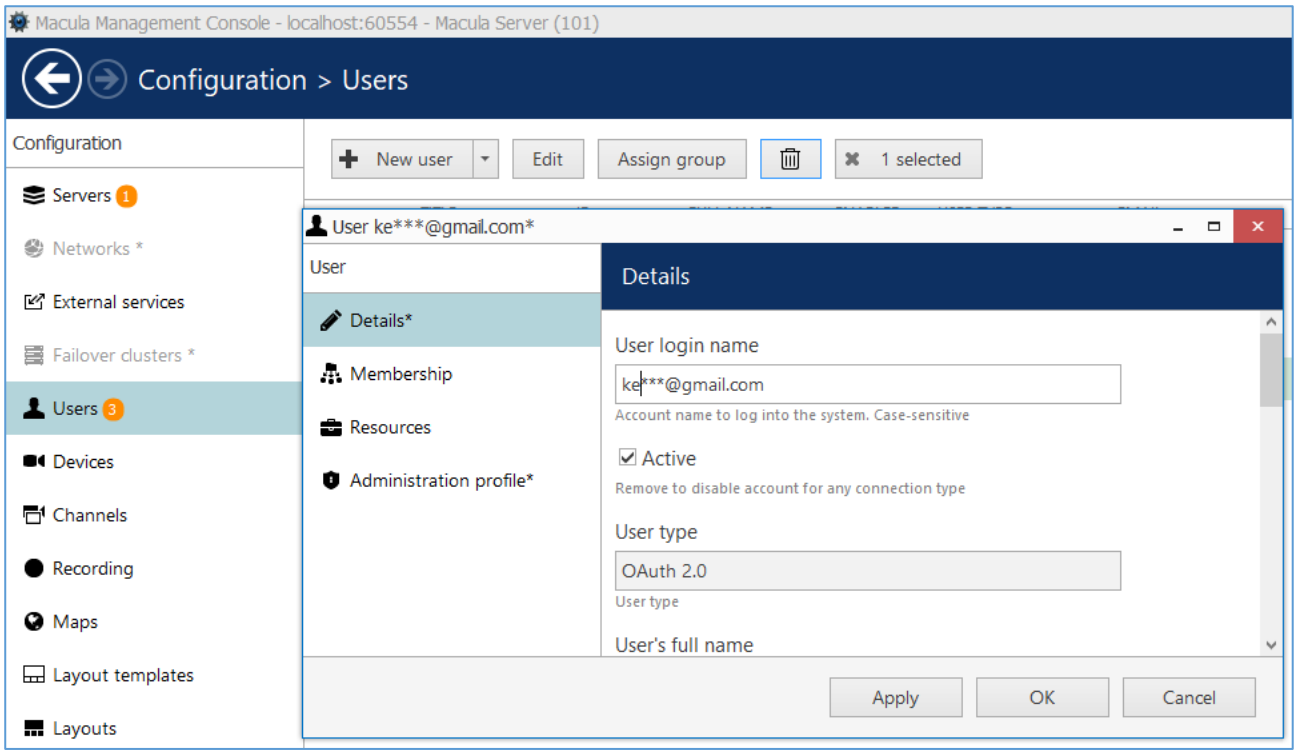
Click OK to Save the newly created provider, then OK again to close the server settings dialog box.



Add Users

In Macula Console, go to the Configuration section and choose Users on the left. Click the drop-down arrow next to the *New user* button and choose New OAuth 2.0 user. It is a special user type for external authorization, which is first created in Macula Console and then activated after the user logs in for the first time, thus binding the internal user to the external authentication means.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Checklist:

1. In the login field, enter the target user's **full login**, which they would normally enter into Google to log in. If the domain name is different from gmail, make sure to specify the full email address.
2. Grant the user the necessary **permissions**.
3. Save the settings, then copy the security **token** and send it to the user - they will need it when they log in for the first time.

After the user logs in, the account entry in Macula will become bound to the external authentication provider, and the security token here will be replaced with security ID. The user's name and full email address will be filled in automatically.

The rest of the settings are similar to the regular user settings.

Login

Users can now log into Macula servers using OAuth via both Macula Console and Macula Monitor. In either case, it is necessary to choose OAuth as login method.

When logging in for the very first time, they will have to enter the user token from Macula Console to bind the accounts. Provide them with the token to ensure they can use the OAuth login method.

5 Devices and Channels

The traditional idea of cameras as surveillance software entities has been developed, resulting in the concept of **devices and channels**. Essentially, it represents the separation of physical and data layers for reasons of security and easier management.

"Device" refers to any piece of physical equipment that serves as a data provider; a hardware piece delivering video, audio and event streams to the server. IP cameras, video encoders, capture boards, USB web cameras - these are all examples of devices that can be added to Macula software. Devices do not include any data streams.

"Channel" refers to any actual video stream (with corresponding audio/event stream, if applicable) delivered to the server from any of the configured devices. Software licensing mechanism counts channels and not devices.

In Macula Console, devices hold camera TCP/IP and user settings, as well as actual hardware model. By contrast, channels do not possess these properties: this allows them to be handled as virtual entities, detaching and re-attaching them from/to devices. Channels feature video stream configuration settings - resolution, frame rate, bit rate and others - as well as all supplementary data streams, such as audio, motion and digital input/output events, PTZ control and camera-side analytics information.

As there are also some multichannel devices, e.g., capture boards and video encoders, each device can have one or more channels attached to it - these can either be assigned or detected automatically; maximum number of channels for each specific device is stipulated by the device model.

Devices only appear within Macula Console, allowing the administrator to apply all necessary configurations. Macula Monitor only displays the channels and does not provide any access to the devices' properties to the end users.

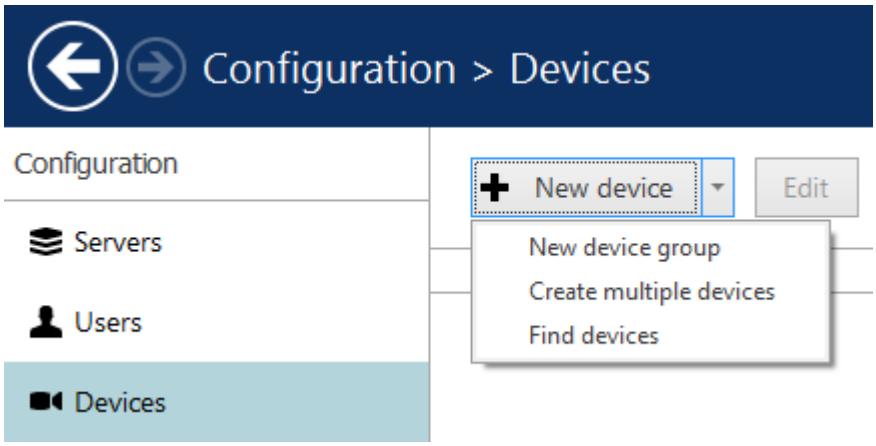
Both devices and channels can be grouped independently. For internal Macula Console management, device groups and channel groups are available; for Macula Monitor channel grouping, visual groups can be used.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

5.1 Add Devices Using Autodiscovery

Use automatic device discovery feature to find all available devices. This method is of great help when dealing with large amounts of cameras, and also when exact addresses of devices are not available.

To access the configuration dialog box from Macula Console, open *Configuration* section and select *Devices* in the menu on the left; in the upper panel, click down arrow near *New device* button and then select *Find devices*.



Scan Parameters

First, select scan mode; the following options are available:

- scan IP address range: specify a continuous LAN segment to be scanned
- scan network adapter address range: select one or more network interfaces to be fully scanned
- scan attached devices: the local hardware system will be scanned for capture boards and Direct Show video sources

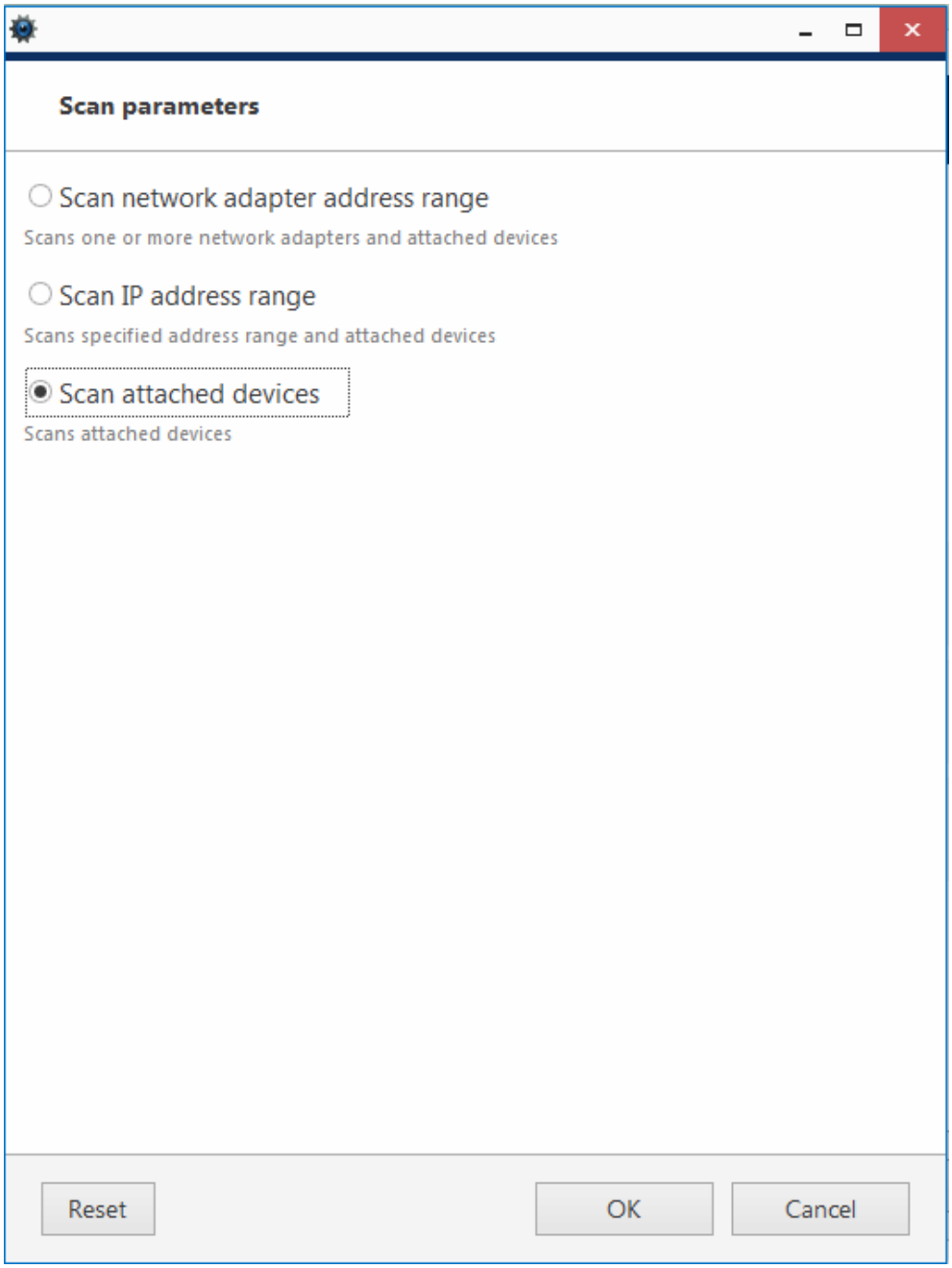
If you have chosen to search for IP video sources, you should review additional connection settings and change or update them, if required:

- ports: HTTP ports, comma separated
- user credentials: pairs of comma-separated user names and passwords, one pair per line

Use the Reset button below to discard all changes and start entering scan parameters again. When you are ready, press *OK* button below to begin scanning.

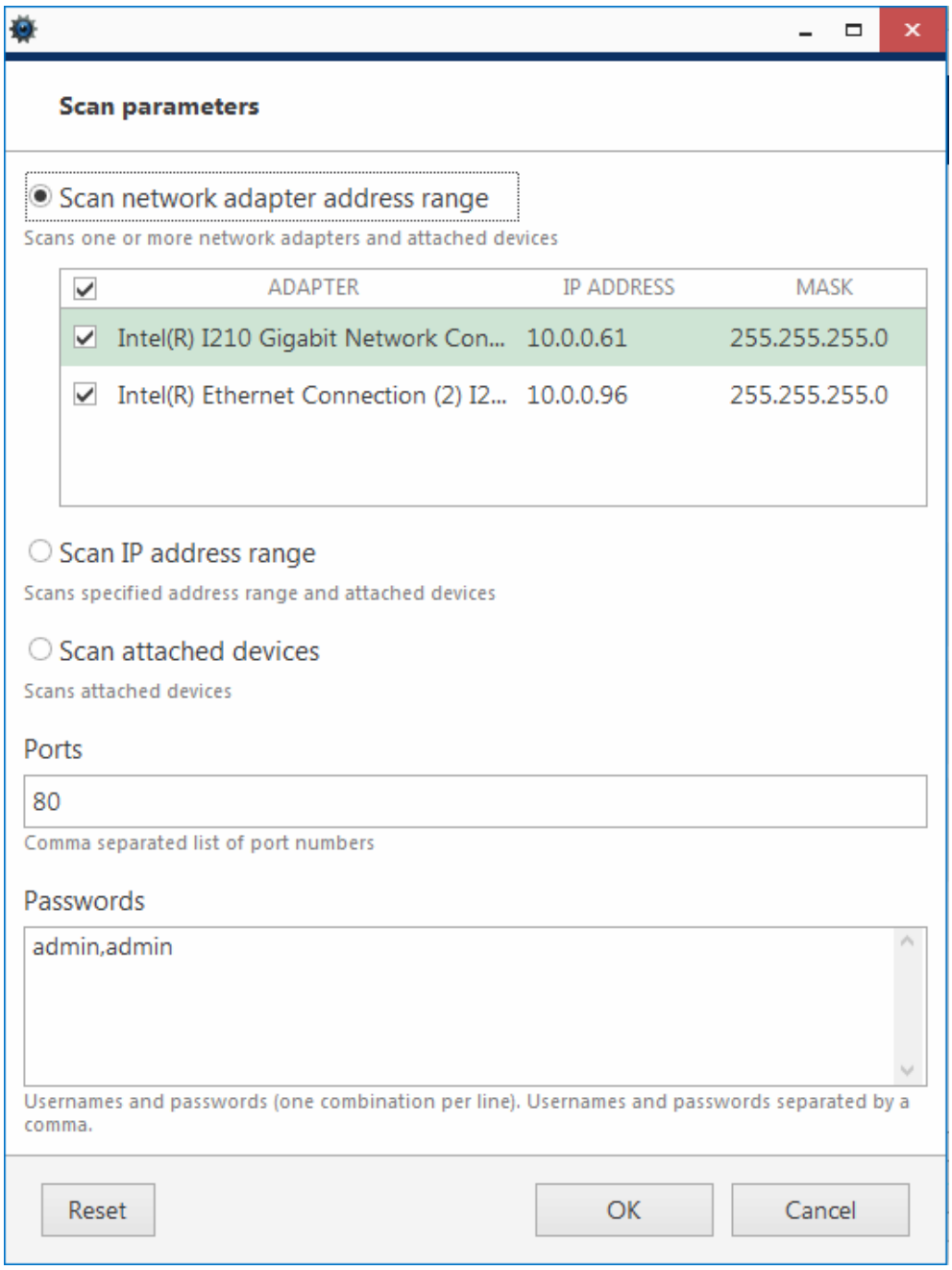
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

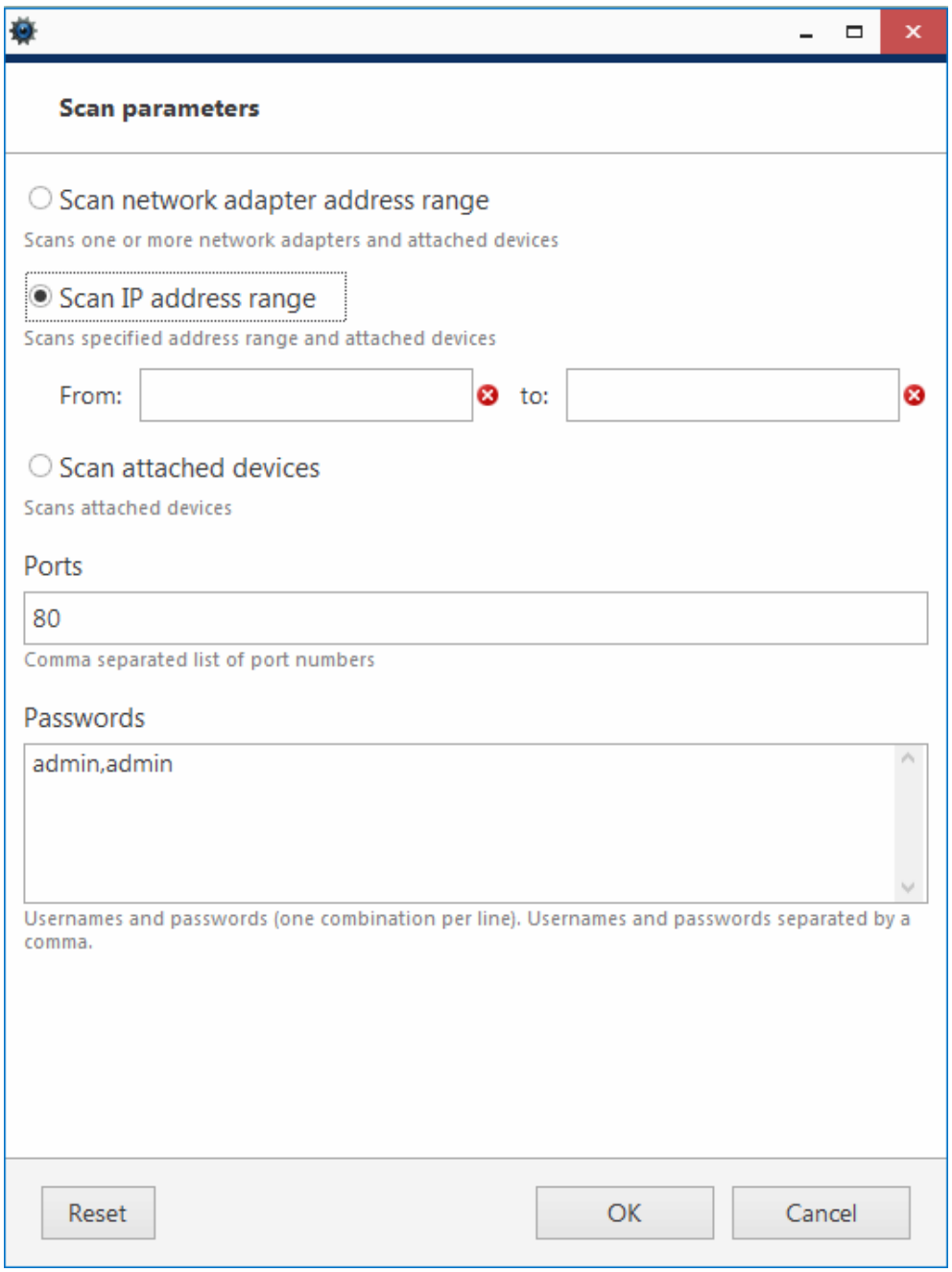
Macula® Professional Administration Guide



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide





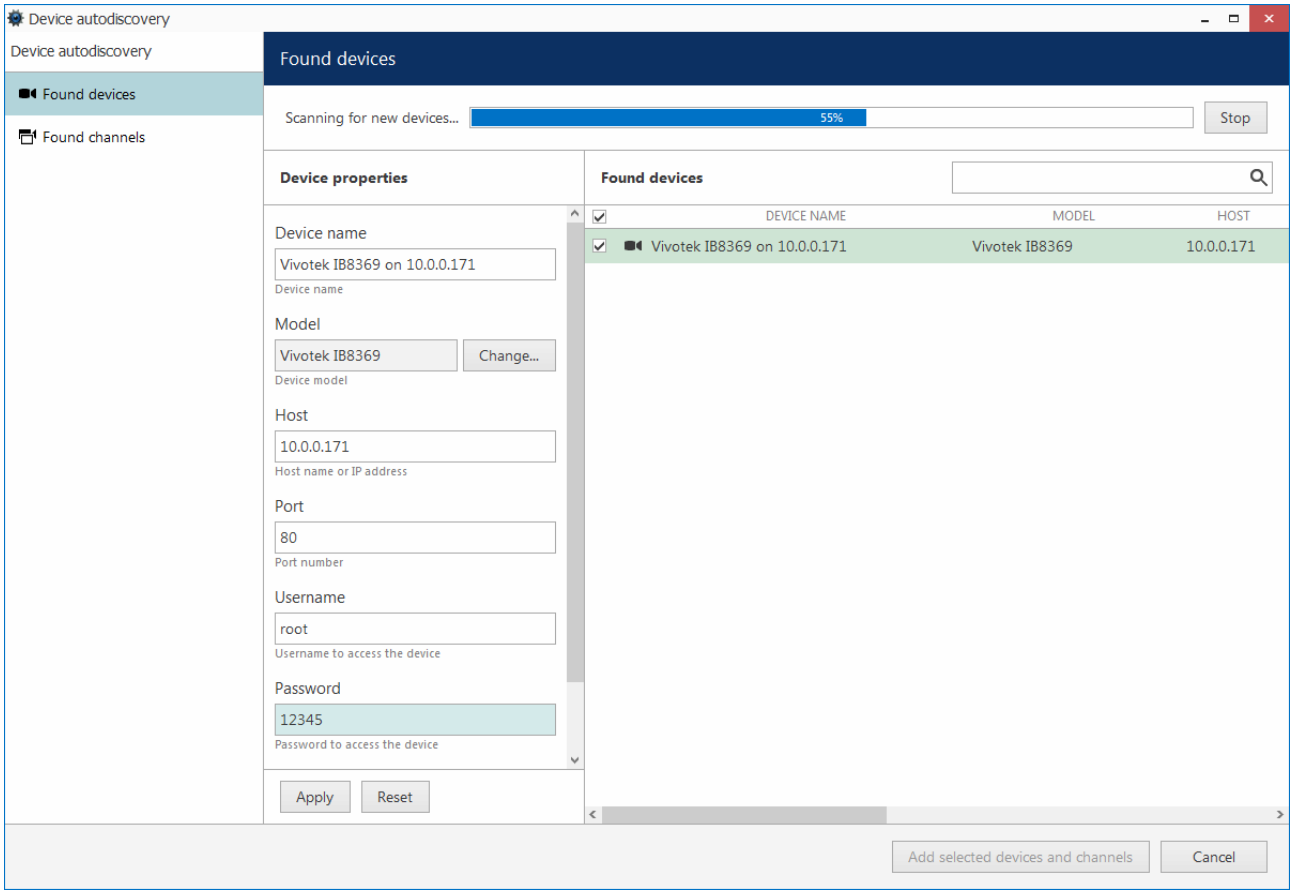
Device Autodiscovery

After scanning has been completed, you will be taken to the Device Autodiscovery dialog box, which will allow you to review the found devices and their channels, and enter/modify related settings. Use the *Search* field in the upper-right-hand corner to find a specific device by name, model, IP, port or hardware ID (for IP devices, ID includes MAC address).

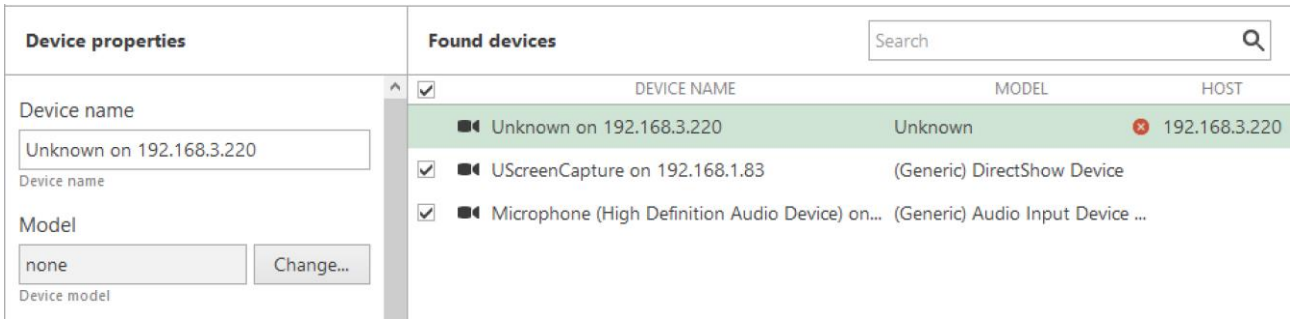
There are two types of selection in the item list: checkboxes and color highlight. **Checkboxes** are used to choose the items to be added to server configuration after you close the dialog box; **highlighted** items are subject to immediate properties changes. Use *CTRL+click* or *Shift+click* to select all or several items at once to change their settings.

Macula® Professional Administration Guide

Click a device in the item list to load its settings into the *Device Properties* window. Note that some settings may be missing for some of the automatically found devices; this depends mostly on device and whether user data was correctly provided. In such cases, simply fill in the missing data manually and click the *Apply* button below to save the configuration changes.



If device is not integrated with the software (native support), it may be detected as generic type (e.g., ONVIF). If you think some devices have not been discovered, check if they have different HTTP ports; also, try adding them manually.



If the device cannot be matched with a model in the list and it also does not respond as generic ONVIF, it may be discovered as *Unknown*; in that case, try settings its model manually to the closest one (from the *Suggested models*), or try Generic RTSP and specify an RTSP URL in the channel settings. This may happen to devices that are not listed as an exact model and are also old enough not to support ONVIF Profile S.

Setting	Description	Default value
Device name	User-defined video source name	Autodetected model + IP, empty if not detected

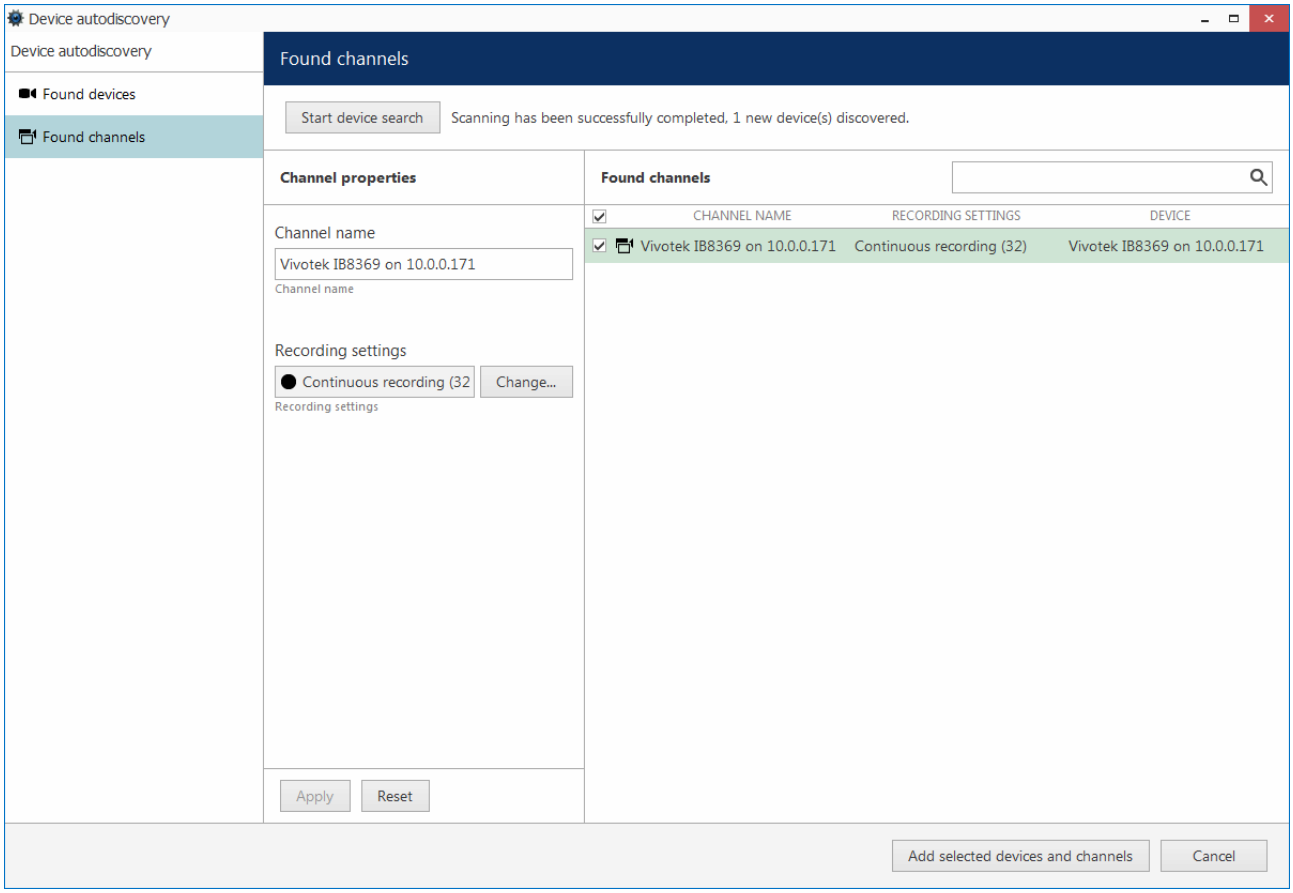
Model	Device manufacturer and model, or generic type	Autodetected vendor and model, empty if not detected
Host	Device IP address	Autodetected
Port	Device HTTP port	Autodetected
Username	Device user credentials; note that you have to provide administrative profile credentials in order to be able to change device settings via software interface	Appropriate username from provided list or autodetected
Password	Device user password	Appropriate password from provided list or autodetected

Make sure you select all the devices you wish to add by putting a checkmark next to them. Devices with missing configuration (model and/or IP) are unchecked by default and will not be added to active server configuration.

⚠ If the autodiscovery **does not find any cameras** or all of them are Generic ONVIF instead of proper models:

- check models
- check IPs and passwords and ports
- make sure that the UPnP Device Host service is functioning properly on your system.

Switch to *Channels* tab to review the detected video channels of the discovered devices: this is particularly important if you are using multichannel devices, e.g., capture boards and encoders. Use the *Search* field in the upper-right-hand corner to find specific channels by name or device name.

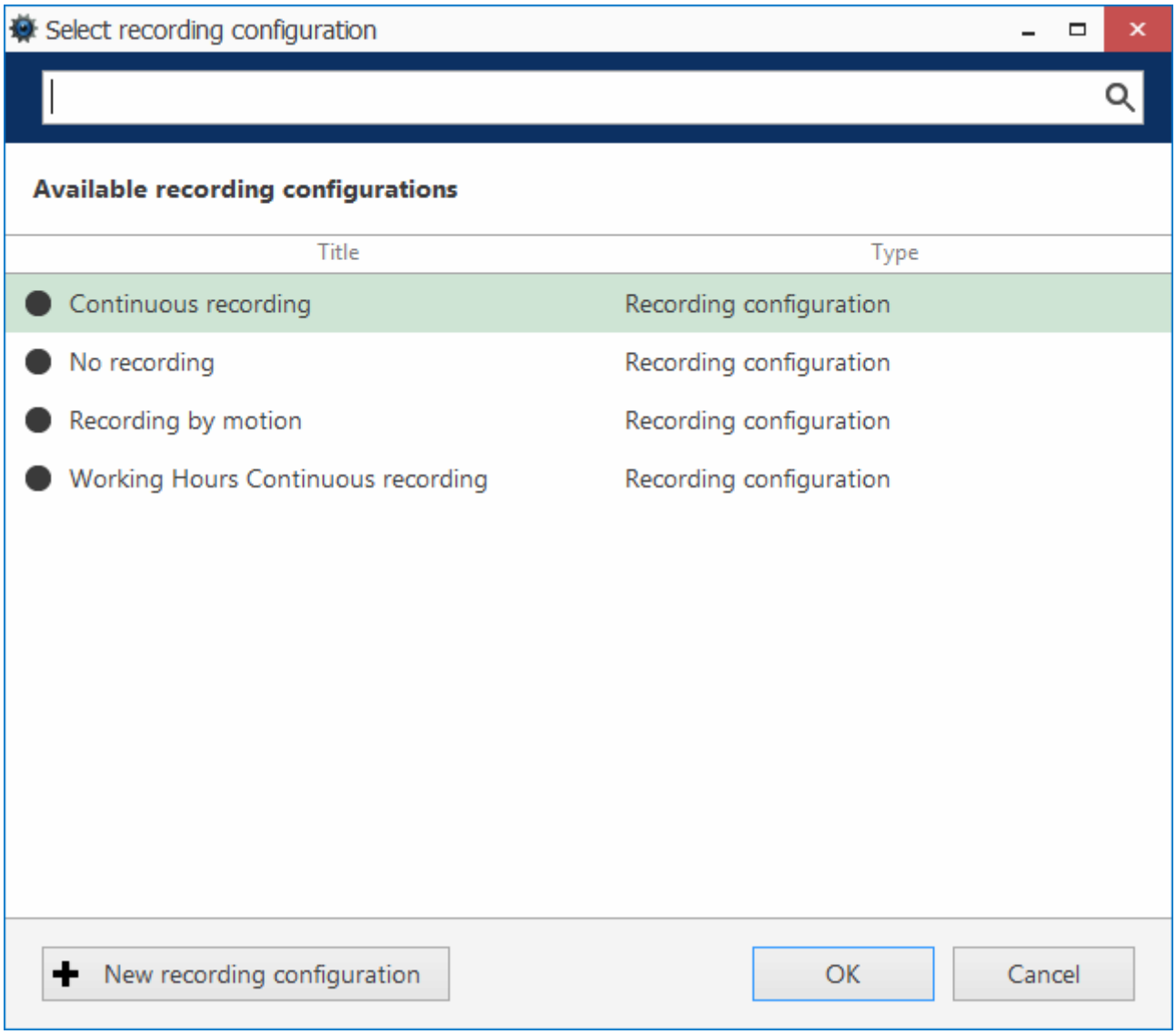


Here you can edit the channel name and assign recording configuration. By default, recording is enabled for all channels: click the *Change* button near *Recording* settings to manage recording profiles and assign

them to your channels. To add a new recording profile, click the + *New recording configuration* button below; you can find more details about recording profiles in the corresponding section. Click *OK* to save and return back to devices and channels; click *Apply* to save configuration changes.

⚠ After changing the channel recording configuration, do not forget to click *Apply*, otherwise the changes will not take effect.

Recording configuration here is assigned to the **main streams** of the target channels. In order to set up substream recording, please go to channel configuration.

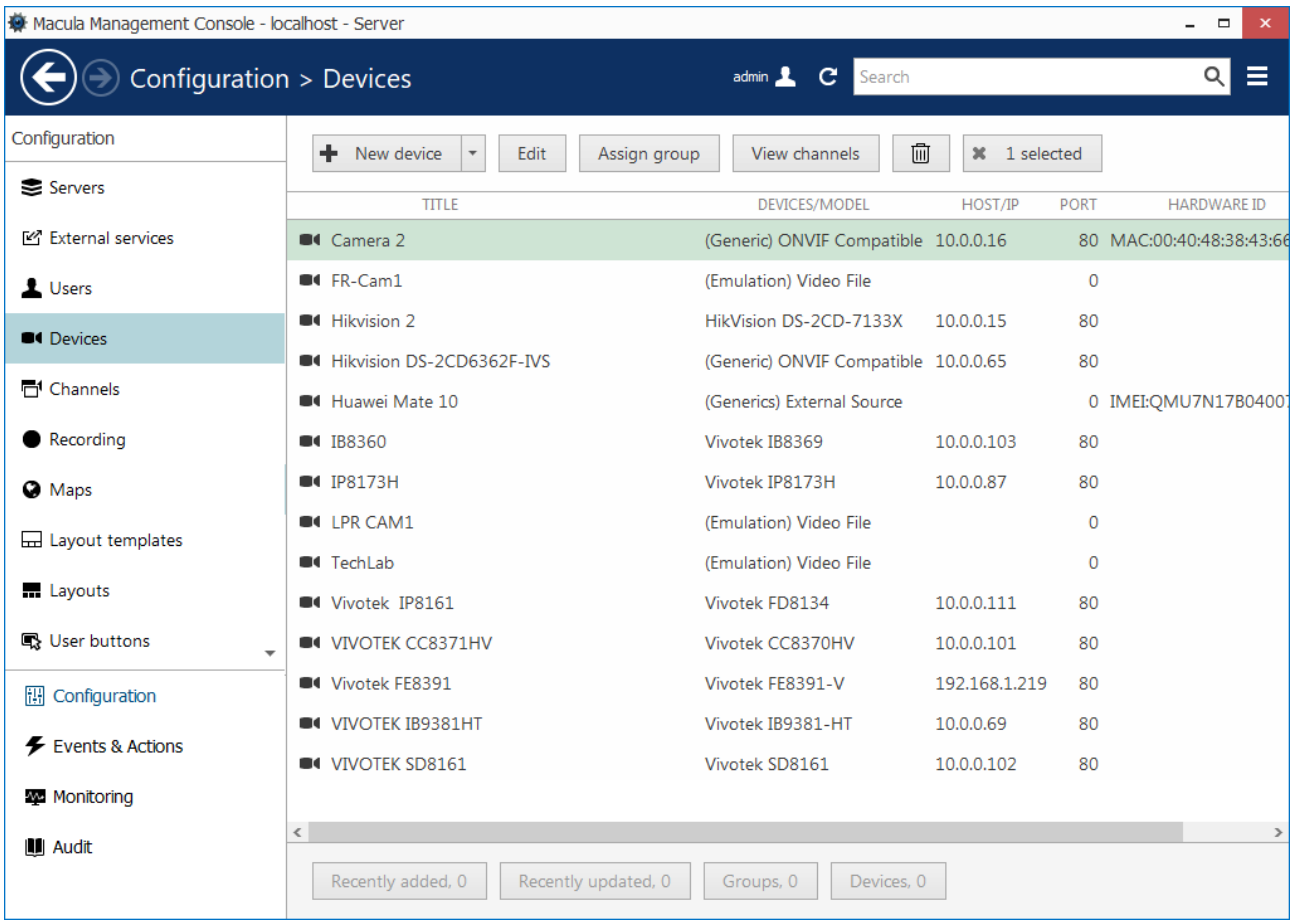


Click the *Start device search* button above at any time to restart device discovery.

⚠ All previously discovered devices and all configuration changes will be discarded if you restart camera autodiscovery.

When you are ready, click the *Add selected devices and channels* button below; all checked devices will be added with selected corresponding channels. Newly added devices and channels will be added to the item list.

Macula® Professional Administration Guide



Use the buttons on the upper panel to manage your devices. You can now add new devices and/or device groups, launch autodiscovery again, assign devices to groups, as well as removing both devices and groups.

> ⚠ When deleting devices, remember that corresponding channels will **not** be **removed** at the same time and therefore your newly discovered devices may not be added due to license limitation. Go to the *Channels* tab to manage them separately.

5.2 Add Devices Manually

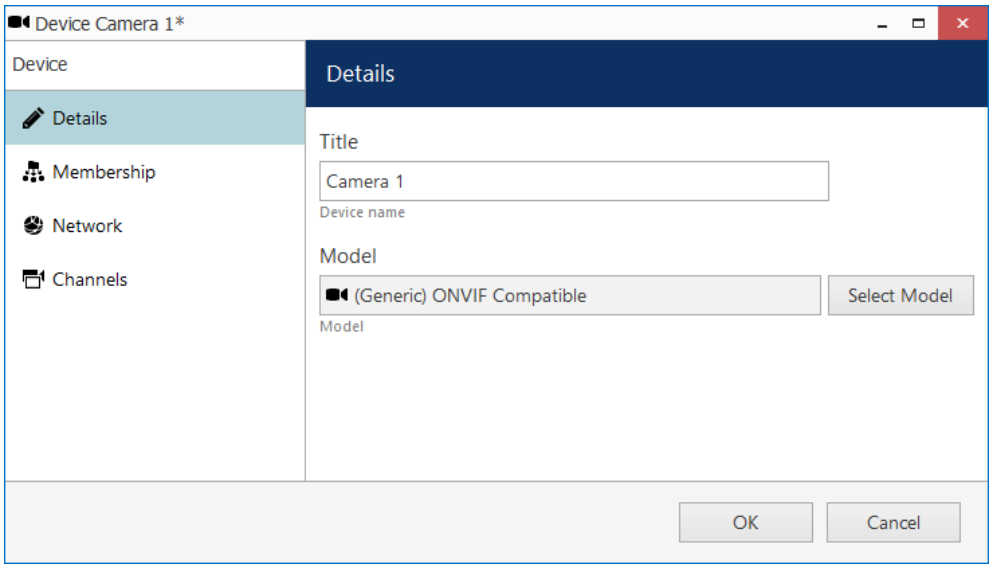
You can add devices manually instead of using autodiscovery in the following cases:

- actual devices have not been connected yet
- devices are not connected at the current stage but it is planned that they will be connected later
- the server needs to be configured while being away from its future position
- some devices in use cannot be automatically discovered

> Only IP devices can be added manually. Attached devices (e.g., capture boards) require autodiscovery.

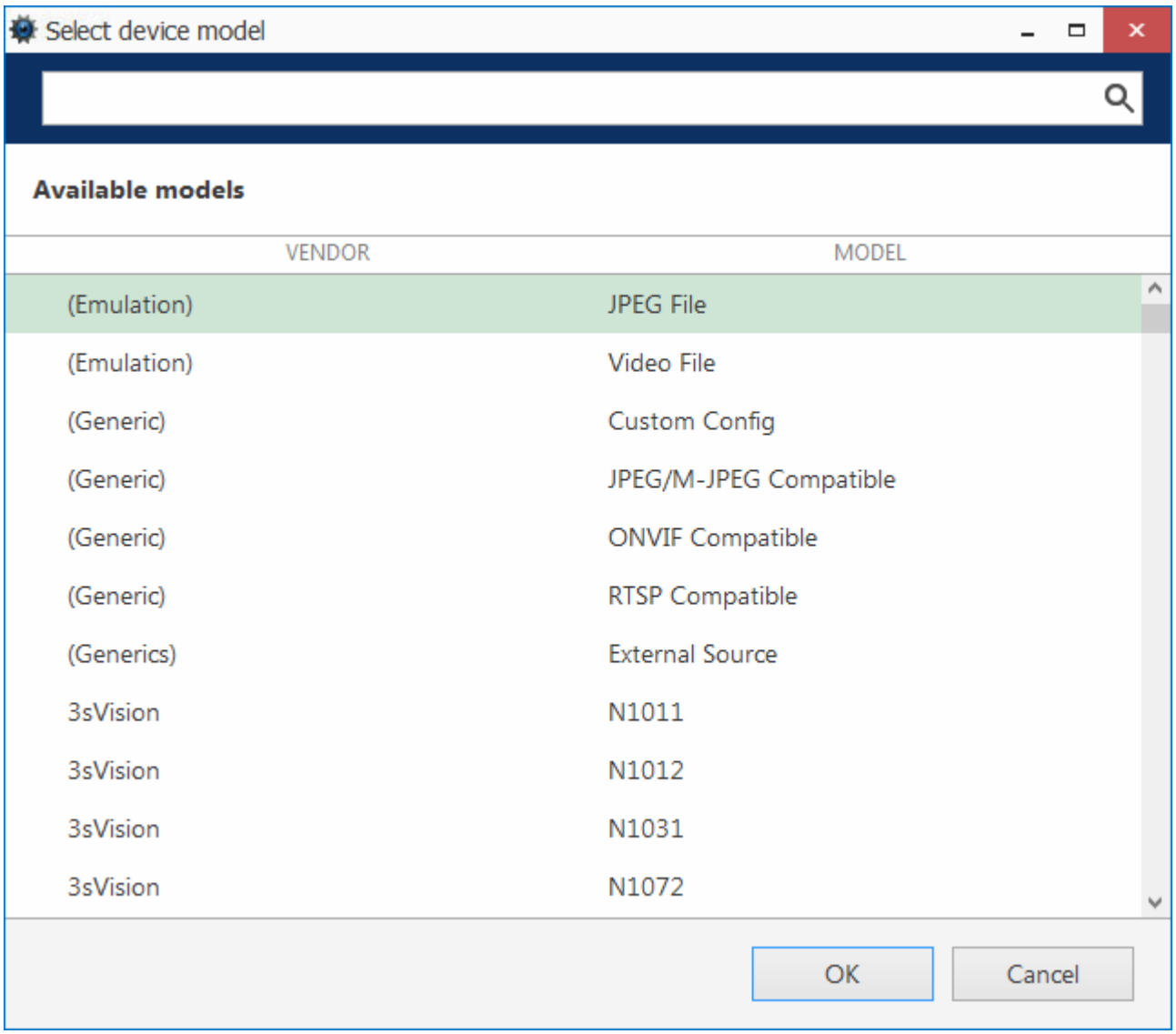
Add single device

To access the configuration dialog box from Macula Console, open the *Configuration* section and select *Devices* in the menu on the left; in the upper panel, then click the + *New device* button.



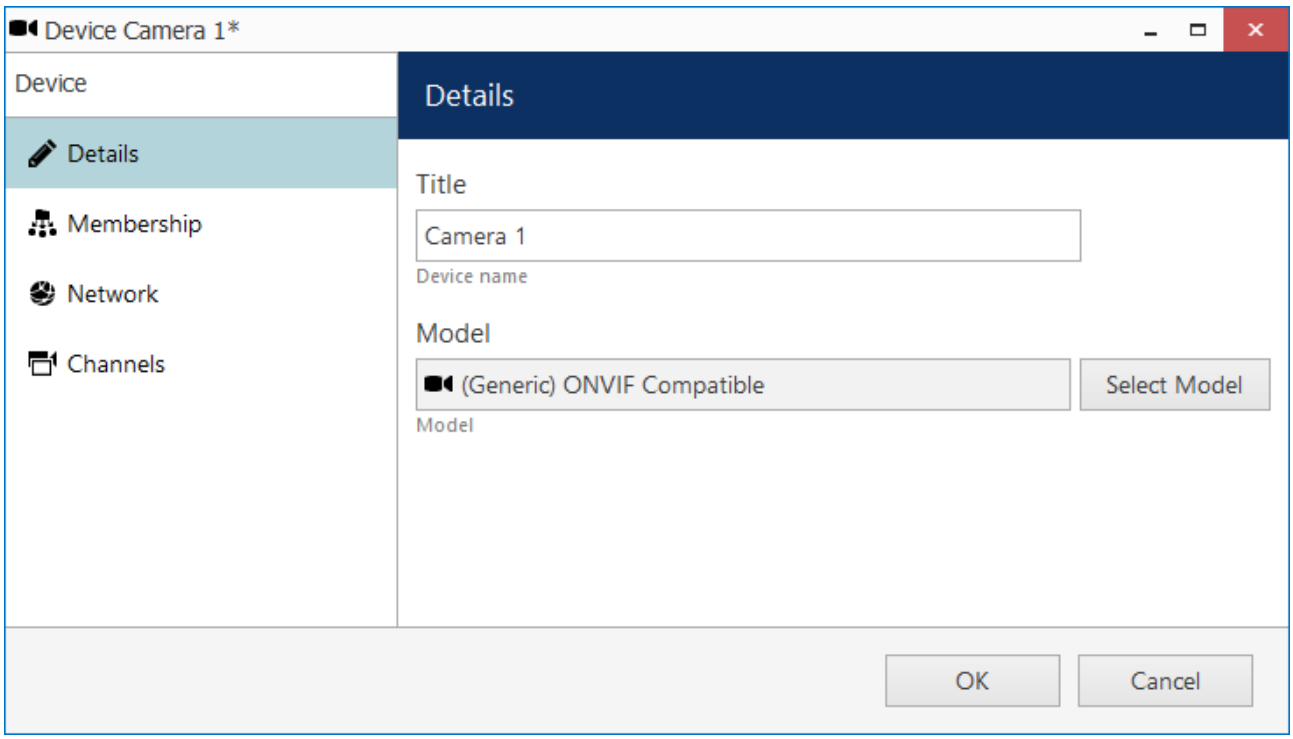
Enter a user-defined name for your new device and pick a model. If your camera model is not listed, select the closest similar model or choose a generic type.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



After you have chosen manufacturer and model, additional tabs will become available in the main configuration dialog box: *Network* and *Channels*. These tabs are described in details later in this section.

Macula® Professional Administration Guide

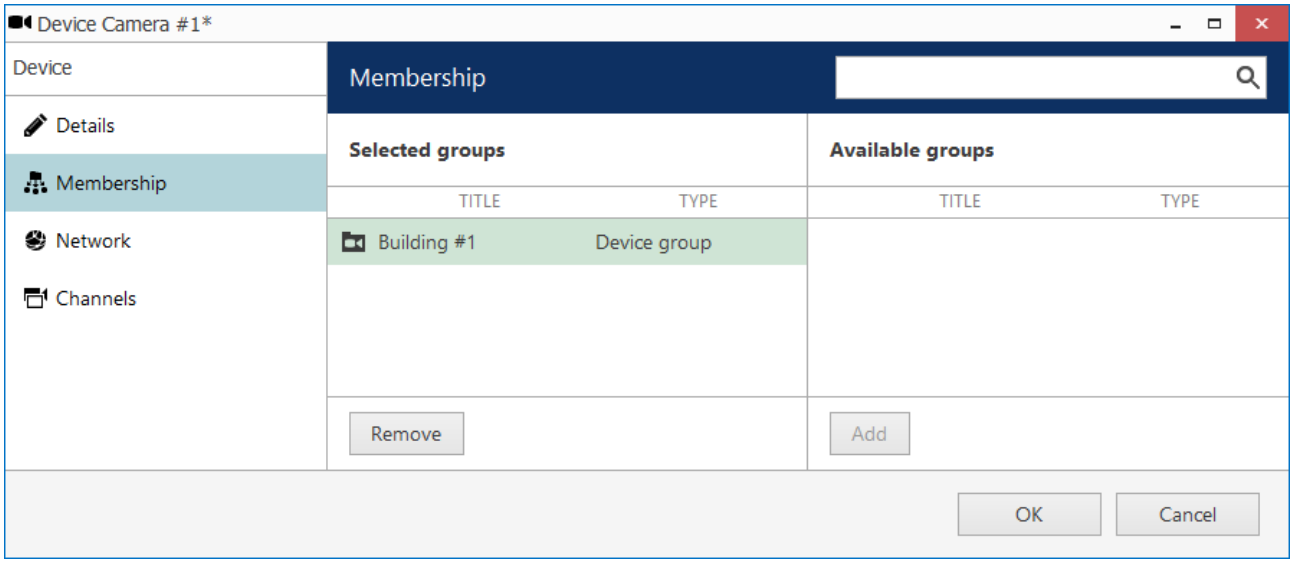


Details

Setting	Description	Default value
Title	User-defined device name	[empty]
Model	IP device manufacturer and model, or generic type	[empty]

Membership

Choose groups for the current device to become a member of. Use *Add* and *Remove* buttons below or double-click to manipulate groups. One device may belong to several groups at once.

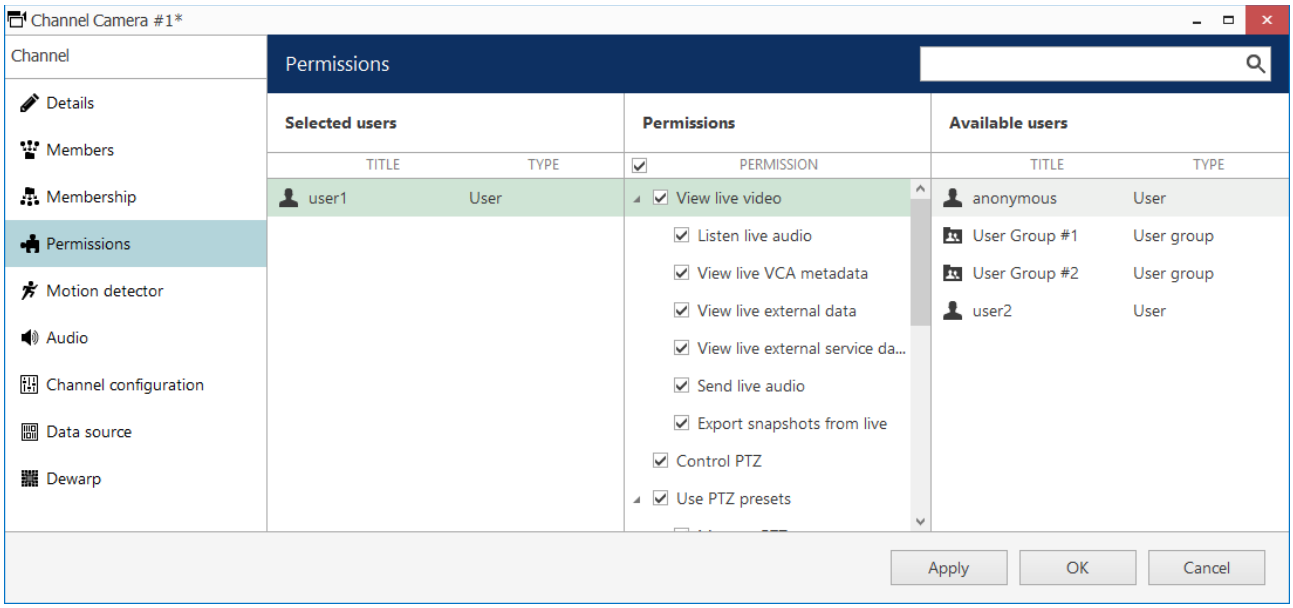


© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

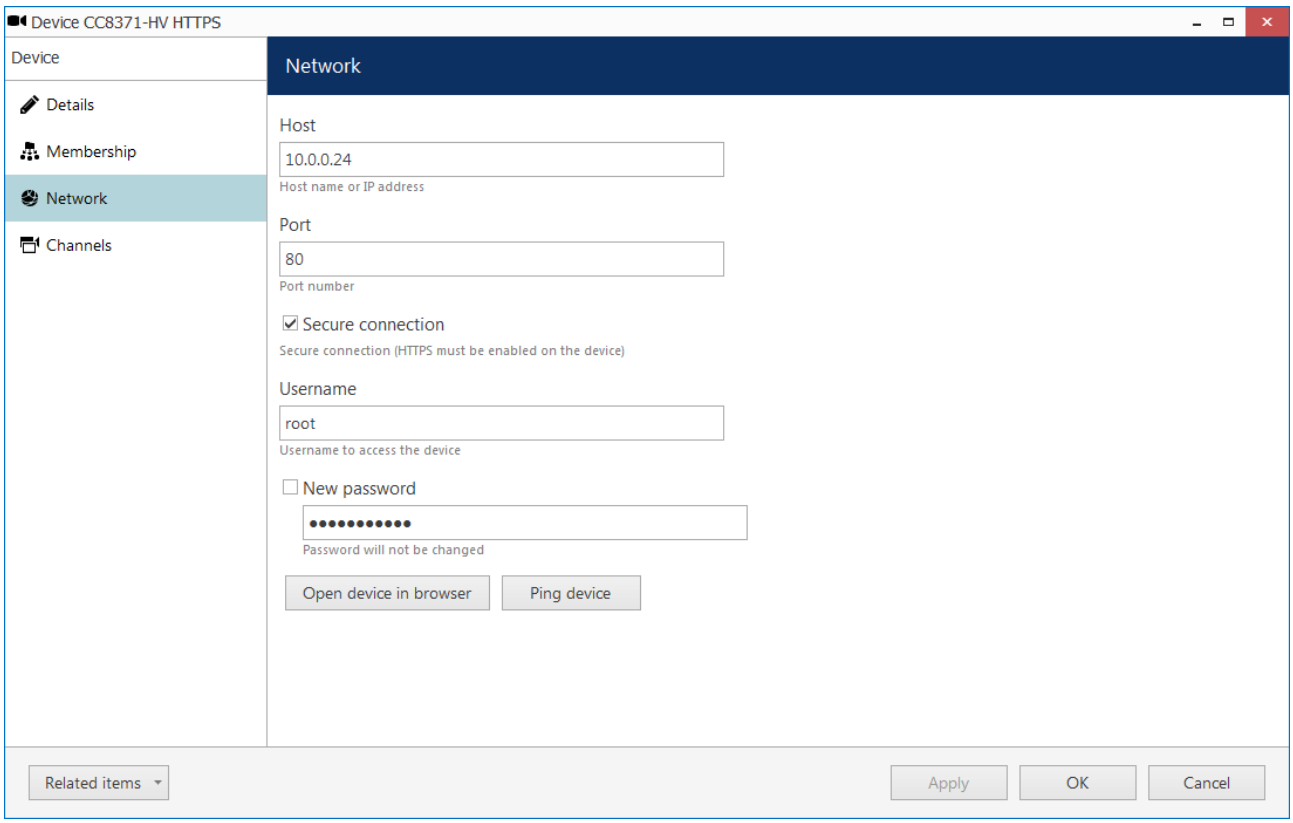
Permissions

Add users and/or user groups simply by checking at least one permission for the target server; remove by clearing permissions - either by deselecting them or by clicking the *Clear* button below. You can also double-click users to remove them from the list of privileged users. Devices with an empty permission list will not be available to anyone except for the root (global) administrator.



Network

Enter TCP/IP settings for device access here.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Before filling in the details, make sure the settings match those on the camera. If device has not been connected yet, ensure that the same settings are applied during the camera installation. You can use the *Ping Device* button to check camera availability and/or verify your settings; the *Open Device in Browser* button will try to reach your camera Web interface using you default browser.

Setting	Description	Default value
Host	Device IP address	[empty]
Port	Device HTTP port	80
Secure Connection	Secure connection (HTTPS must be enabled on the device)	Disabled
Username	Device user credentials; note that you need to provide a valid administrative user profile to be able to change device settings via software	[empty]
Password	Password for camera access	Enabled

In order to enable HTTPS connection:

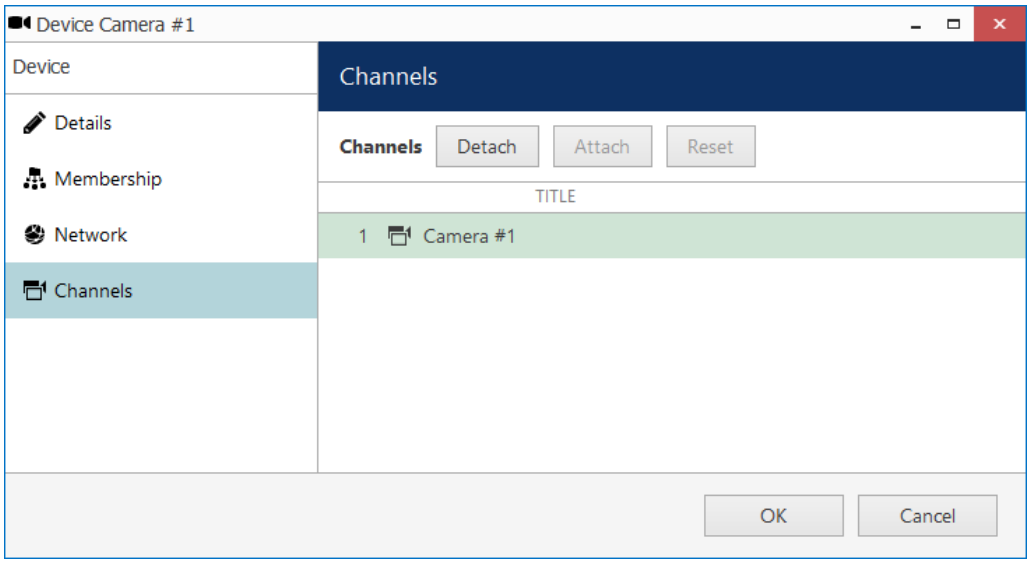
- change port to 443 (or whatever port is used/forwarded for secure HTTP)
- enable Secure connection option

Note that HTTPS must be enabled on the device side for this feature to work properly. On the other hand, if you are not planning to enable HTTPS in the software, disable HTTPS on the device side. Different settings on the device and software side may cause malfunctions (e.g., device metadata will not be available).

Channels

Here you can detach automatically detected channels from the device and replace them with one of the existing 'free' channels (not attached to any device). Use the *Reset* button to undo any changes made to the channels (this only works for current editing session, reset will not be available after you save the changes and reopen this dialog box).

If you wish the original camera channel(s) to stay attached to the device, just leave the channel list as it is.



Macula® Professional Administration Guide

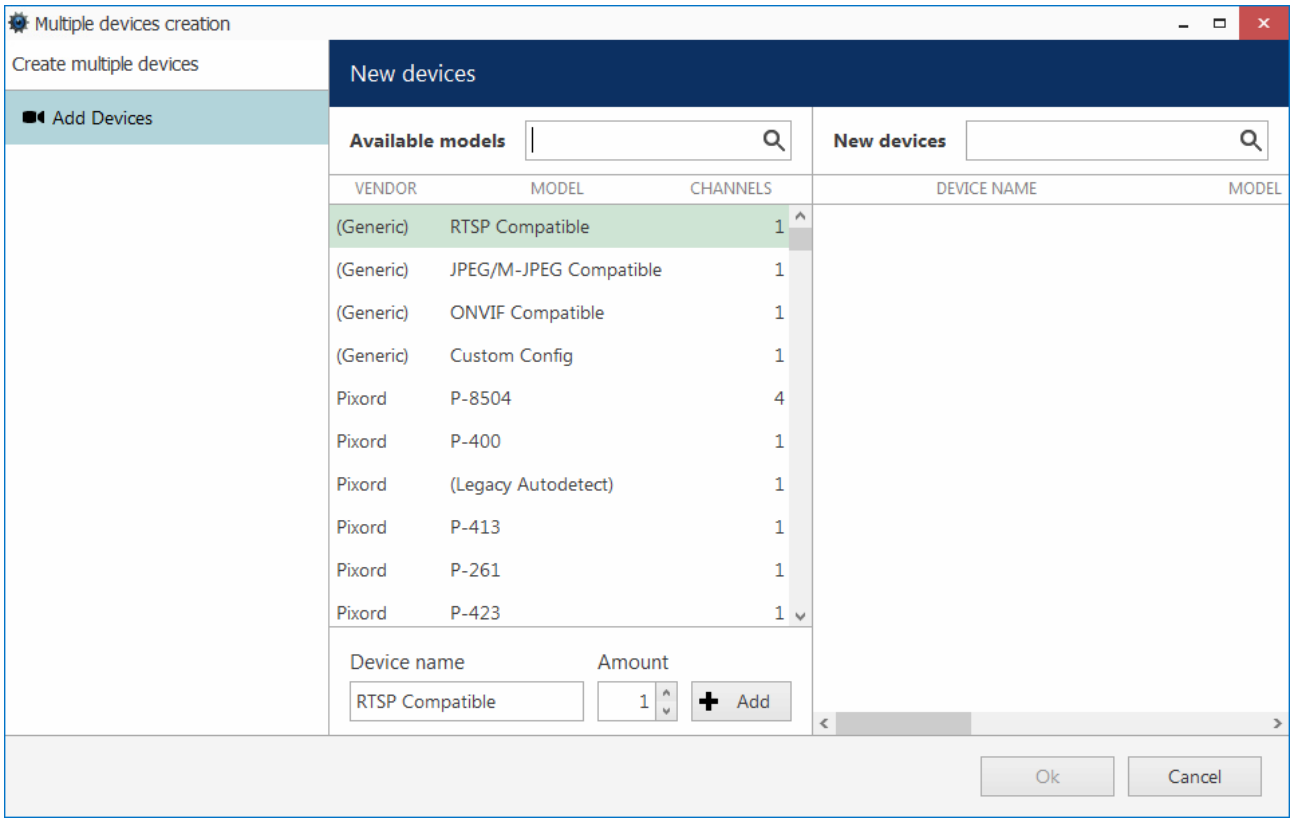
Add multiple devices*

*Feature is subject to license limitations and may be **unavailable in some software editions**.

If you have a number of devices of the same type in your system, you can add them all at once to save time. This method is also suitable is you have multiple groups of devices of the same type.

Open the *Configuration* section and select *Devices* in the menu on the left; in the upper panel, click the little arrow next to the + *New device* button and select *Create multiple devices*.

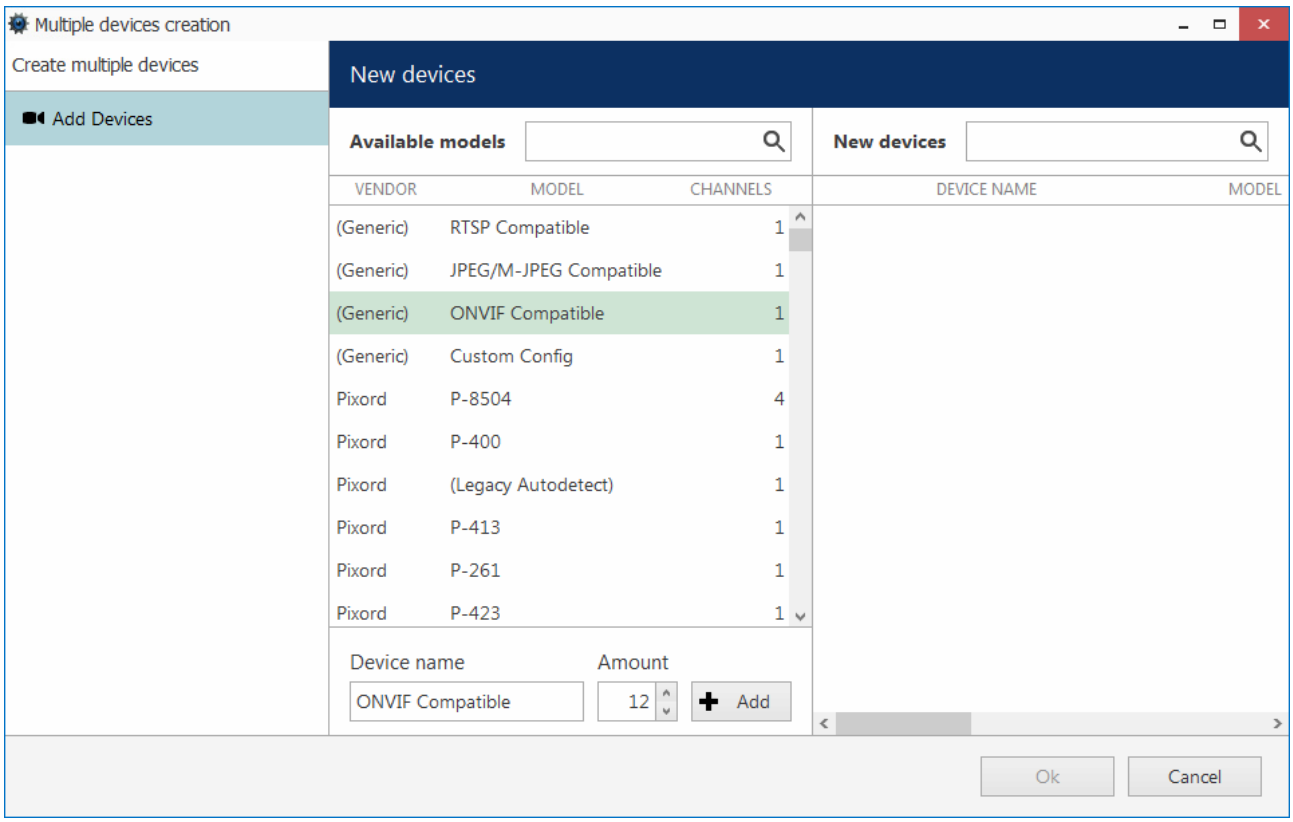
Add devices



You can add any number of different devices here (assuming this is permitted by license limitations). First, select the device model from the list, and then enter your desired number of existing devices of the same model.

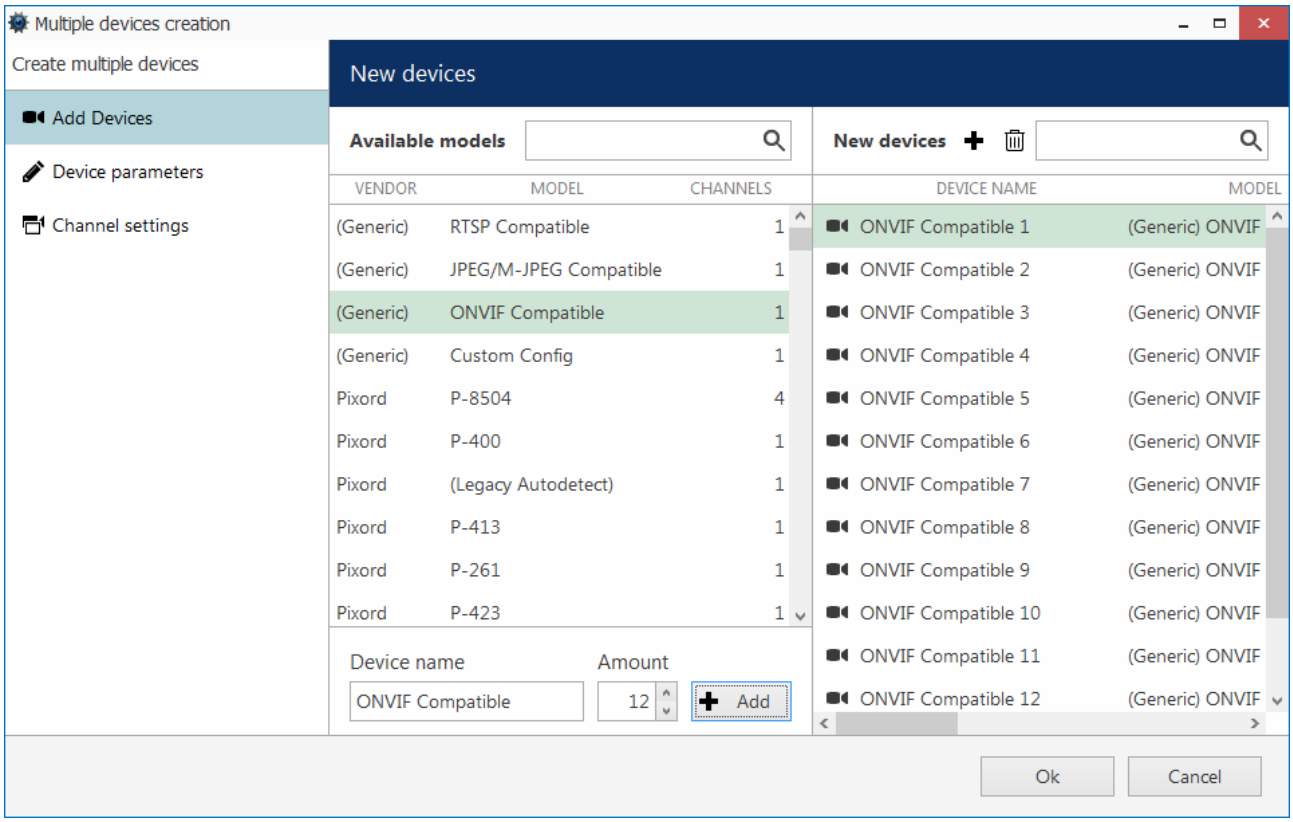
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



When you are ready, click the + *Add* button below to attach the camera set to the new devices list. As soon as there is at least one device, additional tabs will become available: *Device Parameters* and *Channel settings*. Device list on the right will be available in all tabs.

To **remove** any of the listed items, select them with your left mouse button (use *CTRL+click* or *Shift+click* to select multiple devices at once) and hit the *Delete* button on the upper panel or on your keyboard. Select any device and use the ✚ *Add* button on the upper panel to add a copy of that device.



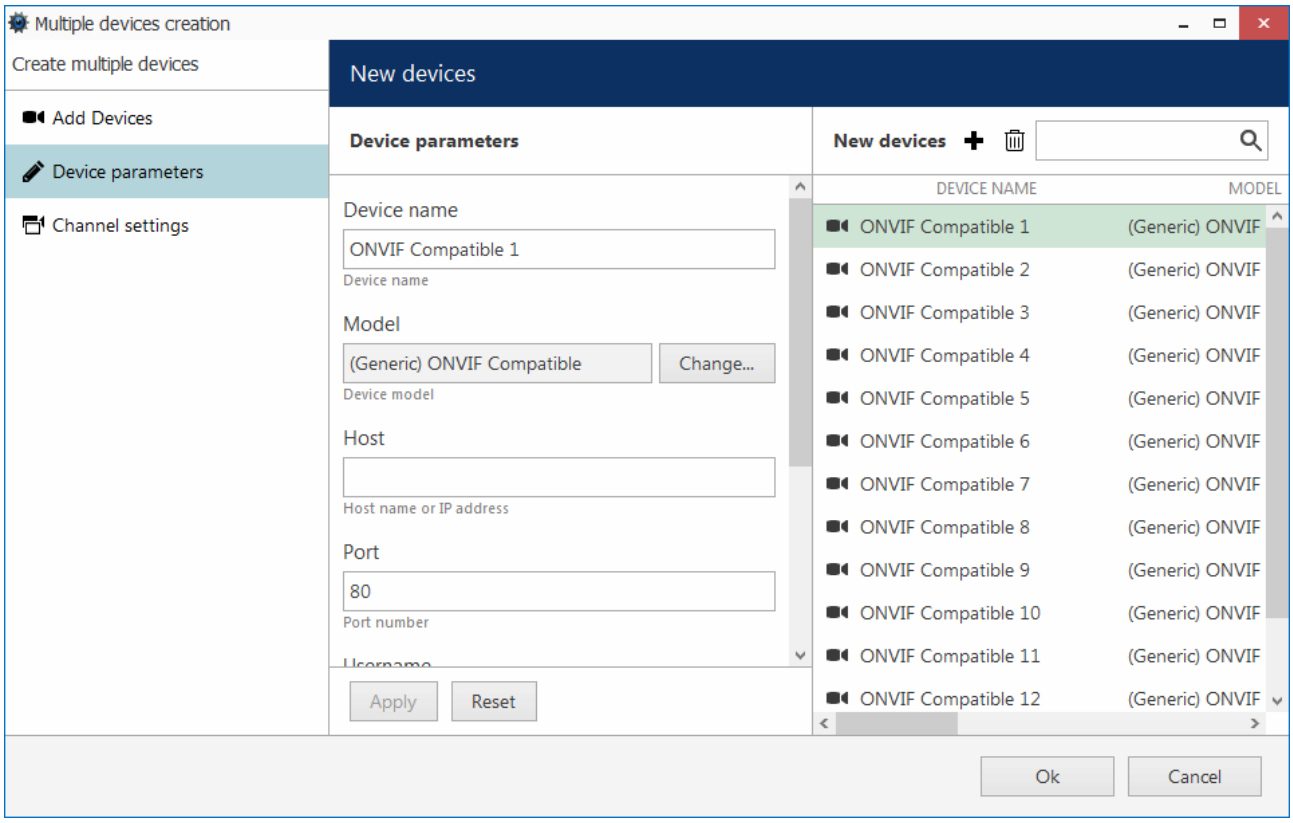
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Starting with version 1.26, the system no longer uses Legacy authentication by default when adding multiple devices manually. If your cameras use legacy auth (old/legacy cameras and firmware versions), please do the following after adding devices:

1. Go to Configuration > Devices and select your device.
2. In the pop-up window, navigate to Advanced Configuration.
3. Check the Use Legacy Authentication checkbox.

Device parameters

For each added device, enter corresponding settings. Note that you can skip IP and port on this step if you wish to use automatic incremental IP assigning (see *IPs and Ports* tab description below).



Select a device by clicking on it in the item list: it will become highlighted green and related available settings will be displayed in the *Device parameters* window. You can select multiple devices by holding *CTRL* or *Shift* when clicking.

Setting	Description	Default value
Device name	User-defined device name	Device model
Model	Device manufacturer and model, or generic type; click Change to alter	Loaded automatically
Host	Device hostname or IP address	[empty]
Port	Device HTTP port	80
Username	Device user credentials; note that you need to provide a valid administrative user profile to be able to change device settings via software	[empty]
Password	Password for camera access	[empty]
Server	Target server, to which the device will be attached	Central Server

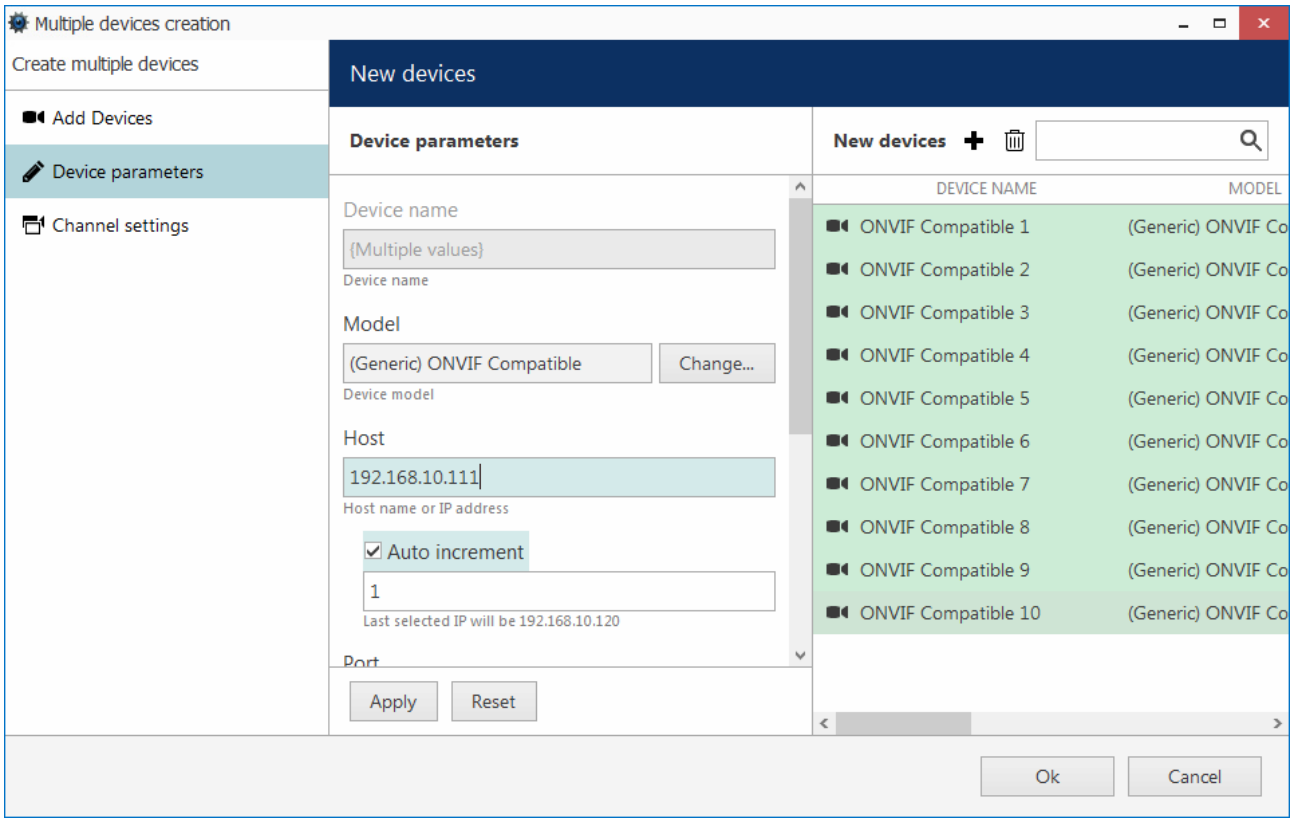
When you have finished, click the *Apply* button below for the changes to take effect.

> ⚠ If you do not apply the modifications, they will be discarded when you select a different device from the item list. Remember to always click the *Apply* button.

You will be asked to review the list of modified fields and confirm the changes.

Click *OK* to accept the changes and go back to the configuration dialog box.

You can select multiple devices and assign IP addresses incrementally with the defined increment. Similarly, it is possible to change the HTTP port for all devices at once, if required (port value stays the same for all selected devices, with no increment). In order to do this, select desired devices by using *CTRL+click* or *Shift+click*, then start entering the IP address: the field will expand, giving you the option to enter the increment.



Click the *Apply* button below to save the changes, similarly to the previous step.

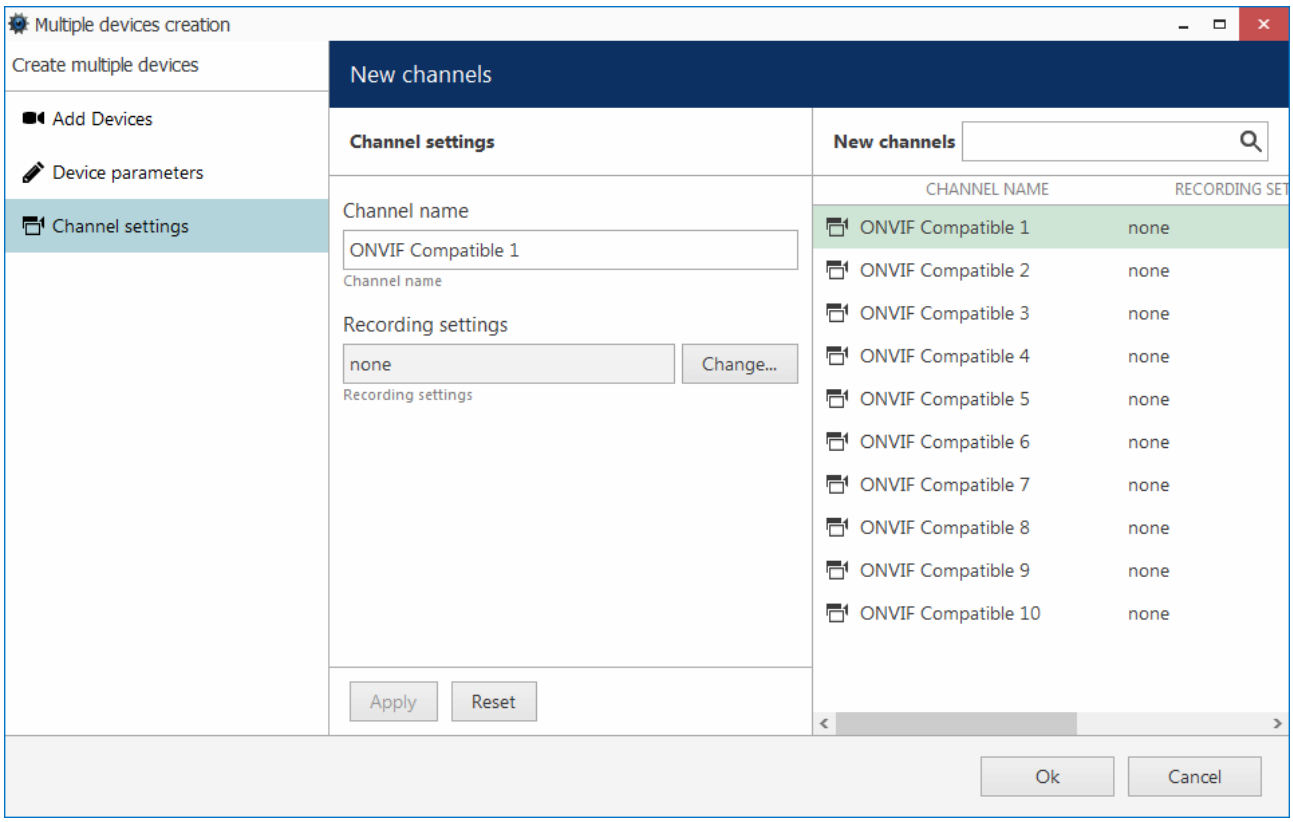
Channel Settings

Here you can modify channel names and recording configuration. Note that channel name is not copied from the device name.

Unlike with automatic device discovery, default recording configuration here is [none], meaning that recording is not conducted. Select one or multiple devices and then click the *Change* button in order to choose an existing recording configuration for the target devices or create a new one.

Depending on the selected device model, the number of channels may coincide with or exceed the number of devices, e.g., when device is a 4-channel encoder.

Macula® Professional Administration Guide



Select one or multiple devices and click Change, then select appropriate recording profile or create a new one.

When you have finished, click OK to add all the new devices and their channels to your server configuration.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

5.3 Manage Devices and Device Groups

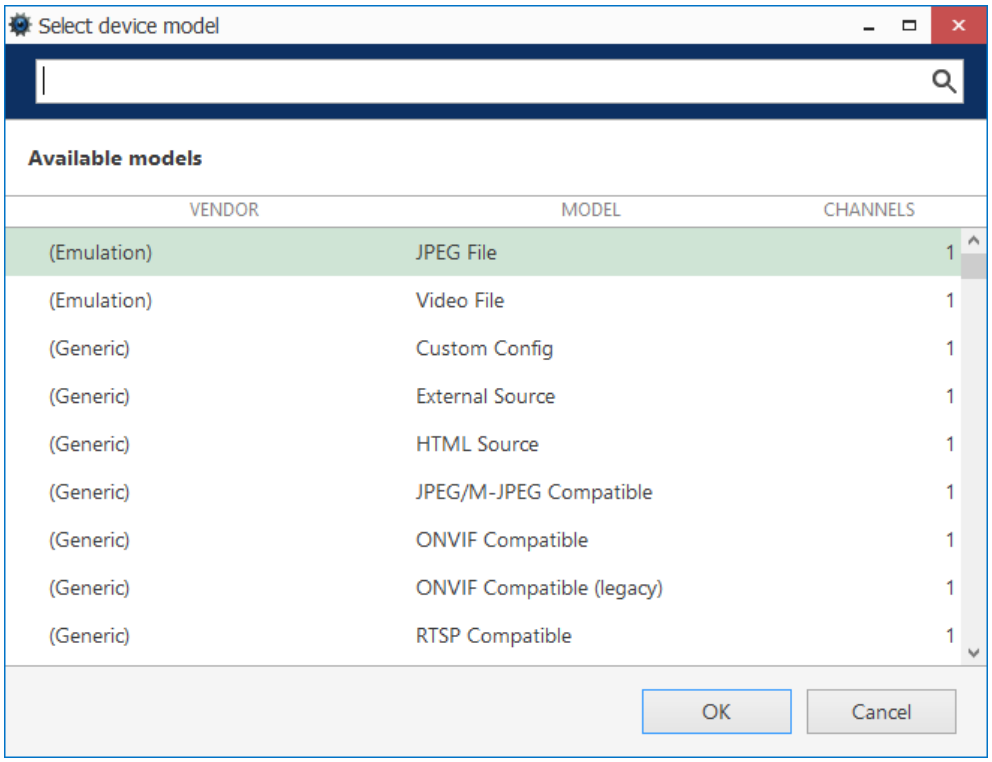
This topic describes general device handling as well as common use cases in device management.

Device Drivers (Models)

There are several device types available in the Macula model list:

- emulation
- generic
- models by vendor

Each group of models is further explained in more details. The selected model affects device-specific functionality; server-side functions (e.g., motion detection, Open VCA) will be available regardless of the device model.



Emulation From File

Emulation devices allow using a video/image file as the video source. This is an auxiliary driver often used for demo purposes, or when configuring/troubleshooting license plate or facial recognition. Still images must be in JPG/JPEG format. Video files must be in AVI format, encoded as MPEG4 AVC h.264; video files exported from Macula Monitor or Portable Player will work, too, provided that they were exported as AVI with JPEG compression.

After creating an emulation device, go to its channel's properties and specify the full local path to the target video/image file (*Channels* > open channel for editing > *Channel configuration* tab > *Channel*

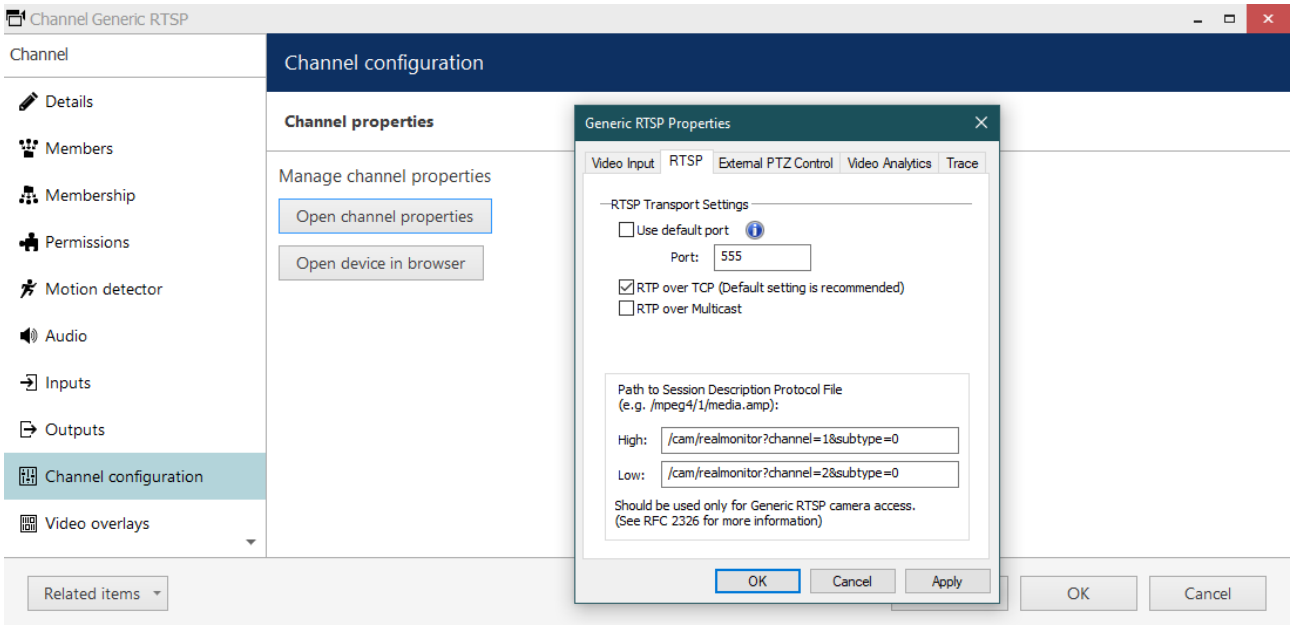
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

properties > *Settings* > *Location*). If you move such a device to another server, make sure to copy the file to the new server, or adjust the path in the channel settings.

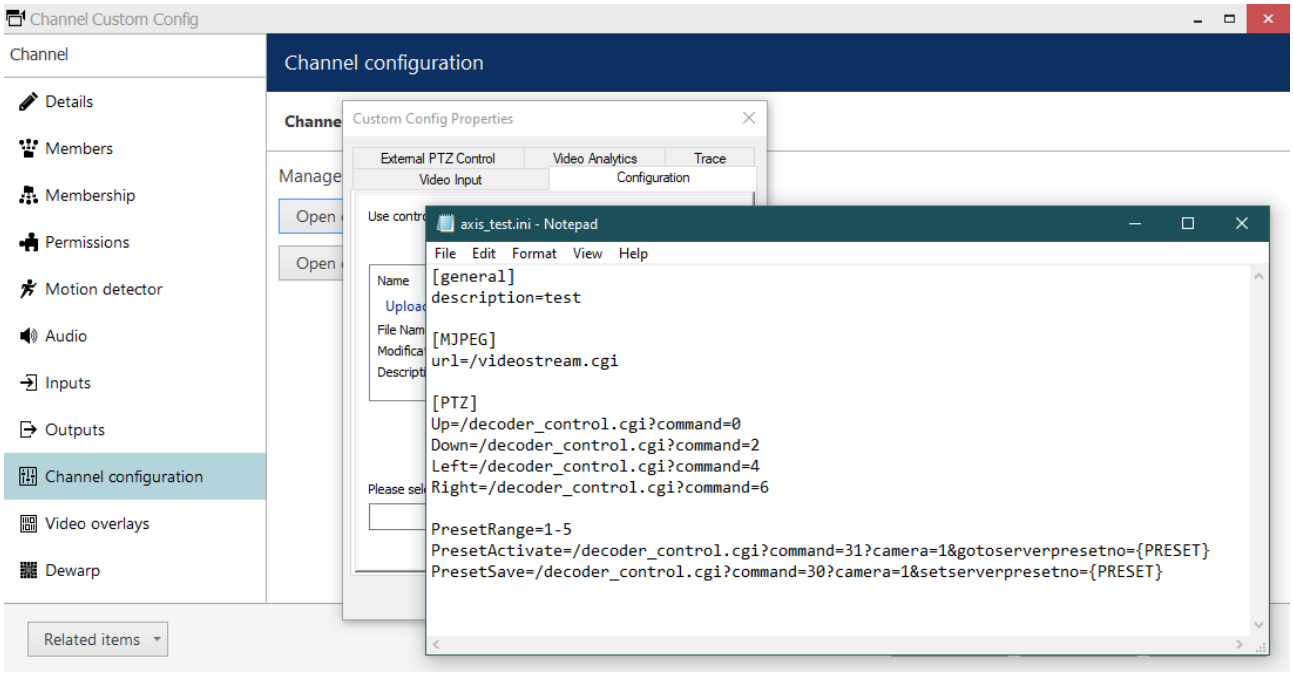
Generic Streaming Drivers

Generic drivers are based on common video transfer protocols, so these can be used for legacy hardware, non-integrated cameras/video servers, or non-traditional video sources (e.g., screen capturing software).

RTSP uses **generic RTSP** streaming over TCP/UDP, and includes two video streams and also audio (G.711). After adding this kind of device, go to its channel properties and specify the RTSP tag for both main and secondary video streams (*Channels* > open channel for editing > *Channel configuration* tab > *Channel properties* > *RTSP* > *Path to Session Description Protocol File*). The RTSP tag is the URL part after the IP address, so it should look something like */mpeg4/media.amp* or */videostream.cgi*. You can find this information in the device HTTP/CGI documentation provided by the manufacturer. You can also specify a **custom RTSP port** here, in case the device configuration uses a non-standard port, or if port forwarding is set up.



Custom configuration driver is similar to the generic RTSP driver, but it allows adding RTSP flags and PTZ commands via .INI file (text file with configuration, formatted in a special way). The file should contain the desired HTTP/CGI commands and URLs, according to the device documentation. The path to the configuration file is also specified in the channel properties, in the *Configuration* tab. Browse for the file, then hit *Apply*: you should see the configuration details appear above. If there are no details and the date is incorrect, the file has incorrect extension, or is not formatted properly.



JPEG/MJPEG driver is also similar to the generic RTSP driver, the only difference being that the transport here will use HTTP instead of RTSP. This model is rarely used, mostly for legacy devices not supporting RTSP/ONVIF.

ONVIF Driver

This driver can be used for all devices that are ONVIF Profile S conformant. By default, the *ONVIF Compatible* model is recommended (and it is also used when auto-detecting devices). If it does not work with older cameras, try the *ONVIF Compatible (legacy)* driver.

> ⚠ Due to extensive changes in ONVIF standards, older ONVIF driver marked as **legacy** - named (Generic) ONVIF Compatible (legacy) - has reached its end of life. It will still be available if you have cameras configured to use this driver, but no new devices can be created with this driver starting from the software version 1.23.1.
>
> Starting from the software version 1.24, channel settings are disabled for devices that use the legacy ONVIF driver. This means, you can change the settings on the camera side, but the software will only be able to read them.
>
> Please switch to the newest, *ONVIF Compatible* device driver wherever possible. If your ONVIF cameras do not operate correctly with this latest driver (e.g., some features are unavailable), kindly contact support@gsfcorp.com with details.

In device autodiscovery, this model will be used alongside with the native integrations: for not-yet-integrated brands/models, ONVIF model will be assigned wherever possible (i.e., if device responds properly to the ONVIF communication).

External Source

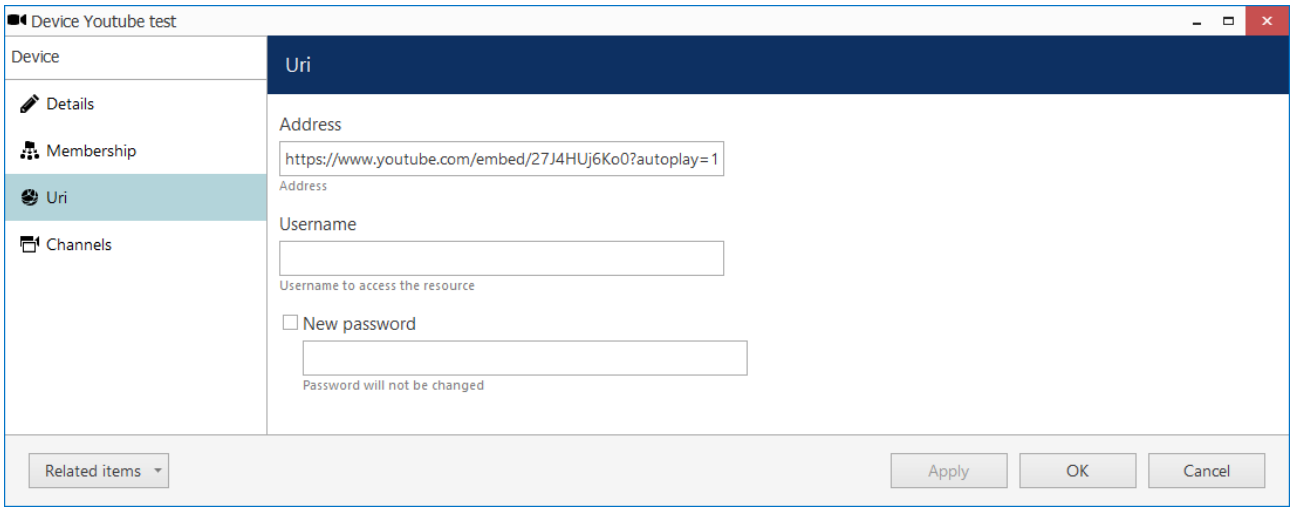
This device type is reserved for receiving streams from the Macula Mobile applications. Channels belonging to such devices are only counted by the license when the app streaming is active.

After adding this device, copy the *Code* from its properties to your Macula Mobile app to enable streaming from the app to the Macula server. You will find more details in the mobile app section of this document.

HTML Source

Choose this model to add streaming emulation from a website UI. The contents rendered from the specified URL will be displayed as a single, **static** (non-interactive) live **video stream**, with an option to record it. You can use this device driver for streaming from public services, monitoring web services, sites with dynamic contents etc.

Unlike for the generic RTSP driver (where you set the device IP and then add the RTSP URL in the channel properties), here you need to specify the full URL in the device settings at once. Channel properties for webpages will have a separate tab, *Web page configuration* (*Channels* > open channel for editing > *Web page configuration*).



The device settings include full resource URL (mandatory) and username/password (optional, you only need to specify the user account is the target web service requires it).

As the webpage contents will be static in the Macula Monitor application, you need to take care of the contents transition. To force refresh contents from the Macula side, use the auto refresh parameter in the channel properties. In the example here with YouTube streaming, the video is looped by adding URL parameters; the final link will look as follows:

https://www.youtube.com/embed/VIDEOID?autoplay=1&mute=1&loop=1&playlist=VIDEOID – video added in such a way will be played on repeat indefinitely.

Please note that this type of device uses Macula **channel license** as any other regular IP camera.

CrossLink Devices

Two types of devices are available here: **interactive Web pages** and **interactive remote desktop** applications. Both are fully functional server-side devices that provide live and recorded contents. All interactive items require a special license type called CrossLink.

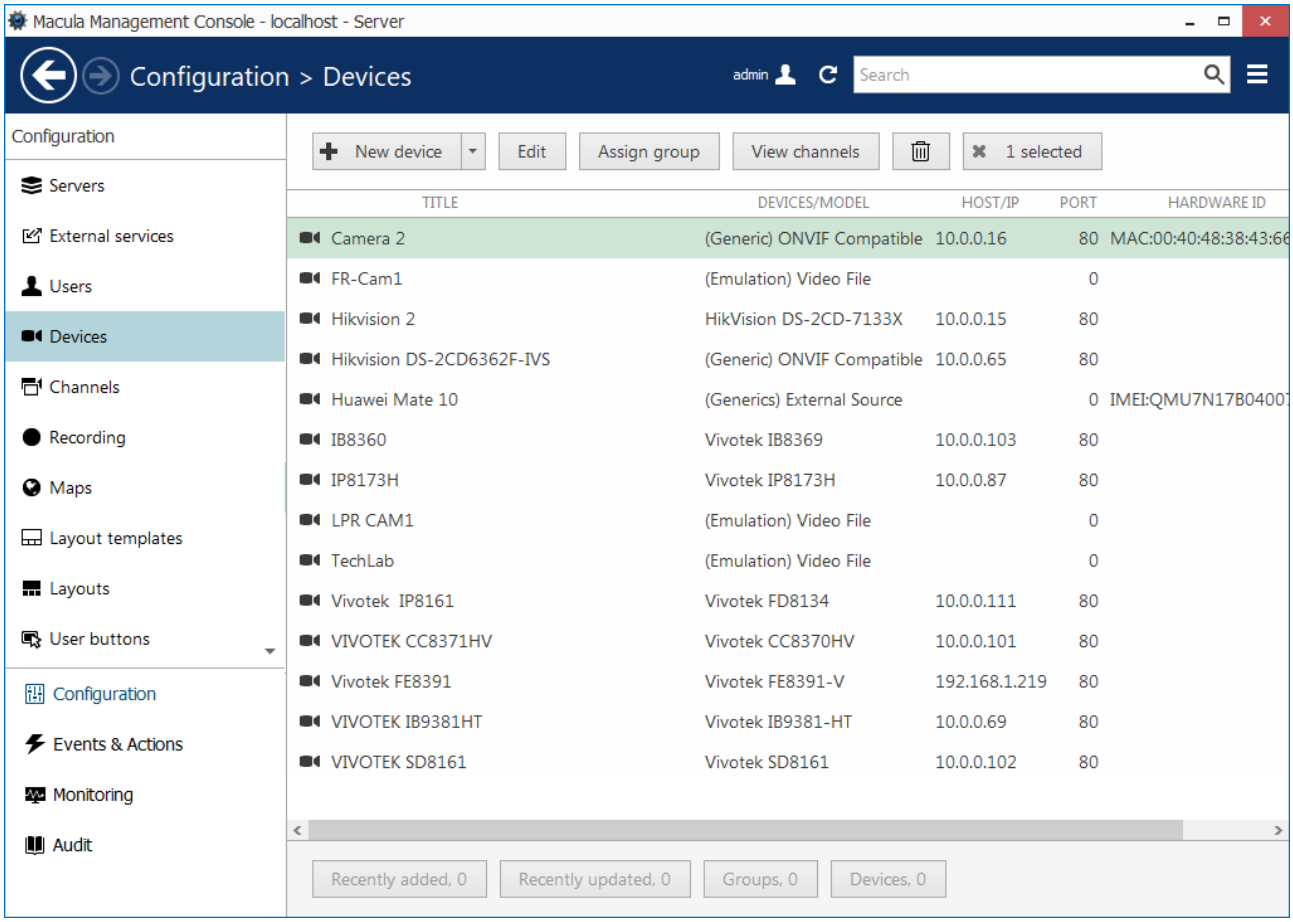
Models by Brand

Native device integrations are available for over 140 manufacturers and their 5000+ device models. This list includes cameras, NVRs, video encoders, and I/O modules. Models from this list are used when running device autodiscovery, and you can also use them when manually adding devices.

If you cannot find your exact device model in the list, try the closest available model: quite often, cameras within a series are intercompatible. Also, if you know the device's OEM brand, you can try models from that manufacturer.

Manage Devices

Device management is accessible via Macula Console *Configuration* section, under *Devices* category in the menu on the left.



Upper panel items allow you to add devices automatically or manually, edit, view and remove them, as well as quickly assign groups and servers. Double-click any device to open it for editing; click *View channels* on the upper panel to open channel-specific controls in the same window. If device has multiple channels, all of them will be listed.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

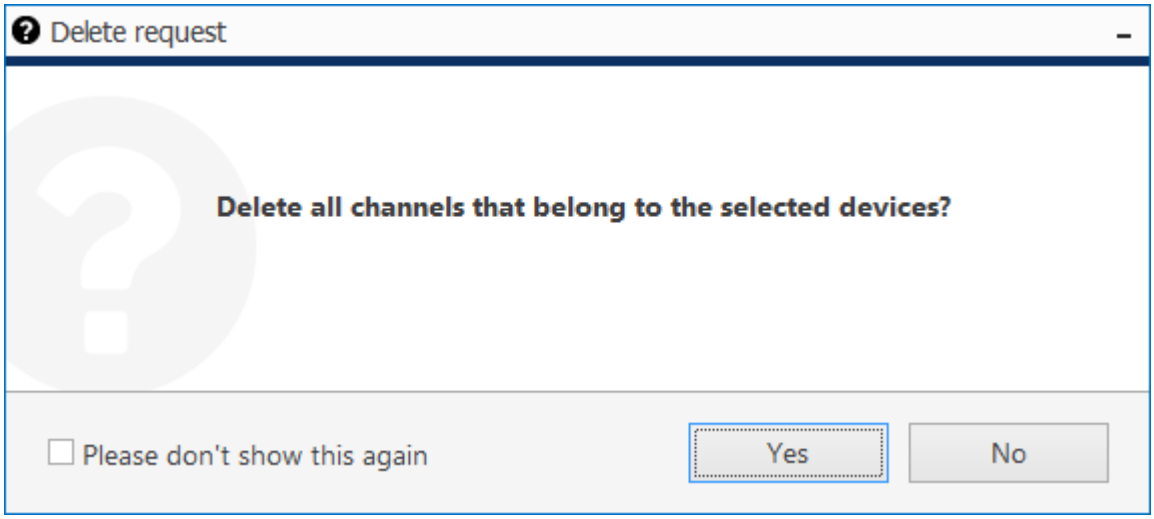
If you have opened a device for editing but there is a need to **open** the associated **channel's properties at the same time**, use the *Related items* buttons in the bottom left corner of the *Edit device* dialog box.

Please refer to the *Add Devices Manually* section of this document for detailed description of all available tabs and settings.

Use bottom panel buttons to quickly filter recently added/updated devices, choose groups only or solely devices not assigned to any of the servers.

Remove Devices

To remove a device, select it in the item list and use the *Recycle bin* button on the upper panel to delete the target device. Use *Shift+click* or *CTRL+click* to select multiple devices, or *CTRL+A* to select all.



You will be offered to remove all the attached channels together with the device(s). Press *Yes* to delete the channels or choose *No* to leave the channels: they will appear as detached in the channel list then and you will be able to re-attach them to other devices, keeping the channel recording configuration. If you choose *Yes*, all existing shared channels based on the channels of the target device will be removed automatically as well.

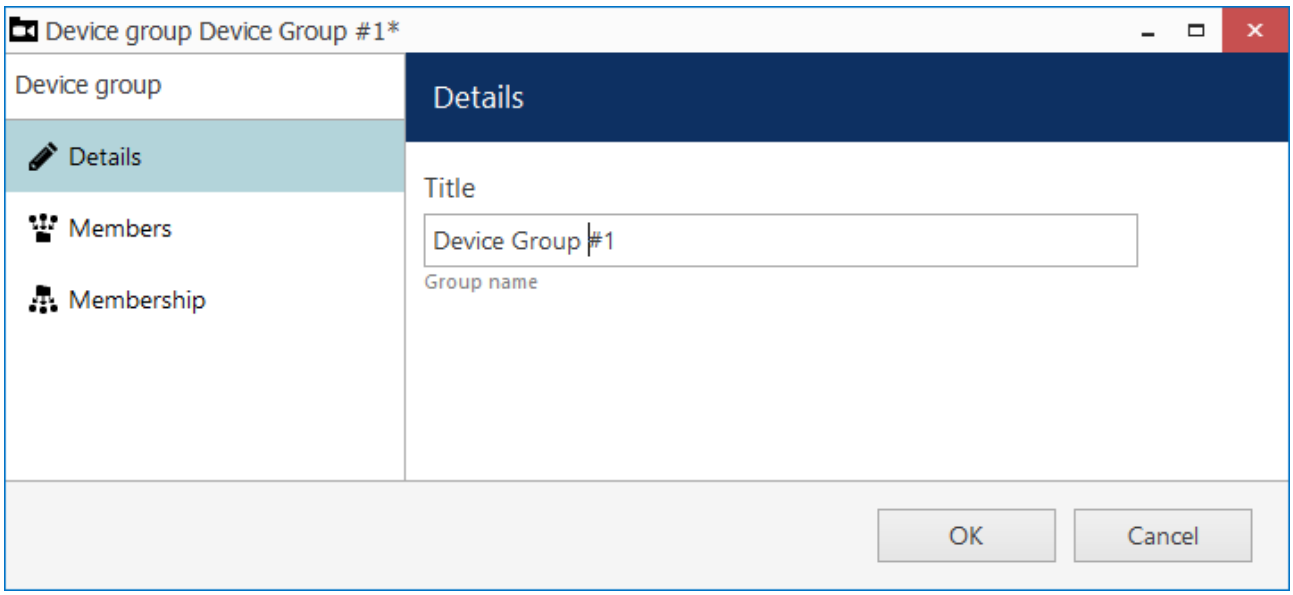
If you try deleting a device that has **associated rules** in the Event & Action Configurator, you will get a warning dialog box with those rules listed. You can either proceed with removing the target device, its channel(s) and its rule(s), or cancel the deletion.

Add Device Groups

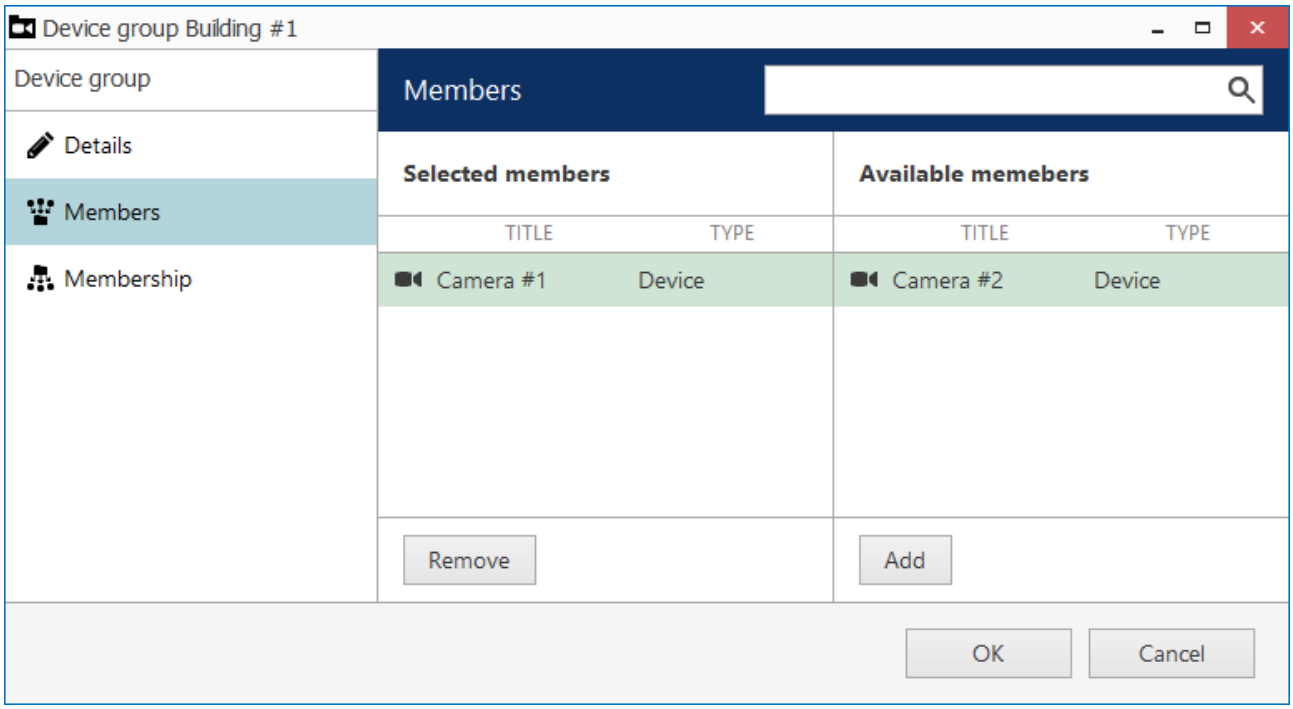
As with other resources, devices can be grouped together for easier management. Click the little arrow near + *New device* button and select *New device group.*

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

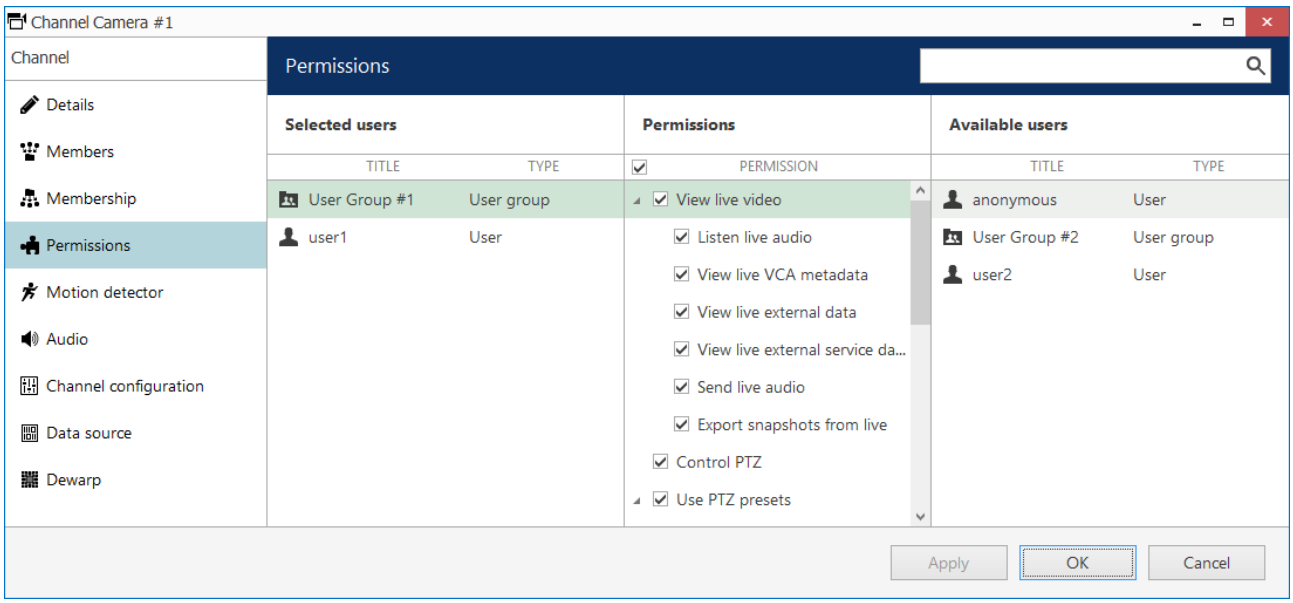


Enter a name for the device group in the *Details* tab, then switch to the *Members* tab and choose devices to join this group. Double-click items or use the *Add/Remove* buttons below to select and deselect devices.



In the *Membership* tab, you can select 'higher' level groups to contain this device group (nested architecture).

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Finally, open the *Permissions* tab to assign user privileges for this device groups: check at least one permission to select the user or user group, uncheck all or use the *Clear* button below to deselect. When you have finished, click *OK*; the newly created group will then appear in the item list.

Double-click any group to open its contents in the same window; use the buttons on the upper panel to edit/remove it. Click *Edit* to adjust group settings: procedure is similar to that of creating a new device group.

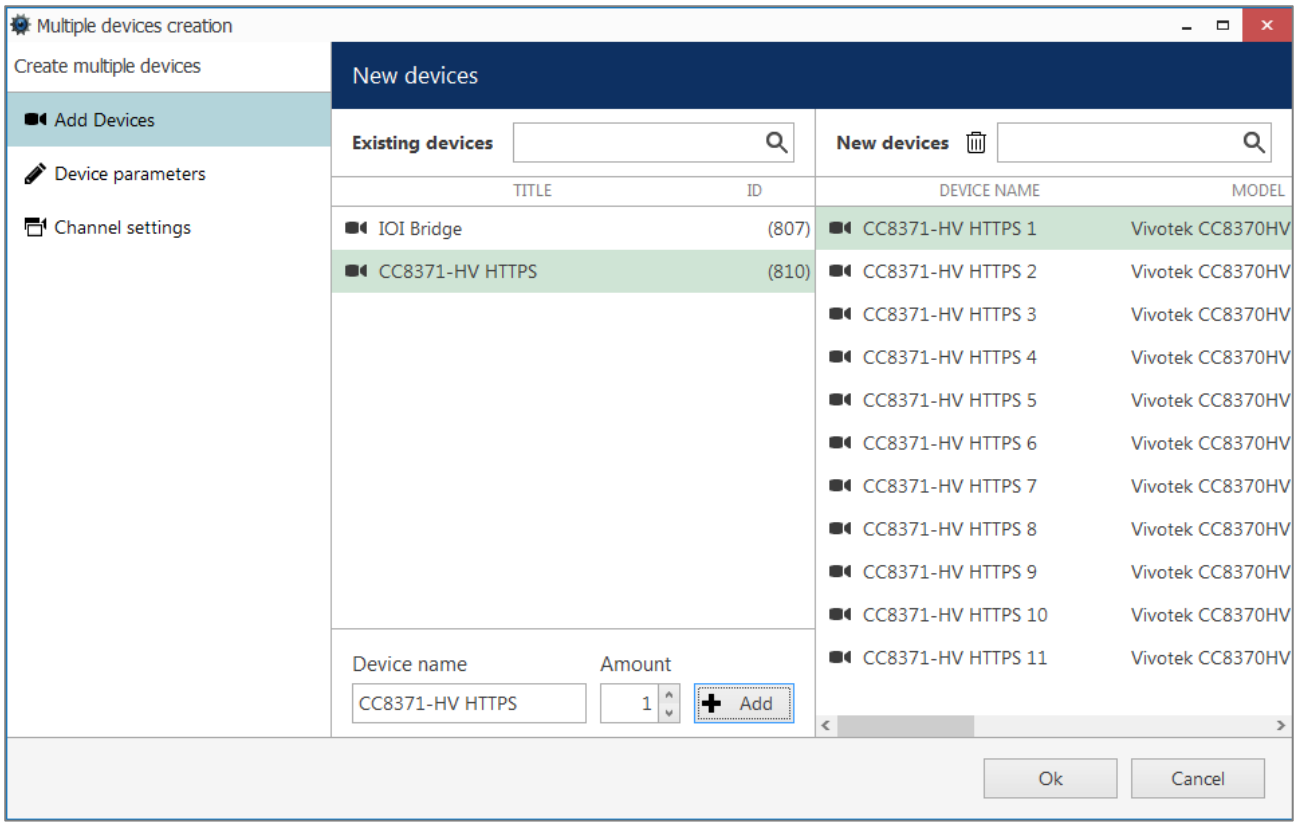
Copy Device*

*Feature is subject to license limitations and may be **unavailable in some software editions**.

Starting from the Macula version 1.11.0, it is possible to **copy an existing device** and its channel(s). To copy a device, click the little arrow next to the + New device button on the upper panel and choose *Create copy* from the drop-down list. The related channel(s) will be copied automatically.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



In the dialog box that appears, you can create one or multiple copies of any device(s) currently present in the Macula server configuration. In the list on the left, all existing devices will be listed; in the list on the right, your copies will appear.

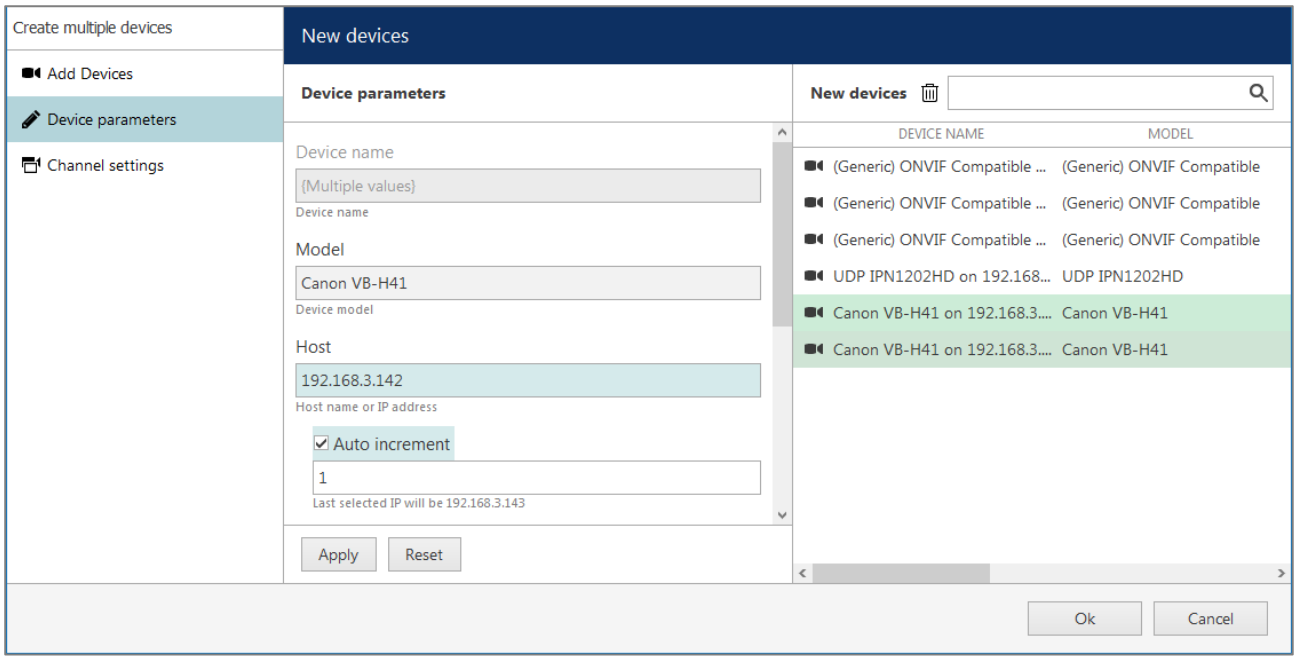
First, choose the source for the copy in the *Add devices* tab:

- select one of the existing devices in the list on the left (a single device can be selected at a time),
- set the number of target copies below,
- when ready, click the + *Add* button to **create** the selected copies,
- repeat previous steps with other devices, if required.

To add a single device copy, you can simply double-click it in the list.

Use the search fields on top of the lists to find the necessary item in a long list. If you no longer wish to add any of the created copies, you can select multiple items using *CTRL+left* click or *Shift+click* and **remove** them using the *Recycle bin* icon above.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



In the Device parameters tab, you can adjust:

- the **name**(s) of the target copy (copies),
- their **IP addresses**, with an option to select multiple with CTRL+left click and then assign a range of IP addresses using auto increment with the specified step,
- HTTP **port** and **user credentials**.

After you have altered any settings here, do not forget to hit the *Apply* button to **save** them, otherwise the changes will be discarded when you deselect the device(s) or switch to a different tab. Use the *Reset* button to **roll back** to the original settings (this works if you have not applied the settings yet).

Note that, at this step, the new device **model** remains the same as the source device model and it cannot be changed at this point. This is necessary for the Macula engine to successfully create a duplicate. You will be able to change the model later via editing the desired device.

The same applies to the **server** where the device is attached: at the moment of cloning, the new devices are created on the same server. If you are using Macula Enterprise, you will be able to move the devices to a different server after you have added the copies by editing the target device(s).

In the *Channel settings* tab, the only available parameter at this point is the **channel name**. You will be able to edit other settings after creating the copy (copies) by editing the target channel(s).

When finished with the settings, click the *OK* button to **save** your newly created device+channel copies. They will be automatically added into the server configuration database.

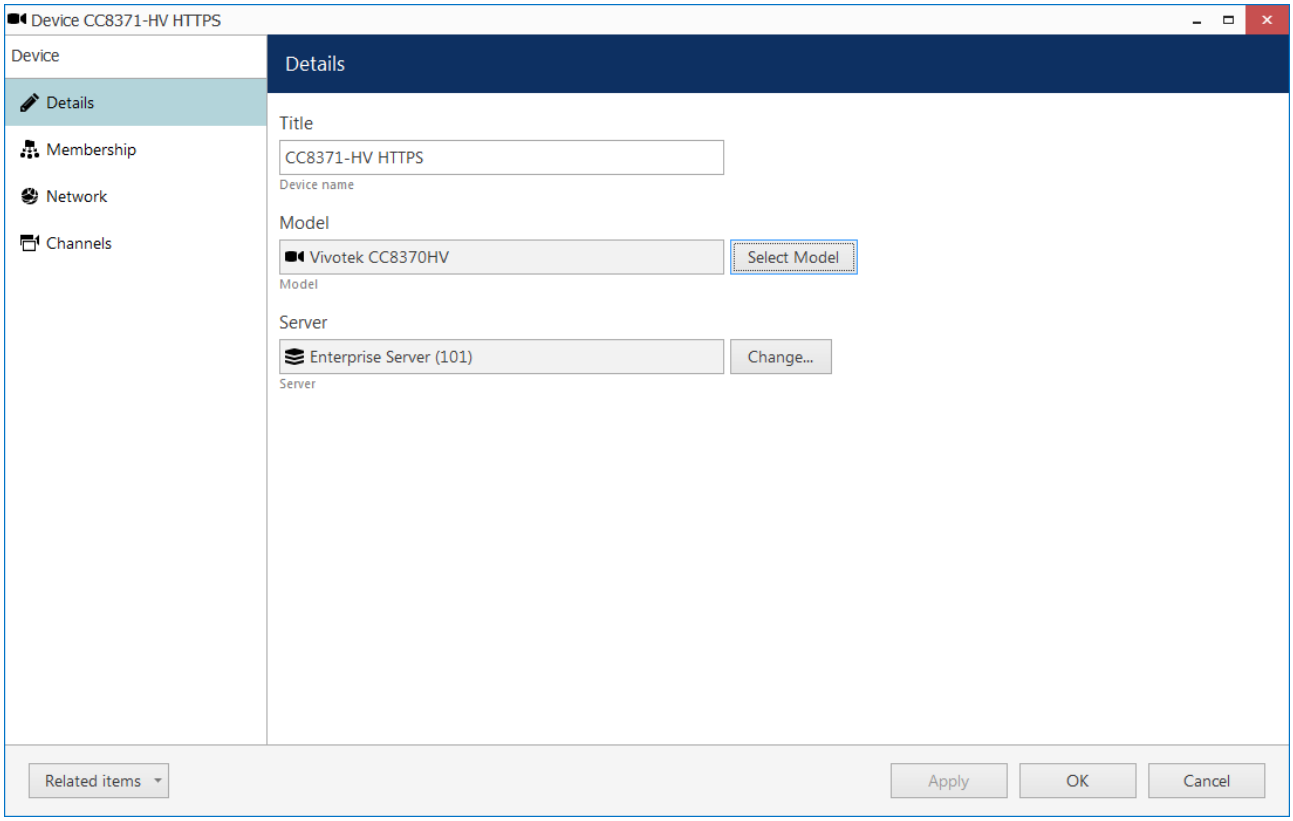
> ⚠ After you have added new devices using this method, please allow **some minutes** for the configuration to be saved. After that, you will be able to change the newly created device and channel settings.

The associated **channel**(s) will be added **automatically** with all the existing settings, including the assigned recording configuration.

Replace Camera

In the Macula versions up to 1.11.0, it was impossible to alter the device model, so a special procedure was foreseen if the camera needed a replacement.

Now, if you replace the hardware, you can simply **change the device model** by opening the target device for editing - either by double-clicking it in the device list, or by using the *Edit* button on the upper panel. Note that, when you change the model of an existing device, you will only see model suggestions with the same **number of channels**, and not the whole list of available devices.



To quickly open the associated channel settings without closing this dialog box, use the *Related items* button in the bottom left corner.

> ⚠ When you change the device model, all the **channel settings** that are configured via Channel properties dialog box are **discarded**. These settings include video stream properties, audio, DI/DO etc.
> Channel settings that are **preserved** are: motion detection, dewarp, data source, user permissions and recording configuration.

5.4 Configure Channels

Channels are video streams received from physical devices attached to the system. Several channels can originate from a single device - in the case of multichannel devices, i.e., capture boards, but single channel can only be attached to one device at a time, as it makes no sense for a video stream to come from two cameras at once. Channels are created automatically at the same time as the source device but can later be detached and attached to different devices.

Channels include the video stream configuration settings - resolution, frame rate, bit rate and others - as well as all supplementary data streams, such as audio, motion and digital input/output events, PTZ control and camera-side analytics information. Recording configurations are assigned to channels and they are also displayed in Macula Monitor.

To access the channel configuration dialog box in the Macula Console, open the *Configuration* section and select *Channels* from the menu on the left side. Use the filters on the bottom panel to quickly access specific channel sets.

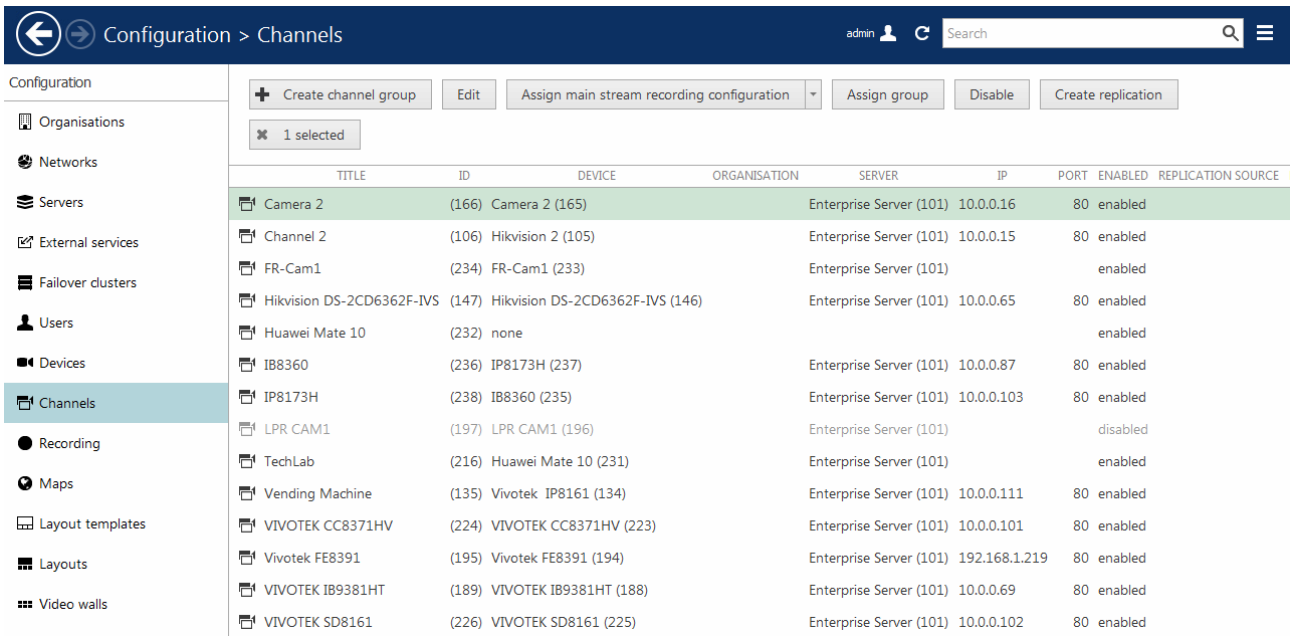
The upper panel buttons enable you to create new items in this category, as described below, and perform channel-specific actions, such as editing, assigning groups, assigning recording configuration and deleting selected channels. To select multiple items, hold *CTRL* or *Shift* and click items in the list.

⚠ Channels currently **bound to devices** cannot be deleted: the recycle bin button will only appear when detached channels are selected. To **remove a channel**, go to *Devices*, open properties of the target device and disengage the channel on the *Channels* tab by clicking the *Detach* button; also, you will be offered to delete all associated channels when you remove the device itself - this will also remove any existing shared channels.

⚠ Channels that have any associated **rules** in the Event and Action Configurator **cannot be removed**. If you try deleting such a channel, you will get an error saying *The channel cannot be removed because it is in use*.
In order to remove such a channel. you need to delete the rules related to it first. To do so, just go to the *Events & Actions* section, choose *Rules* in the menu on the left, select the target server and open the configurator, then remove the necessary rules from the central column by using the < and > buttons.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

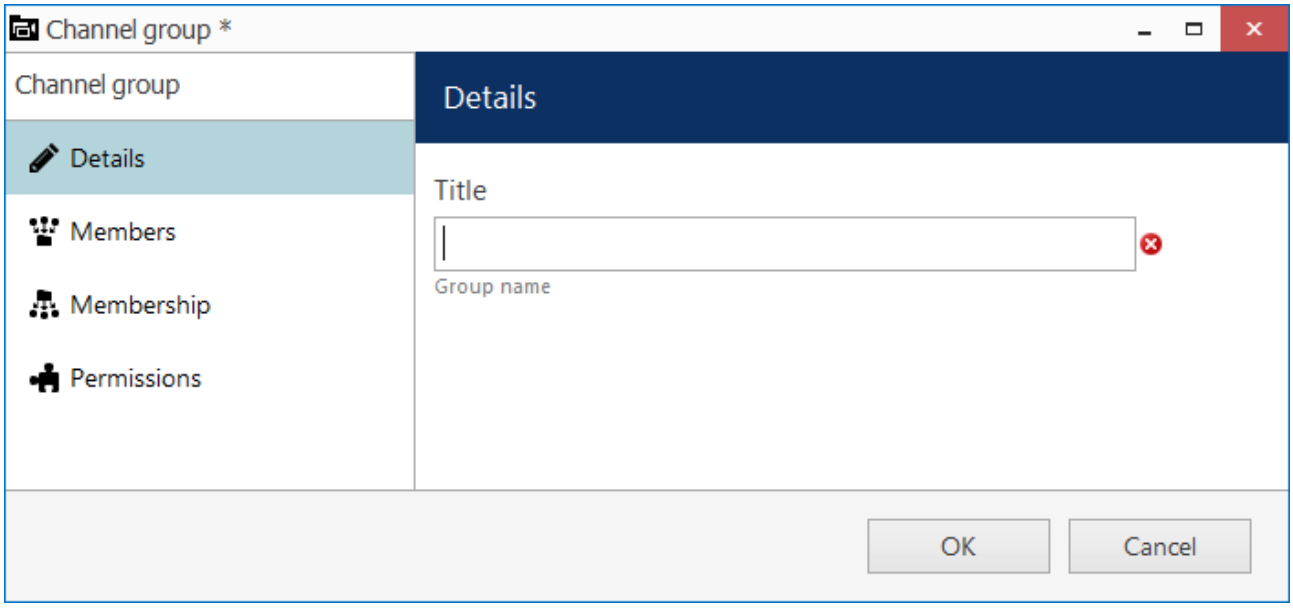


All available channels and channels groups will be listed here. The upper panel offers a range of configuration opportunities.

Create Channel Group

Channel groups can be added for easier management in Macula Console; by default, there exist no built-in channel groups. Click + *Create channel group* button to bring up the corresponding dialog box.

Enter the group title here, select channels to be group members and select higher level group(s) to contain target group as a member, if desired. Set user permissions for channels in this group.



Click *OK* when you are ready: newly created group will appear in the item list.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Edit Channel Group

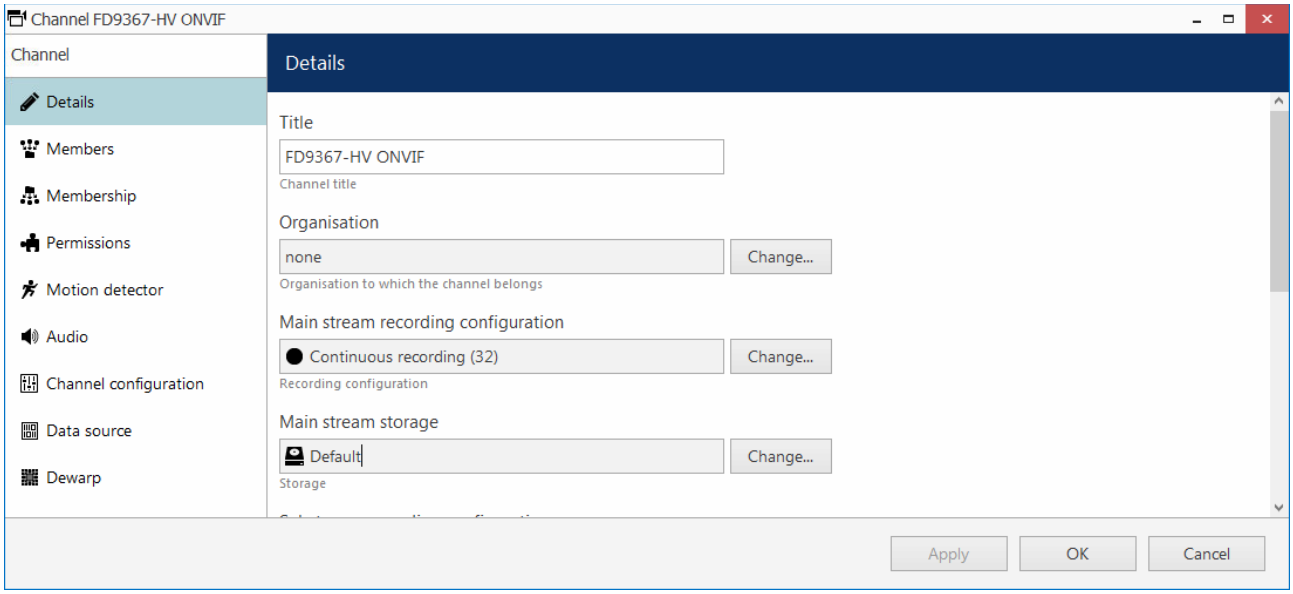
Double-click any existing channel group in the list or use the *Edit* button in the upper panel to bring up the configuration dialog box. Available options are analogous to the ones displayed during group creation time.

Edit Channel

Channels are automatically created together with each newly created device; it is not possible to create a channel separately. Click any channel in the list twice or use the *Edit* button on the upper panel to manage the channel properties.

> Channels with the same device driver (e.g., ONVIF), can be edited **together**. You can select multiple channels by holding CTRL and then open the settings dialog box.

Some of the settings (e.g., recording properties) can be edited for multiple channels simultaneously. Use the CTRL or Shift buttons to select multiple channels.



The configuration dialog box enables the following changes:

- **Details tab:** change channel title and assign recording configuration
- **Members tab:** bind user buttons to channels so that they appear together in the Macula Monitor
- **Membership tab:** make the channel a part of a channel group or a visual group
- **Permissions tab:** grant channel access permissions to users and user groups
- **Video file configuration**: settings for the generic video emulation driver: main and substream file path and delay between frames
- **Motion detector* tab**: choose between a camera-side or software-side motion detector, default state is disabled
- **Video analytics**: server-side video analysis configuration
- **Audio tab**: combine current channel with audio from another source
- **Inputs/Outputs**: DI/DO settings
- **Channel configuration**: open an additional channel configuration dialog box to manage video stream settings, frame adjustments and DI/DO

- **Video overlay:** configure different overlay elements, e.g., textual contents received from data sources or use channel shortcuts aka "Portal" with different resources
- **Dewarp tab**: select dewarp profile for fisheye and Panomorph lenses
- **Video configuration**: main and secondary stream adjustment (for newer device drivers)
- **RTSP configuration**: RTSP port and transport selection (for newer device drivers)
- **Edge configuration**: configuration of edge (device-side) synchronization (for newer device drivers)

Please refer to the Channel Settings topic for detailed description for each of the tabs.

*****Motion detector on the software side has two options: high performance and high accuracy:

> *High Performance mode:* this type of analysis is performed for only key frames whose frequency can vary from several frames per second to one frame every few seconds - this is less sensitive for picture quality, but greatly affects detector operation. CPU consumption is significantly lower due to this, and it can be additionally reduced by increasing time interval between two analyzed frames.
>
> *High Accuracy mode:* this mode performs motion analysis for the whole video stream, so we recommend selecting this option when you want to achieve best detection results. The lower time interval means higher precision. Keep in mind that CPU and virtual memory usage is much greater if this mode is selected.

If you have opened a channel for editing but there is a need to **open** the associated **device's properties at the same time**, use the *Related items* buttons in the bottom left corner.

Live Channel Preview

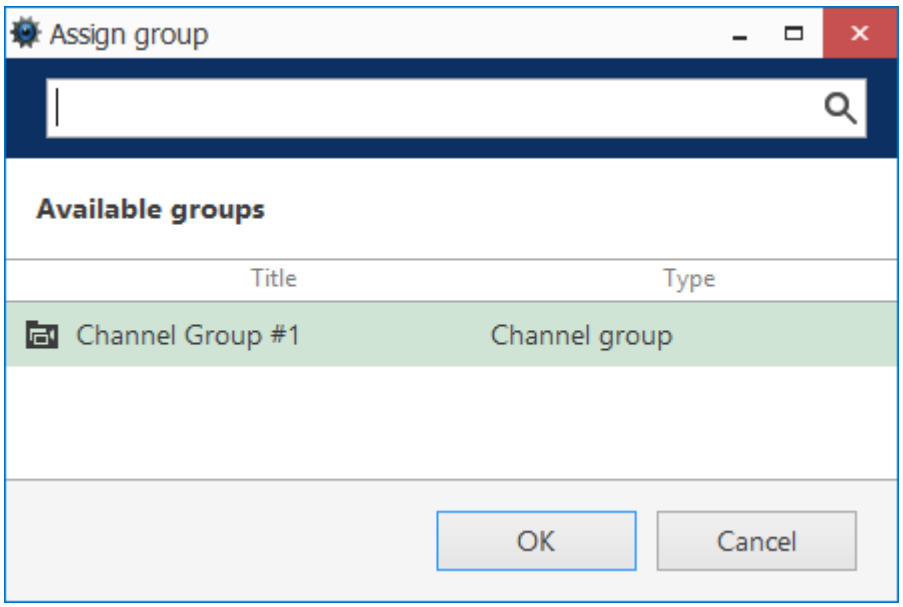
After a device and its associated channel has been added to the configuration, it is vital to check if the actual video is received. There are several methods to do this in Macula Console:

- click the Show video button on the upper panel in the *Configuration* > *Channels*: you can switch from main to the secondary stream and back
- go to the *Monitoring* section > *Channels* and check the channel status
- open the target channel for editing and go to *Dewarp* or *Data source* settings

Assign Group

Channel membership can be managed via the channel properties dialog box. To quickly assign group to any of existing channels, select desired channel(s) (use CTRL+click or Shift+click to select multiple items) and click *Assign group* button on the upper panel.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Pick a group from the existing channel groups' list and click *OK* to save. If any of the channels already belonged to some group, it is not a problem: membership in multiple channel groups is allowed.

Quick Assign Recording Configuration

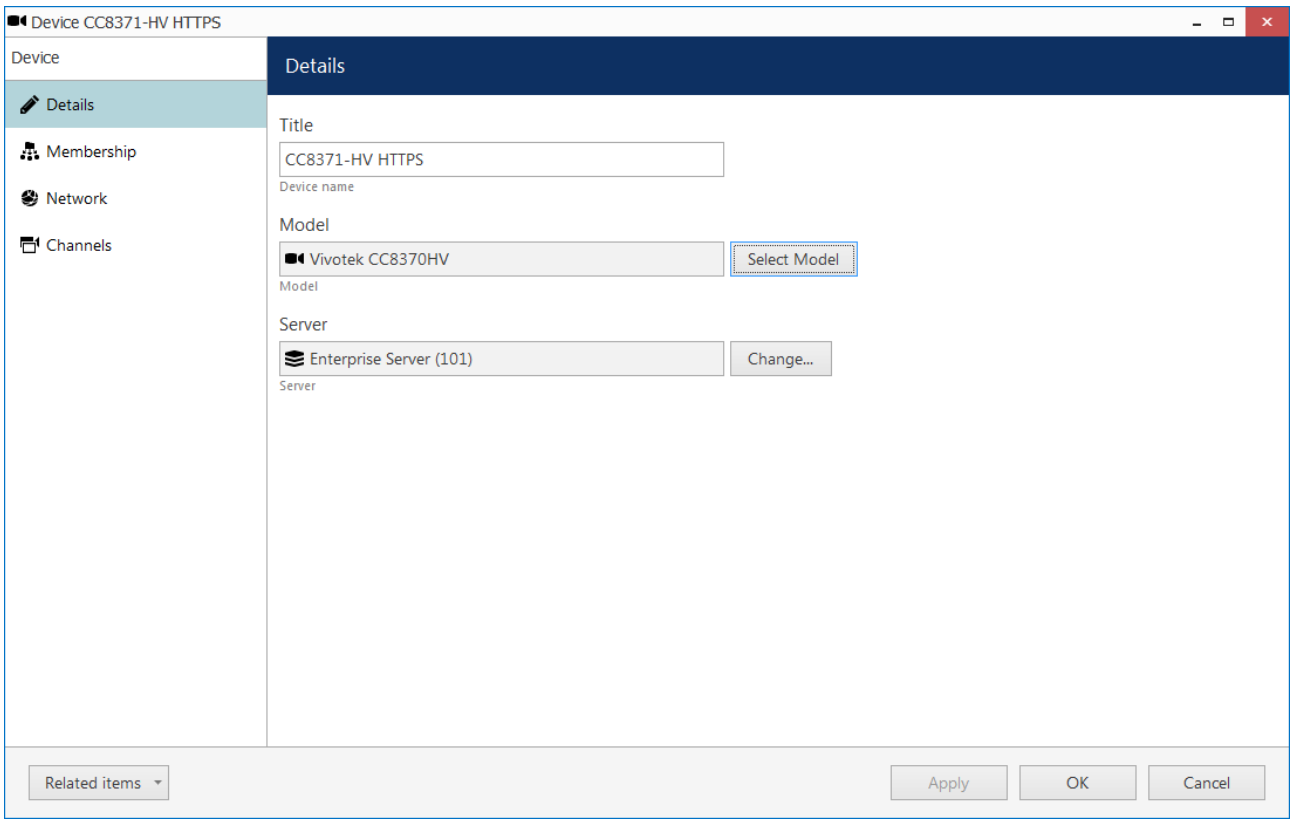
Select one or multiple channels and click the *Assign Recording Configuration* button on the upper panel, then either select an existing recording configuration from the list or create a new one from the dialog box currently in use (the newly created configuration will be automatically chosen after creation). The recording scheme will be applied to the **main streams** of the selected channels; in order to assign configuration to the **secondary streams**, click the arrow near the *Assign recording configuration* button and choose *Assign substream recording configuration*.

Replace Camera

In the Macula versions up to 1.11.0, it was impossible to alter the device model, so a special procedure was foreseen if the camera needed a replacement.

Now, if you replace the hardware, you can simply **change the device model** by opening the target device for editing - either by double-clicking it in the device list, or by using the *Edit* button on the upper panel. Note that, when you change the model of an existing device, you will only see model suggestions with the same number of channels, and not the whole list of available devices.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



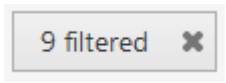
To quickly open the associated channel settings without closing this dialog box, use the *Related items* button in the bottom left corner.

> ⚠ When you change the device model, all the **channel settings** that are configured via *Channel properties* dialog box are **discarded**. These settings include video stream properties, audio, DI/DO etc.
> Channel settings that are **preserved** are: motion detection, dewarp, data source, user permissions and recording configuration.

Other

Select one or multiple channels/channel groups and click the *Disable* button on the upper panel to deactivate target items. **Disabled** channels will not be requested from actual physical devices, and, as a consequence, will not be recorded; neither will they be displayed in Macula Monitor application(s).

The filter panel at the bottom enables you to view recently added/updated items, as well as other relevant filters. The filter that is currently active is highlighted blue: click the *N filtered* button to reset all filters and display all the available items again.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

5.5 Channel Settings

The channel configuration dialog box offers several setting categories. As you move across the tabs and alter the configuration, the tabs containing **unsaved changes** will be marked with an asterisk (*).

Some of the tabs are present for all channels. Other tabs only appear for special driver types (e.g., Web page, Video emulation etc.).

Details

Here you can change the channel title and assign a recording configuration to both main and secondary streams, as well as changing Organization membership for the target channel.

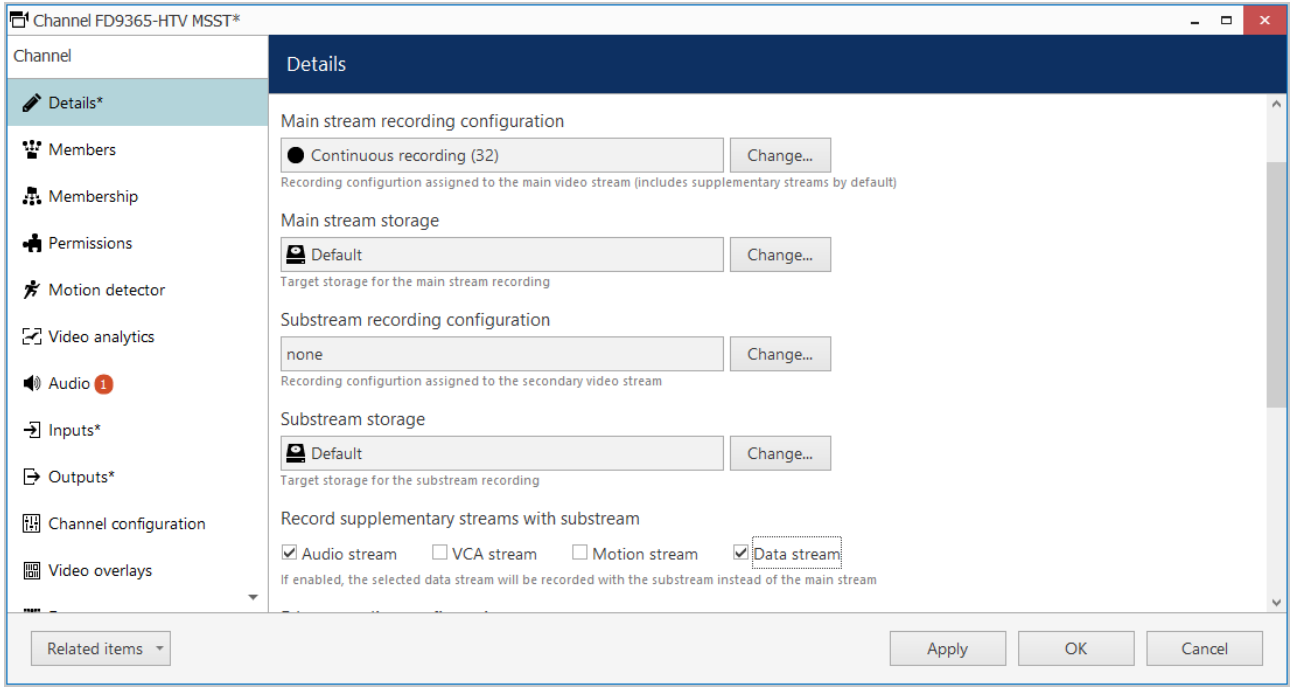
- **Title**: user-defined cannel name, as it will appear in Macula Console and Macula Monitor applications
- **Organization**: assign this channel to an Organization, if applicable
- **Main stream recording configuration**: choose how the first video stream (usually, higher resolution) will be recorded
- **Main stream storage**: destination storage for this stream (may differ from other streams)
- **Substream recording configuration**: choose how the second video stream (usually, lower resolution) will be recorded
- **Substream storage**: destination storage for this stream (may differ from other streams)
- **Edge stream recording configuration**: choose how the edge stream will be recorded, if used (available for ONVIF Profile G conformant devices and also for offline recordings made by Macula Mobile)
- **Edge stream storage**: destination storage for this stream (may differ from other streams)
- **Record supplementary streams with substream***: if enabled, the selected auxiliary data streams will be stored with the substream
    - *Audio*: incoming sound track
    - *VCA*: video analytics metadata
    - *Motion*: motion detector data
    - *Data*: data from data sources (serial text like POS etc.)
- **Video lost time**: the amount of time in seconds for Macula to wait after all channel's video steams disappear and before triggering a *Video loss* event
- **Recording identifier** (only displayed if Show object IDs option is enabled in the application settings): unique channel identifier that is used as its folder name in the archive

If you enter a custom **title** for a channel, a special button on the right side will allow you to revert to the device title with a single click.

***By default, all **supplementary data streams** are stored with the main stream, and the secondary stream is recorded is video only. However, if you wish to keep the secondary stream for a longer period (e.g., 7 days for the main stream and 30 days for the substream), you may wish to keep the data streams with the substream so that these tracks are available when you play back the archive. Otherwise, the supplementary data will be erased with the main stream based on the quotas. This setting is also useful when you use different storages for both streams and it is crucial where the supplementary data goes.

Macula® Professional Administration Guide

> ⚠ Each of the supplementary data streams - audio, MD, metadata, and serial data - can only be recorded once: either with the main or with the secondary video stream. None of these streams are copied. Thus, for example, if you keep the substream longer than the main video stream, you may want to record the audio together with the secondary stream.

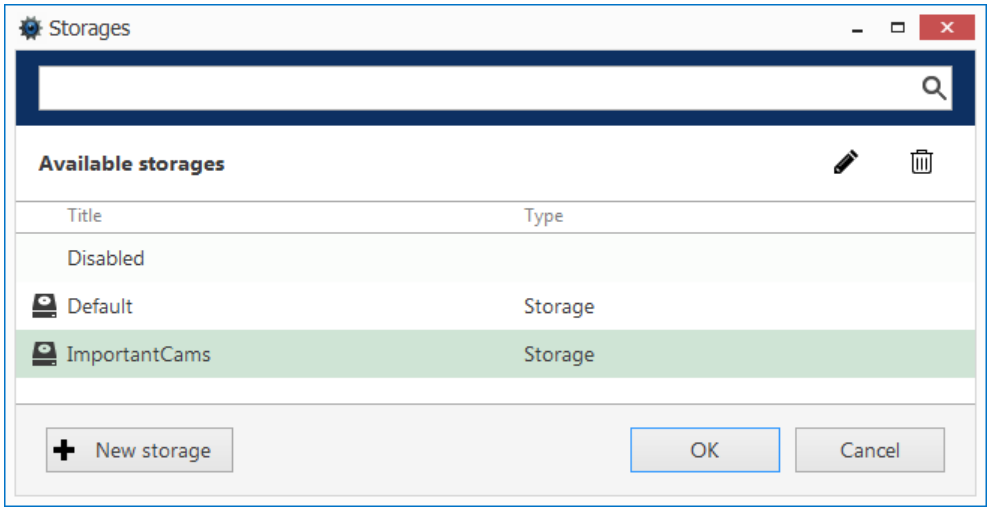


You can either use *Default* storage category for target streams, or use a different storage profile. The latter can be used for manually distributing streams between storage different directories:

- storage directories are marked with the relevant storage profiles
- each channel is assigned a recording location

To choose a storage profile that is not *Default*, select storage location from the *Directories* list and click *Change* button.

Select one of the built-in storage profiles or create and edit a new one.



The built-in storage types are:

- **Disabled**: storage location will not be used

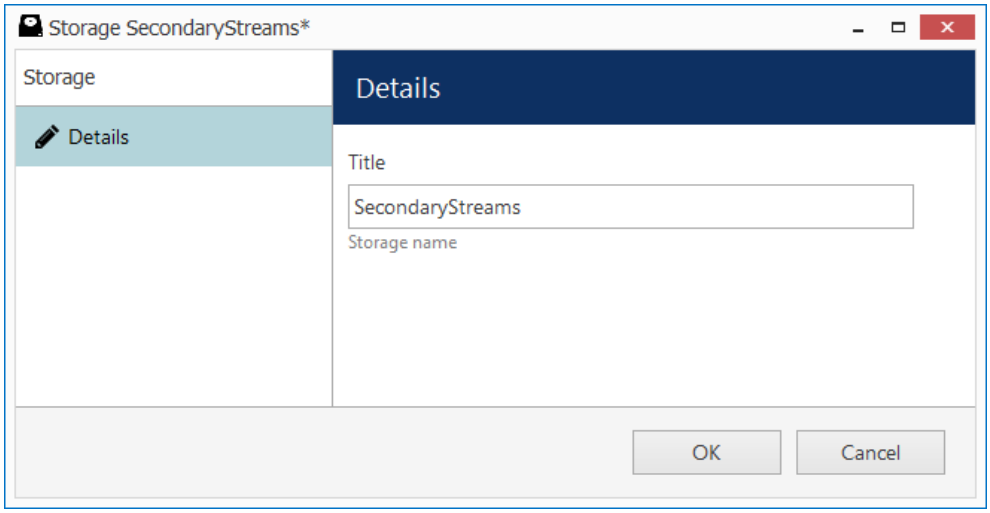
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

- **Default**: default storage tag
- **Fallback**: storage destination to be used if all the storage units with specified tags have failed
- **Readonly**: existing data will be available for reading and will not be erased; no new recordings will be appended to this location

These profiles cannot be edited or removed. Fallback storage settings are available in the corresponding tab of the *Storage properties*.

Readonly storage type can be used, for example, in the following cases:
- it is necessary to view the old data from a different Macula server when you need to insert the disks originating from another computer and you do not wish that these data are erased
- some storage unit contains important footage that has been requested to be kept for a longer time so that the recordings are not erased over time while still allowing access to the footage

Click + *New storage* button to create a new storage profile, or select an existing one and click the *Edit* button in the upper-right-hand corner to change its name.



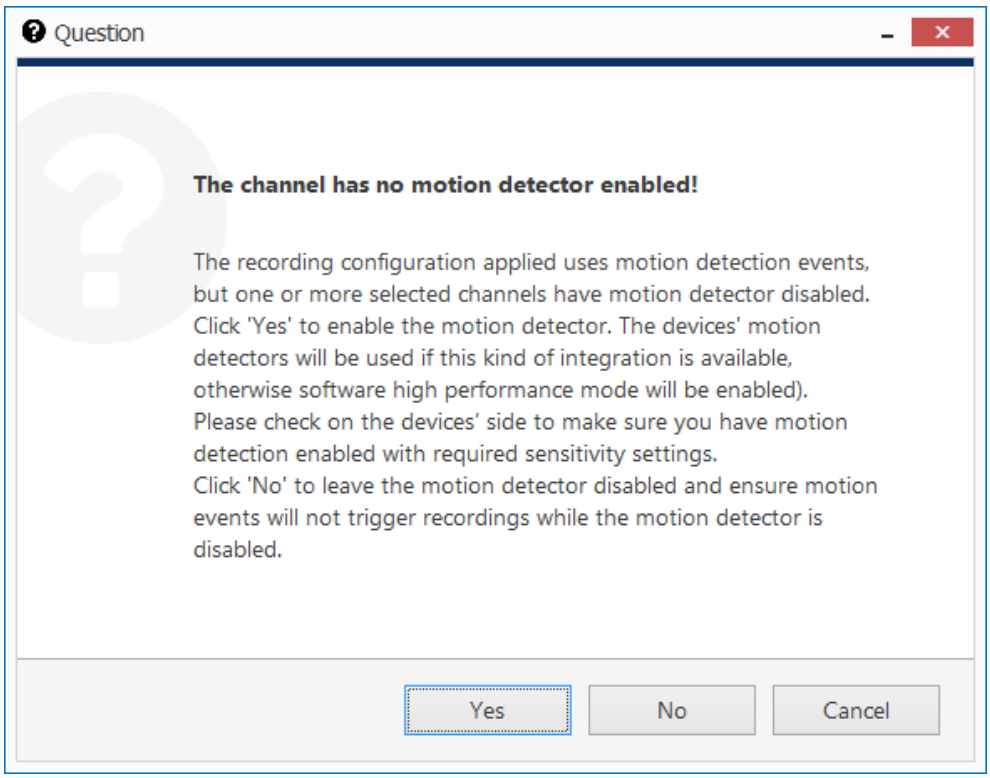
Enter the storage profile title and click *OK* to save and exit.

Click the *Change* button to choose the recording configuration: you can pick an existing configuration or create a new one, or a schedule on the spot from the same dialog box.

Please choose *Continuous Recording* configuration for **edge** streams to ensure proper recording.

When you assign a **motion-based recording configuration** to a channel with a disabled motion detector, the software will automatically suggest enabling motion detection for the target channel. The camera-side detector is given priority; if it is not available, the software-side detector will be enabled and set to the high-performance mode. We recommend that you **review** the motion detector settings to make sure it operates as desired, especially if the camera-side detector is in use.

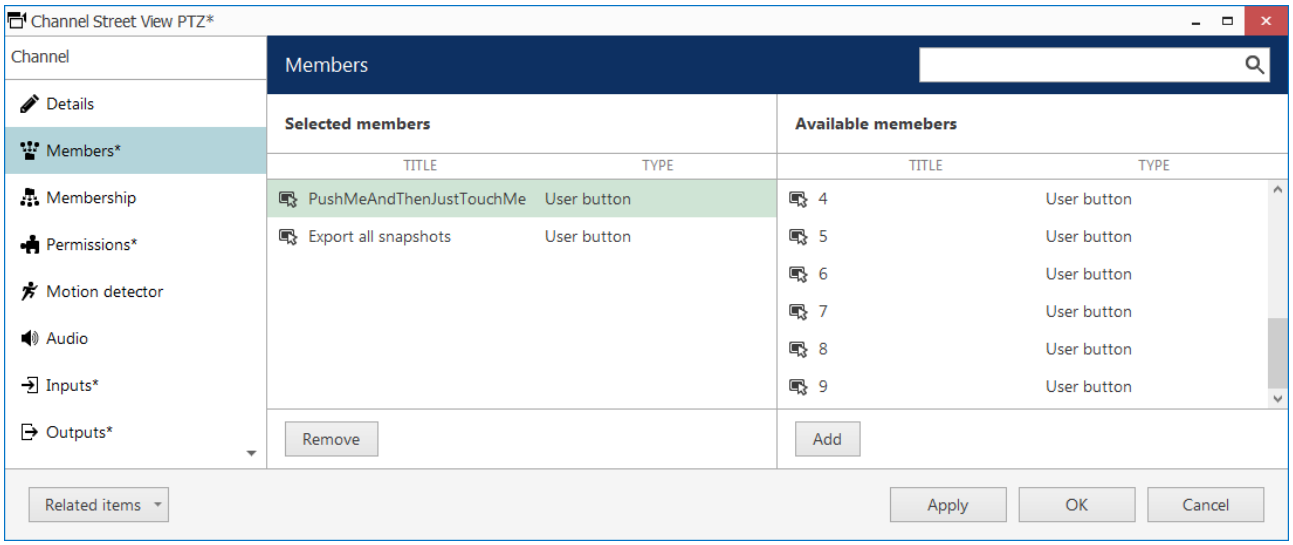
Note that if you leave motion detection OFF and assign motion-based recording configuration to the target channel, no data will be recorded.



Members

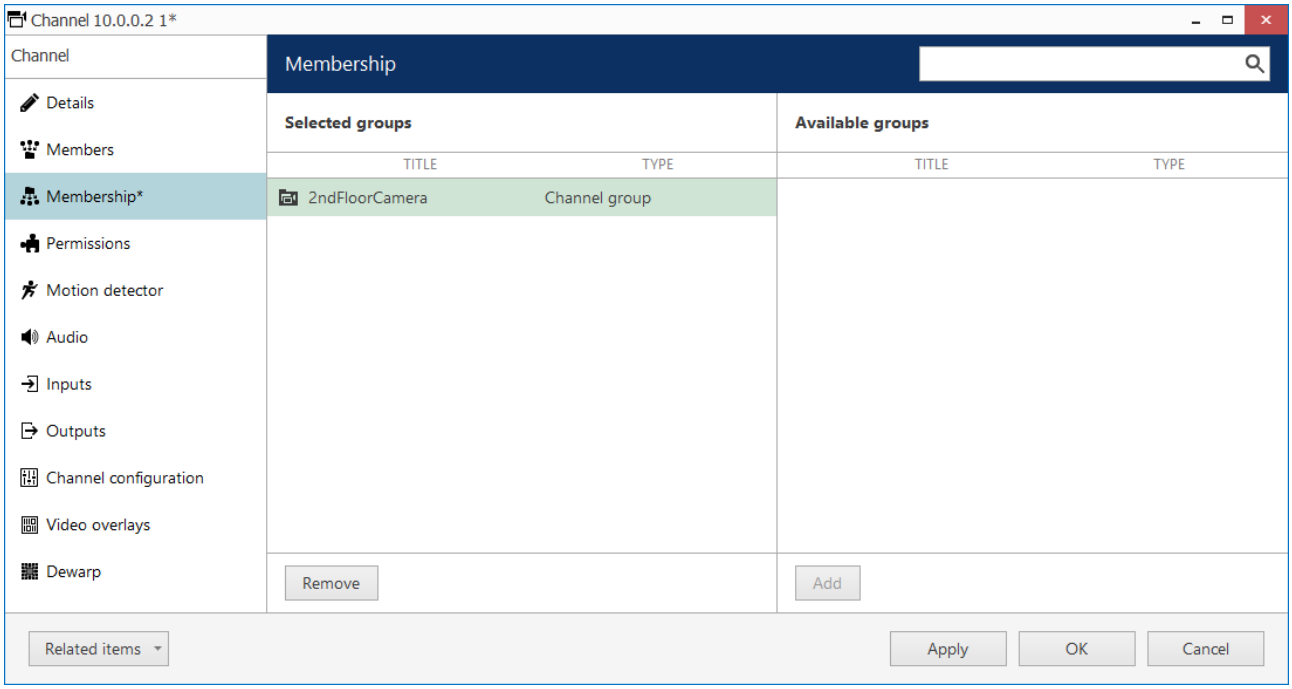
This section allows you to attach [user buttons]to channels, so that they appear together in the Macula Monitor application. User buttons bound to channels in this way will appear as video overlay controls when the target channel is placed into a viewport.

If you are editing a channel group, this tab will allow you to put other channels and channel groups into the target group



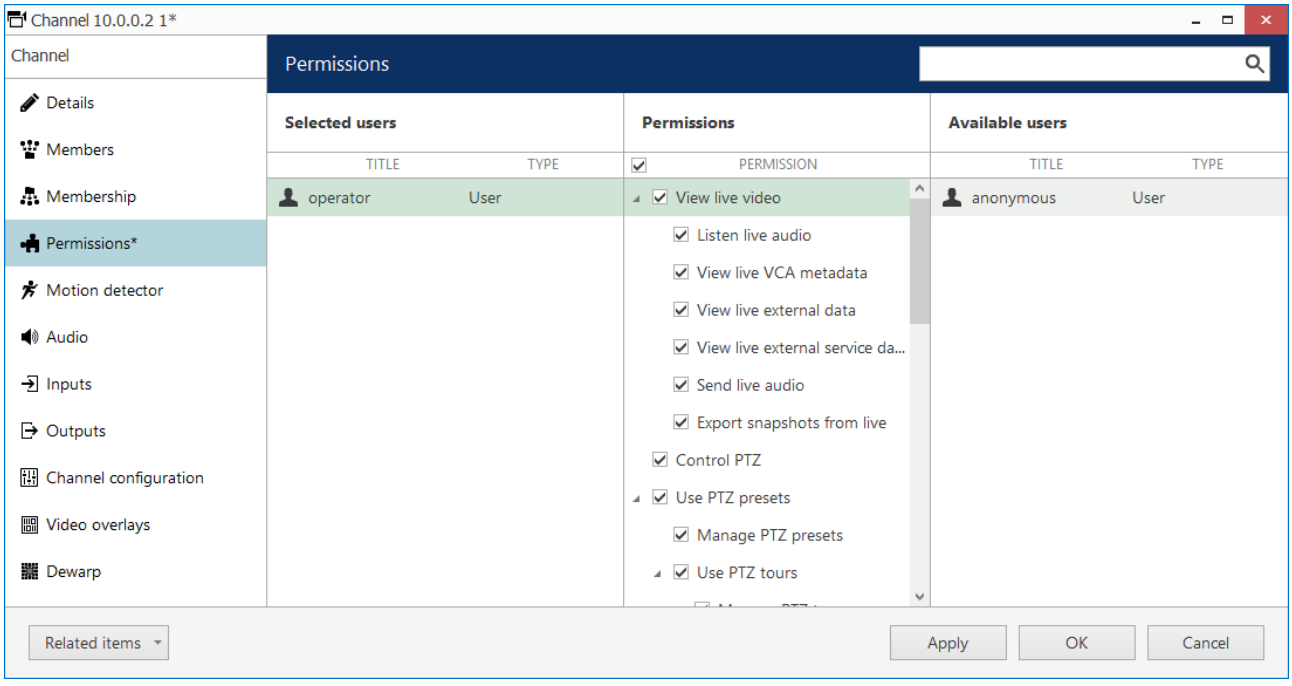
Membership

Choose the group(s) you want to contain the target channel as a member: double-click the relevant items or use the Add/Remove buttons below to select/deselect. You will have both channel groups (internal in Macula Console) and visual groups here.



Permissions

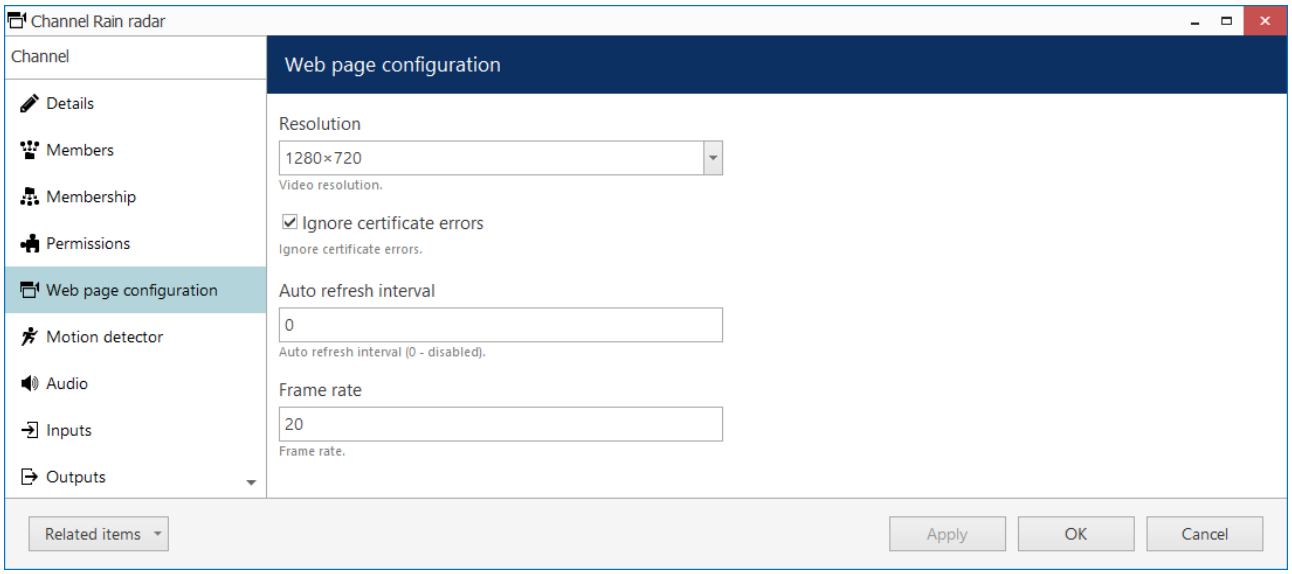
Allow users and user groups to access and administer the target channel. To **add** a user or user group, simply select at least one permission, and the user (user group) will be automatically moved to the *Selected users list*. To **clear** all permissions, double-click the user in the left-hand column. You can also use the **checkbox** next to *Permissions* in the central column to toggle between **all/none** (if not all permissions are selected, the checkbox will be filled with a black rectangle).



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Webpage configuration

This kind of tab will only appear for Crosslink channels and channels bound to devices with the *HTML Source* model (generic model specifically dedicated to static streaming from web), and will affect both live and recording.



The following settings may be available here are:

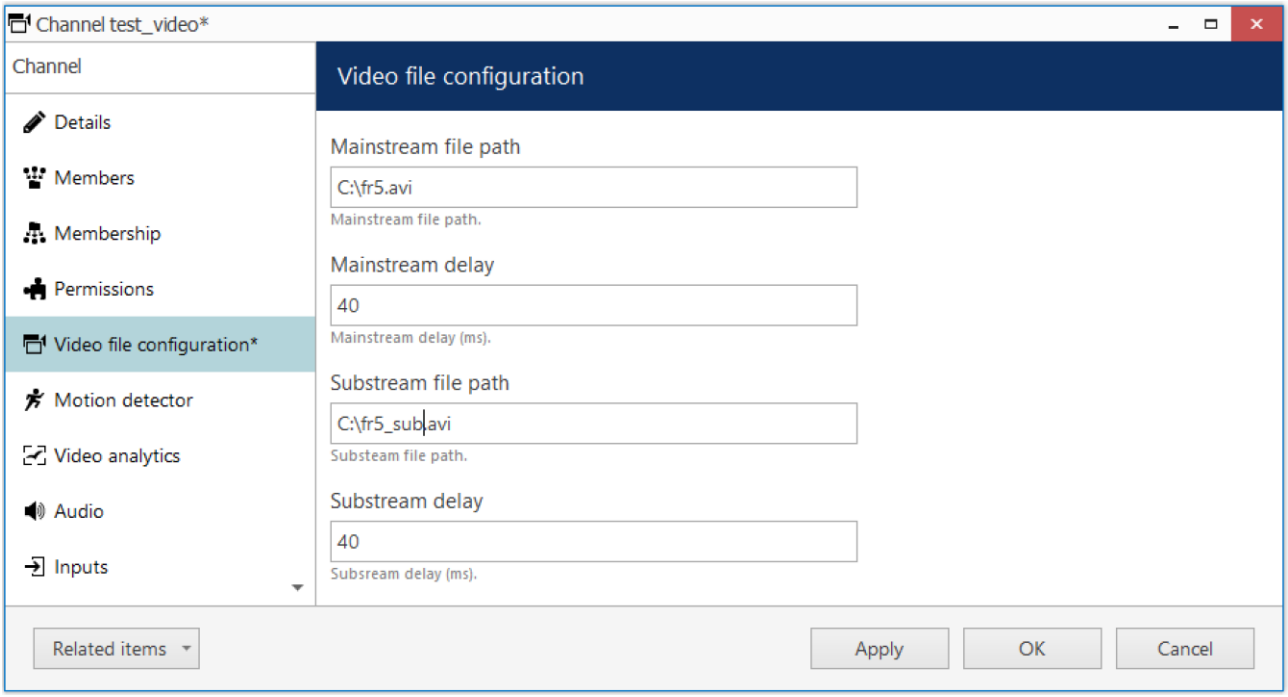
- **Ignore certificate errors**: if the target webpage has a self-signed certificate, the built-in browser may be unable to open it; choose this option to prevent certificate-related issues (unsafe but more likely to operate)
- **Auto refresh interval**: if the page contents is not dynamic (i.e., does not refresh itself), define a refresh period in seconds here (0=disabled, for dynamic contents)

Resolution and frame rate settings have been moved to the *Video configuration* tab.

Video File Configuration

This tab only appears if the underlying device is of the *(Emulation) Video File* type. Here, you can specify the paths to the video streams that will act as main and secondary stream.

Click the *Browse* button to choose the file using Windows Explorer.



For both streams, you can adjust the frame delay: this will affect the speed of the video.

Motion detector

Choose between **camera-side** or **software-side** motion detectors; the default detector state is *disabled*, meaning that no motion information is received or recorded for the target channel. If you are using motion-driven recording profiles, make sure to enable motion detection for the selected channel(s).

> ⚠ When selecting **camera-side motion detection**, make sure to go to device Web interface to enable and configure motion detector. Settings may vary depending on device manufacturer; also, check with GSF to make sure hardware motion detection is supported for the target device.

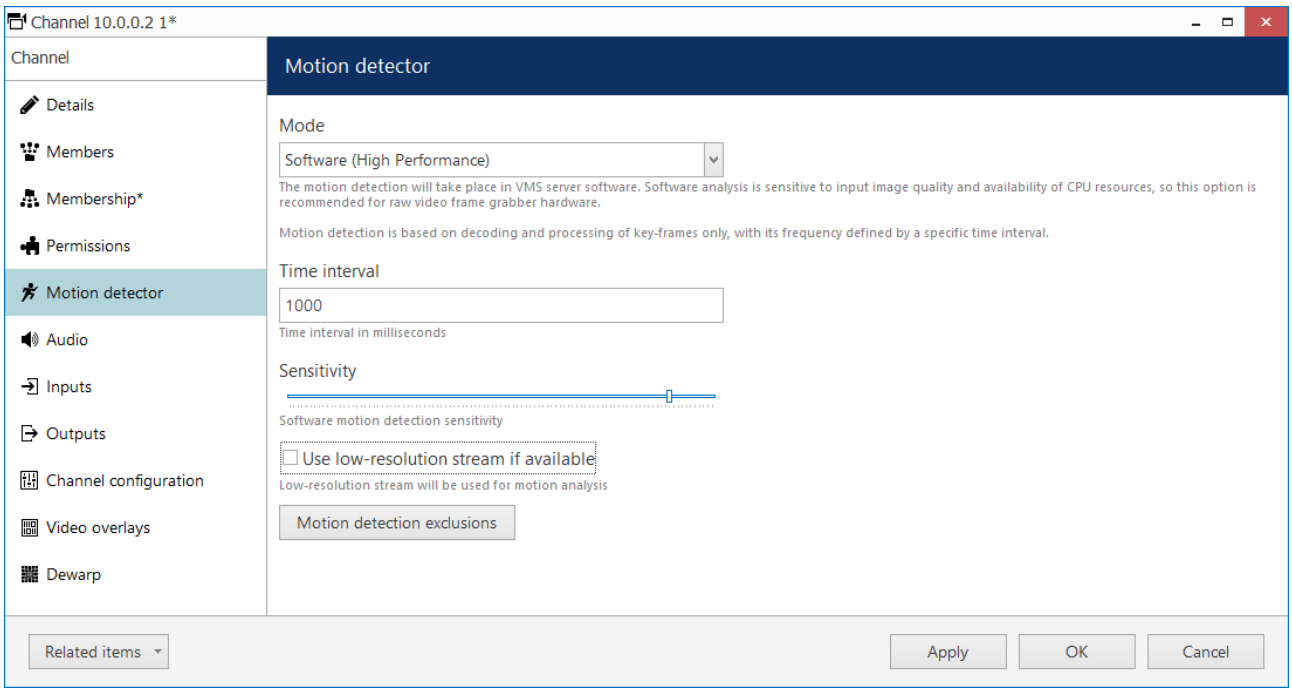
Camera-side motion detection is recommended for two basic reasons:

- computational load is transferred from servers to devices, decreasing server load, and
- on most devices, hardware-side motion detection is performed on raw video stream, which means superior accuracy compared to software-side detector, as software only gets access to compressed stream.

Software-side motion detector is a preferable choice if:

- legacy devices without MD support are used, or
- there is a necessity to use build heatmaps - in this case, grid-like MD on the software side is helpful.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



The motion detector on the software side has two options: high performance and high accuracy:

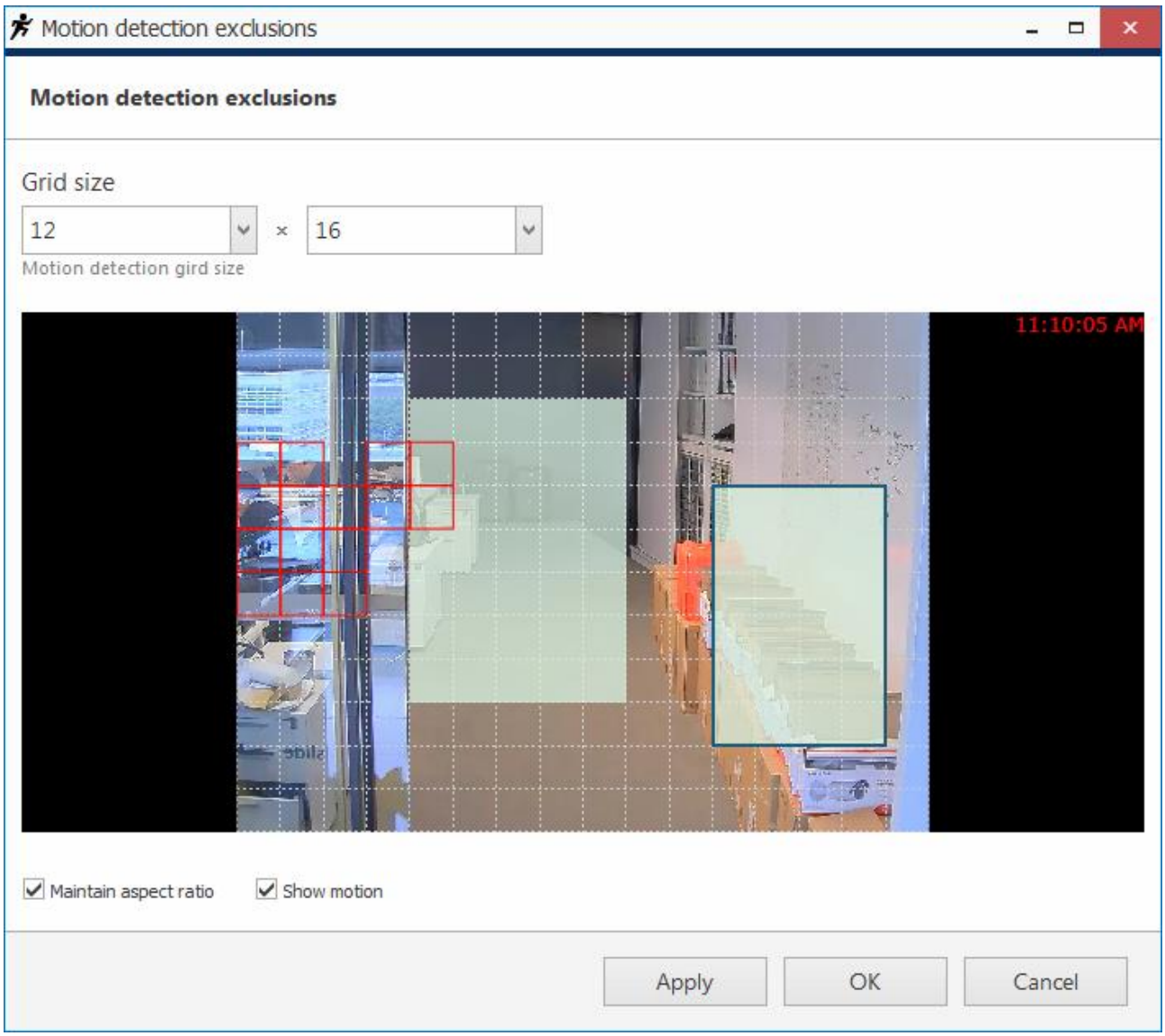
> ***High Performance*** *mode:* this type of analysis is performed for only key frames whose frequency can vary from several frames per second to one frame every few seconds - this is less sensitive for picture quality, but greatly affects detector operation. CPU consumption is significantly lower due to this, and it can be additionally reduced by increasing time interval between two analyzed frames.
>
> ***High Accuracy*** *mode:* this mode performs motion analysis for the whole video stream, so we recommend selecting this option when you want to achieve best detection results. The lower time interval means higher precision. Keep in mind that CPU and virtual memory usage is much greater if this mode is selected.

In both modes, the **level of sensitivity** can be adjusted, as can the time interval setting which defines the frequency of frame analysis.

Regardless of which mode you select, you can further decrease the amount of server-side calculations by using a **lower-resolution stream** (if available). For example, if your main stream is 3MP and your substream is D1, the motion detection engine will spend much less system resources on D1 analysis than it would spend on a 3MP image. Note that some cameras deliver lower-resolution streams as cropped high-resolution images (not resized, as it would be expected) - in such cases, using a substream for MD analysis will produce wrong results and therefore doing so is not advisable.

> Most cameras provide second stream as first stream image scaled to fit low resolution; however, some devices crop the center of a high-resolution image to fit the small frame, and thus the substream picture appears as if it were zoomed in. Keep this in mind when you are using substream for live view and especially for software-side motion detector analysis.

Click the *Motion detection exclusions* button in order to set up **exclusion zones**. Note that these settings only cover the software-side motion detector; in order to configure the exclusions for the camera-side motion detector, go to the Web interface of the target device.



First, choose the **grid size** for the detector: this will define the size of the smallest detection region. Minimum grid size is 2x2 cells (resulting in four detection areas), and maximum size is 64x64 cells. Then, mark your desired exclusion area simply by clicking and dragging on the viewport; you can **draw** several rectangles to form a complex polygonal area. Exclusion area(s) will be highlighted light green. In order to cancel the selection, simply draw a rectangle over it.

Settings in the bottom are here to ease the configuration process:

- *Maintain aspect ratio*: displays original picture proportions, if selected, or stretches the picture to fill the viewport
- *Show motion*: shows currently present motion, if selected

In order to test the behavior of the selected grid size, enable the *Show motion* option, the click *Apply* and see how the detector works with your defined grid.

When you have finished, click *OK* to return to the main channel configuration dialog box.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Video Analytics

Macula servers have a built-in CNN-based engine for the video analysis (VA) with object classification, zones, lines, counters, and rules. In this tab, you can enable and configure the detection parameters for the target channel.

There are several supported neural network **engines** that do the analytics processing:

- Object detector: generic object detector (people, vehicles, animals) with multiple performance options.
- PPE Detector: personal protective equipment detector (vests, head covers).

Choose one of the engines to be used for object detection on the target channels. (It is not possible to enable multiple detector engines to run in parallel).

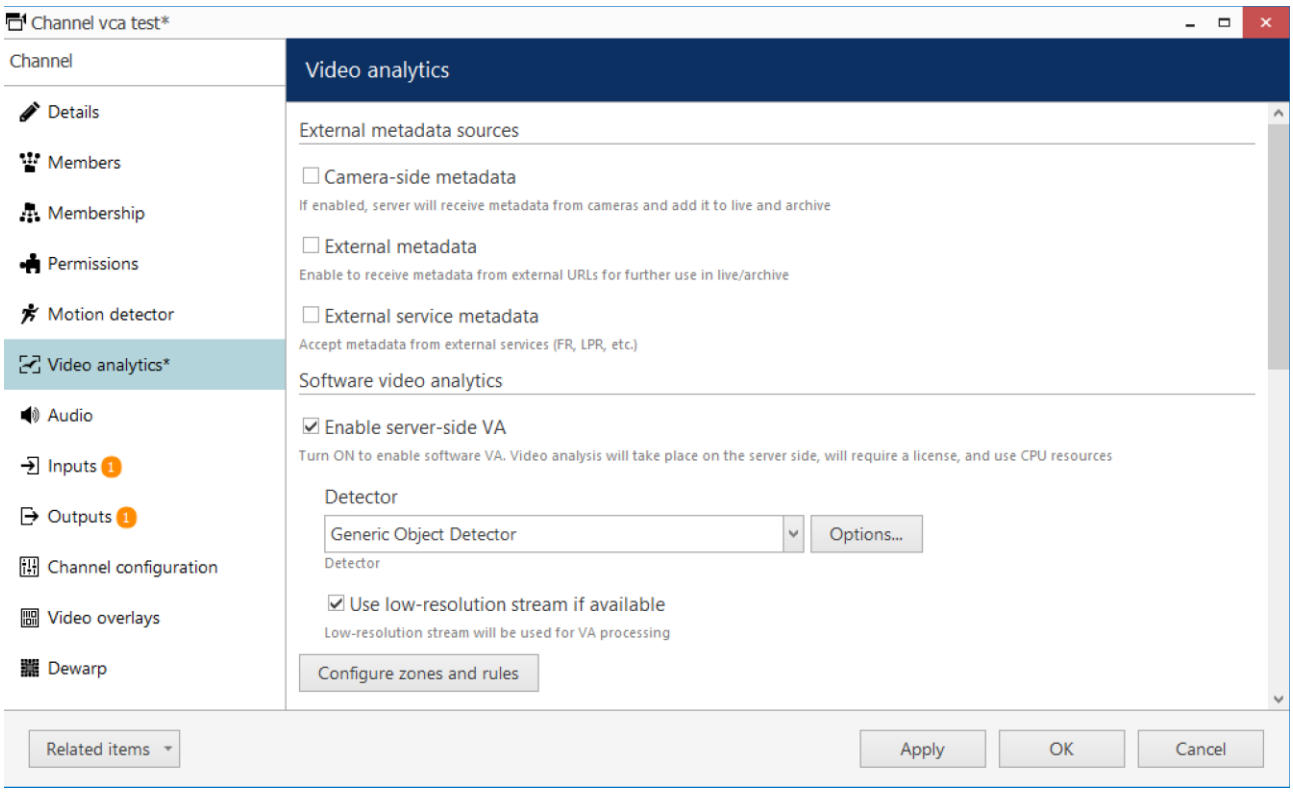
Generic object detector engines use the same neural network. The numbers next to the name designate the size of the downscaled image that will be fed to the VA engine. The bigger the image, the higher the CPU/GPU load will be; larger images also mean that smaller objects will be detected better. Model aspect ratio also may affect detection quality. Overall, it is recommended to test different models and settings for each individual scene.

Please see the dedicated documentation on VA and separately for PPE Detector for more details and recommendations.

> You can configure VA without enabling it for the target channel. This may be convenient when you have a limited VA license but still want to pre-configure the detection.

Before enabling VA for the channel, make sure your VA license allows it. Each Macula installation included 1 (one) generic VA channel free of charge. Specific engines like PPE Detector require a separate license. You can check what channels are using VA license by adding the corresponding column in the *Channels* section. To do this, click the grid icon in the upper right corner of Macula Console and move the *Video Analytics* column to the list on the left, then click *OK*.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



The following settings are available here:

External metadata sources: metadata coming from any source other than Macula embedded video analytics. This also includes old generation Open VCA (embedded into older Macula versions).

- **Camera-side metadata**: if enabled, metadata received from the device (edge VA) will be displayed in Macula Monitor overlaying the video stream, and will also be used for event triggering.
- **External metadata**: if enabled, server will accept metadata sent by external sources in JSON format for video overlay, event triggering, and search
- **External service metadata**: if enabled, server will accept metadata from integrated services that are configured as external services, for the purposes of live/playback overlay, search, and event triggering

Software video analytics: here, you can enable and configure server-side VA.

- **Enable**: if selected, the server will perform video analysis for the target video channel, and metadata overlay will be turned ON on the Macula Monitor side (affects all connected Macula Monitor applications)
- **Use low-resolution stream if available**: similarly to motion detector, VA can be performed on the secondary video stream in order to save server resources. We recommend that you keep this setting ON.
- **Detector**: choose one of the available detection engines.
- **Options**: click to set the engine-specific parameters.
- **Configure zones and rules**: click the button to enter overlay setup
- **Classes**: click *Change* and choose the object classes that you want to be detected in the target video (deselected classes will be unavailable for rules)
- **Detection interval***: time (delay) in milliseconds between two successive detections (similar to MD), default: 200ms

- Object loss timeout: time interval in seconds, after which the object out of sight will be considered lost (and will be detected as new object if appears again), default: 6 seconds
- **Scene dynamics****: relative speed of the objects in the scene
- **Confidence threshold**: minimum level of confidence to decide if the object belongs to a class (detections with lower confidence will be disregarded), default: 70%
- **Object similarity threshold*****: the minimal level of object similarity between two detections to decide that it is the same object (objects with lower similarity will be detected as new), default: 85%, optimal range: 50-90%
- **Maximum object size**: percentage of the image height and width that can be occupied by a single object at max. Enable this option to eliminate false detections of large non-existent objects.

***This is the minimum time between two detections. If the video stream FPS is low, the actual interval may be longer.

***This is the minimum time between two detections. If the video stream FPS is low, the actual interval may be longer.

****This setting teaches the VA engine where to look for the same object in the next frame. Slower option means the object is present in more frames. Faster means the object is present in less frames during its appearance. Choose slower options for calm scenes with low-speed objects (e.g., people walking), and faster for dynamic scenes (highway etc.).

*****Highly affects the engine ability to track the objects. If the value is too low for the target scene, different objects may be considered one. Too high (close to 100) causes each detection to produce a new object each time. We recommend that you start with the default value, and change it slowly when testing. Scenes with many similar objects (e.g., items on the conveyor belt) require slightly higher similarity and correct object speed (see above).

Engine Options

Click the *Options* button next to the VA engine drop-down list to open the engine-specific settings. These mostly refer to GPU usage.

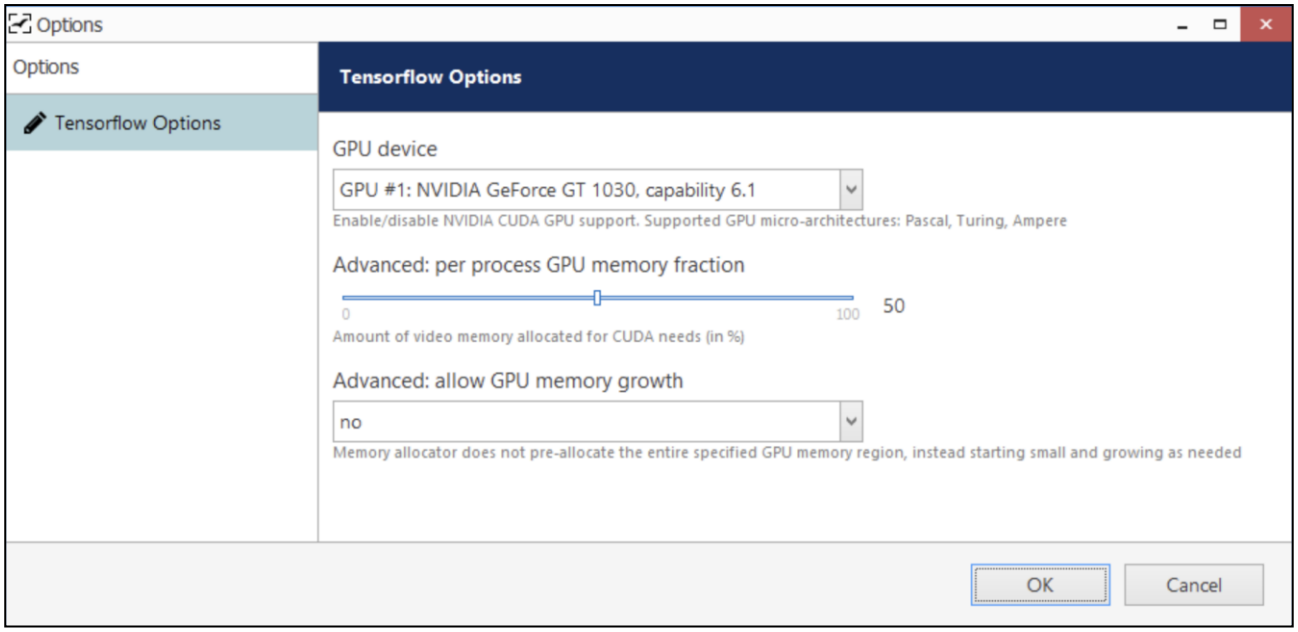
For the **generic object detector** engine, the following settings are available:

- **GPU device***: choose one of the supported graphics cards, or choose *Disable* to leave VA running on CPU
- **Advanced** (only change this if you know what you are doing!)**: per process GPU memory fraction**: amount of video memory in % to be allocated for CUDA; default value 50%
- **Advanced** (only change this if you know what you are doing!): **allow GPU memory growth**: set this to *Yes* this if you prefer the entire video memory chunk to be pre-allocated instead of gradual growth

*Supported GPUs are NVIDIA video cards with capability parameter 6.0 or higher (Pascal, Turing, or Ampere architecture).

⚠ In order to enable GPU usage for video analytics, please install **NVIDIA CUDA toolkit redistributable** package, which is NOT a part of the Macula installation. You can download the

toolkit from the GSF website (usually available with the latest GSF Macula version), or request it from GSF or via support@gsfcorp.com.



If you have **multiple** video cards, you can assign different cards to different channels. Leave the **advanced settings** the same for all channels that use the same graphics card. You can also leave some channels to run on CPU (for example, the generic 300x300 model is optimized for mobile CPUs and will therefore better perform on CPU, not GPU).

Create VA Zones and Rules

Click the *Configure zones and rules* button to bring up the video overlay dialog box. By default, only VA overlays are displayed, but you can use the *Show all* checkbox to see if there are other overlays (e.g., data sources) configured for this channel.

In the top right corner, there are VA markers: **counter**, counting **line**, and polygonal **zone**. Drag and drop the marker onto the picture to place it, then adjust its size and position.

Zone and Line Properties

Click a **zone** or a **line** to see its properties in the rightmost column:

- **Type**: corresponding element type (line, polygon)
- **Title**: user-defined item name, e.g., Lobby
- **Color**: choose the element color using the standard palette
- **Opacity**: color opacity (0=transparent, 100=solid)

Additionally, each **zone** has some properties that affect event triggering and are individual for each zone:

- Object **presence** time: time in seconds for the object to stay inside the zone before the "object entered or appeared" event is triggered (default: 1 second)

- Object **absence** time: time in seconds for the object to stay outside the zone for the "object left or disappeared" event is triggered (default: 1 second)
- Object **intersection threshold**: percentage of the object area to cross the zone border for it to be considered a crossing (default: 50%, half of the object)

For example, with default settings: if more than half of the object stays inside the zone for longer than one second, the "object appeared" event is triggered.

⚠ Please note that markers are just **visual** elements: you need to add **rules** and then create **E&A rules** to trigger some event chains.

💡 Zones are rectangular by default but you can add **new nodes** by right-clicking on the zone border and selecting *Add*.

Rules and Counters

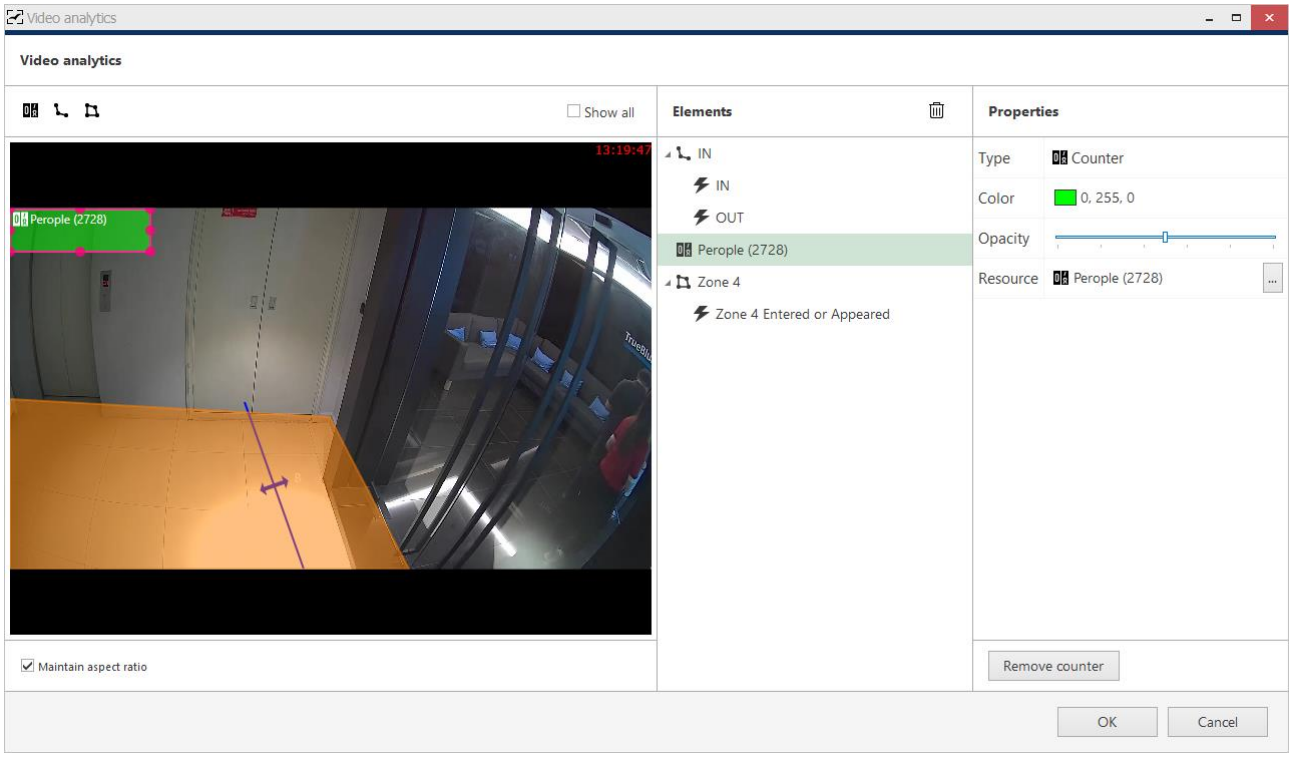
For each **zone** or **line**, you can create rules, which can be later used to trigger events in E&A. For example, such rules can increment counters:

- for reflecting the current number of objects in the zone, use the special *Zone counter type*,
- for other rules, create new counters and then go to the E&A configurator to add rules that will increment those counters.

For each **counter marker** in VA, you will need to map it to a real counter to make it work.

- to **track the number of people in any zone**: create *Zone counter* under the zone, then drag and drop a counter marker, and bind it to the zone counter
- to **count objects** appearances for **lines** or **zones**: create a new counter (or choose an existing E&A counter from the list), then drag and drop the counter marker and bind it to the counter

In such a way, you can use the same counters from E&A for multiple channels' VA, for example, to count the total number of customers coming via different doors.



For each zone/line rule, you can choose one or multiple **object classes** to be tracked. You can only choose among classes that have been enabled for the current channel in the previous dialog box.

Available **line rules**:

- *Crossed AB* or *Crossed BA*: object has crossed the line in the specified direction
- *Crossed*: object has crossed the line in any direction

Available **zone events**:

- *Entered or appeared*: the object appeared in the zone either by crossing its border from outside to inside, or appeared directly inside (e.g., if the zone border is equal to the frame border, or there is a door inside the zone)
- *Leaved or disappeared*: the object departed from the zone either by crossing its border from inside out, or simply disappeared inside the zone (e.g., there is a door inside the zone)

Available counter types:

- zone counter: reflects the current number of certain objects in the zone
- counter: E&A software counter

Use the buttons below the objects and their properties to create and remove rules. Note that these rules only exist in VA configuration; in order to set up reactions, go to the Events&Actions section of Macula Console.

VA Configuration Examples

Workflow **example**: count the number of people who entered the zone.

1. Drag and drop a zone marker onto the picture. Stretch the zone and add new nodes to cover the desired area.

2. Click the *New rule* button, then select the *Entered or leaved* event type, and set class to *Person* on the right.
3. Drag and drop a counter marker onto the picture.
4. Click the counter, then click the ... (three dots) button in the properties column on the right and choose a counter. If there are none, create a new one using the *New counter* button below the list.
5. Save the video analytics settings.
6. Go to Events&Actions, create a new event of the *VCA event* type, choose your VA camera as source, and your VA zone event from step 2 as VCA rule. (Note that the rules will not be listed if VA is disabled for the target channel).
7. Create a E&A rule using the event from step 6 and a built-in action *Increment counter* for the target counter.

Zone counters can only reflect the current number of typed objects in the zone, therefore, these cannot be incremented or decremented.

Example 2: pop up camera if there are 3 people in the zone.

1. Drag and drop a zone marker onto the picture. Stretch the zone and add new nodes to cover the desired area.
2. Click the *New zone counter* button below the zone list. The counter will appear in the same list.
3. Save the video analytics settings.
4. Go to Events&Actions, create a new event of the *Counter value* type. Select the counter you created on step 2 as event source. Set the operator to Equal and value to 3.
5. Create a E&A rule using the event from step 4 and a built-in action *Pop up camera on screen*. Set the desired channel as rule target to define, which camera pops up

Audio

Here, select the **audio source** for the target channel. The available options are:

- **None**: the channel will have no audio track
- **Internal**: built-in or line-in camera microphone will be used as the audio source (G.711 only!)
- **Attached**: a microphone that is physically connected to the server will serve as the audio source (server must be the one having this channel in its configuration)
    - **Audio source**: select one of the devices from the drop-down list. If the list is empty, make sure that the server has a microphone connected and that it is visible/working in the Windows Control Panel.
- **External**: use audio from another channel. Audio will be combined with the target channel video in both live and playback.

When fetching audio from the device side (**internal** source), make sure to choose the **G.711** codec. Other codecs are not supported at this point, and selecting them may result in unavailable video stream, too, when both video and audio are packed into the RTSP stream.

For audio sources that are **attached** to the server: you can use both line-in microphones, as well as ones connected via audio board, which supports multiple microphones at once. There are three important requirements here:

- the target channel and the target audio device must belong to the same server
- the attached audio device(s) must be recognized by the operating system

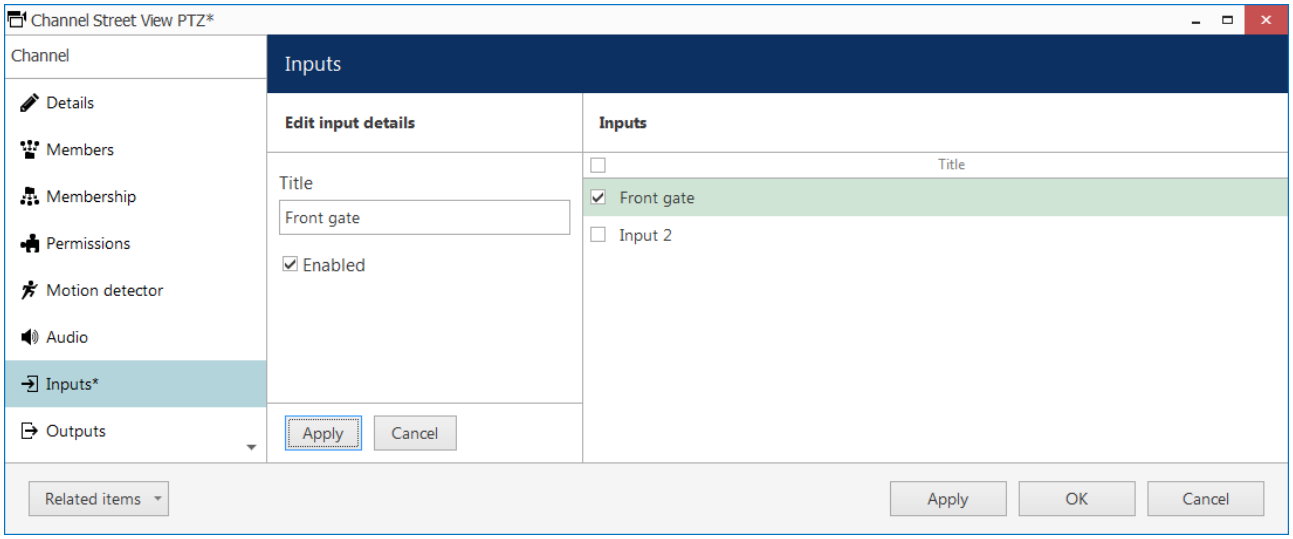
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

- the list of audio devices is retrieved live, so the target server must be online for you to apply the configuration

Digital Inputs

If digital inputs (DI) are supported for the underlying device, the available inputs will be listed here. Mark them in the list in order to allow event generation from those inputs: events can be later set up in the E&A Configurator using the *Digital input* event type. After changing the DI name, click *Apply* below for the changes to take effect: the setting will not be saved if you simply switch to another tab.

Note that the tab contents is retrieved in **real time** from the target device, therefore, it may take several seconds for the contents to become available. In case the target device is offline/unavailable, or if there is no support for DI for the selected device model, the list will be empty and a corresponding warning will appear.

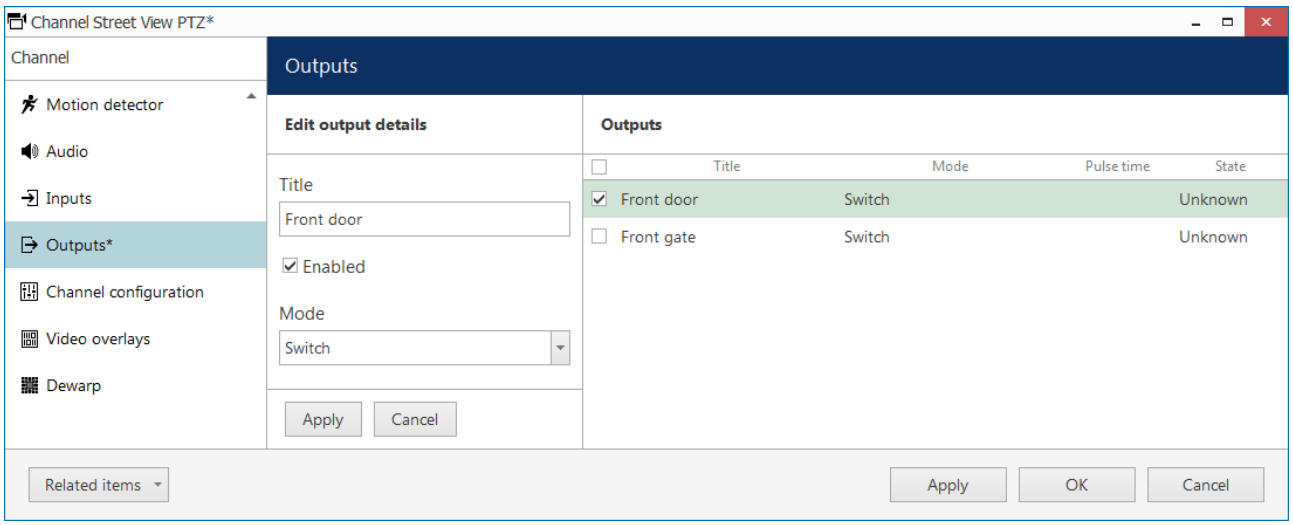


Digital Outputs

You can change the state of **digital outputs** (DO) from the E&A Configurator (target action type: *Control digital output*). For the DO to be available in actions, select them here by putting a mark in the corresponding checkboxes. Optionally, you can also change the DO names. Click the *Apply* button below the output details to save the changes before moving to other settings.

For each relay output, you can also specify the desired **mode**: switch, inverted switch or pulse. This defines the command that will be sent to the device when DO action is triggered in E&A.

Note that the tab contents is retrieved in **real time** from the target device, therefore, it may take several seconds for the contents to become available. If the target device is offline/unavailable, has no DO, or if there is no support for DO for the selected device model, the list will be empty and a corresponding warning will appear. In case your device does have DO but they are not supported by software, you can still change their state from Macula E&A by using CGI/HTTP commands (action type: Send *HTTP request* or *Run program*). The exact command text depends on the device and can be found in the device documentation.



Video Overlays

Here, you can create **channels shortcuts** and also choose a data provider to **embed** some **textual data** with the video. The section below explains channel shortcuts; for setup guidelines on the data overlay, please refer to the Data Sources section of this document. Video analytics visual elements are explained above.

> By default, only channel shortcuts and data source overlays are displayed here. Enable the *Show all* option above the video preview to **see all visual elements** (e.g., video analytics).

Channel shortcuts are interactive video overlay elements intended for instant switching between video channels in the Macula Monitor application's live view mode. In other words, these are visual controls that appear on top of the video and clicking them will open other (pre-defined) video channels in the same viewport. These "portals" are configured in Macula Console and then used in the Macula Monitor application.

Video Overlay Shortcuts a.k.a Portals

Starting with version 1.25 it is possible to mark video overlay shortcuts not only as a rectangle but as a free-form polygon too. Also, it is possible to create video overlay shortcuts for:

- **Data and video channels**
- **Maps**
- **Buttons**
- **Webpages**
- **Shared layouts**

By clicking the dedicated area inside the *channel*, in the Macula Monitor, you can switch data and video channels, trigger events assigned to buttons, and switch between saved *shared layouts*.

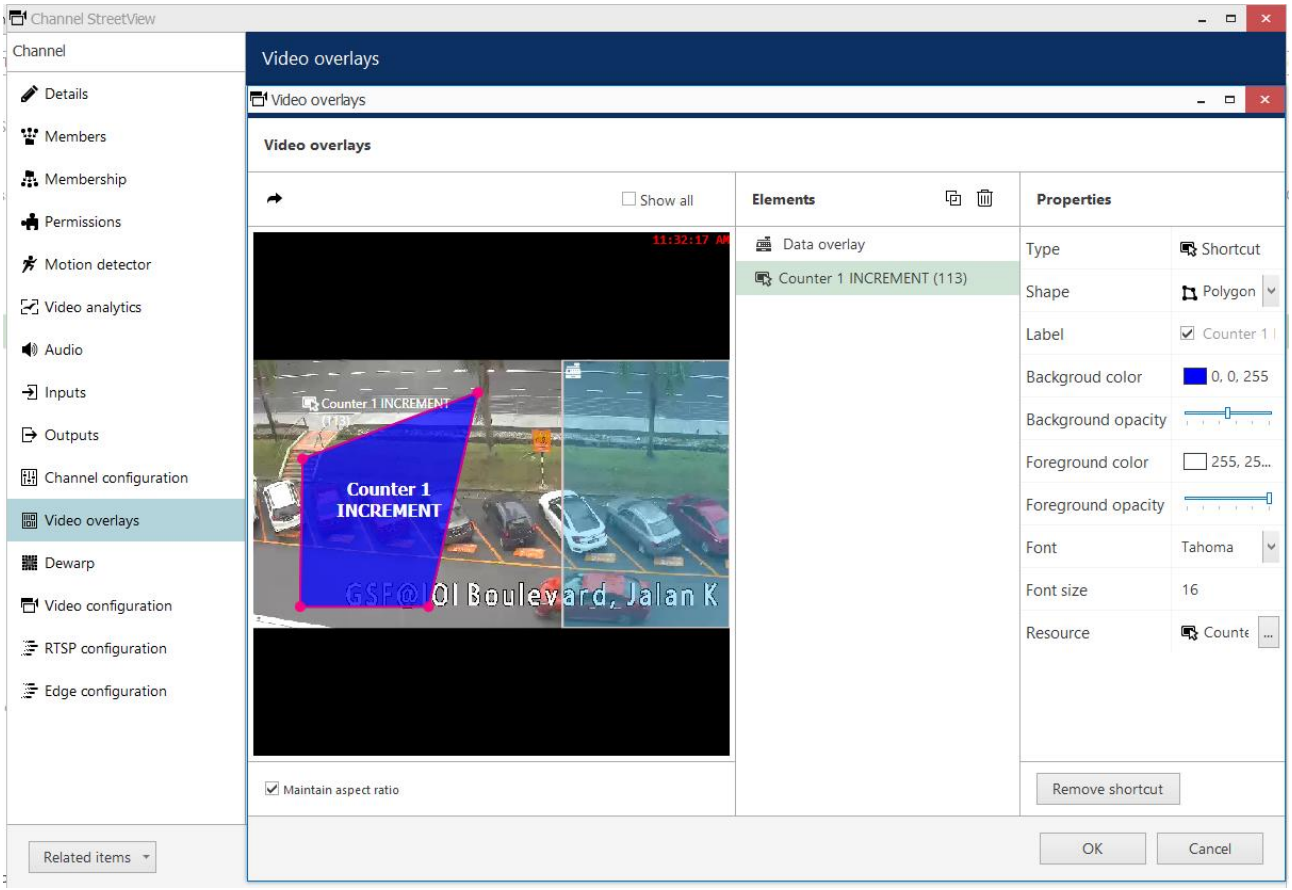
Adding portals to channels

To add a new "portal" to the *channel*, in the Macula Console go to:

1. *Configuration ->channels->* Select a preferred *channel* and then click the *Edit* button on top or double-click the preferred *channel*
2. Select video overlay and klick *Configure video overlays* button
3. Drag the "portal" icon to the *channel* layout view and mark the zone you want to use as a shortcut.

To assign existing resources to a shortcut, select your shortcut in the *Elements* panel, then in the *Properties* panel, click on *Resources* and assign from the available list.

> ⚠ **N.B.** User buttons assigned as video overlay shortcuts do not have any indication and work with a single click. To check if the button was actually triggered, go to the Alert tab in Macula Monitor



> ⚠ Make sure the video from the target channel is available before setting up the channel shortcuts in order to ensure correct shortcut placement.

The video Overlay window contains three tabs. The first tab is for the channel camera view and all the overlay markings. The Elements tab allows you to switch between added overlays, and the Properties tab contains options specific to the chosen overlay.

Shortcut Overlay Properties

- **Type:** type of video overlay
- **Shape:** can be rectangle or polygon
- **Label:** optional text to display with Overlay in Macula Monitor viewport
- **Background color/opacity**: shortcut color and its transparency

- **Foreground color/opacity:** shortcut font color
- **Font/Font Size:** face and size of displayed shortcut font
- **Resource:** resource linked to Video Overlay shortcut

Data Overlay Properties

- **Type:** type of video overlay
- **Line count:** how many lines are allowed per video port
- **Timeout:** how long data will be displayed since the last data input
- **Text color:** data Overlay viewport font color
- **Data Source:** data source connected to the selected channel
- **Data ID:** data ID

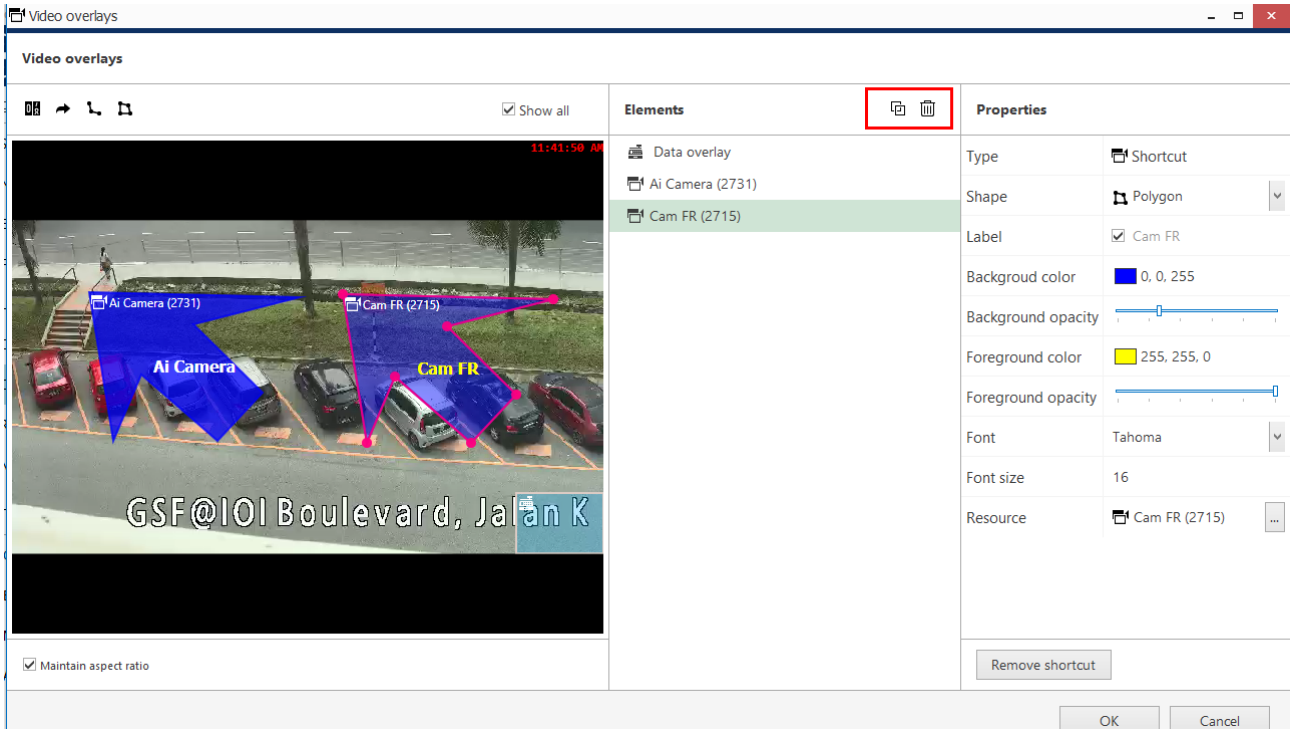
Counter Overlay Properties

- **Type:** Type of video overlay
- **Text:** Optional text to display with Overlay in Macula Monitor viewport
- **Color:** Displayed text color
- **Opacity:** Displayed text opacity
- **Font/Font Size:** Face and size of displayed shortcut font
- **Resource:** resource linked to Video Overlay shortcut

To **remove** any unneeded *Shortcut, Counter* or *Data Overlay* - select it in the video viewport or in *Elements* tab and click the *Recycle bin* button in the panel above the video.

To **save** the video overlay settings, click *OK* to close the dialog box and then click *Apply* or *OK* in the *Edit channel* dialog box. If you click *Cancel* to discard changes in the *Edit channel* dialog box, adjustments in the video overlays will not be saved.

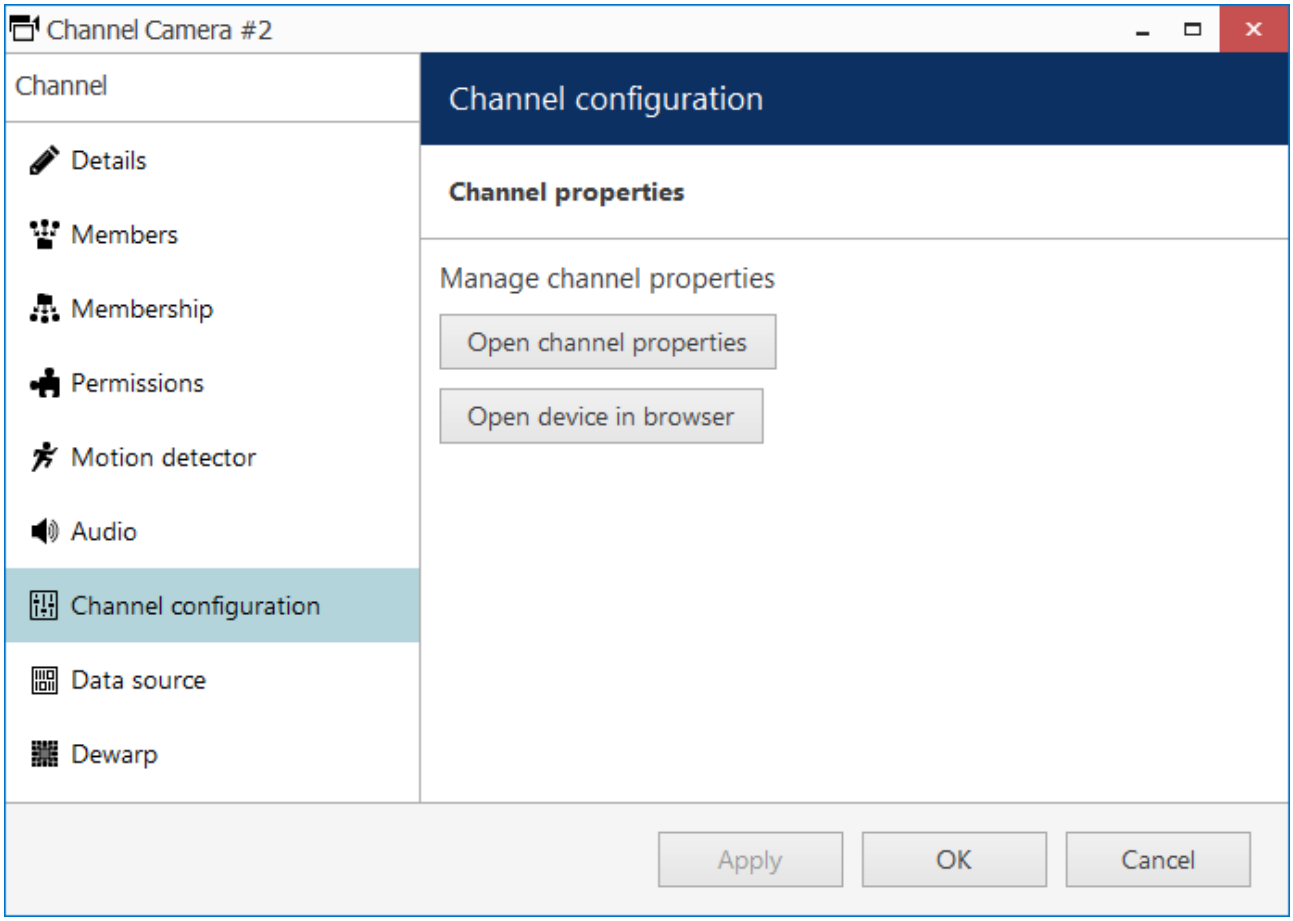
Shortcuts and *Counter Overlays* can be duplicated. To do so, select the *Overlay* you want to duplicate. At the top of the *Elements* section, you will find two buttons, one for deleting the overlay and the second for duplicating. Click on the *Duplicate* button. This will create a copy of the selected overlay.



Channel Configuration

The *Channel Configuration* tab allows you to adjust advanced channel settings. Some of these can be changed via Macula Console but sometimes software does not cover some of the device settings, so you are also given the option to go straight to the device Web interface - simply click the *Open device in browser* button to do this.

For ONVIF channels (if device model is set to (Generic) ONVIF Compatible), there is an option to set up **imaging settings**: the corresponding button will appear next to the *Channel properties* button. Please see below for more details.



Click *Open channel properties* to access the additional channel configuration dialog box. The available tabs depend on the device model and capabilities: for some cameras, only basic configuration options are present, while for others, advanced settings are accessible. If you see that a camera has certain capabilities that are not configurable via Macula Console configuration interface, go to the device's Web interface in order to change that specific setting.

- **Video Input tab**: set video transport (the available list of options depends on the device type and model; common types include HTTP, RTSP***** and native transport)
- **Video Adjustment tab**: fine-tune picture settings such as brightness and contrast level
- **Substream tab:** enable second (lower resolution) stream
- **Video Configuration tab**: choose streaming settings******
- **Motion Detection tab:** with some devices, the camera-side motion detector must be explicitly enabled here

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

- **External PTZ tab**: adjust external PTZ controller settings; communication port must match the communication port that the RS232/485 controller is connected to, and baud rate has to match the baud rate of your PTZ controller/analog PTZ camera
- **RTSP tab**: appears if RTSP transport type has been chosen; set RTSP port and mode (TCP/UDP/multicast***) here

*You may have to specify the RTSP port on the corresponding tab if it differs from default (port 554 for most cameras). To do this, select the RTSP transport type and then click *Apply*: as a result, the RTSP tab will become available. For ONVIF devices, the RTSP port is set automatically.

**Remember, the higher the resolution/bitrate/quality/frame rate you set, the more storage space and bandwidth it will use when recording. These settings also affect CPU/virtual memory resource consumption for live video and software-side motion detection.

***Multicast mode availability depends on device integration.

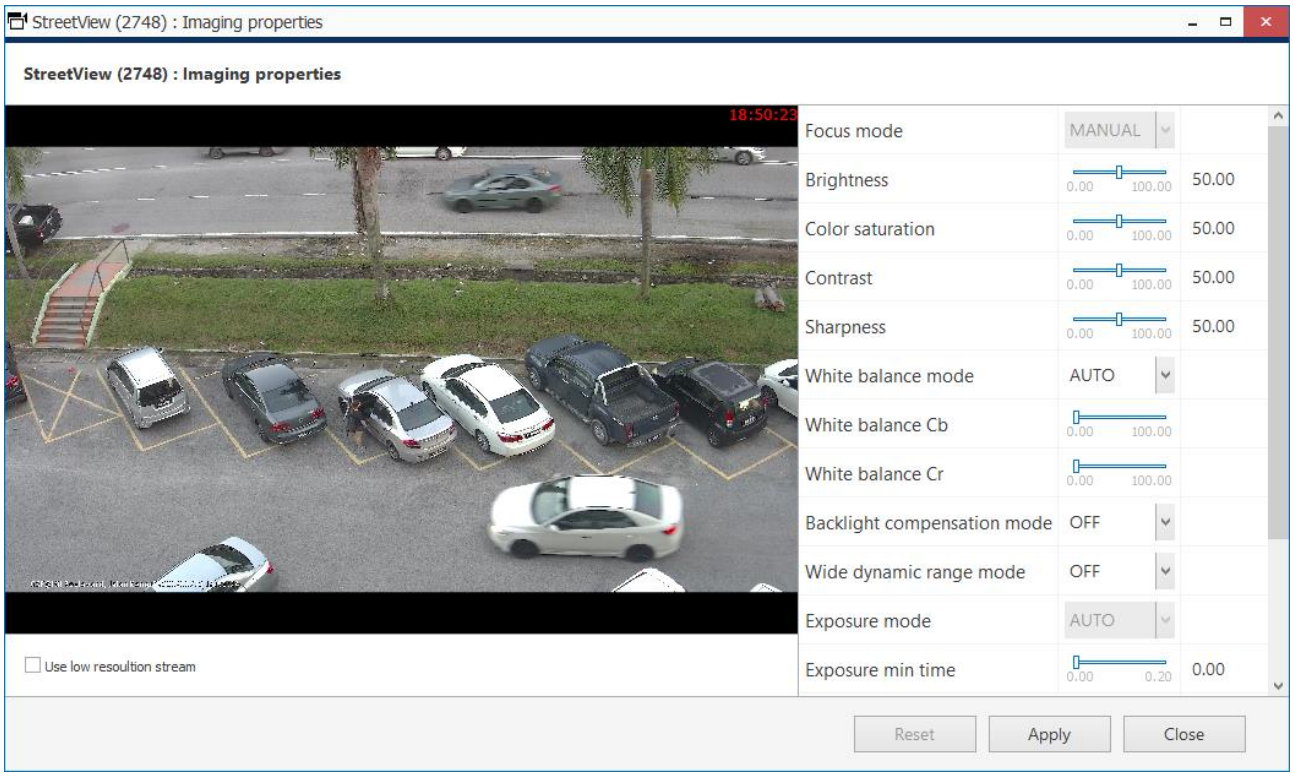
Note that a valid administrative account login and password for the camera should be provided in *Device* settings in order to access and set the device configuration.

Imaging Settings

For ONVIF device channels, it is possible to adjust the image settings like brightness, saturation etc. To access these settings, open the channel for editing, choose the *Channel configuration* tab, then click the *Open imaging properties* button.

Adjust the settings, then click *Apply*. If you like the result, click *OK* to close the dialog box and exit.

Use the *Reset* button to revert the latest changes. If you save the changes and close the window, next time you open it Macula Console will treat the previous settings as default and will reset to them (and not some other set of values). To reset the imaging settings to the factory defaults, use the camera Web interface.



Use the low resolution stream for image preview to compare the pictures and make sure the applied imaging settings look good on both streams (e.g., make sure important elements are visible).

Dewarp

Here, you can configure generic dewarp settings or enable dewarp engine for the Panomorph Enables® lens. For details, please see the subsequent topic on dewarp setup.

Video Configuration

This tab is only available for certain device drivers like ONVIF. For other devices, go to the *Channel Configuration* tab (described above).

Here, you can select stream properties for both **main** and **secondary** video streams. The options are fetched from the device so the availability may differ depending on the vendor.

> ⚠ The settings are changed on the device side, too, so make sure the target device is not configured in some other video management software in order to avoid configuration conflict.

Available settings:

- **Profile**: choose one of the video streams profiles (built-in or pre-configured on the device side)
- **Encoding**, **resolution**, **quality**, **GOV length***, **frame rate**, **bitrate**, **bitrate mode**: choose one of the available settings according to your needs

By default, camera-side settings are used (whatever is currently set on the device side). You can override all settings or only some of them.

> 💡 Note that a valid administrative account login and password for the camera should be provided in Device settings in order to access and set the device configuration.

***Too long GOV intervals (hence, low i-frame rate) may cause recording and **playback issues**. Channels with too low i-frame rate will have a warning (orange color) in the *Monitoring* section of Macula Console, under *Channels*. To view this column, click the grid icon in the upper right corner and move the columns *Main stream GOP size* and *Substream GOP size* to the left, then click *OK*.

RTSP Configuration

This tab is only available for certain device drivers like ONVIF. For other devices, go to the *Channel Configuration* tab (described above)ss.

By default, the **default port of 554** is used for obtaining video over RTSP. Here, you can **override** the default port, and also choose between unicast and multicast.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Edge Configuration

This tab is only available for certain device drivers like ONVIF. For other devices, go to the *Channel Configuration* tab (described above).

For some devices, Macula can fetch the recording done on the device side (on camera SD card). This tab contains some settings related to the edge stream synchronization.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

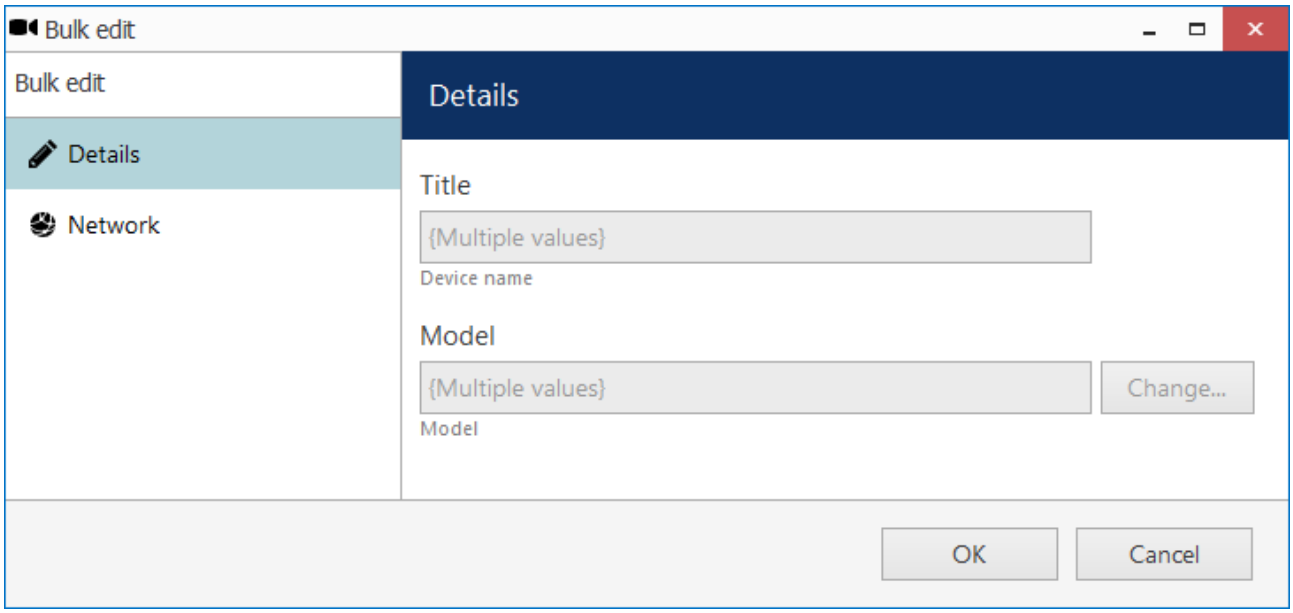
5.6 Bulk Edit for Devices and Channels

For easier resource management, it has been made possible to edit certain settings of devices and channels, e.g., recording settings and motion detection, for multiple items at once. To do so, simply select more than one device or channel in the item list using CTRL+click or Shift+click (use CTRL+A to mark all) and then click the *Bulk Edit* button on the top panel. Note that the button will not be there unless at least two items are selected.

- Some settings will be grayed out, indicating that these either cannot be changed at all or specifically via bulk edit
- *{Multiple values}* text in the setting field indicates that selected items have different options, e.g., have different recording configurations
    - leave such a field untouched if you wish to keep these settings different
    - change the value of such a field to something specific using the *Change* button to assign the same setting to all selected items
- Fields containing specific values or empty fields indicate that all selected items have the same setting (often default); change the value to assign the setting to all items at once

Edit Multiple Devices

Select at least two devices in the list and click *Bulk Edit* on the top panel to bring up the corresponding dialog box. Some settings will be grayed out, indicating that these settings either cannot be changed at all or specifically via bulk edit.



For devices, you will be able to modify the following settings:

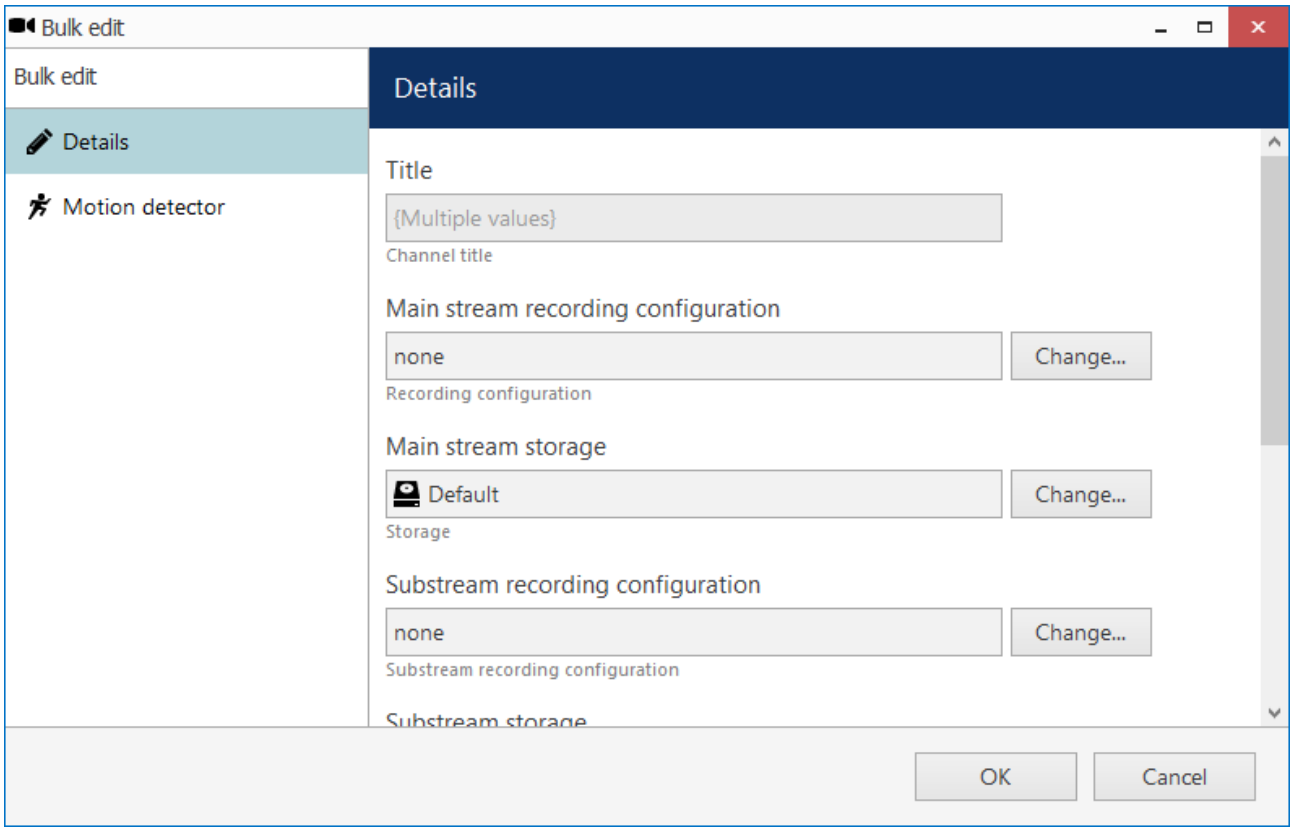
- *Details* tab:
    - **Server**: the server where the devices belong
- *Network* tab:
    - **Port**: HTTP port to connect to the device (for IP devices)
    - **Secure connection**: use HTTPS
    - **Username and password**: user credentials to log in with

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

When done, click *OK* to save and close the dialog box: the settings will be applied to all the selected devices.

Edit Multiple Channels

Select at least two channels in the list and click *Bulk Edit* on the top panel to bring up the corresponding dialog box. Some settings will be grayed out, indicating that they either cannot be changed at all or specifically via bulk edit: for instance, it is impossible to change the title field this way, as each channel normally has its own name, which therefore should be edited for each channel individually.



For channels, the following settings can be changed via bulk edit:

- *Details* tab:
  - **Organization***: the Organization the channel belongs to
  - **Main stream recording configuration**: default recording setting for the main stream
  - **Main stream storage**: main stream recording destination
  - **Substream recording configuration**: default recording setting for the secondary stream, if available
  - **Substream storage**: secondary stream recording destination
  - **Edge** recording configuration**: set *Continuous Recording* here for proper operation
  - **Edge** storage**: recording destination for the footage fetched from the device
  - **Video lost time**: timeout for streams absence, after which the video stream is considered lost and the corresponding event is raised in the E&A engine
- *Motion detector* tab:
  - **Mode*****: choose between camera-side or software-side (high performance or high accuracy software modes available) motion detection

***Macula Enterprise edition only

****Only for channels coming from ONVIF devices

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

*******You will find more details on the motion detection modes in the *Channel Configuration* topic

When done, click *OK* to save and close the dialog box: the settings will be applied to all the selected channels.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

6 Recording Profiles, Schedules, and Configurations

This section describes how to create and configure recording entities: recording profiles, schedules, and configuration.

To access recording configuration dialog boxes in Macula Console, select the *Configuration* section and choose *Recording* in the menu on the left.

There are three types of resources in the *Recording* tab:

- **profile**: choose what data streams are recorded and in what mode (continuous/alert triggered)
- **schedule**: set a recording timetable based on profiles
- **configuration:** a profile- or schedule-based recording configuration that is assigned to channels

These entities are not related to storages

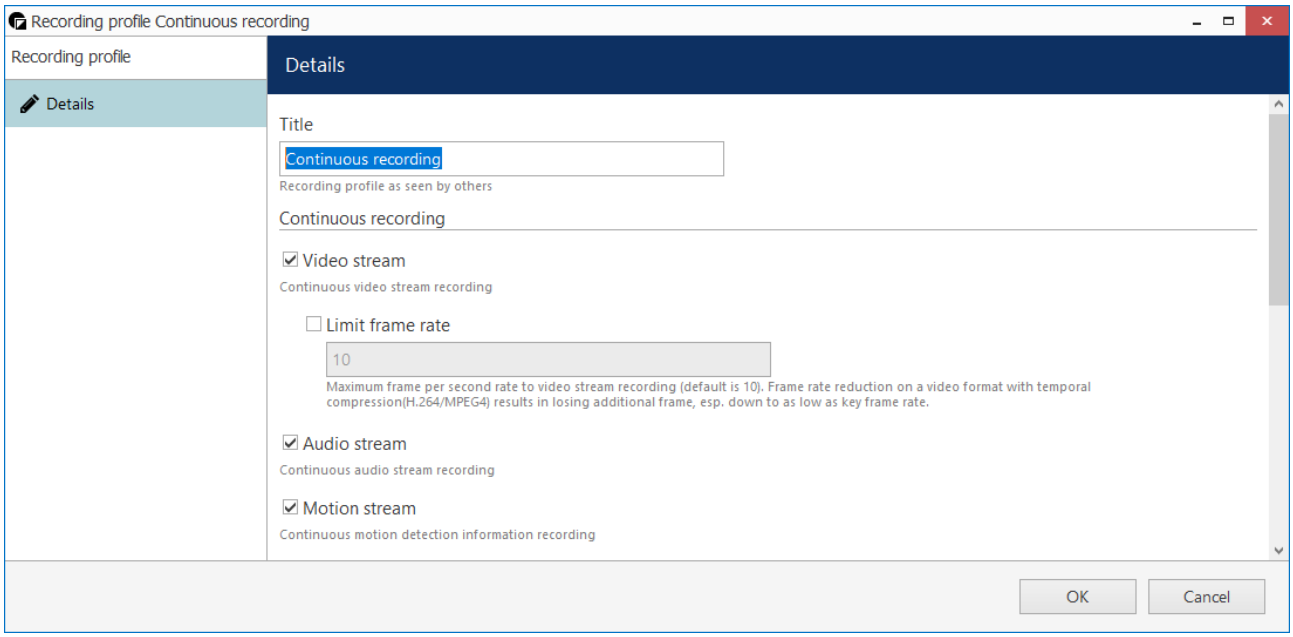
The buttons on the upper panel give the option to create, edit and remove recording resources.

> ⚠ Recording resource cannot be deleted if it is currently in use, i.e., when a recording profile is assigned to a recording configuration or a schedule, or when any of the recording resources are assigned to a channel.

Create Recording Profile

Recording profiles allow users to set which data streams are recorded and how. Profiles cannot be assigned directly to devices; instead, they are used as components for recording schedules and recording configurations. For this reason, profiles do not include settings like pre-recording interval: this setting is defined separately for each channel and, consequently, is defined in the recording configuration settings.

To add a new recording profile, click the down arrow button next to + *New recording configuration* and select + *New recording profile*. The profile creation dialog box will appear.



This dialog box has two sections: one for continuous and one event-driven recording. Note that you can only select one mode at any time for video and audio streams: if continuous recording is selected, alert-based recording options will be grayed out.

You can use the existing built-in recording profiles as the basis when creating your own recording profiles. Also, the most popular scenarios (motion-based, continuous, no recording) are covered by the built-in profiles so you only need to create custom profiles.

To configure **motion-based recording**, enable *Video stream* in the *Alert recording* section and enable the *Detected motion triggers alert* setting. If you wish to record **still frames** at a low rate while there is no motion taking place, keep the *Video stream* option in the *Continuous recording* section enabled and set your desired frame rate, e.g., 1FPS; then set either a high FPS or unlimited FPS in the *Alert recording* section. In case you only wish to record while motion is taking place, deselect *Video stream* in the *Continuous recording* section.

When you assign a **motion-based recording configuration** to a channel with a disabled motion detector, the software will automatically suggest enabling motion detection for the target channel. The camera-side detector is given priority; if it is not available, the software-side detector will be enabled and set to the high-performance mode. We recommend that you **review** the motion detector settings to make sure it operates as desired, especially if the camera-side detector is in use.

Setting	Description	Default Value
Title	User-defined recording profile name	[empty]
Video stream (continuous)	Select to enable continuous video recording	Disabled
Limit frame rate (for continuous video recording)	Set a frame rate restriction for recorded video; note that for compressed video streams (e.g., H.264) actual frame rate may differ due to compression algorithms	10 FPS
Audio stream (continuous)	Select to enable continuous audio recording	Disabled
Data stream	Select to enable data recording from the associated the data source	Disabled
VCA stream	Select to enable continuous video analytics event recording	Disabled
Video stream (alert)	Select to enable alert-driven video recording; video will only be recorded after alert generation, for the time period defined in the *Post-recording interval*	Disabled
Limit frame rate (for alert video recording)	Set frame rate restriction for recorded video; note that for compressed video streams (e.g., H.264) actual frame rate may differ due to compression algorithms	10 FPS
Audio stream (alert)	Select to enable alert-driven audio recording; the video will only be recorded after the alert generation, during the time period defined in the *Post-recording interval*	Disabled
Post-recording interval	The time interval during which alert-driven recording will be conducted after alert generation	10 seconds

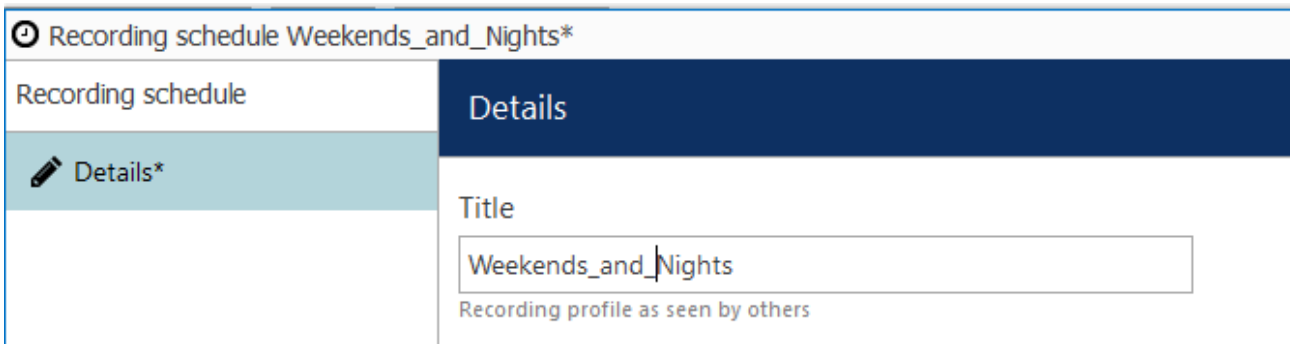
Detected motion triggers alert	Motion will act as a trigger for recording; enable this setting to set up motion-based recording	Disabled

When done, click *OK* to save the recording profile: it will appear in the item list of the *Recording* section. The profile is now ready to be used for further configuration.

Create Recording Schedules

Recording schedules are **sets of recording profiles** that define what recording profiles are used depending on the day and time of the week. In other words, a schedule defines how the profiles are switched over time basis. Alike recording profiles, schedules need a recording configuration on top of them to serve as a proxy in order to be assigned to channels.

To add a new recording schedule, click the down arrow button next to + *New recording configuration* and select + *New recording schedule*. A schedule creation dialog box will appear, allowing you to enter a name of your choice for the new schedule and add the profiles to define the recording timetable.



To create a new schedule:

1. Enter its title
2. Choose a calendar (optional) or just use a weekly schedule
3. Define the points in time when the profiles will change (using either grid or list view)
4. Save the schedule

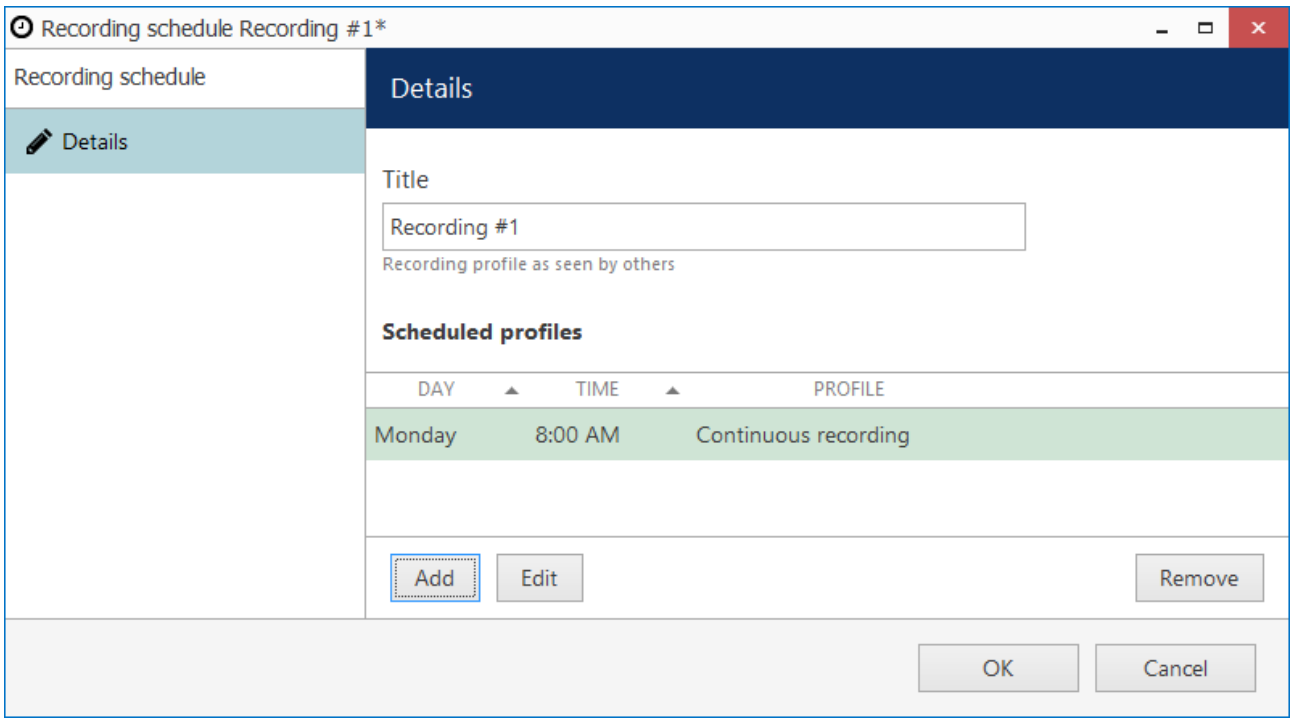
Here are detailed explanations of what the schedule elements do and how they are configured.

Schedule Visualization

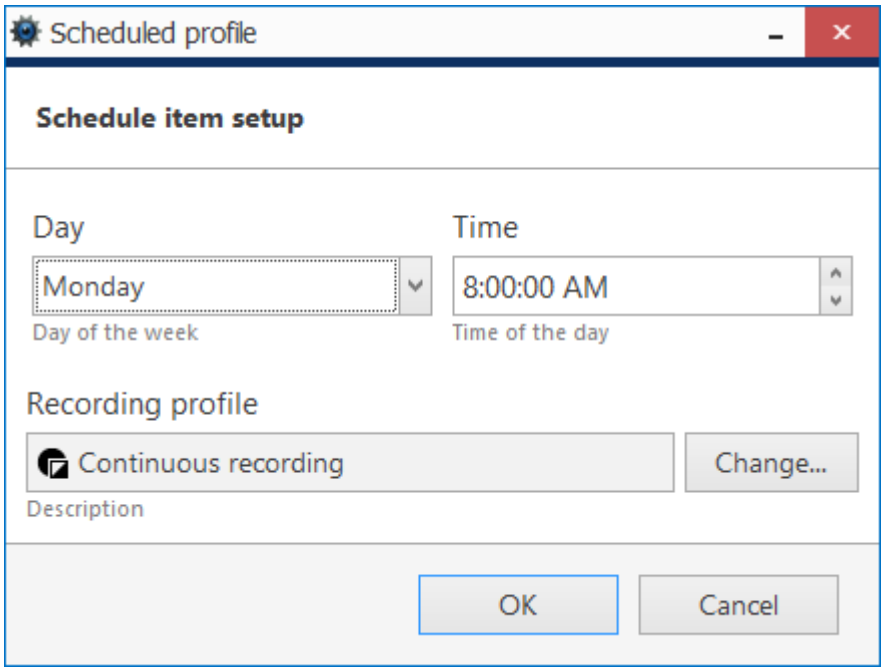
The schedule configurator has two modes: **list** view and **grid** (graphical) view. The graphical mode is used by default; you can switch between the two views by clicking the toggle button in the upper right corner.

List Mode

In this view, each line represents a point in time when a specific profile is activated.



Click the *Add* button below to insert a new profile with a defined start time. To change an existing item in the list, double-click it or use the *Edit* button.



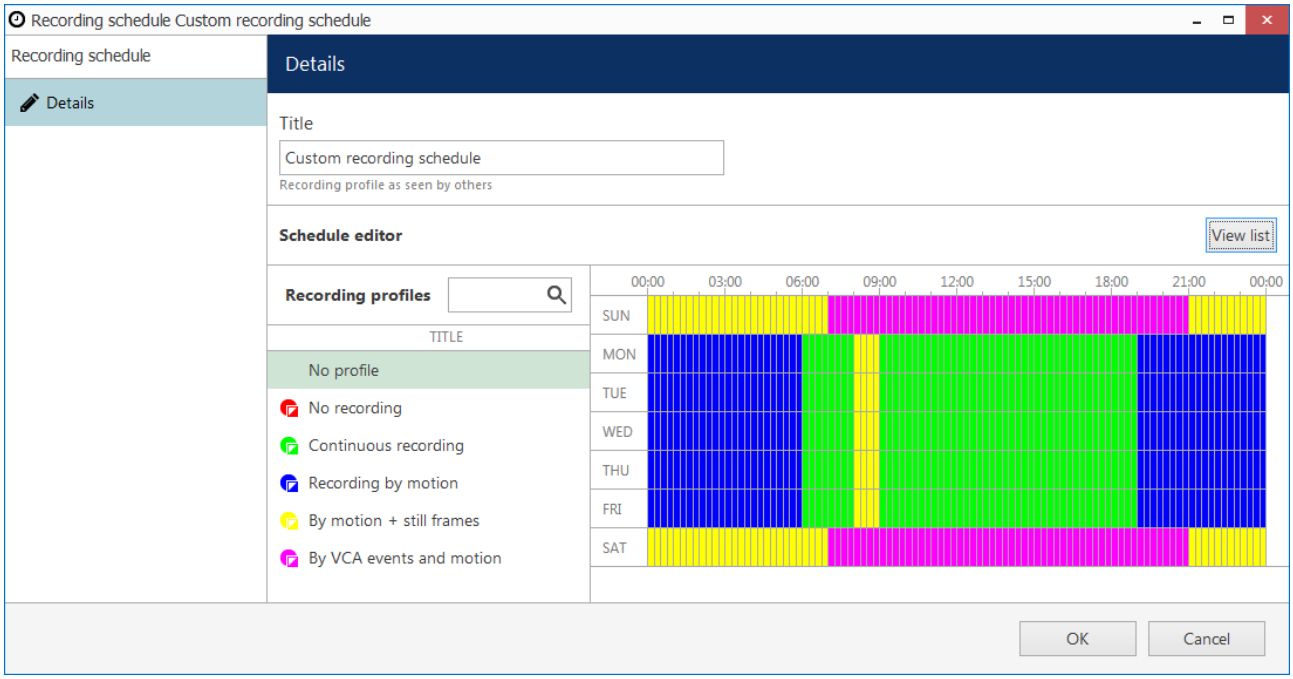
Note that only begin time is set for each added profile: the end time is determined by the start time of the next profile. For example, if you require continuous recording during weekdays and motion-driven recording during weekends, your continuous recording profile should be scheduled to start on Monday at 12 a.m. and motion-driven one - on Saturday at 12 a.m..

Click *OK* to save and add the profile to the schedule. Multiple profiles will be automatically sorted based on their start time.

Use the *Edit* and *Remove* buttons below to manage the profiles added. When you are finished, click *OK* to save; the newly created schedule will be added to the item list in the *Recording* section.

Grid Mode

Graphical schedule view is more convenient for complex timetables, where many different recording profiles or profile combinations are used.



Simply **select** the desired profile in the list on the left, then **mark** the target period on the grid view. **Repeat** with all desired profiles.

As you create new profiles, they are automatically assigned different **colors** and appear in the profile list.

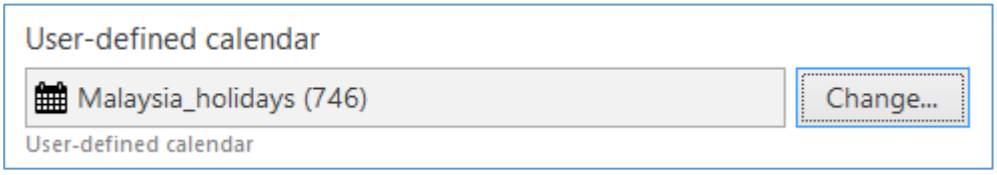
> As you create new profiles, they are automatically assigned different colors and appear in the profile list.

> It is not necessary to fill the whole timetable. You can leave some of the grid **empty** (white): empty time periods will be analogous to the *No recording* profile and nothing will be recorded during that time.

Schedule Calendars

The core of a regular recording schedule is the **week.** In the simplest approach, you define how the profiles are switched on a weekly basis by coloring the week grid, and your Macula server will cycle through the week accordingly.

A more detailed approach takes into account the **whole year**. This covers non-standard weeks, when some of the weekdays should follow the recording pattern of the weekends (e.g., state holidays) or vice versa. For this, you can build a **custom calendar** with exceptions.



How to decide if you need a calendar?

- If you only need a typical weekly schedule throughout the year, use the weekly schedule.
- If you have a need for custom daily schedules, use a custom calendar.
- If you need to change the day type sometimes and "change Saturday into Thursday", use a custom calendar.

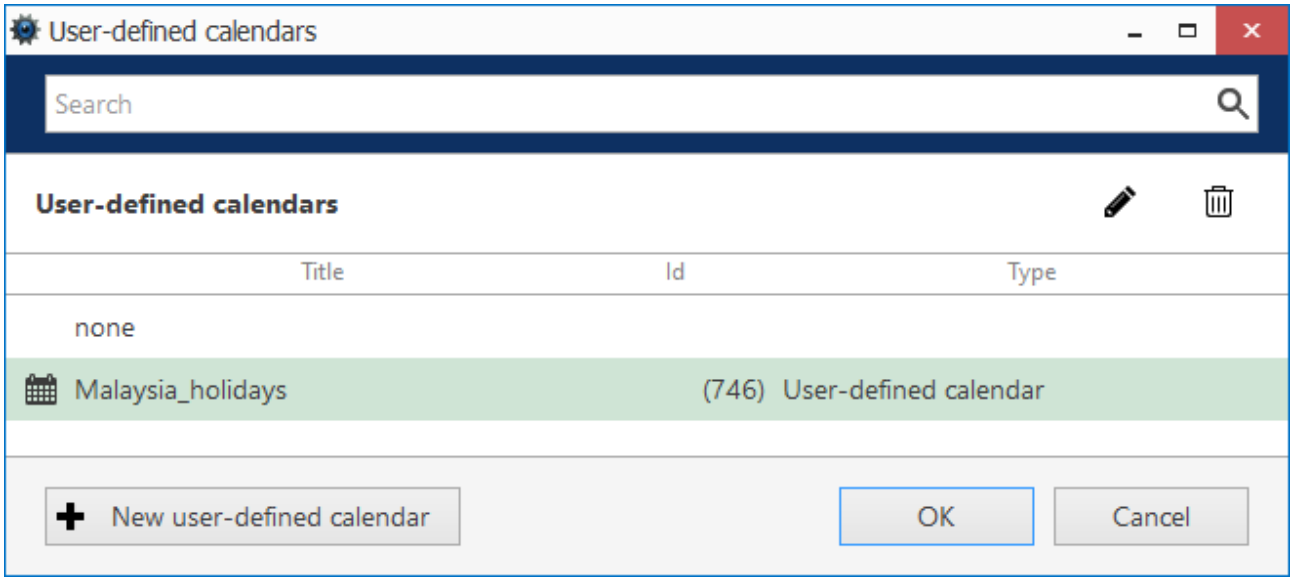
When you only use the regular 7-day week without a calendar, ignore the "Custom days" section.

Add Custom Calendars

User-defined calendars provide an option to define a yearly basis for the recording. While the weekly basis is simpler, having a year long calendar allows configuring special dates (e.g., holidays).

Each calendar assumes the same **weekly schedule** as its base, and then you can add exceptions by explicitly assigning the recording pattern to specific dates. You can choose that pattern from the weekly schedule (7 different days) or from the custom days (5 additional daily patterns), which you can pre-define.

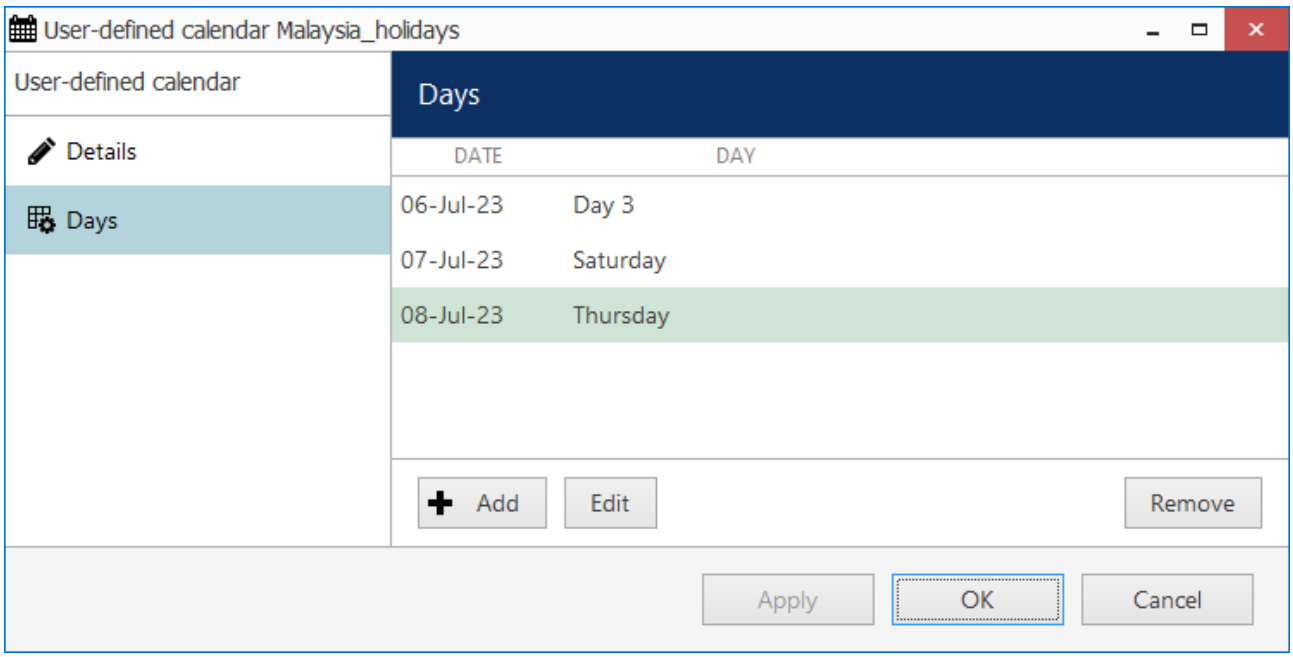
You can add as many calendars as you like, use them in various recording configurations, and change them by adding/removing items at any point. When you change the day type for the current day (e.g., today is Saturday and you add a calendar entry that forces Thursday on this date), the new recording profiles are enforced immediately after you save the configuration.



To add a **new calendar**, open the recording schedule creation dialog box, and click *Change...* next to the *User-defined calendar* option. You will see the list of existing calendars (empty by default). Click the + *New user-defined calendar* button to open the dialog window.

In the list of calendars, you can also edit the list (remove unnecessary items by clicking the *Recycle Bin* button) and open existing calendars for editing (by selecting the target calendar and then clicking the *Pencil* button).

> If you run multiple installations in locations that use the same calendar, you don't have to create it again for every installation. Simply create the calendar, save the Macula configuration database file, and then import the calendar from it.



Enter the calendar name and switch to the *Days* tab. It is empty by default (which means the calendar solely operates on the normal week basis). To create exceptions:

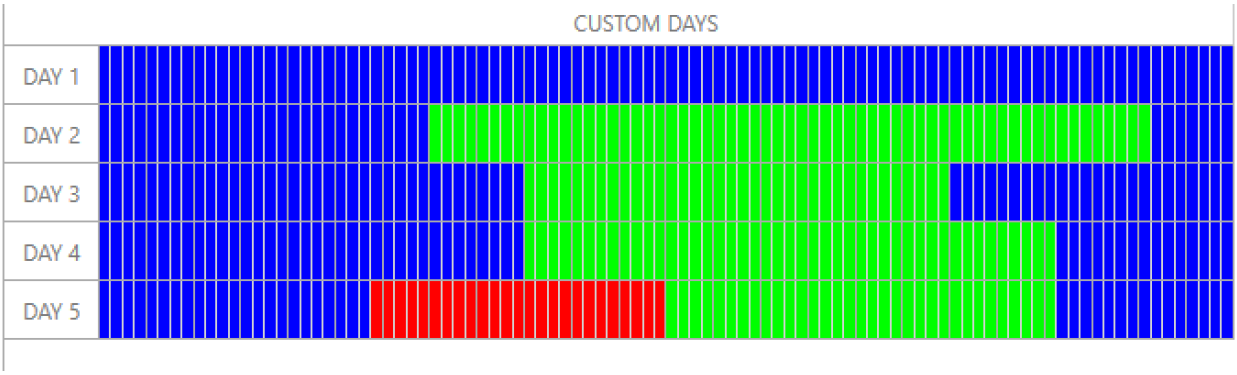
1. Click the + *Add* button.
2. Choose the date.
3. Assign the day for that date.
4. Click *OK* to add the special day.

Repeat this process until you have entered all the desired custom calendar days. Click *OK* to save and close the dialog box: the calendar will appear in the calendar list, allowing you to assign it to your recording schedule.

In the list of days, click any entry and then click the *Pencil* icon to open it for editing.

Custom Days

Apart from the weekdays and weekends, you can define up to five additional alternative days and use them in your custom calendars. This feature is convenient when there are days when no daily recording pattern can be applied, e.g., early release pre-holiday days or other days with a special schedule.

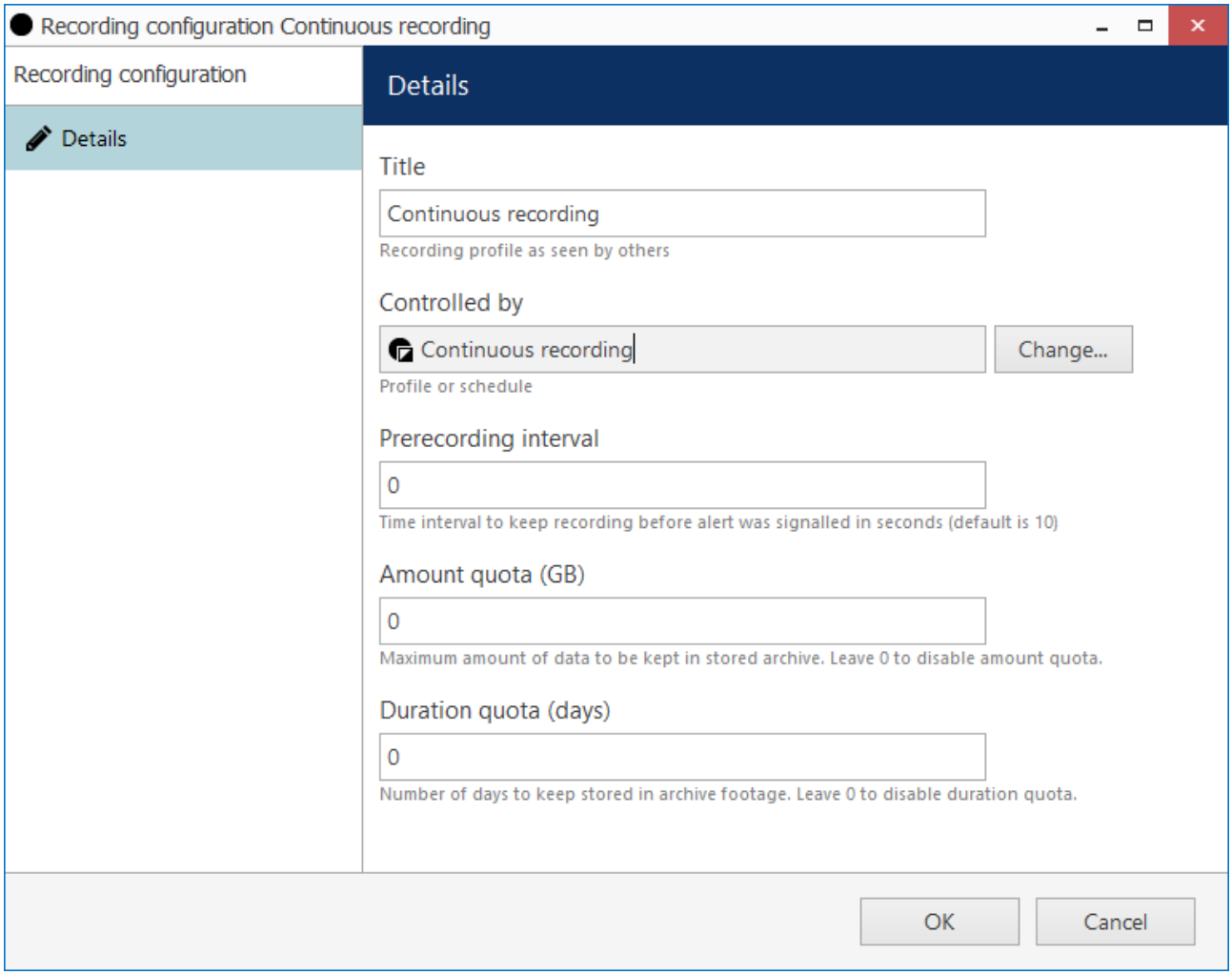


Custom days do not participate in the regular weekly schedule (without a calendar). You can assign any custom day to a particular date in your user-defined calendars.

Create Recording Configuration

Recording configurations are global recording arrangements that can be assigned to a per-channel recording setup. Recording configurations can be based on a single recording profile or on a pre-defined recording schedule.

To add a new configuration, click the down arrow button next to + *New recording configuration.*



The corresponding dialog box will then appear, allowing you to enter the configuration properties.

Setting	Description	Default Value
Title	User-defined recording configuration name	[empty]
Controlled by	Choose existing recording profile or schedule for current configuration or create a new one from the sub-dialog	[none]
Pre-recording interval	Set the pre-recording interval for alert-driven recording, if applicable; note that large pre-recording interval will increase virtual memory usage - if the used profile is not alert or motion driven, set 0 here to decrease memory usage	10 seconds
Amount quota	Storage quota in GB: the maximum amount of space that can be taken up by recordings, if the maximum size is reached, the oldest footage will be deleted; set 0 to disable any limitations	0 (unlimited)

Duration quota	Duration quota in days: the maximum number of days that recordings are kept in the archive; after this, recordings will be erased; set 0 to disable any limitations	0 (unlimited)

Before setting recording limitations, make sure there is sufficient space in the server storage for all cameras. The quotas may be ignored if actual storage size is insufficient, and this will result in shorter footage durations.

Note that maximum the **pre-recording** time is 60 seconds. Larger values will be ignored by server core. Also, actual pre-recording buffer may be smaller if the server detects that it is not required (see below). The **actual buffer size** in seconds will be displayed in the *Monitoring* section, under *Streams*. It may differ from your prerecording setting in the recording configuration. Macula server applies smart logic here and traces situations when larger buffer is not necessary, or even preventing the system from normal operation. Thus:

- if the currently used recording profile does not involve any pre-recording (e.g., *Continuous recording*, or event-driven with no defined E&A events), the buffer size will be reduced to 0 - this is absolutely normal, once you add any recording-triggering events, Macula will automatically increase the buffer size
- if there is not enough memory for all channels (the server is overloaded), the server will reduce prerecording buffers; channels with largest frame cache size will have their buffers reduces first of all upon server startup, the buffer size is increased gradually for smoother start

If your pre-recording buffer size requires more memory than there available, you will see channels with top buffer size (in MB) appear marked red and with an * (asterisk) in the *Monitoring* section, under *Streams.* Also, the *Audit* section of Macula Console will contain events from the corresponding server stating that there is *Not enough memory to process frames*. If this happens regularly, review your server hardware using GSF provided hardware calculator and add more RAM to your server, or decrease the pre-recording interval duration wherever possible

Note that quotas do **not** give priority to channels that are assigned configuration. For example, if you set the duration quota to ten days, it merely means that the maximum recording duration will be ten days for a channel with given configuration; this will **not** reduce recording duration for other channels.

For security reasons, it has been made impossible to erase recordings from individual channels and/or time periods, so that archive integrity is preserved. Recordings are erased automatically when storage or duration quota is reached; if you need to erase footage from an existing channel, simply assign a recording configuration with an individual quota to it, wait until the footage is erased (actual timing depends on archive size) and assign a new recording configuration.

When you have finished, click *OK* to save and exit. Recording configuration will now be added to the item list and will become available in channel recording configuration.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

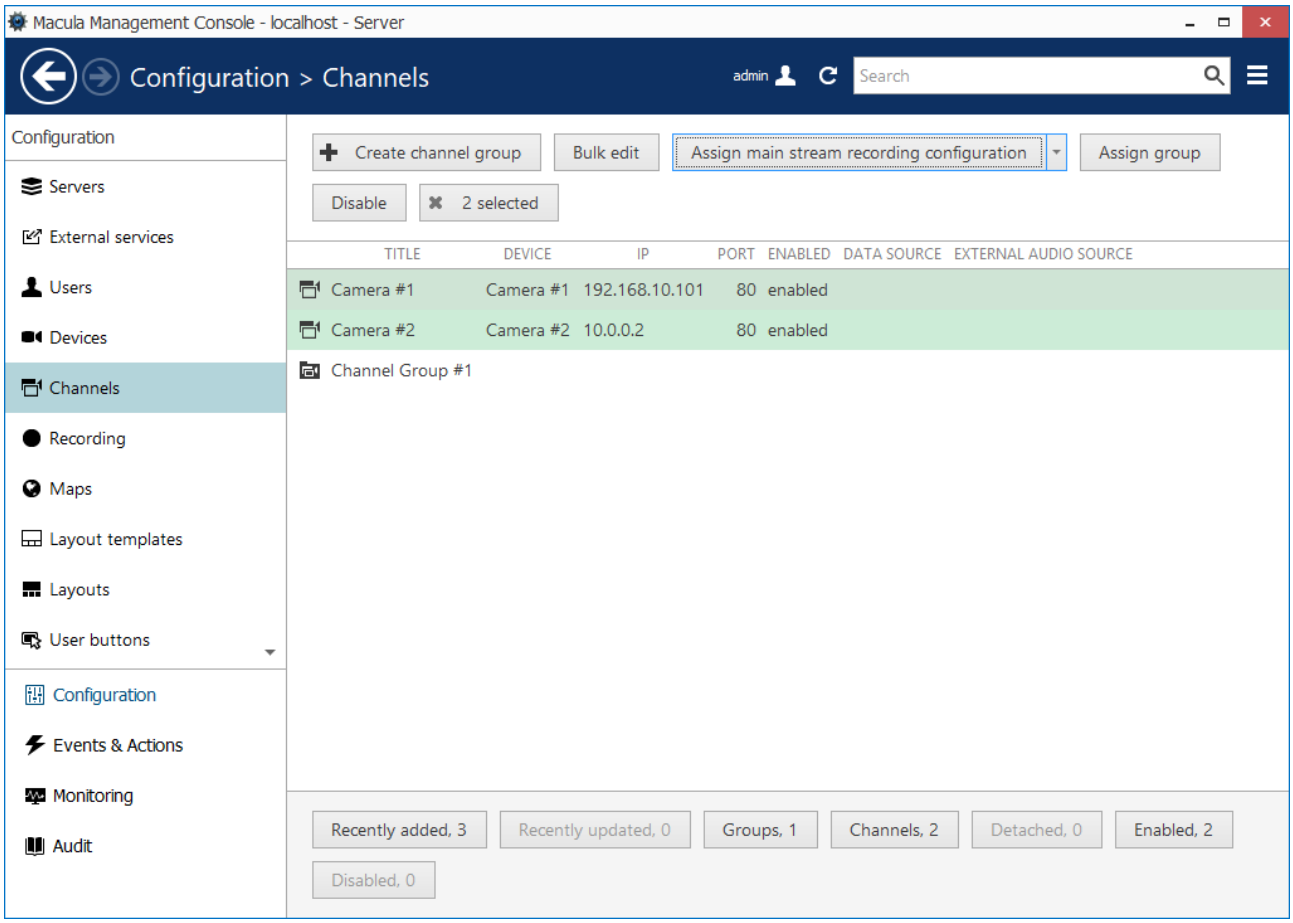
6.1 Assign Recording Configurations

Recording configurations can be assigned to channels and channel groups to define how data streams are recorded. There are several ways to assign a recording configuration:

- when using device autodiscovery: via *Found channels* tab (automatically discovered channels are assigned the *Continuous recording* configuration by default)
- when creating multiple devices: from multiple channel creation dialog box, *Channel settings* tab (manually added devices are set not to be recorded by default)
- after adding a single device manually: via *Channels* section, *Edit channel* dialog box, *Details* tab (manually added devices are set not to be recorded by default)
- for existing channels, per channel: via *Edit channel* dialog box, *Details* tab
- for existing multiple channels: via *Channels* section, using *Assign main stream recording configuration* button on the upper panel

Topic body below explains how to assign configurations via main Macula Console window (latter option). All the rest alternatives are similar: you are offered configuration selection list at once from corresponding setup window.

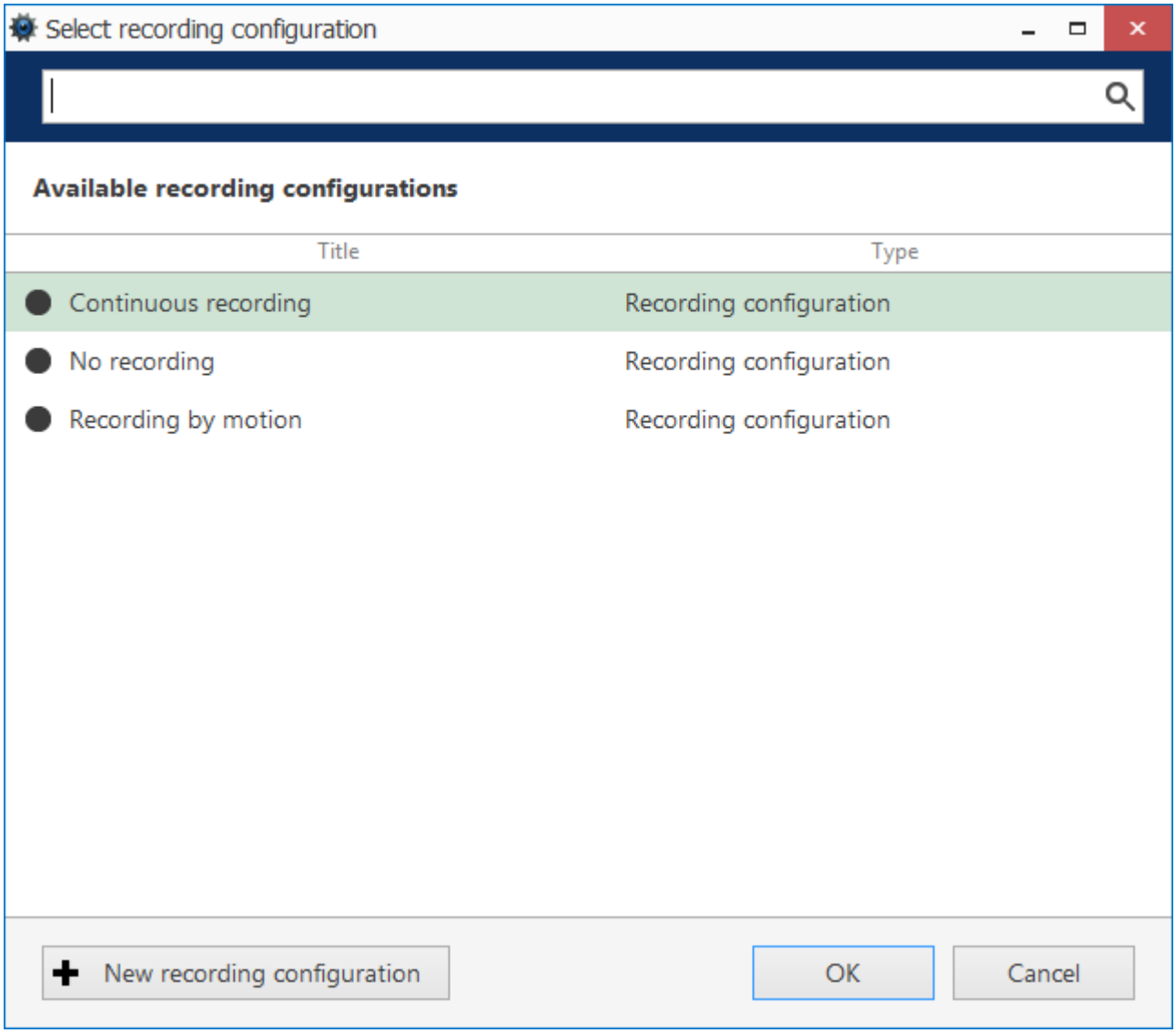
Enable Recording



In Macula Console, choose *Configuration* section and select *Channels* from the menu on the left. Select one or multiple channels and/or channel groups (use *CTRL+click* or *Shift+click* to select several items at once)

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

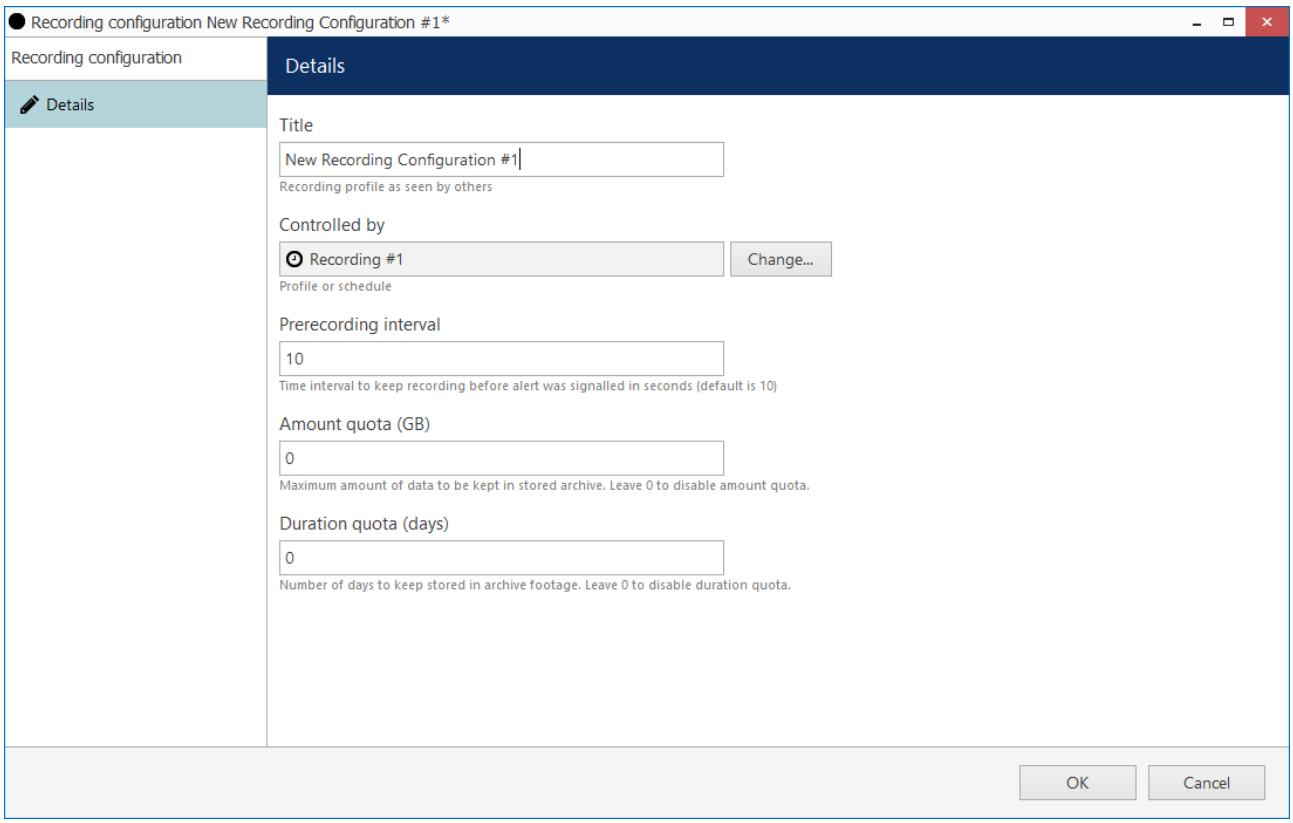
and then click the *Assign main stream recording configuration* button on the upper panel. The list of available configurations will appear.



Note that you can only directly assign **configurations**, not profiles or schedules. Configurations are based on profiles or schedules (sets of profiles); please refer to the *Configure Recording Profiles* section of this document for details.

Click the + *New recording configuration* button below to create additional configurations from existing profiles/schedules at this point.

When you assign a **motion-based recording configuration** to a channel with a disabled motion detector, the software will automatically suggest enabling motion detection for the target channel. The camera-side detector is given priority; if it is not available, the software-side detector will be enabled and set to the high-performance mode. We recommend that you **review** the motion detector settings to make sure it operates as desired, especially if the camera-side detector is in use.



Press *OK* to save and go back to the channel list: newly created recording configuration will be automatically assigned to channels previously selected.

Disable Recording

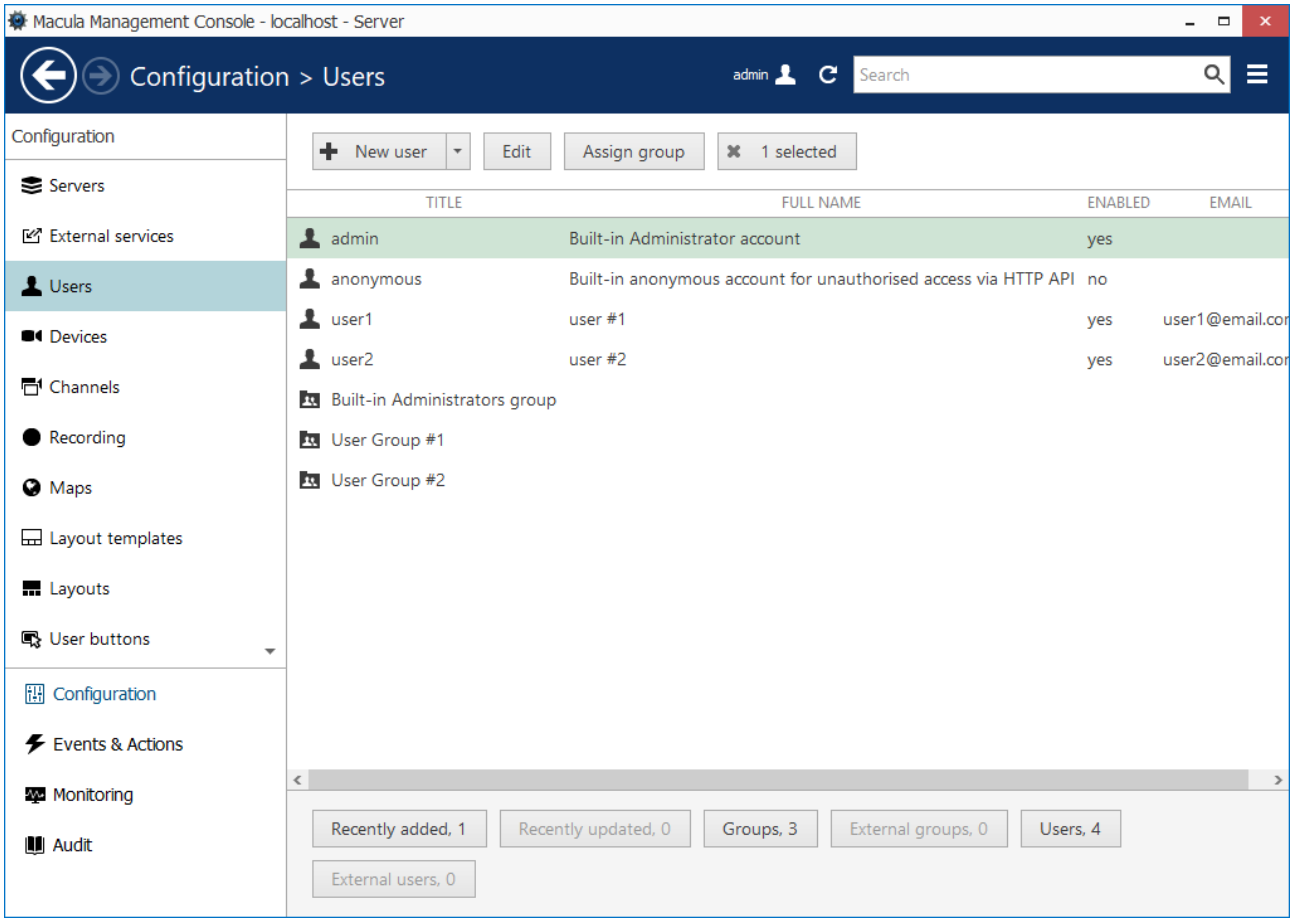
To disable recording for any channel(s), choose the *No recording* configuration, which is present in the list by default. If you have deleted it, simply create a new recording profile without any streams selected for recording and then create a recording configuration for this profile.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

7 Add Users and User Groups

User management is accessible via the *Users* component of the *Configuration* section. By default, the system already features a built-in global Administrator account and built-in Administrators group.

> The built-in Administrator user account and built-in Administrators group are root users with access to absolutely all the available resources. As a result, resources choice is unavailable for the Administrators group, and it is also impossible to add Administrator user to any other group.
>
> Any users added as members to the built-in Administrators group will have the same full authority as root users.



Add Users

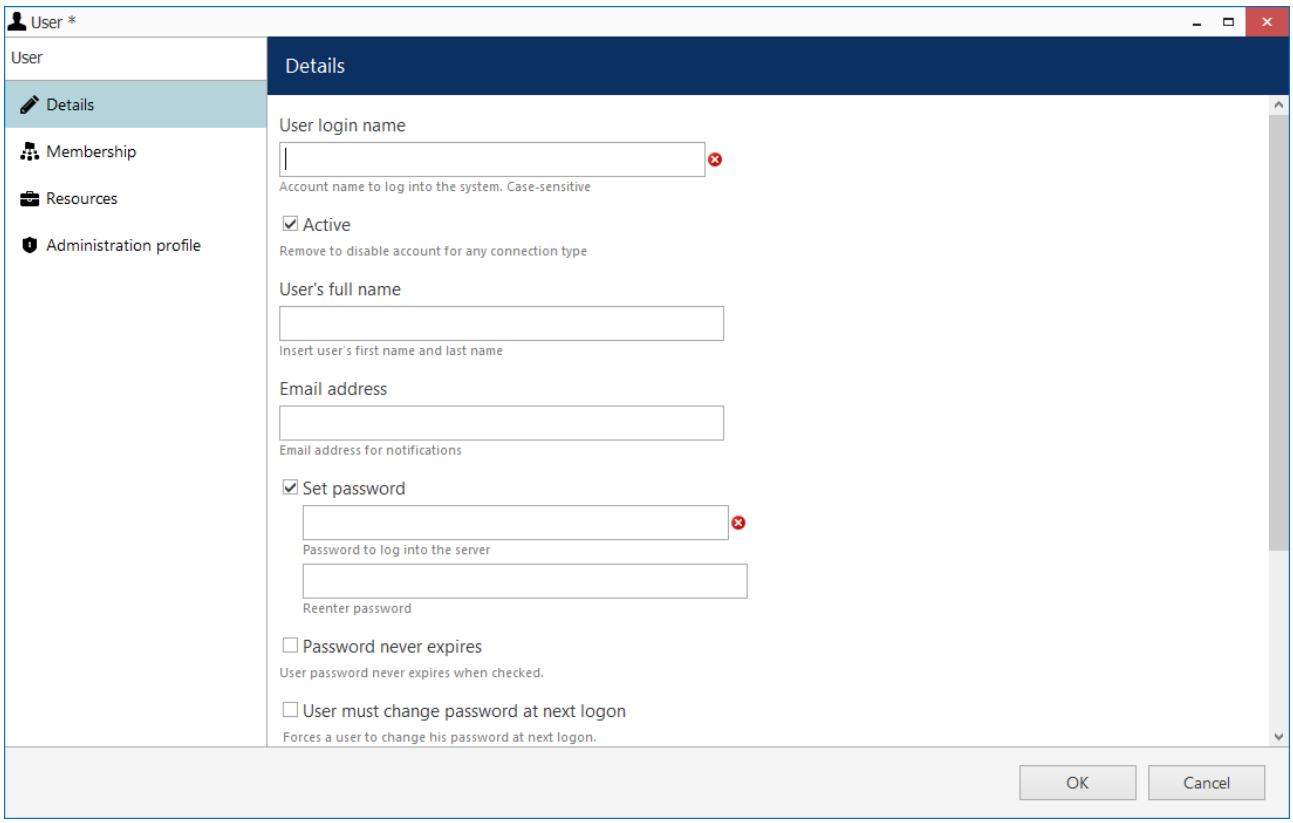
Click the + *New user* button on the upper panel to bring up the configuration dialog box.

Details

Enter user login information here.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



The table below describes in detail the available settings.

Setting	Description	Default Value
User login name	Alphanumeric user name for login, **no spaces** allowed	empty
Active	Allow the user to log in via Macula Console and Macula Monitor: any users who have been disabled will not be able to use software	Enabled
User full name	User full name	empty
Email address	User email address used for notifications	empty
Phone number	Phone number in international format (with country code) for 2FA	empty
Set/new password	Check to enter a password - this is obligatory when creating a new user	empty
Password never expires	User will not be prompted to change his password once in a while; enable this to ensure a permanent password for this user account (this setting can be overridden by the *User must change password...* setting in the same dialog box); otherwise, password will expire after the number of days specified in the server security policy	Disabled (not selected)
User must change password at next logon	User will be prompted to change his password upon his next logon attempt; enable this if you want to force user change the password even if his password is set to never expire	Disabled (not selected)
User cannot change password	Enable this to prevent the user from changing his password; this option is not available if user password is not permanent or if you have selected to force user change their password at next logon using the settings above	Disabled (not selected)
PTZ priority	Used for PTZ cameras and interactive CrossLink devices. 0 = lowest, 10 = highest	5

Override default limit of simultaneous connections	Maximum number of simultaneous connections allowed from this user account; the setting has priority over server-defined limitations; 0=unlimited	Disabled (not selected)
Set account activation time	If option is enabled and user is not Active - this will enable account at particular date and time.	Disabled (not selected)
Set account expiration time	If enabled, the user account will be automatically deactivated on the specified date at the specified time	Disabled (not selected)

*****See below to learn more about how PTZ priorities work.

PTZ Priority will be used to for **PTZ control** of speed domes, and also for the control of interactive video channels (CrossLinks allowing users to control **remote Web and Desktop** applications). After each action (click), the control will be locked onto the user with the higher priority for the amount of time specified as PTZ Priority Timeout (10 seconds by default).

If two or more users try using PTZ control of a device at the same time, **PTZ priority** is used to decide who gains access first: user with a lower priority is blocked for ten seconds to allow a higher-priority user to use PTZ. If two users with the same PTZ priority have an access conflict, they will be both granted PTZ access simultaneously.

Default PTZ priority for all users, including those built-in and imported, is equal to five (medium priority). You can assign any user a higher PTZ priority (six to ten) or a lower one (four to zero) by editing individual user properties.

> Some user settings like PTZ priority are not updated immediately: the user will have to log out and then back in for the changes to take effect.

> Deleting a user also removes all the settings related to that user; restoring these may be time-consuming. Use the *Active* setting to temporarily block access for selected users: users not marked as **active** will be unable to perform any actions in Macula and can be restored with a single button click.

PTZ Priorities

PTZ priority is used to for:

- manual control of PTZ cameras (speed domes),
- automated PTZ control (tours and presets),
- control of interactive video channels (CrossLink devices allowing users to control remote Web and Desktop applications).

PTZ related user actions include manual PTZ control (mouse clicks) and the calling of PTZ presets and tours. CrossLink control involves manual interaction (mouse clicks).

> PTZ tours always have zero (the lowest) priority, no matter who initiates it, so that any user can interrupt it.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

After each user action, the control is locked onto the user with a higher priority for the amount of time specified as PTZ priority timeout (10 seconds by default). PTZ priority is used to decide who gains access first: user with a lower priority is blocked for N seconds to allow a higher-priority user to use PTZ. If two users with the same PTZ priority have an access conflict, they will be both granted PTZ access simultaneously.

If two or more users try controlling the **same device at the same time**:

- if both users have **the same** PTZ priority, the timeout will be ignored and each user's action will immediately take effect
- if user A has a **higher priority**, his first action will take control from user B with a **lower priority** and lock the control for the specified timeout, preventing everyone with a priority lower than A's from controlling the device; once the time is out, any user can try gaining the control again

Thus, the PTZ priority timeout is only taken into account when taking over control, and does not matter when the users have equal priorities.

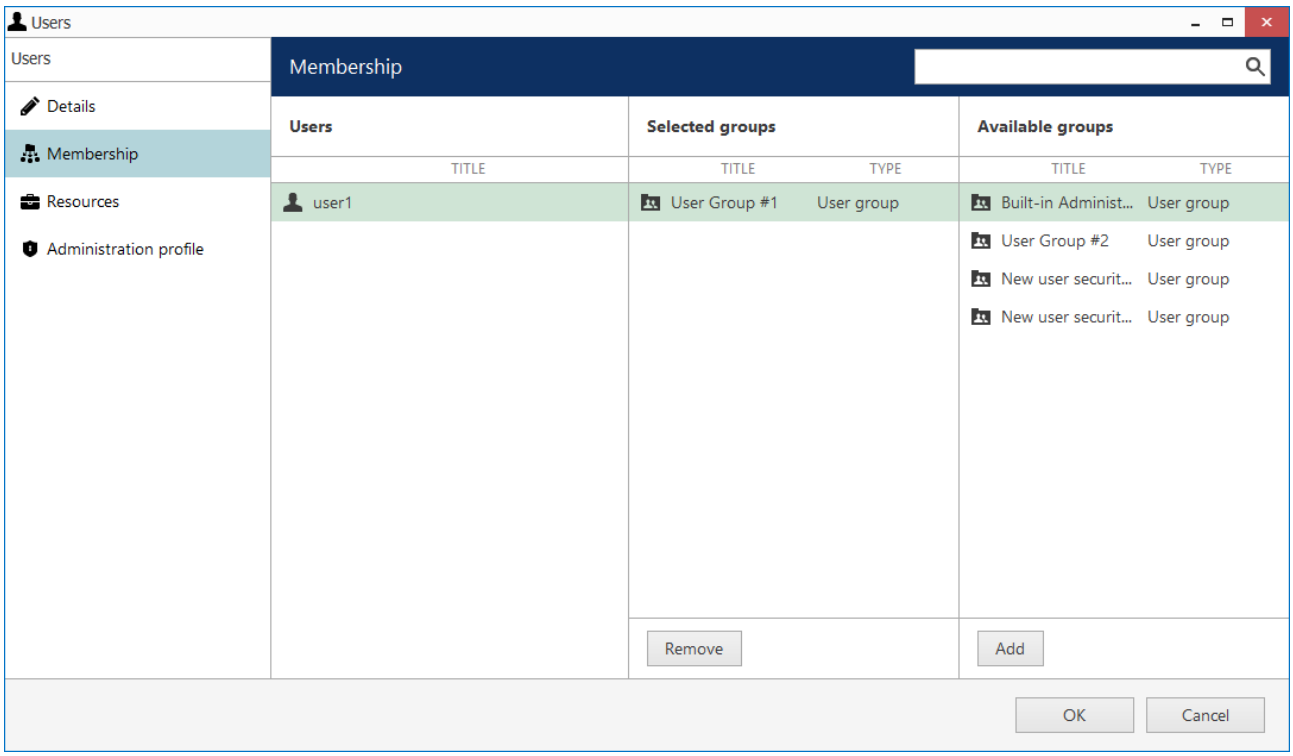
Default PTZ priority for all users, including those built-in and imported, is equal to 5 (five, medium priority). You can assign any user a higher PTZ priority (six to ten) or a lower one (four to zero) by editing individual user properties.

For **PTZ preset actions** in E&A, you will be asked to specify the PTZ priority when creating the action. For **PTZ tour actions**, the priority is always 0, allowing any user to interrupt the preset execution.

Membership

Choose which groups you want the selected user to be a member of. Every user can participate in one or multiple groups, depending on the system structure.

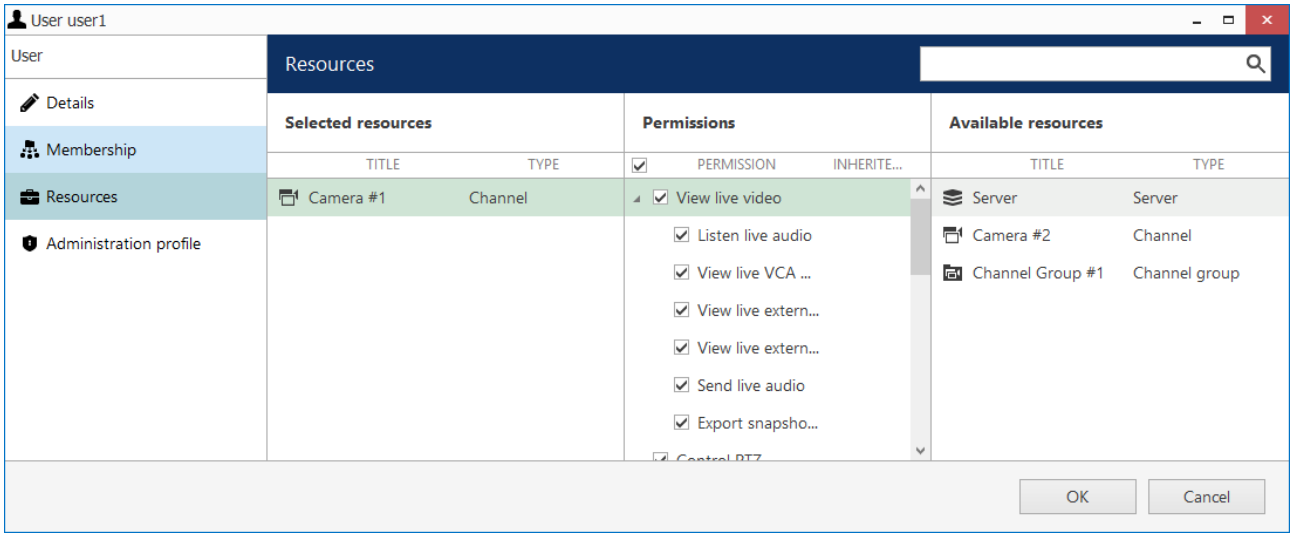
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Manipulate the groups by double-clicking a group or using the *Add/Remove* buttons below. Use the *Search* field in the upper-right-hand corner to filter the groups available.

Resources

Each user can be granted permissions for server and channel/channel group administration. Select resources by adding at least one permission; remove them by clearing permissions using the *Clear* button below, or simply by double-clicking them in the *Selected resources* list.



Click *OK* when you have finished to return to *Users*; the newly created account will be added to the item list. Use the buttons on the upper panel to edit user details at any time, to quickly assign groups and remove specified users (hold *CTRL* of *Shift* to select multiple items at once).

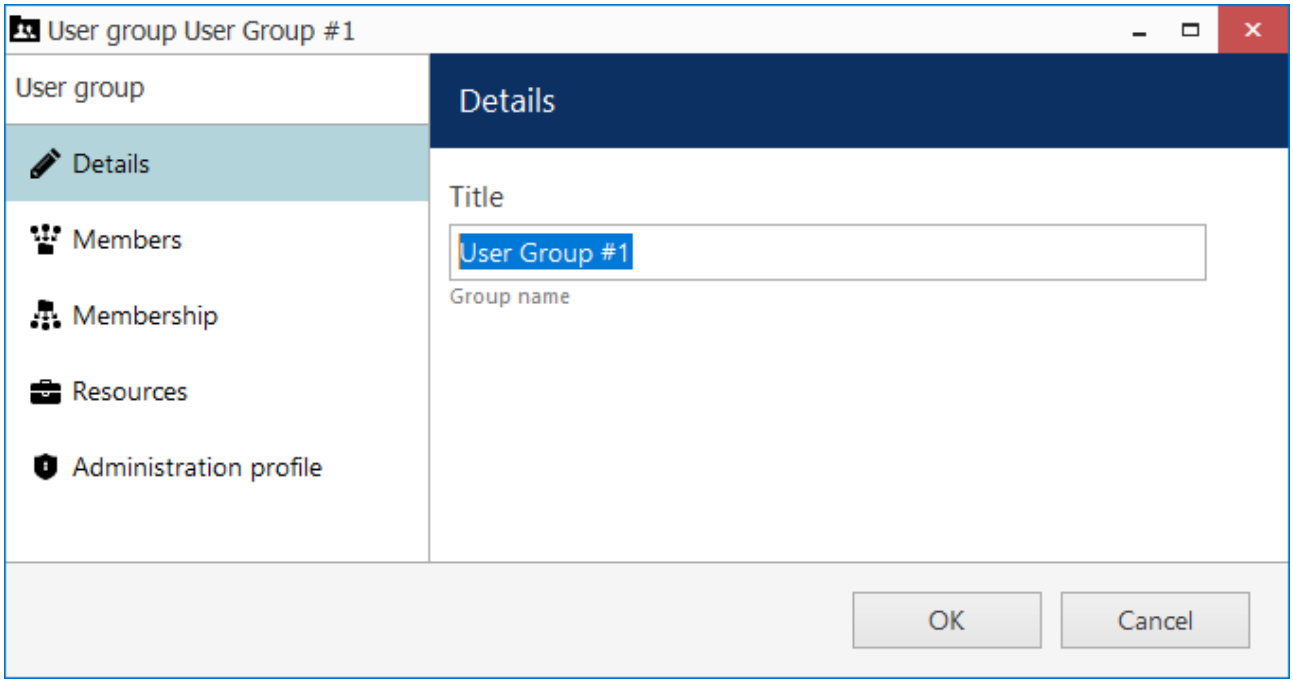
If there are a large number of user accounts, the *Search* field in the upper-right-hand corner and the content filters in the bottom panel can help you quickly find the accounts you are looking for.

If some resource permissions are defined for some user via **user groups**, these permissions will be displayed if you open permission list of the target user: these will appear **gray** and will not be available for editing.

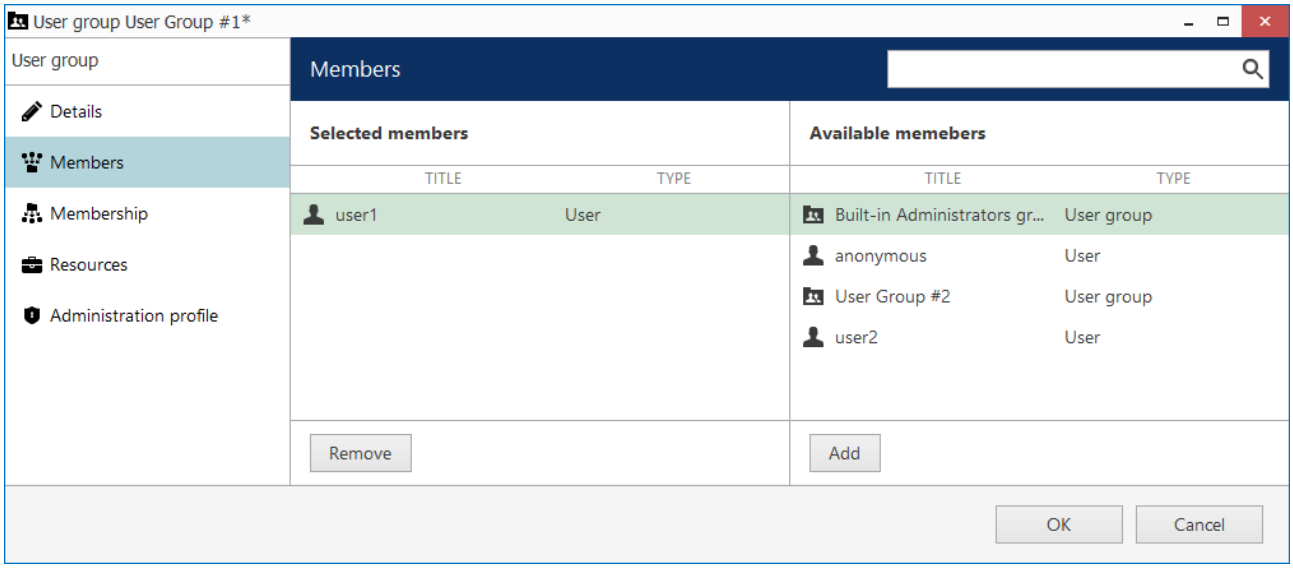
Add User Groups

When the number of users is large, it may be more convenient to create multiple user groups and then distribute resources between user groups, rather than between individual users. One user can be a member of several groups.

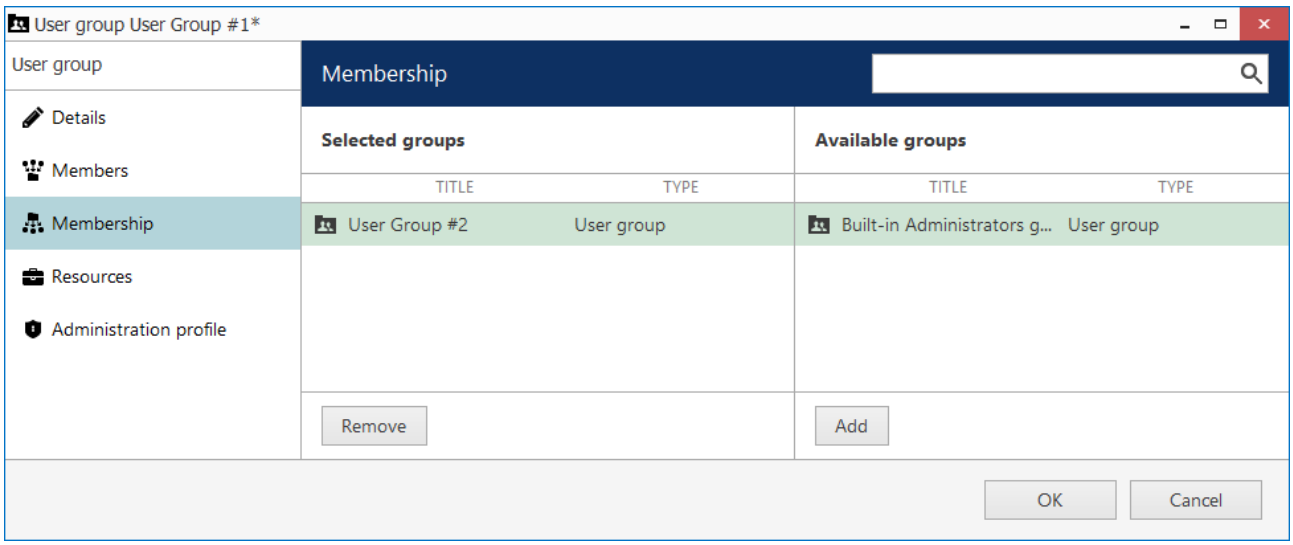
Click the down arrow near the + *Create new user* button and select *New user group* from the drop-down list to bring up the configuration dialog box.



In the *Details* tab, enter group name.



In the *Members* tab, choose which users and/or user groups will become members of the target group: manipulate items by double-clicking them or using the *Add/Remove* buttons below.



In the *Membership* tab, select the group(s) you want to include the current group as a member: manipulate items by double-clicking them or use *Add/Remove* buttons below.

Finally, you can grant resources permissions using the *Resources* tab in a similar way to adding a single user. Select resources by adding at least one permission; remove them by clearing the permissions using the Clear button below, or simply by double-clicking them in the *Selected resources* list.

Click *OK* when you have finished to return to *Users*; the newly created group will be added to the item list. Use the buttons on the upper panel to edit the group details at any time. If there are a large number of user accounts, the *Search* field in the upper-right-hand corner and the contents filters in the bottom panel can help you to quickly find the accounts you are looking for.

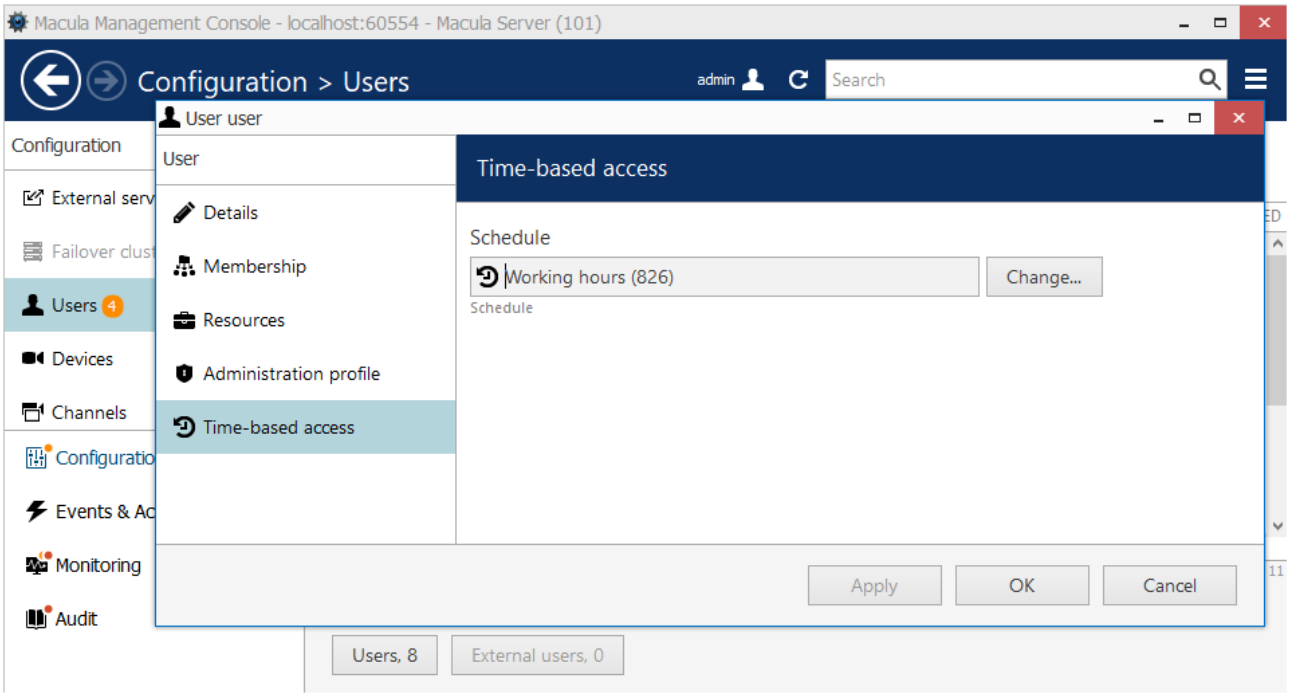
Time-based Access

Starting with version 1.26, you can limit user access options based on the **schedules**. To do so, go to:

1. *Configuration -> Users ->* your particular user
2. Inside the *User* pop-up window select *Time-based access ->Change* button
3. Pick up the existing *Schedule* from the list or create a new Schedule by pressing the *+New Schedule* button
4. confirm your choice with the *OK/Apply* buttons.

After that, user access will be limited by the applied Schedule.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



⚠ If user belongs to multiple groups and user access is enabled at least in one group - user will have access!

Activate/deactivate User Accounts by Date and Time

It is possible to disable user accounts by setting up a date and time. To set timings, go to:

1. *Configuration -> Users -> affected user -> Details*
2. Scroll to the bottom of the section and mark the checkbox *Set account expiration time*.

By default, new users are created as *active* users, so if you want to set up account activation time, do the following:

1. Go to *Configuration -> Users -> affected user -> Details* and unmark the checkbox *Active* next to the *User Login Name* field.
2. Scroll down to the bottom, check the checkbox *Set account activation Time*, and set the date and time for a particular user account to be enabled.

⚠ **N.B.** By default, disabling the user account on the schedule does not disconnect the user automatically, and, while the session continues, the user will preserve all the provided access options.
To restrict user access instantly, you need to set up Server behavior. Go to *Configuration -> Servers -> your server -> Security policy*, scroll down to the bottom, and mark the *Disconnect disabled users* checkbox. That setting will ensure that any disabled user is disconnected from the server instantly no matter if the current session is still active.

7.1 Active Directory and LDAP User Import

Macula allows you to import users and user groups from the existing Active Directory/LDAP service database. The only thing that is left to do is to specify permissions for the imported users and/or user groups (referred to as *AD users* further in this topic).

Please keep in mind that in multi-server systems - using Macula Enterprise - all recording servers must belong to the domain for the AD/LDAP imported users to be able to access their resources - streams and the recorded video archive. If some of the servers are out of the domain, external users will be unable to connect to them (this happens automatically, in background) and there will be errors instead of the video streams.

Active Directory and LDAP user import is available in the following Macula versions:

- Macula Enterprise - fully supported for all versions
- Macula Professional v.1.4.1 - 10 users
- Macula Professional v.1.5.0 and newer - fully supported

AD/LDAP imported user accounts can be used to log into Macula Console, Macula Monitor, and Web client for Macula Streaming Server. These user accounts **cannot** be used in Macula Mobile applications at this point.

Note that it is not necessary for you to be logged into Windows under the same AD account; rather, once AD accounts are imported as external users into Macula, you can use any valid AD account credentials to log into Macula Console or Macula Monitor. Also, note that you are always required to enter the password for the AD account, even if you are logged under the same user account in your current Windows session.

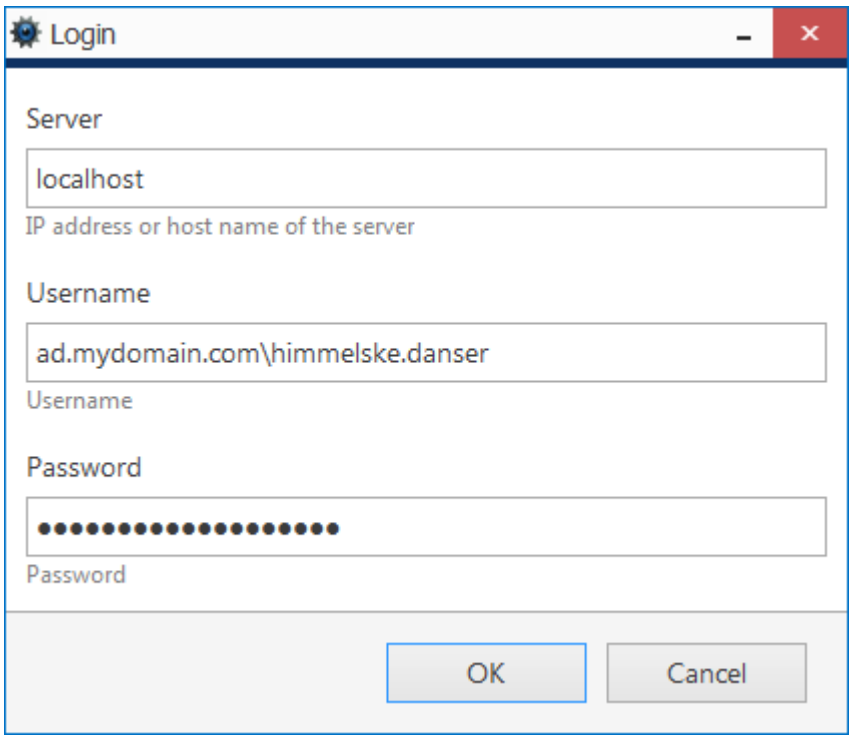
If you are using AD/LDAP user accounts for the Web login, we strongly recommend that you turn on HTTPS for enhanced safety. Plain HTTP will work, too, but is not recommended for security reasons.

For you to be able to log into a Macula server with an AD user account, you must be able to log into the target server computer with the same AD account. If you are unable to do so, contact your Windows administrator and let him check the effective policies.

In order to use your imported AD account with Macula, type in your full domain name and user name, and then specify the password. Please see the description below on how to add your AD users into Macula.

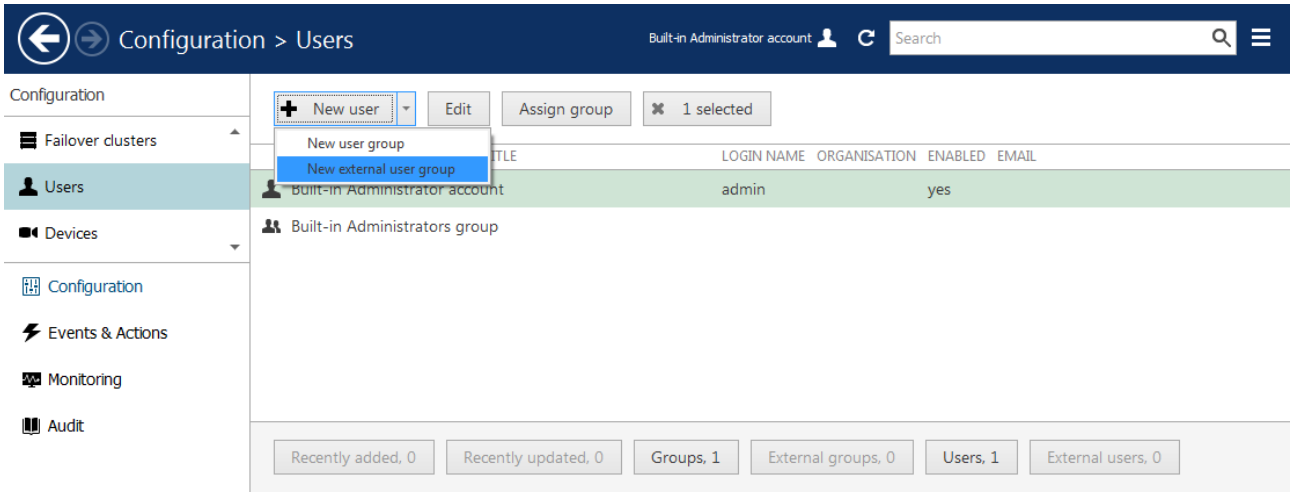
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

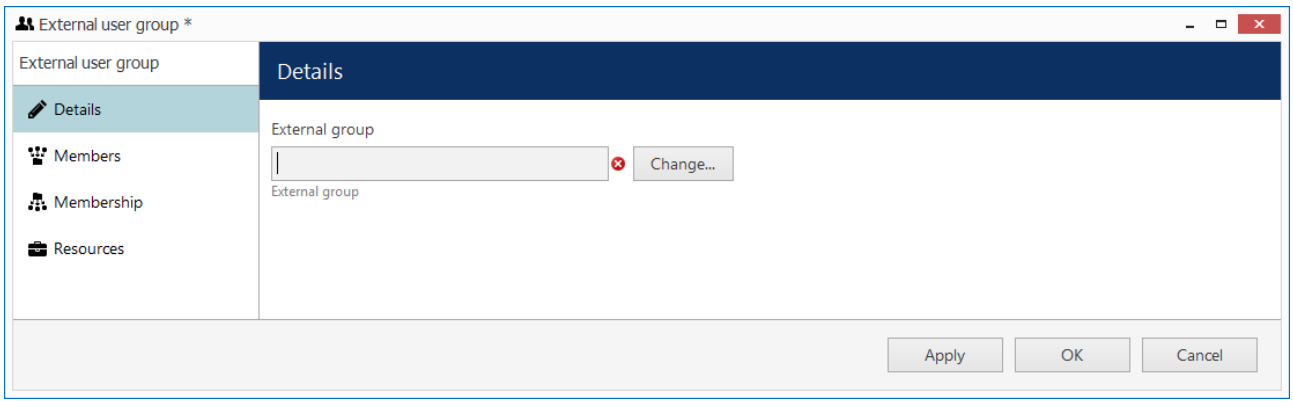


Add Active Directory and LDAP Users

In Macula Console, open the *Configuration* section and choose *Users* from the menu on the left; then, click the little arrow next to the *+New user* button and choose *New external user group* from the drop-down list.

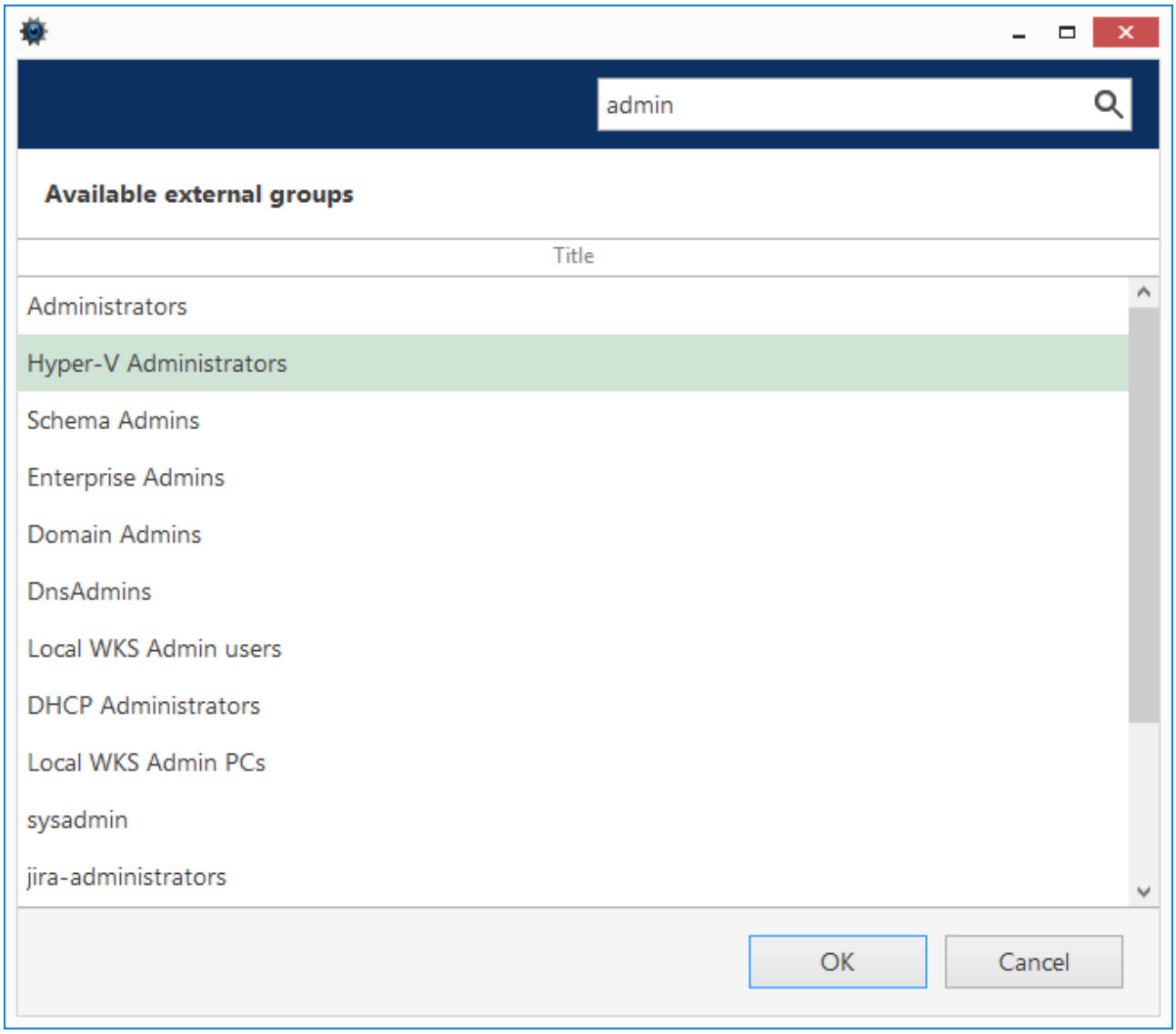


On the *Details* tab, click the *Change* button next to the empty *External group* field in order to load the available AD group list in a separate dialog box.



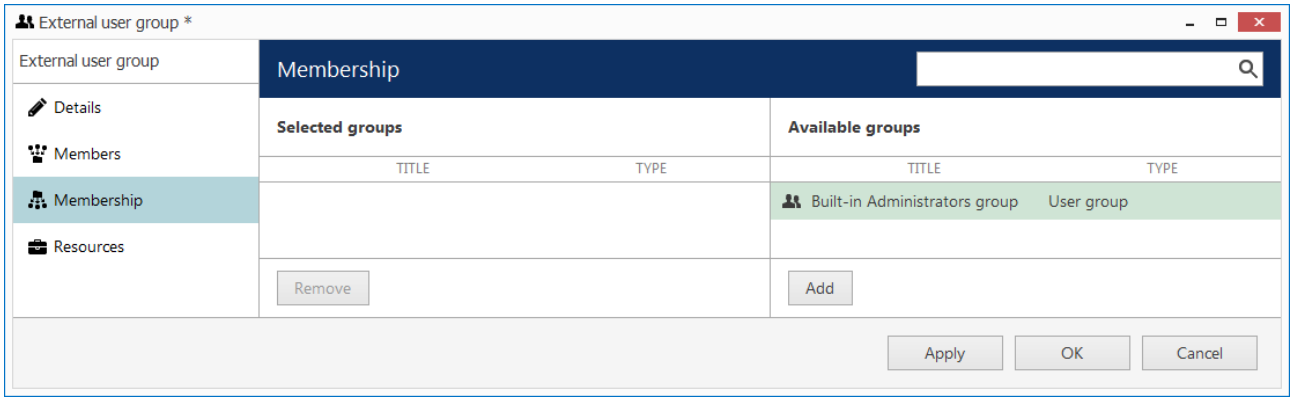
Macula® Professional Administration Guide

Macula will automatically fetch all user groups available via your Windows AD service. Pick a group from the list of available AD user groups and confirm your choice either with a double-click or using the *OK* button below.

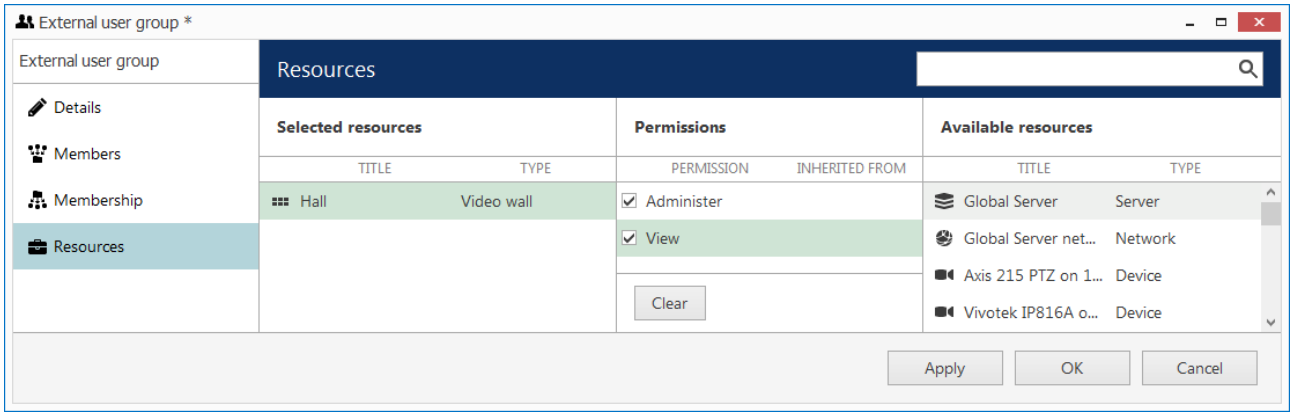


The selected user group will appear in *External group* field in the *Details* tab. Switch to the *Members* tab to view the imported user list.

On the *Membership* tab, you can choose an internal user group to contain the newly imported external user group (nested grouping). All user permissions inherited from the higher level group will be applied to the members of the imported external user group and will be displayed as grayed out in the *Resources* tab.



If you have decided to make no nested groups or wish to add more permissions specifically to the AD user group, go to the *Resources* tab to manage the user permissions.



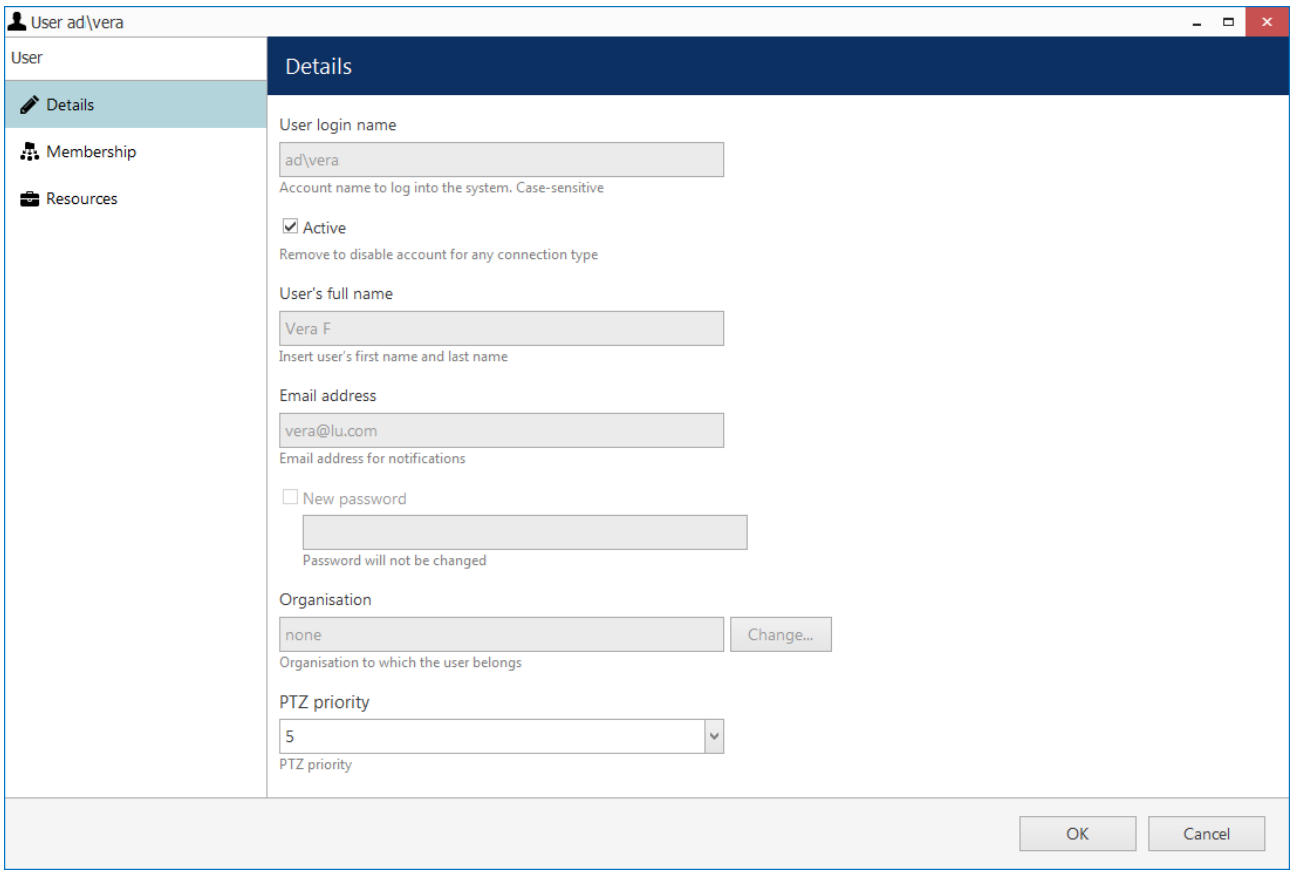
Select resources by adding at least one permission; remove them by clearing the permissions using the *Clear* button below, or simply by double-clicking them in the *Selected resources* list.

Click *OK* when you have finished to return back to *Users*; the newly created external user group as well as all users contained in that AD group will be added to the item list. Use the buttons on the upper panel to edit the group details at any time. If there are a large number of user accounts, the *Search* field in the upper-right-hand corner and the contents filters in the bottom panel can help you to quickly find the accounts you are looking for.

Edit External Users Or User Groups

After adding the external user group, you can edit the group properties as well as individual external users. In order to do this, select the target user/user group in the list and click the *Edit* button on the upper panel, or, alternatively, simply double-click the desired item to bring up the configuration dialog box.

Editing an external user group will be pretty much the same as adding a new one; individual external user settings will have some differences comparing to the regular, built-in user settings.



On the *Details* tab, the only settings available for editing will be user account status (enabled by default) and PTZ priority (which will be 5, by default). All the other properties will be grayed out as they cannot be changed via Macula and should be changed via Active Directory instead.

If two or more users try using PTZ control of a device at the same time, **PTZ priority** is used to decide who gains access first: user with a lower priority is blocked for ten seconds to allow a higher-priority user to use PTZ. If two users with the same PTZ priority have an access conflict, they will be both granted PTZ access simultaneously.

Default PTZ priority for all users, including those built-in and imported, is equal to five (medium priority). You can assign any user a higher PTZ priority (six to ten) or a lower one (four to zero) by editing individual user properties.

On the *Membership* tab, you can choose an internal user group to contain the AD user as a member. All user permissions inherited from the group will be applied to the target AD user and will be displayed as grayed out in the *Resources* tab. You can assign additional user-specific permissions on the *Resources* tab.

7.2 Permissions and Membership

You can handle the user and user group **access permissions** for channels, devices, servers and other resources via the *User* and *User group* configuration dialog box -> *Resources* tab, or via resource settings -> *Permissions* tab. **Administrative permissions** are handled in the *Edit User*/*User group* dialog box, under the *Administration profile* tab. Most of the events that are raised as a permission is used are logged in the *Audit log* and are available in the *Audit* section of Macula Console.

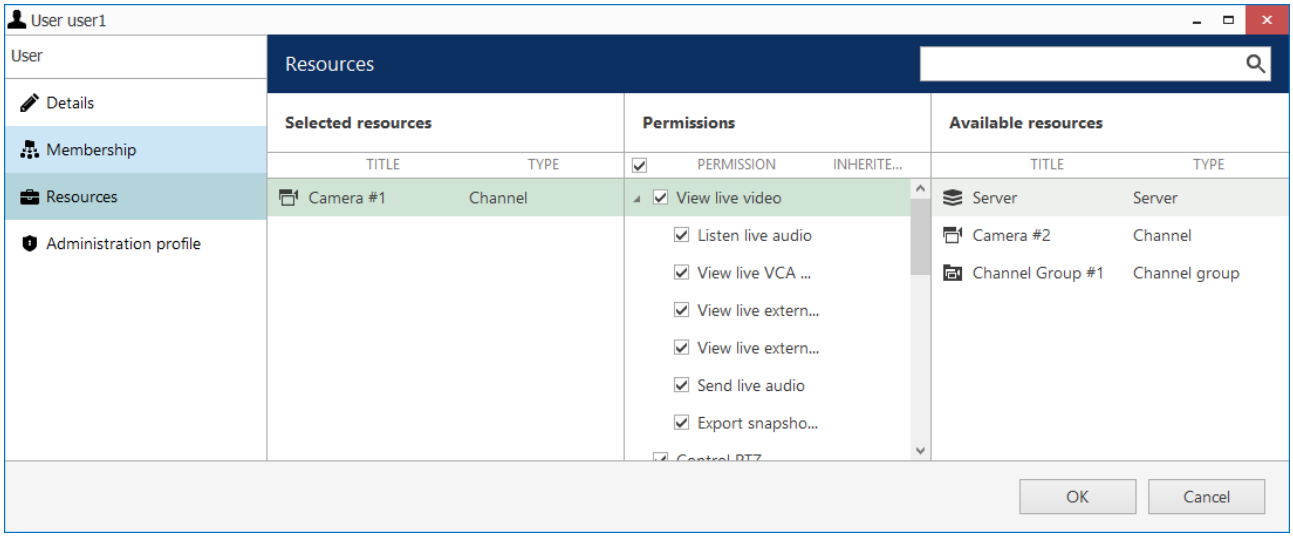
Please note that some of the permissions may not be applicable to your software license edition.

In Macula version **1.6.0**, major changes were made to permission management. As a result, configuration imported from an **XML** file (from old product) will **not** contain any user permissions: you will need to **review and set all user permissions after importing the configuration**.

Access Permissions

All the available resources are listed in the column on the right; click any item to load the permission list in the central column. Then, **mark** all the permissions you wish to grant; resources having at least one permission enabled will be automatically moved to the left column.

All permissions also affect all corresponding requests over API connections.



To **remove** all permissions for some resource, simply double-click it in the *Selected resources* list on the left.

It is not possible to select **multiple** resources for the permission management. You are welcome to use resource **grouping** (e.g., channel groups) for easier and faster permission management.

When permissions are inherited from some group(s), a corresponding mark will appear in the central column next to the permission type.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

The following types of permissions are available (each one can be defined separately):

- **Server**
  - **Playback**: allows users to access recorded video, audio, VCA metadata and external data from the specified server for those recordings that do not have corresponding channels in the server configuration (i.e., **orphan archive tracks**)
  - **Export**: allows users to export video clips and snapshots from such recordings
- **Channel**
  - **Live**: access live video, audio, VCA metadata, external service data, external data (from *Data Sources*), send audio OUT and export snapshots from the live view mode
  - **PTZ:** general **PTZ control**, preset and tour usage, preset and tour management OR **interactive control** of CrossLink devices
  - **Playback**: access to recorded video, audio, VCA metadata, external service data, external data (from *Data Sources*), snapshot and video clip export from all playback modes, view and manage bookmarks
  - **Restricted playback**: same permission set with a time limitation**
  - **Uncategorized**: back up and delete archive, protect archive from deletion, remove protection
  - **Push external metadata**: if this user is used for an external service connection, make sure to add this permission for the server to accept the external service metadata (e.g., analytics bounding boxes)
  - **Trigger channel external event**: if this permission is enabled, the target user account can be used to trigger individual channel's external events
- **External Service Group**
  - **View live data**: see the live data coming from the external services in the target group
  - **External service search**: browse recorded external service data
- **Layout**
  - **View**: see and use the layout in Macula Monitor
  - **Manage**: delete or replace existing layouts via Macula Monitor
- **Layout Group**
  - **View**: see and use layouts from the target group in Macula Monitor
  - **Manage**: add new shared layouts from Macula Monitor and delete existing layouts
- **Visual Group**
  - **View**: see visual group contents in Macula Monitor*****
- **Map**
  - **View**: see and use the map in Macula Monitor
- **Webpage**
  - **View**: see and use the webpage in Macula Monitor
- **Software Counter**
  - **Access archived VCA metadata**: see the counter in Reports in Macula Monitor
- **Video Wall**
  - **View**: see and use the video wall in Macula Monitor
  - **Manage**: change video wall contents via Macula Monitor
- **User Button**
  - **View**: see and use the target user button to viewports in Macula Monitor and in Macula Mobile applications

Starting from the software version 1.15.0, it is possible to grant individual rights for software counters. However, if the *Access archived VCA metadata* permission has been given for the **whole server**, the target user or user group will have access to **all counters** on that server, regardless of the individual counter permissions.

> *A visual group will only be displayed in Macula Monitor if the user has permissions to see at least one visual group element.
> **The permission sets under **time-limited** *Restricted video playback* and **full** *Video playback* are essentially the same. The difference is that restricted access only allows users to access the last N minutes/hours/days of the archive. Therefore, the two sets are mutually exclusive. The **restricted interval** is defined individually for each server in the server **storage settings**.

When you have finished, click *OK* to save and exit.

Administrative Permissions

Administrative permissions for the resources, servers and connections can be managed via *Administration profile* tab in the user management dialog box.

> Giving a user at least one permission from the *Console* section will allow this user to log into the target server via Macula Console. The corresponding resources will be available for configuration and all the rest of the contents will be hidden.

The following types of permissions are available for per-user/per-user group configuration:

- **Client**
  - Login via **Monitor**: connect to the target server via Macula Monitor application
  - Login via **Monitor** without entering **login reason**: if unchecked, the user will be prompted to enter a justification (comment) before logging in
  - Login via **HTTP**: connect to the target server via Web client and from external services, including LPR and FR
  - Login via **Mobile**: connect to the target server from Macula Mobile and OS X app
- **Console**
  - Manage **Organizations**, **servers**, **users**, **permissions**, **networks**, **external services**: enables the user to access the configuration of the corresponding server contents
  - Manage **devices**, device **channels**, **visual groups**, **layouts**, **layout templates**, **video walls**, **maps**, **data sources**, **user buttons**, **shared channels**: enables the user to edit existing and create new (if applicable) resources of the given type
  - Manage recording: create and edit **recording profiles, schedules** and **configurations**
  - Manage Event & Action rules: create, remove and edit events, actions and all the related resources in the **Events & Actions section**, including mail servers, conditions etc., regardless of permissions for the source items
  - Access **audit log** and **monitoring section**: view all the information in the server *Audit* and in the *Monitoring* sections
  - Manage **auto backup**: access scheduled backup configuration
  - Start wizard: allows users to run the **quick setup wizard** via Macula Console for step-by-step configuration

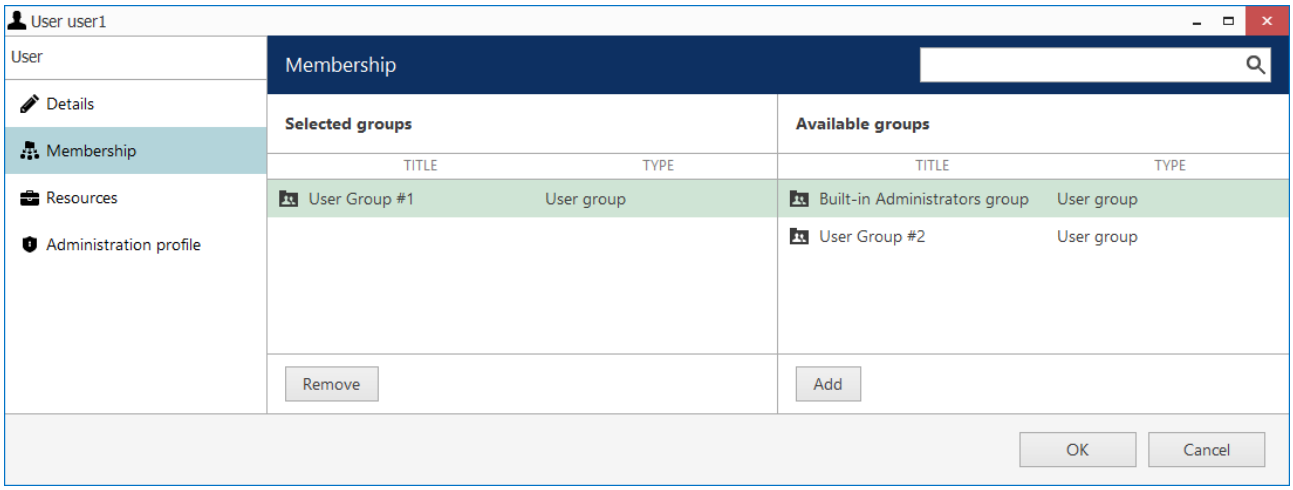
- **Remote upgrade**: access the remote upgrade section of Macula Console, set up and do the remote upgrade procedure
- **Import configuration**: load configuration from XML (from the old product version) and import existing Macula database

Starting from version 1.13.0, there is an additional user permission under *Administration profile*: log into Monitor application without entering **login reason**. If this permission is granted, users will log into the Macula Monitor application as usual; if not, an additional prompt will pop up, asking them to enter a justification for logging into the server.

Membership

Users can be grouped logically to make permissions management easier. Groups can overlap, meaning that a single user can belong to multiple groups at once, and some groups can be nested - i.e., one group can contain one or more other groups. In addition to own permissions, each user inherits permissions from all the groups he is currently in.

To manage user membership from the user configuration dialog box, double-click any user. This will open the properties window, where you can switch to *Membership* tab. Here you can pick which group - or groups - this user will be a member of.



Double-click on groups or use the *Add/Remove* buttons below to move groups between columns. When you have finished, click *OK* to save changes and exit.

Alternatively, you can select one or multiple users from the users list, then click the *Assign group* button on the upper panel: a list of available groups will appear, allowing you to select one of the existing groups. After this, click *OK* to add selected users to the target group.

We strongly recommend grouping users and resources as it makes the permission management process much easier. Individual user permissions can be combined with permissions inherited from multiple groups at once.

Permission Sets and Dependencies

Permission management in Macula is flexible and allows each individual user permission to be enabled separately, thus giving the Macula administrator full control over the system. Sometimes, in order to give enough user rights for specific use case, several different permissions should be granted. This section

covers some examples and gives you an idea of what permissions may be related, as well as explains some peculiarities about the permission management in Macula.

General

Administration profile permissions to manage maps, visual groups, live podcasts etc. include access to all channels from the *Edit* dialog of these entities. For example, a user is granted permission to manage maps but does not have any per-channel permissions: when creating a map, he will be able to put channel markers on it and associate these markers with any channels on the server. At the same time, he will have no access to the channel management whatsoever.

Allow a User to Add New Devices

In order to enable a user to add new cameras or devices of other types, it is necessary to grant the following permissions from the *Administration profile*:

- *Manage devices*
- *Manage device channels*

This is necessary as devices and channels are related entities in Macula and a single Manage devices permission is not enough as new channels are created automatically alongside with the newly added devices.

The *Manage devices* permission itself allows the user to change device settings (e.g., IP address, group membership) and create new device groups.

Access Data from Third Party Services

To see the data from external services (e.g., LPR/FR recognitions) in the live view notification panel or search the past records, the following permission sets are required:

- **Live**:
  - *View live external service data* (per-channel permission under *View live video* permission group)
  - *View live external service data* (permission for the external service group)
- **Archive**:
  - External service search (per-channel permission under *Video playback* permission group)
  - *External service search* (permission for the external service group)

This allows to cover the case when one channel belongs to several different external service groups.

Archive Backup

Archive backup permissions have the following logic:

- *Make archive backups* permission from the *Administration profile* allows Archive Backup Wizard login

- *Backup archive* per-server permission from the *Video playback* permission group grants access to the orphaned archive tracks (recordings that exist on the server but do not have any existing channels in the system configuration associated with them)
- Backup archive per-channel permission under *Video playback* permission group grants access to the footage of the target channel via Archive Backup Wizard

Snapshot Export

For a user to be able to save multichannel snapshots from the *Archive playback* mode, the *Export snapshots from playback* permission must be granted for all channels present in the layout.

7.3 Anonymous User

Anonymous user is a built-in user account, which has been designed for unauthorized access to video streams via HTTP API - a very basic example of Macula API usage.

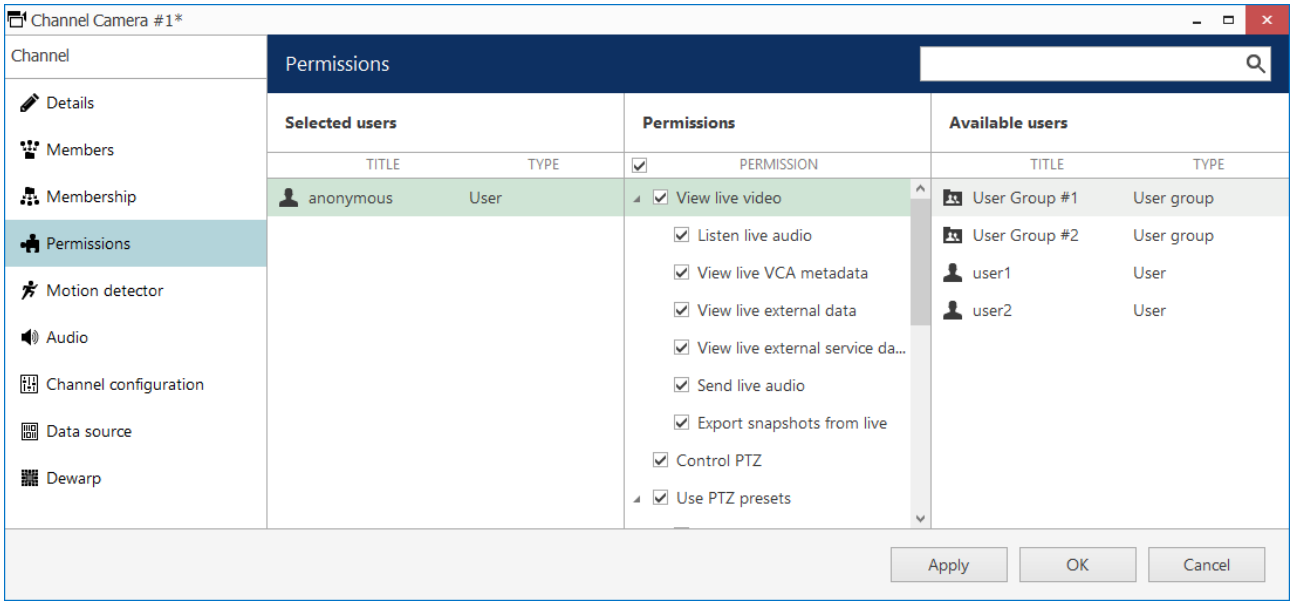
Briefly, here is the procedure that enables you to get video via link:

1. Enable Anonymous user
2. Grant them permission(s) to view live channel(s)
3. Enable resource IDs in the Macula Console settings
4. Look up server IP and port, and channel ID to form the link

The procedure is described in more details below.

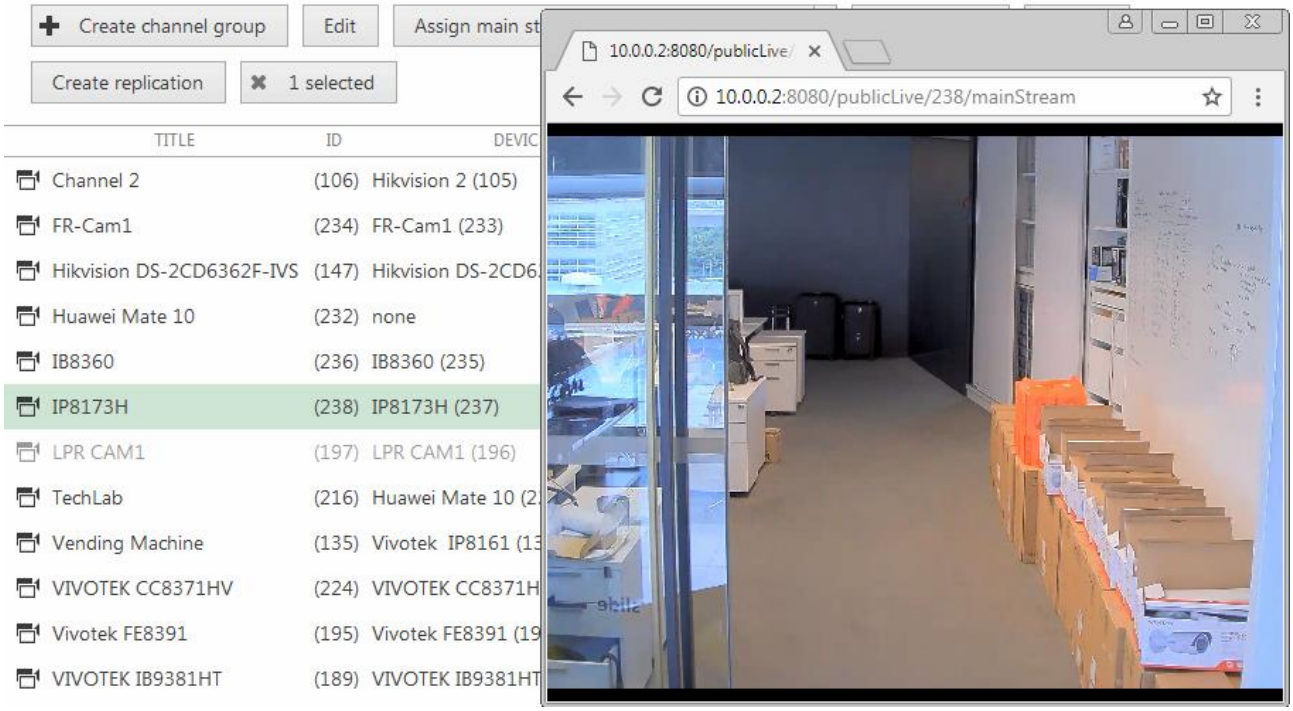
The anonymous user is **disabled by default** and does not have any permissions. In order to allow HTTP access:

- **enable** the anonymous user: double-click him in the user list, mark him as active, then save;
- **add** the *View live video* **permission** for this user in the properties of the target channel(s).



Now you can use a short link to receive live video feed over HTTP from your configured channels without authorization.

Macula® Professional Administration Guide



The link can be embedded, for example, into your own webpage to provide 'Live Cam' functionality.

HTTP **link** is built as follows:

- *IP:PORT/publicLive/<channel_id>/mainStream*

where

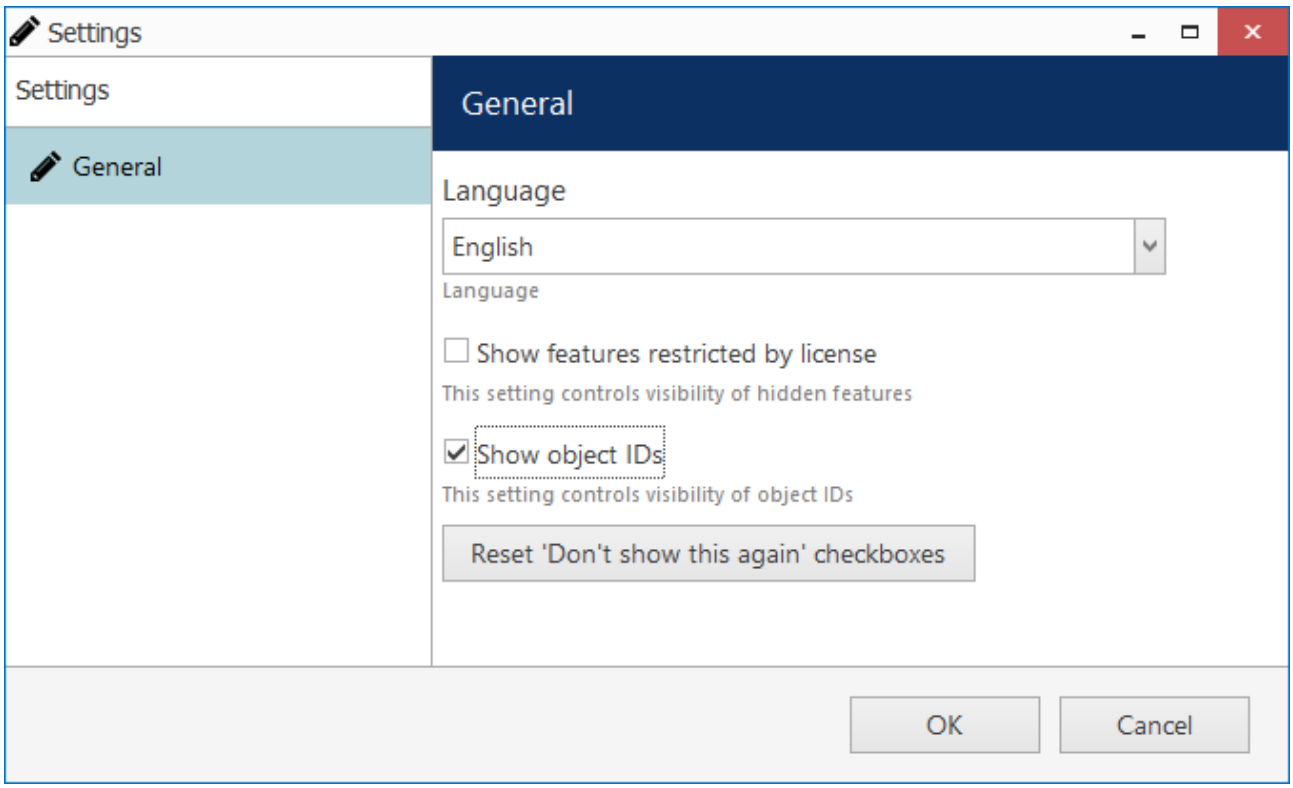
- *IP* is server IP address or hostname,
- *PORT* is server HTTP port (8080 by default),
- *<channel_id>* is internal channel identifier, which can be looked up in Macula Console when IDs are enabled in the application settings.

Example: *192.168.1.83:8080/publicLive/184/mainStream*

⚠ This functionality requires that Streaming Server is enabled (HTTP port is not set to zero in the target server settings).

In order to see the channel identifiers in Macula Console, go to the application settings via main menu button in the upper-right-hand corner and choose *Settings*. In the dialog box, enable the *Show object IDs* option and save.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



⚠ Starting with Macula Console version 1.25, you can also use all the available permissions for the *Anonymous* user.

To add custom permissions to Built-in Anonymous user:

1. Go to *Configuration -> Users -> Anonymous* and double-click on it or click the *Edit* button.
2. Select *Resources* from the left menu and use the *Permissions* tab as with any other user.

Read more on how to manage *Permissions*.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

8 Streaming Server Configuration

Get permanent access to live streaming and archive video, no matter where you are in the world. The Macula Streaming Server allows quick and easy access to your cameras via web browser and/or native mobile applications.

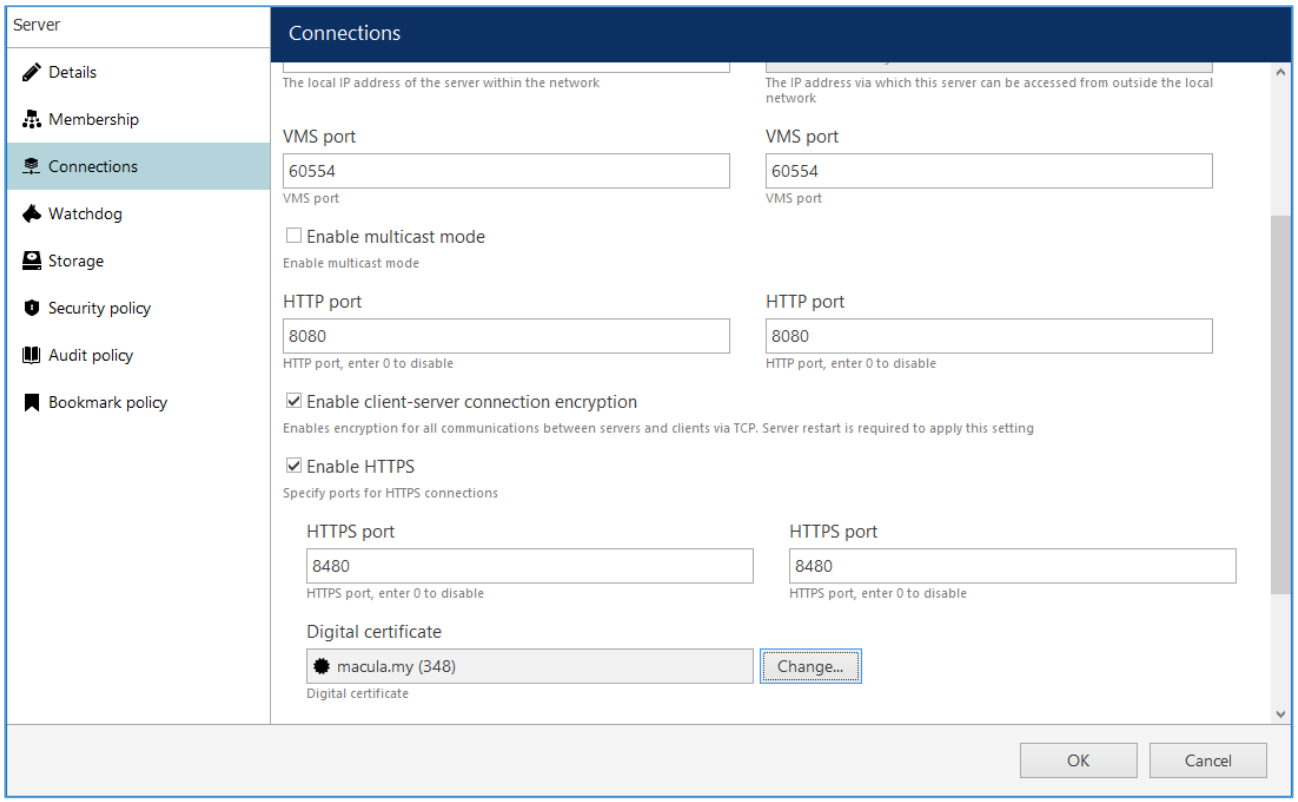
Macula Streaming Server is a part of Macula software integrated into the Macula Server core. It is designed for video streaming to multiple web-browsing platforms such as Mozilla Firefox and Google Chrome. Some major Macula Streaming Server features are: video stream live view, archive playback, Pan-Tilt-Zoom control. The Macula Streaming Server optimises video streaming for web or mobile clients, to a degree dependent on connection speed and device viewing capabilities.

Macula 1.27 Update: The *Server Watchdog* now automatically monitors the *Streaming Server*, enhancing system stability and reliability. This integration ensures uninterrupted streaming and improved performance, with no additional settings required.

If you are using AD/LDAP user accounts for the Web client login, we strongly recommend that you turn on HTTPS for enhanced security

At this point, the browsers recommended for clients are Google Chrome and Mozilla Firefox. Audio and event streaming are **not** supported by the Macula Streaming Server.

Macula Streaming Server configuration on the Macula Console side is simple and only consists of HTTP port for streaming connections. To access the Macula Streaming Server setup in Macula Console, go to the *Configuration* section and then click *Servers* in the menu on the left; double-click the target server to bring up the configuration dialog box and switch to the *Connections* tab.



You only need to define a HTTP port for Macula Streaming Server; the default port is 8080. On top of that, you can secure your connection and use a HTTPS port for the same purpose. Secure HTTP will require a valid digital certificate, either a self-generated (generate on the fly, will require trust confirmation everywhere) or issued by authority (paid, bound to your domain).

⚠ Please make sure that your chosen HTTP port:

- is opened on the target server firewall;
- is properly configured for port forwarding on all intermediate network equipment, if necessary;
- is not being used by any other application or service on the target server.

If you are using HTTPS with your own **CA certificate** (bound to your domain name), remember these important guidelines for the mobile app setup:

- when connecting via local network, use server IP address
- when connecting over internet (4G etc.), use the hostname instead of IP (main domain must be the same as in the certificate)
- if port forwarding is used (local HTTPS port is different from external), enter the port number as the "Internet port" in the server connection configuration

⚠ If you are using your own CA certificates, create a .pem file with your certificate chain as described here:
https://www.digicert.com/ssl-support/pem-ssl-creation.htm

This is necessary for the certificate to be recognized correctly by all HTTP clients - Web browsers and Macula mobile applications. If you simply apply your CA certificate in Macula Console, there is a chance it is not recognized because some applications require the entire certificate chain.

> Then, apply the .pem file as the certificate together with your key when the importing certificate into Macula Console.

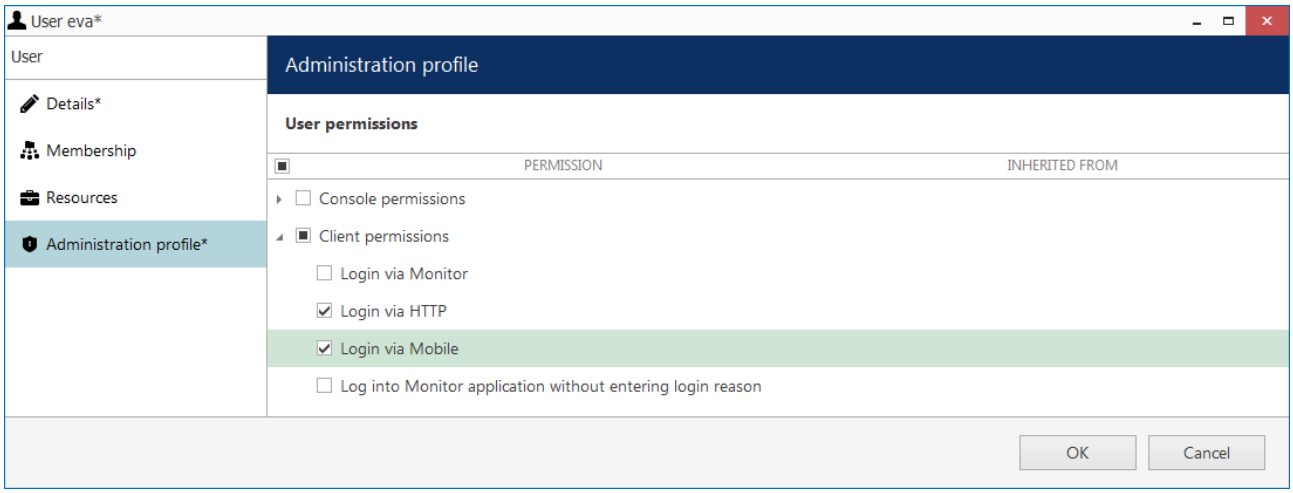
Once you are done with the settings, click *OK* to save and close the dialog box. Your Macula Streaming Server will now be set up and accessible via a local - and, if used, external - IP. You can immediately check the connection at once: just open your browser and type: *<local IP>:<HTTP port>;* for example, server configuration for the snapshot above will require *192.168.1.83:8080.*

User Permissions for Macula Streaming Server

If you are going to create a non-administrative user account for Macula Streaming Server access (designated or combined with other permissions sets), the following user permissions should be granted in the user properties dialog box:

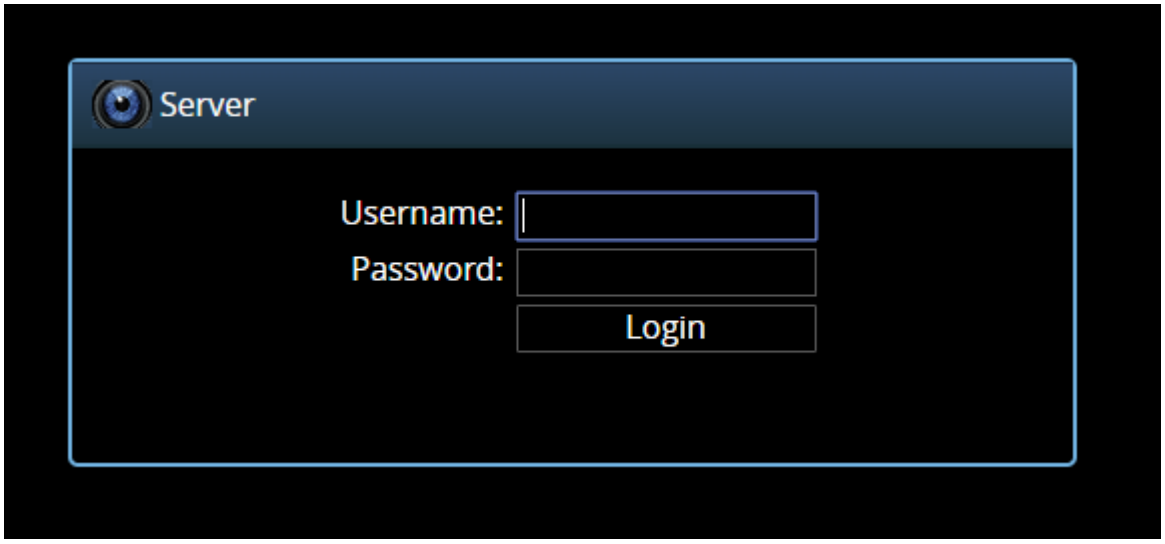
- for Web browser and API login: under Administration profile > Client permissions > Login via HTTP
- for the Macula Mobile access: Login via Mobile
- to allow editing HTTP connection properties: Console permissions >Manage servers (this will automatically enable Macula Console login, and also grant access to other server settings)

In the Resources tab, select channels and features you wish to grant acess to. There are separate permissions for live and archive access, PTZ, audio, and bookmarks.



8.1 Streaming Server User Interface

Macula Streaming Server provides HTTP connections for Web browsers and native Macula Mobile applications, OS X Thin Client (similar in functionality to Macula Mobile), as well as services that use Macula HTTP API, which includes Macula own external services (VDS, License Plate Recognition, Face Recognition modules) and third-party integrations. While the Web browser client functionality is very basic, Macula Mobile applications support many useful features, such as two-way audio, push notifications, mobile edge recording, streaming from device camera to the Macula server and many more.



When configured, Macula Streaming Server is accessible via browser from the server itself and from computers on the local network, and, if system is not isolated, from the Internet. This is the simplest way to make sure your Macula Streaming Server is running and reachable. To access the Macula Streaming Server, open your browser and type:

<Server IP>:<HTTP port>

then press Enter. Your browser will connect to Macula Streaming Server, and user authentication will be requested: enter your user name and password to proceed.

> Starting with Macula version 1.14.0, you can also use your **AD/LDAP user accounts** for the Web browser login. The user name should be entered in the following format:
> domain.name\user.name
>
> The field is case-insensitive, meaning that you can use either *user.name* or *User.Name* notation.

After logging in, you will see Macula Streaming Server user interface:

- **left menu**: channel list and setup tabs
- **main window**: live-streaming area
- **upper-right-hand corner**: layout templates and layouts
- **upper-left-hand corner**: the Macula Streaming Server logo; click the logo to extend viewing area by minimizing the menu on the left

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Access Permissions

The channel and feature availability depends on the user permissions; the built-in administrator has access to all resources. For the Web browser connections, only HTTP connection, live, archive and PTZ access permissions are applicable, as other functionality (e.g., audio) is not present.

In order to allow a user to connect to Macula Streaming Server, go to *Configuration* section of Macula Console, choose *Users*, then select the user or user group for editing and open the *Administration profile* tab:

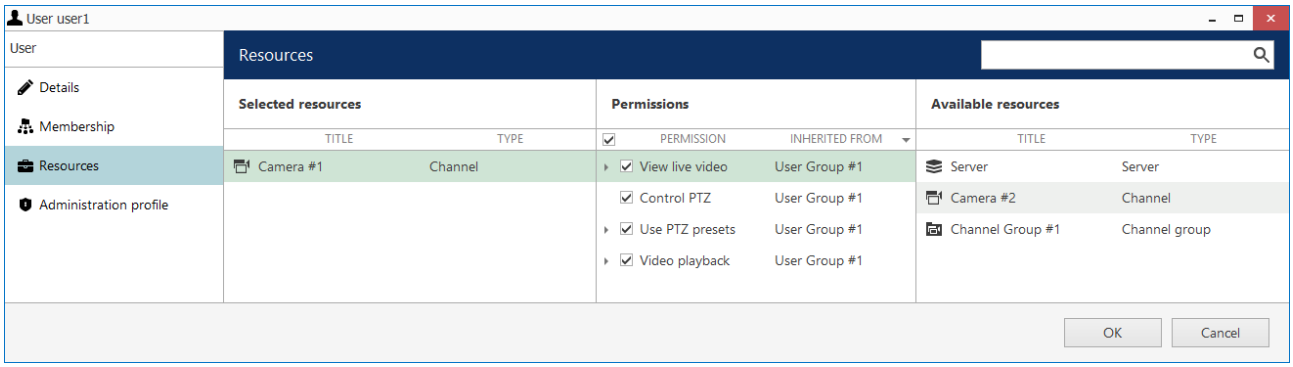
- add the *Login via HTTP* permission to allow Web browser and/or HTTP API connections
- add the *Login via Mobile* permission to allow connections from mobile apps and OS X client

To allow channel access, add per-channel or per-channel group privileges in the *Permissions* tab:

- *View live Video*: enables live view
- *Listen live audio*: enables incoming audio (from the camera)
- *Send live audio*: send audio to camera (talk back)
- *Control PTZ*: pan, tilt and zoom controls
- *Use PTZ presets*: access to existing PTZ presets
- *Use PTZ tours*: access to existing PTZ tours
- *Video playback*: enables access to recorded video data
- *Audio playback*: access to the recorded audio data

Additional permissions for the Macula Mobile applications:

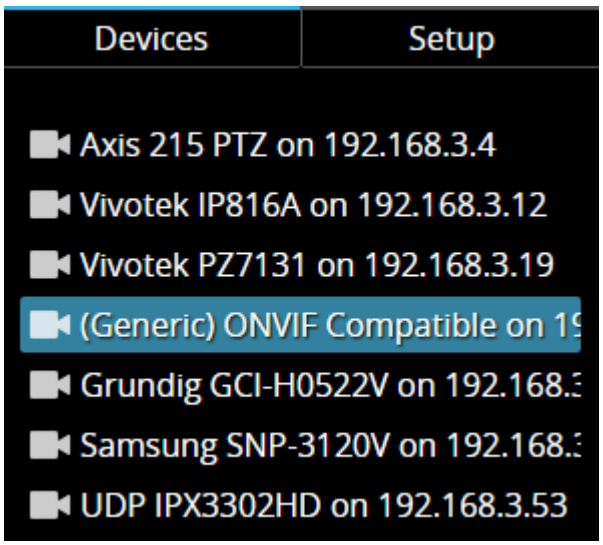
- for *User Buttons*: the *View* permission allows you to see and use the user button



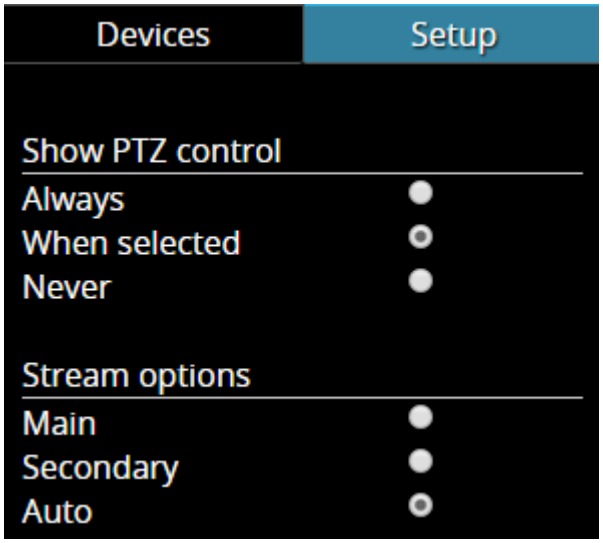
Channel, channel group and user button permissions can also be changed in the *Channels* section, by double-clicking the corresponding channel or channel group in the list and then selecting the *Permissions* tab.

Web Interface: Configuration

The menu on the left has two tabs: *devices*, which shows which channels are available, and *setup*, which contains streaming settings. Click on the titles to switch between them.



The video sources are loaded in a single list. To start streaming from a particular device, select layout template from the menu in the upper-right-hand corner, then click your desired viewport so that it is highlighted blue, and then click a device from the list.



The *Setup* tab allows you to choose PTZ control behavior and configure stream options:

- **PTZ controls**:
  - **Always**: if the camera supports Pan-Tilt-Zoom, virtual PTZ sphere will be always shown as overlay control
  - **When** selected: if the camera has PTZ capabilities, the virtual PTZ sphere will be shown when the corresponding stream is selected
  - **Never**: do not show PTZ controls at all, meaning that PTZ functionality will be disabled
- **Stream options**:
  - **Main**: only the first (main) stream, [usually] of a larger resolution will be used for all devices
  - **Secondary**: only the secondary stream (substream), [usually] of a smaller resolution will be used for all devices
  - **Auto**: the most appropriate stream will be selected automatically based on viewport size

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

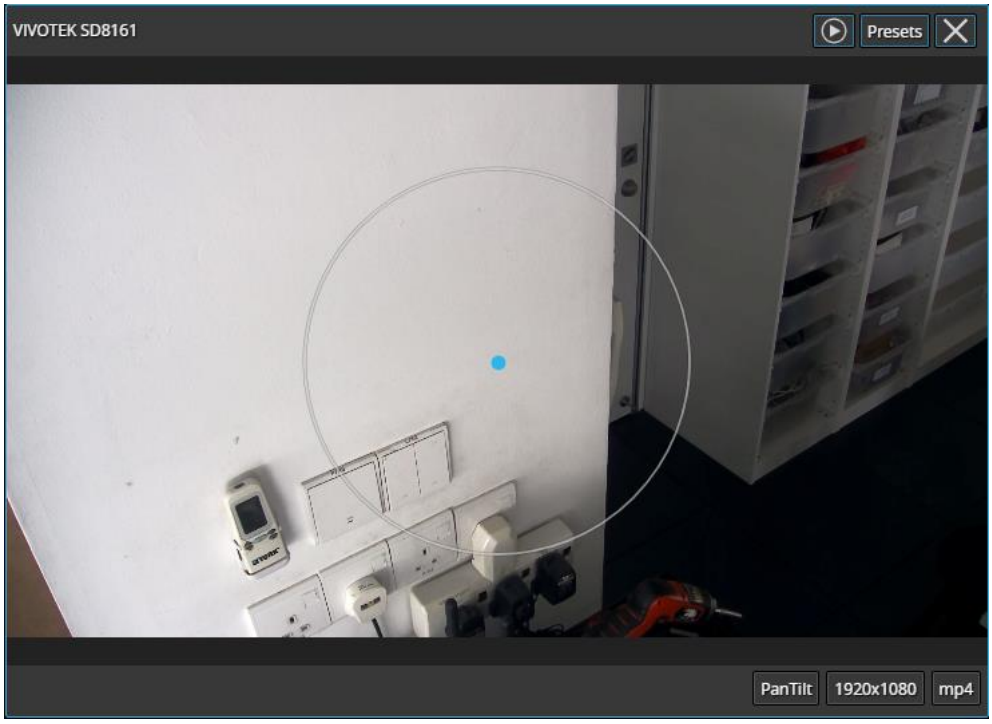
Web Interface: Streams

The Web browser client allows you to view live video and to play back recorded video from the available channels. For live view mode, PTZ controls are available.

Live

To start live-streaming, select a layout template from the upper-right-hand menu (1x1, 1x2, 2x1 or 2x2), then click your desired viewport so that a blue frame selection appears around it, and then choose the target stream from the *Devices* list on the left. To replace the existing live stream, either select it and choose a device 'on top' of it, or click the *X* button in the upper-right-hand corner of the viewport to close it and then assign a new stream to this viewport.

Notice that some images may appear with horizontal or vertical black stripes at the sides: this happens because image aspect ratio is maintained instead of it being stretched to fill the viewport. When the picture size is smaller than the target viewport, there will be a black background on either sides.



Each live view item contains the following information and controls:

- upper-left-hand corner: stream name (static info)
- upper-right-hand corner: archive playback (if applicable), presets button (click to load preset list), *X* button (press to close the live stream and free the viewport)
- bottom-right-hand corner: PTZ mode (if applicable), stream resolution, stream codec (MP4/JPEG/WEBM) (static info) and zoom mode ON (static info)
- center: stream picture, virtual PTZ sphere (overlay control) (if applicable)

To **pan and tilt** the PTZ-capable cameras, use overlay PTZ controls: left-click and hold in the desired direction. By default, pan/tilt mode is enabled for PTZ cameras: notice the *PanTilt* label in the bottom-right-hand corner of live view.

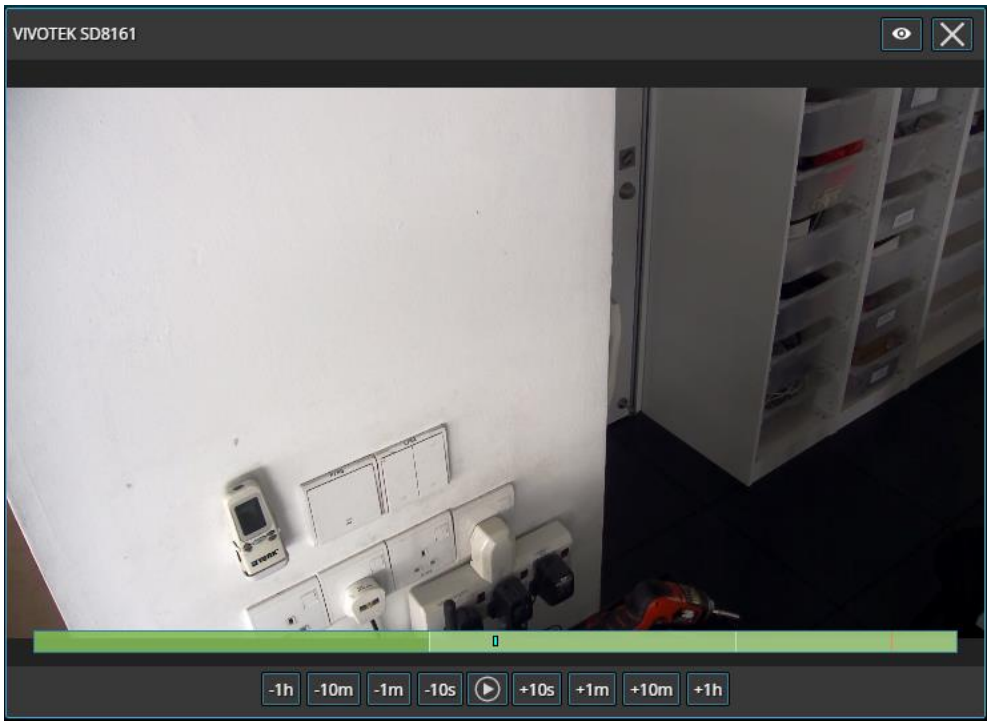
In order to **zoom** IN and OUT: first, scroll your mouse wheel DOWN to enable zoom mode - in the bottom-right-hand corner, a *Zoom* label will appear. In this mode, virtual PTZ sphere works for zoom only: click

and drag UP (upper hemisphere) to zoom IN, and DOWN (lower hemisphere) to zoom OUT. To release zoom mode and go back to the pan-tilt sphere, simply scroll your mouse wheel UP until the *Zoom* label disappears.

For some cameras, you may notice that the further you drag the cursor from the sphere centre, the faster the camera goes: in this way, PTZ speed is controlled; however, for other cameras, only the constant speed is supported either by software or device itself, and the pan/tilt speed will remain constant no matter what position your mouse cursor is in.

Archive Playback

If recording is enabled for the target channel, the stream overlay controls will include an archive playback button in the upper-right-hand corner. Press the button to begin **playback**: the target stream will be displayed in single channel mode. To switch **back to live view,** press the 'eye' button in the upper-right-hand corner; this will restore your previous layout.



Playback view contains the following information and controls:

- upper-left-hand corner: stream name (static info)
- upper-right-hand corner: 'eye' icon to go back to live view, *X* button (press to close the live stream and free the viewport)
- bottom-right-hand corner: timestamp (current time and server time zone shift)
- center: stream picture
- center bottom: playback controls

Overlay controls allow you to start/pause playback and jump back/forward by ten seconds, one minute, ten minutes or an hour.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Web Interface: Layouts

Layout templates allow you to choose viewport layout: 1x1, 2x1, 1x2 and 2x2 are currently available options.

Click on any thumbnail at any time to immediately load the corresponding **layout template** on the screen. If there are any active streams, they will be discarded. If the target layout template has been already used in the same browser and cookies have not been cleared, previously used channels will be loaded; if not, an empty template will be displayed.

If you wish to **save the layout** currently being displayed, click on the 'portrait' button.

The layouts menu will appear, allowing you to save your layout under a user-defined name: enter the layout name and click the *Save* button. Note that, at this point, only Latin characters [A-Za-z] and Arabic digits [0-9] are supported for layout names; special symbols or characters from non-Latin alphabets are not allowed.

From here, you can also load previously saved layouts simply by clicking them; if your layout list is longer than the menu window, use the mouse wheel to scroll down.

The layouts are saved in your browser **cookies**, so:

- Macula Streaming Server layouts cannot be transferred to other browsers, user accounts or computers
- layouts are removed when browser cookie data are cleared

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

8.2 Mobile Application for Streaming Server

Macula Mobile app for Macula servers provides mobile client functionality for smartphones, tablets and phablets. Its functionality range is much wider than that of the Web browser client

You can install the Macula Mobile application from Play Store (for Android users) or iTunes (for iOS users).

Supported OS:

- Android 6 and higher;
- iOS 12 and higher.
- Starting with the Macula Mobile app version 1.19.x you need to have the Macula version 1.23 or higher.

Thin client for macOS has almost identical functionality. It can be downloaded from http://www.gsfcorp.com. Just as Macula Monitor, the mobile and macOS clients are free of charge and do not require any additional license to run. Using these, you can connect to any of your Macula servers, provided that Macula Streaming Server functionality is enabled in their settings, as described earlier.

Below, you will find guidelines on your Macula Mobile configuration and usage.

Getting Started

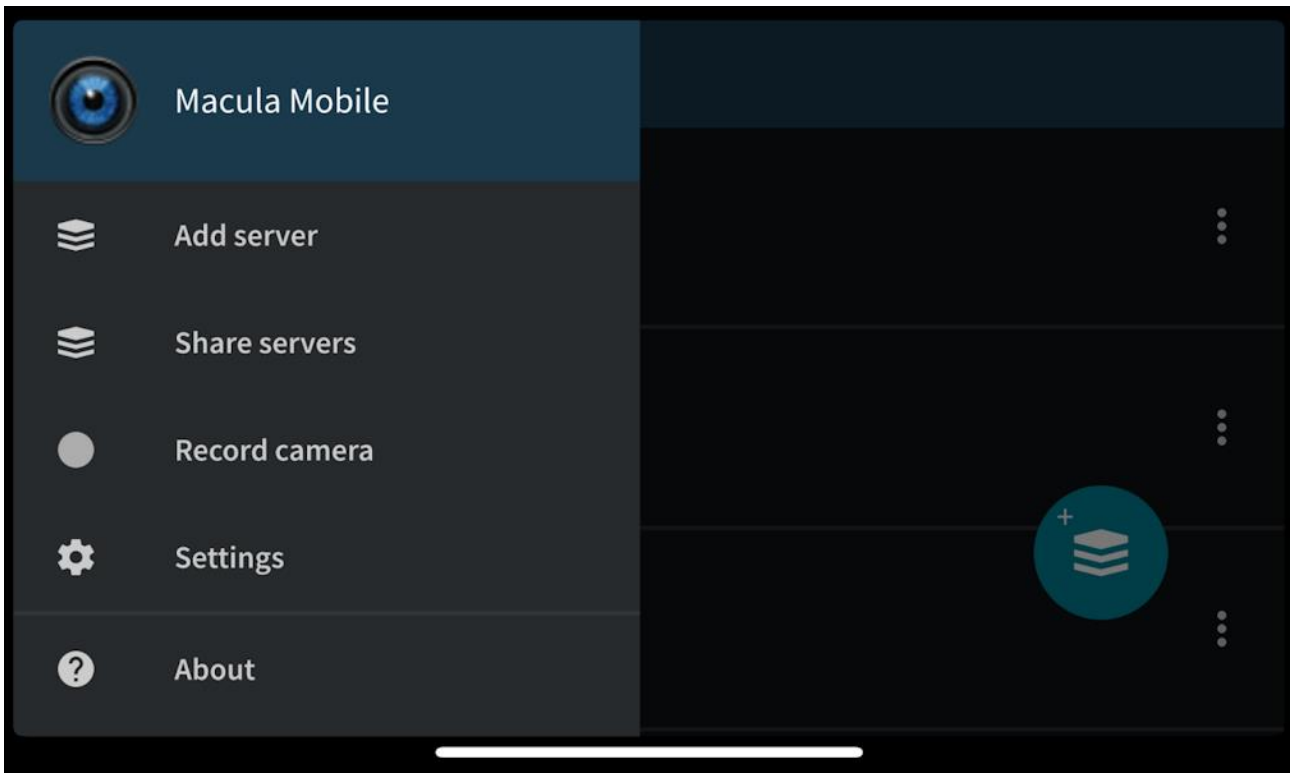
Install Macula Mobile from the corresponding app store, or by following a link from our website http://www.gsfcorp.com.

Interface Overview

Macula Mobile user interface is mostly intuitive: you can interact with the app by tapping or long tapping the interface elements, and also by swiping.

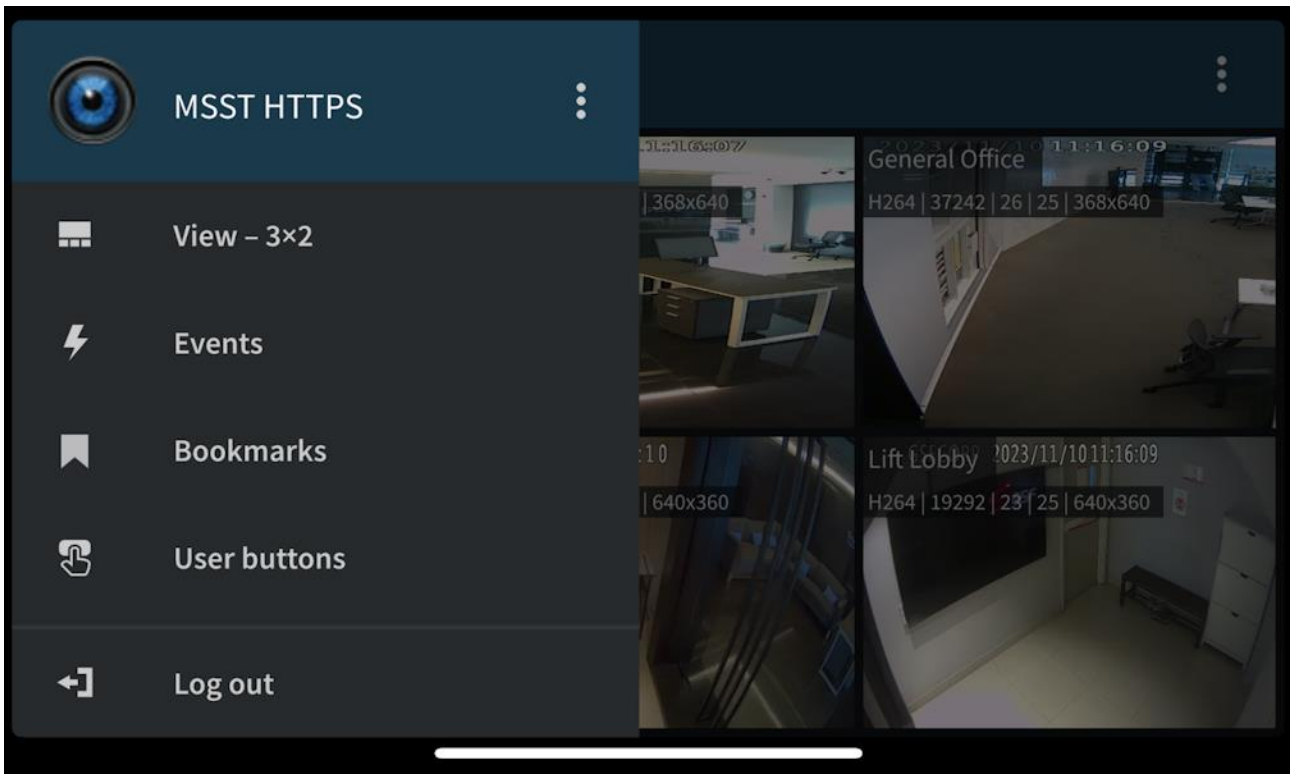
In the top left corner, you will find the **application menu**. It contains:

- *Add server:* an option to add a new server connection.
- *Share servers:* an option to share your existing server setup by sending the recipient server settings XML file.
- *Record camera:* a possibility to record offline in-app video for further upload to any server.
- *Settings:* general application settings.
- Details about the app version.



After you connect to any server, the application menu will be replaced by server menu containing server-specific resources and actions:

- *View - columns x rows:* channel arrangement for live view.
- *Events:* push notifications from the server.
- *Bookmarks:* channel bookmarks from all available servers.
- *User buttons:* any buttons for the current server.
- *Stream camera:* camera streaming option (device >> server).
- *log out* option.



The server menu also has a **submenu** 'three-dots (...)' button next to the server name. Apart from the *Log out* option, it allows you to edit the connection settings (e.g., change the user account) without returning to the server list. The 'three-dots (...)' button is also present in other places within the app, and it offers extra options or actions.

Finally, wherever it is impossible to place the submenu button, a 'hidden' drop-down menu is available. **Long tap** any channel in the multichannel view to see the available quick actions.

> When running in foreground, the app will prevent you phone from going to sleep, so the display will not be switched off automatically. Keep this in mind and do not forget to exit the app or lock the device/turn the display OFF when you do not need the app anymore.

Settings

Tap the 'hamburger' menu button in the top left corner to bring up the main app menu, then tap *Settings*. The parameters here define global app behavior (for all servers); they are preserved as you upgrade the app but are discarded if you uninstall it.

The settings are logically grouped for your convenience. Tap a category to access the settings:

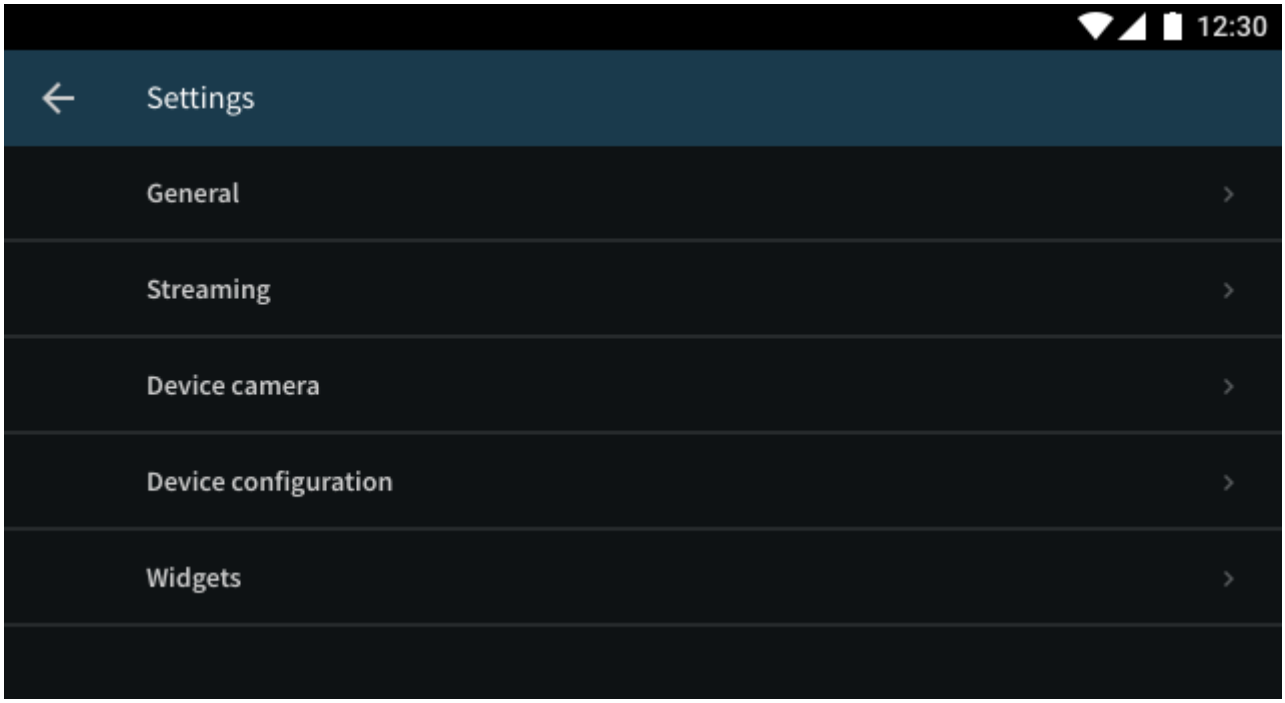
- **General**
  - *Language*: set application interface language here (matches device locale by default)
  - *Date format*: set the date presentation format you want the application to use, e.g., YYYY/MM/DD
  - *Time format*: set the time presentation format you want the application to use, e.g., HH:MM:SS (24h)
  - *Timezone*: choose between your mobile client or connected server time zone
- **Streaming**
  - **Quality preference**

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

        - *Auto*: the most appropriate stream will be selected automatically based on the connection
        - *Main*: only the first (main) stream, [usually] of a larger resolution will be used for all devices
        - *Secondary*: only the secondary stream (substream), [usually] of a smaller resolution will be used for all devices
    - **Display video statistics**
        - *ON/OFF*: defines if the video stream properties (FPS, bitrate) are shown for both incoming and outgoing streams
    - **Decoder** configuration: choose how the incoming streams will be decoded
        - *Hardware and software*: software decoders will be used if required (**warning**: software decoding is battery intensive!)
        - *Hardware only*: hardware decoding modules available on your phone will be used automatically (recommended for battery saving)
        - *Per codec configuration*: choose decoding settings individually for each of the expected codecs
    - **Icons**: descriptive elements overlaying the video
        - *Show* battery intensive decoder icon: the icon will appear in case a software decoder is in use
- **Device camera**: settings related to your phone's camera; the first time you open this section, you will be prompted to run camera detection
    - Camera choice and preferences for the reverse streaming (device >> server) for both live and offline recording modes
        - *Off*: choose this if you do not plan to stream the device's video to the server
        - *Camera 1*: main mobile device camera (normally, back camera)
        - *Camera 2*: secondary camera (normally, front camera with less megapixels)
        - Resolution/FPS/bitrate/codec preference, **microphone** ON/OFF
        - Preview: camera preview with the settings defined above
    - *Detect cameras*: allow the app to retrieve your phone's camera configuration (detection may take some time, making the app unresponsive - expected behavior)
    - *Stream device GPS location* with video to server: when ON, the video streamed from the device camera will be overlayed with GPS coordinates and the device marker will be displayed on the geo maps, if configured
    - **Offline video**: settings for offline video recording (for further upload)
        - *Store offline video*: choose whether you want to store the recorded files in the app directory on the internal storage or on the external storage (SD card)
        - *Offline video storage limit*: restrict the space available for recordings to 100, 200 or 500 MB, 1, 2, 5, 10 or 20 GB, or unlimited
        - *When no space left*: the app can either overwrite the oldest file(s) or stop recording new files
        - *Default video upload server*: choose a server every time you upload the video or set one of the configured servers to be the default destination
- Device **configuration**: **network** and other settings related to your phone (but not directly to its cameras)
    - *Allow app/widgets to use*: choose the preferred network type for the app and for the app widgets separately
        - *WiFi only*: the app will only connect to the server(s) if it is connected to a wireless network (including servers available via VPN)

        - *WiFi and mobile data*: the app will use both wireless networks and enabled data services (3G/4G)
    - *Auto close timeout*: interval in minutes
    - *Auto close application*: Off, always after timeout, After user inactivity timeout
- **Widgets**: all settings related to the app widgets (application extensions)
    - *Widget update interval*: automatically load a new frame every 30 seconds, every 1, 2, 5, 10, or 15 minutes
    - *Allow widgets to use*: WiFi only, or both WiFi and 3G/4G
    - *Panic server:* choose the default server for streaming (panic buttons are widget-like buttons that can be placed on the home screen; tapping the button will start streaming live video to the pre-defined server (device must be registered on the server)
    - *Set up panic button*: suggests to create panic button

⚠ When enabling a camera and turning ON sound, you may be asked to confirm **permissions** for the app to access your phone's camera(s) and microphone. Select YES to grant access to these components if you wish to be able to stream video and audio from your phone to the server and clients connected to it.



To exit, tap the arrow icon in the upper left corner, or use your device's Back button (software or hardware) or gesture.

Add a New Server

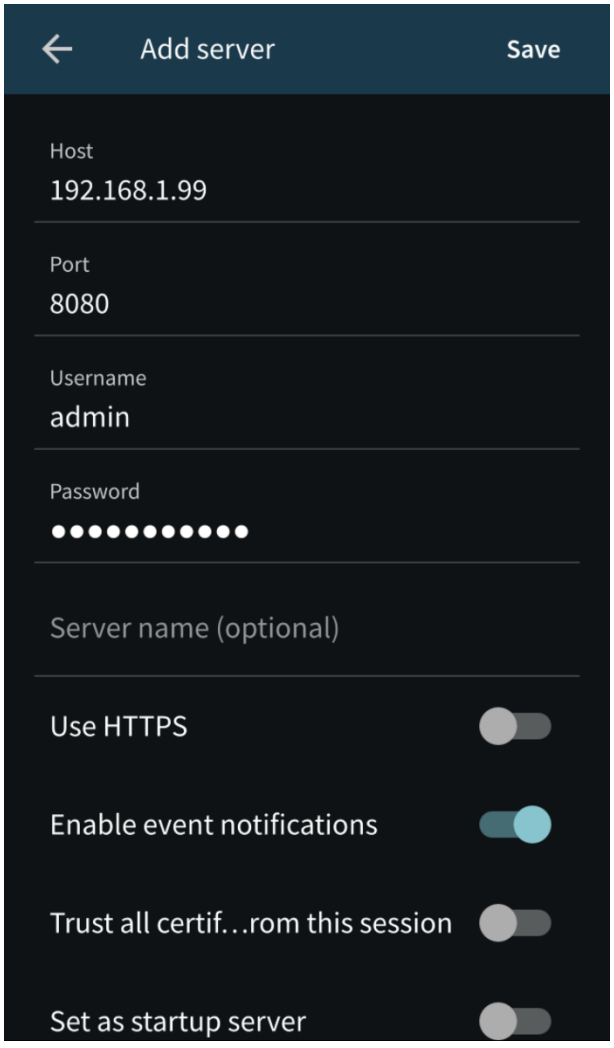
Tap the "plus" button in the bottom right corner to create a new server connection. Alternatively, you can also tap the main app menu in the top right corner, and then select *Add server*. The following parameters should be filled in:

- **Host**: server IP or domain name from your Macula configuration.

- **Port**: HTTP or HTTPS port to use (must match the one configured on the server side), the default HTTP port is 8080.
- **Username and password**: user account credentials to connect to the Macula server (a corresponding permission to connect via mobile must be granted)
- **Name**: user-defined connection title (the value from the Host field will be used automatically if you leave this field empty)

Additional options:

- **Use HTTPS**: use HTTPS over TLS instead of plain HTTP (target server must have HTTPS enabled and configured)
- **Enable event notifications:** turn ON push notifications from Macula servers (notifications should
- be pre-configured via Events & Actions using the Send event to client action)
- **Trust all certificates from this session**: accept all digital certificates provided by target server (required in case you are using a self-signed certificate on the server side)
- **Set as startup server**: select if you wish to automatically connect to the target server on starting the application. On startup, the app will load server list and try to connect to the selected server automatically
- **OAuth 2.0:** Allows to enable OAuth with external authentication providers.



When you are ready, tap *Save* to save the settings and exit the dialog box, or tap the "<-" *Back* to discard the changes and simply go back to the main menu.

To edit the settings for an existing server connection, tap the 'three-dots (...)' menu on the right side next to the server name, and then tap the *Edit* button that will appear in the drop-down menu. Use the *Delete* menu option to remove any existing entry.

OAuth 2.0

If you want to use OAuth2.0 as an authentication method, you need to set an **authentication provider** and **OAuth user** in the Macula Console and then enable this option in the Macula Mobile. Make sure you are logged into your mobile device with the same **user credentials** as the user added via Macula Console.

If your Macula Console is set properly, by setting **OAuth 2.0** as an **authentication method** in the Macula Mobile, you will see the notification with available providers at the next logon. Pick one you are going to use and follow the instructions. Depending on your OAuth provider - you may be asked to input a security code or verify your identity by the methods intended by your mobile device account security options.

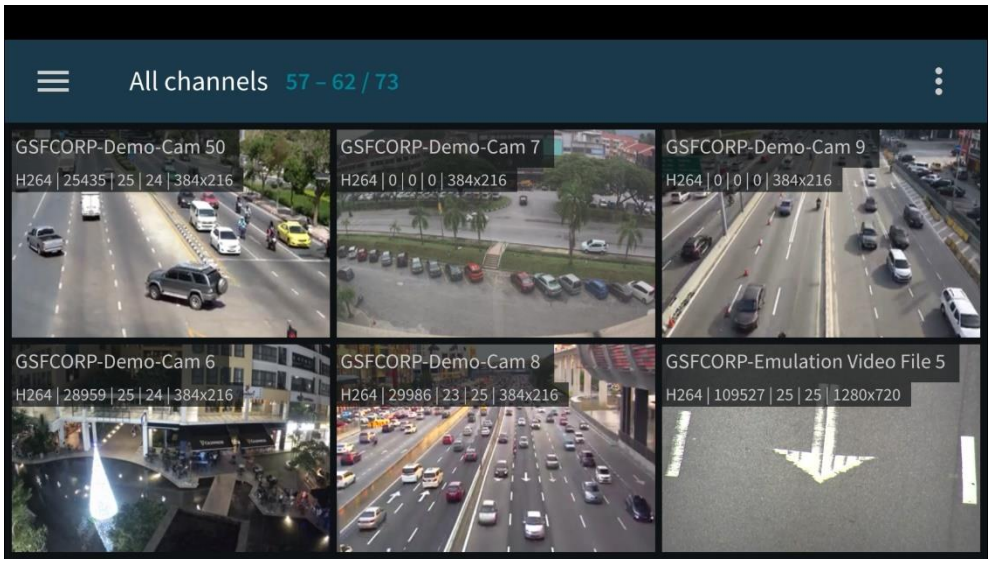
Live View

Tap your pre-configured server in the list to establish connection. If you are using HTTPS with a self-signed certificate, you will have to confirm that you trust the server certificate.

When you connect to a server, the **live view** mode is loaded by default. If you have already connected to the selected server previously, the most recent live view layout will appear. Each channel's name will be displayed in the top left corner of the picture, together with video stream properties - codec, bit rate, frame rate and resolution; stream statistics can be turned OFF via app settings (see above).

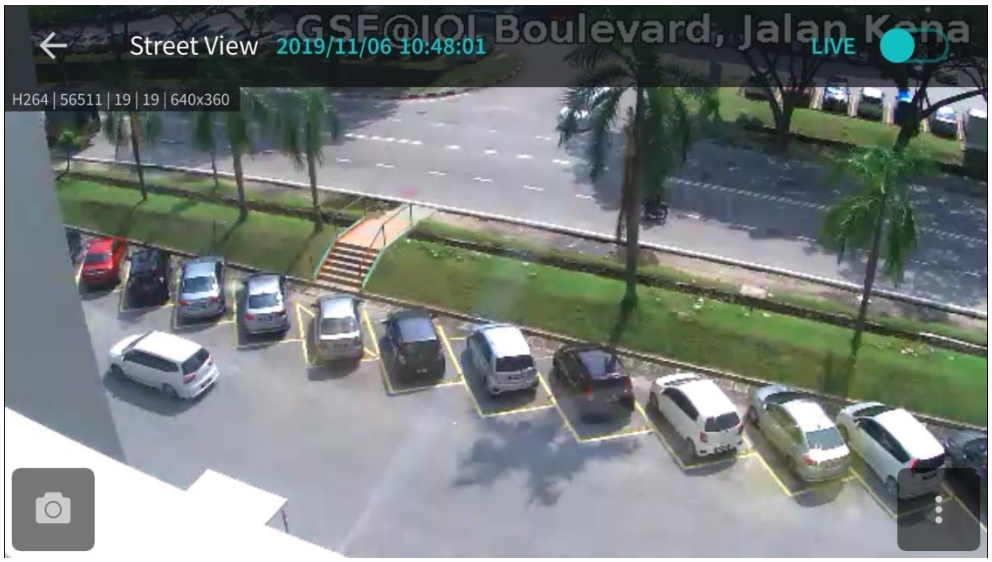
Tap any camera live view video to switch to the **single channel** view. Tap the "<-" Back button in the upper left corner to return back to the channel list. In both multi- and single channel view, you can **swipe** up and down to switch between channels. In the single channel view, they will appear one by one. In the multichannel view, the new portion of channels will be shown.

You can change the multichannel **layout** by tapping the server menu in the upper left corner > *View* > choose the desired layout (1x1, 2x1, 2x2, and 3x2 options are available)

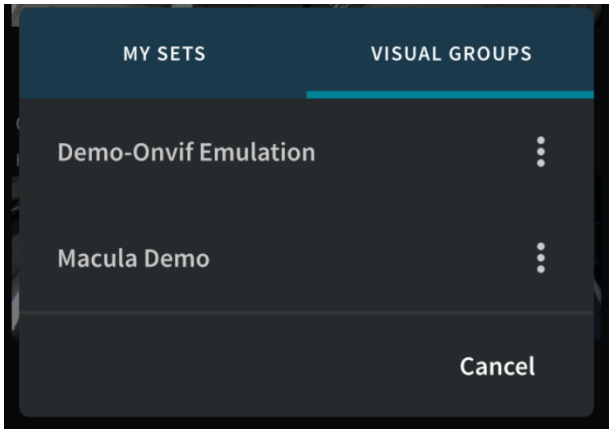


Swipe left/right (while holding the device horizontally) or up/down (for vertical mode) to scroll the channels.

You can pinch the picture to zoom IN/OUT (digital zoom). A tiny picture-in-picture preview will appear in the upper left corner of the viewport. Tap it to reset the DPTZ to the 1:1 zoom level. You can navigate around the zoomed-in image by dragging two fingers over the display.



Tap in live view and then tap “Select another channel set…” to select local layout in MY SETS or shared layout in VISUAL GROUPS.



Tap any channel to replace the currently displayed layout with a single channel view with extra controls. These are:

- Bottom left corner:
  - **Camera icon**: take a snapshot. Tap to save the currently displayed frame onto your device. To find your Snapshot on the Android device - go to the Photos app -> Library -> Pictures folder, and on the iOS device you will be able to find the snapshot in the Photos app, in the most recent photos.
  - **Speaker icon**: audio IN (from the camera). Tap once to enable incoming audio (the icon will turn blue), tap once again to stop. The icon will only appear if the target channel has sound enabled.
  - **Microphone icon**: audio OUT (talk to the remote camera). Tap once to start sending audio back to the camera (the icon will turn blue), tap once again to stop. Note: you do not need

to tap and hold the mic icon, like in the regular Macula Monitor application, simply tap once to enable audio streaming. This icon will only appear if the related functionality is available.

- Bottom right corner - three dots' menu:
  - **PTZ**: toggle PTZ controls (for PTZ capable cameras). While having overlay PTZ controls ON:
    - tap/long tap inside the sphere to pan and tilt (the closer you tap to the sphere edge, the faster the PTZ speed will be)
    - tap/long tap the ends of the zoom bar to zoom IN/OUT
  - PTZ **presets**: tap to see the list of available PTZ presets; tap any to make camera go to the specified preset
  - PTZ **tours**: tap to see the list of available preset tours; tap any to start the tour; tap *Stop PTZ Tour* to terminate any currently executed tour
  - **Cast** to device: tap to cast the current channel to one of the available Chromecast devices
  - *Create bookmark*: Create the bookmark and add the title and the description.
  - Maintain **aspect ratio**: toggle aspect ratio (original/stretch to fit); the setting is applied to **all** channels

Tap the picture again to switch to **full screen** (remove extra controls). You can still swipe up/down (or left/right for landscape screen orientation) to switch between channels.

PTZ *Tours* button will only appear if the target camera has at least one tour configured. PTZ tours can be created and managed via Macula Monitor application.

While in this mode, you can swipe left or right to load previous or next channel in the list. Long tap on the free space (where there is no stream) or on the stream itself (when PTZ controls are OFF) to bring up the list of all available channels: swipe down and up to browse the list, tap any channel to display it.

Server Menu

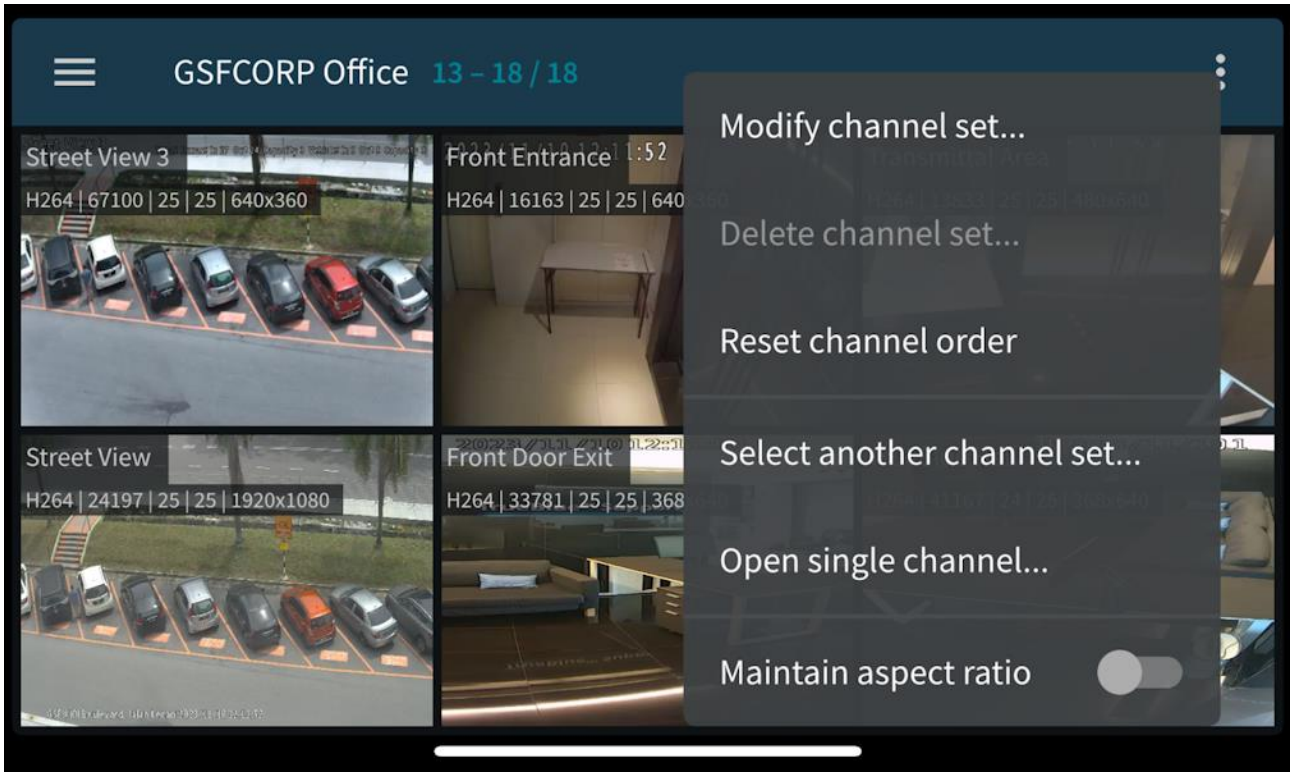
You can find the server controls in both, the upper-left corner "hamburger" menu and the upper-right corner - three-dots (...) menu. The Left and right menu offers different controls over the server. The left menu offers:

- *View - columns x rows*: tap to open layout selection. The layouts currently available are: 1x1, 2x1, 2x2, 3x2. If a larger layout has been selected, existing channels will be mapped automatically and all the extra slots will appear blank. To add more channels, tap the "Cameras" button and pick one; all the slots will become marked with blue frames, tap any of them to place the new video channel there.
- *Events:* push notifications from the target server (configurable via *Event & Action* section in Macula Console).
- *Bookmarks:* channel bookmarks from all the available servers.
- *User buttons:* tap a user button to trigger the action assigned to it (see below for details).
- *Stream camera:* send the video stream from your phone's camera back to the Macula server.
- Log out option.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

You can manage Channel order and create and manage Channel sets by selecting the three-dots (...) menu from the top right corner:

- *Modify channel set:* By marking items in the checkbox list, you can select which Channels to display for the current configuration. To Save or delete your configuration - navigate to the three-dots (...) menu inside the Modify channel set and Save or Delete channel set.
- *Delete channel set:* Delete the current channel set configuration.
- *Reset channel order:* resets order in which channels are represented in the multi-channel view to default order.
- *Select another channel set:* Allows to switch between pre-configured channel sets.
- *Open single channel:* Allows to select and open a particular channel from the channel list.
- *Maintain aspect ratio:* (on/off) allows to enable/disable default aspect ratio for all the channels in the multi-channel view.



Stream Camera

It is possible to send the video captured by your phone's main or front camera back to the Macula server for further live view on other connected clients and also for server-side recording. To do so, you need to add your mobile device to Macula configuration and then confirm it in your app.

First, go to your server configuration via Macula Console, go to the *Configuration* section and choose *Devices* from the menu on the left. On the upper panel, click the *+ New device* button in order to create a new device; enter your desired name and set the *Model* to *(Generics) - External Source*, then save. Note the value appearing in the *Code* field: you will need to enter it into your app.

Next, go to your app -> tap *Settings* in the bottom, find *Device Camera* in the list and choose your video preferences; the contents of each item may vary depending on your mobile device capabilities:

- **Device Camera:**

- *Camera -> Configure camera*: select which camera to use (primary/secondary), set Codec, Resolution, Bitrate, FPS, and microphone.
- *Detect cameras*: Use this if no cameras are shown in the camera menu item.
- *GPS:* Stream device location with video to server (on/off).
- *Store offline video*: You can pick from the list where to save offline video.
- *Offline video storage limit*: pick from the list how much memory you want to allow for online video.
- *When no space left:* You can decide to overwrite the oldest video or just stop the recording.
- *Default video upload server:* Select to which server to upload the recorded offline videos.

After the camera is set for the streaming - you can start streaming to the server by selecting *Server* from the *Server list*, then go to the top-left "hamburger" menu and select *Stream camera.* You will see the video stream preview and the round button in the bottom-middle part of your device screen. Tap this button and the video will be streamed to the server. The button will change its appearance to the red dot "recording" button. To stop streaming tap on this button.

> For Android 6.0 and newer, you may need to go to your mobile device's system permissions and explicitly allow Macula Mobile to use the camera in case you were not asked for this permission or if you have chosen to deny access to this component.

You can now manage this stream as a usual channel in Macula Console meaning that you can record both video and audio from it, analyze if for motion etc. To remove this entity, simply delete the device via Macula Console.

> If you re-install the application on your mobile device, you will need to go to the Macula Console and add your mobile device anew, basically, following the algorithm of adding a new device, or go to the device settings and click *Reset* near the *Code* field to generate a new code, then enter the new code in your app.

Panic Button

Once you have registered your phone on the server, you can set up a **panic button** on your mobile device. This button is placed on your home screen and, when tapped, **initiates live streaming** to the pre-defined server immediately - you do not need to open the app and search for the server. To set up this panic button, go to the mobile application settings and:

- define the panic server where the stream should be sent in the Application main menu -> *Settings -> Widgets ->PanicServer*.
- create a panic button and place it on the home screen.

To create a *Panic button* on your **Android** device:

- tap and hold on your device home screen, on the free space until the widget dialog appears.
- find Macula Mobile widgets in the widget list and expand the menu.
- tap and hold the Macula Mobile panic button, then place it on your home screen.

To create a *Panic button* on the **iOS 12** and newer device:

1. Open your Shortcuts app (https://support.apple.com/en-us/HT208309). You will see the list of existing shortcuts and an option to add a new one. Tap the *Create Shortcut* button.

2. Tap Add action, or just locate the app in the *Search for Apps and Actions* field by entering the mobile app name until it appears in the list. Tap the app icon. You will see the list of actions available for that app: for our mobile application, there will be the *Panic Button* item.
3. Tap the *Panic Button* item. + and ... icons (Add New and Details) will appear.
4. Tap the three dots (...) *Details* icon in the upper-right corner to change the panic button icon appearance and name. Tap the *Add to Home Screen* option to add the shortcut to the home screen. If you don't add it to the home screen, the shortcut will only be available from the *Shortcuts* app or from the *Today View*. Tap *Done* to exit the shortcut properties. The button will appear in the list as the newly added shortcut.
5. Tap *Done* again to finish adding the shortcut. The newly created shortcut will appear in the list in the Shortcuts app and will become available in your *Today View* (the section that appears when you swipe to the left edge of the screen).
6. Exit the Shortcuts app. Your Panic Button will appear on the home screen: tap it to start transmitting video to the selected panic server.

Archive Playback

To switch to the playback mode, tap the *Live*/*Archive* switch on the top-right corner in the single channel view. You can navigate through the archive playback. In the top-middle of the screen, tap on arrows around the date to move in the steps of the whole day.

In the bottom-middle of the screen, there are standard playback symbols to play or jump to the beginning or the end of the recording, navigate by minutes, or tap on the timeline and provide year, month, date, and time if you know the exact moment you are looking for. The default value for the time step interval is 1 minute. You also can change this interval by holding +1M and -1M for a short time. The list with available time intervals will appear (5 sec, 10 sec, 1 min, 10 min, and 1 hour). Tap on your preferred time step interval to use it with a single tap.

You can adjust the playback speed by tapping the circle with the number and _x_ symbol in the right-bottom corner near the three-dots (...) menu.

In the right part of the screen, there is Main stream/substream indicator. You can tap on it to switch between streams.

You can find additional controls for the navigation inside the three-dots (...) menu in the right-bottom corner of the screen.

- *Jump to time*: allows to pick up the exact date and time for the playback.
- *Jump to channel events*: allows to pick the event directly from the channel event list if any exist.
- *Jump to channel bookmarks:* allows to navigate directly to the bookmark if any exist.
- *Previous and Next controls:* allows to set icons around the Play button to move by frame, bookmark, or Motion event.
- *Create bookmark:* provide an option to add a bookmark with a Title and its description.
- *Maintain aspect ratio:* (on/off) allows to maintain proportions of the video or stretch it to the proportions of the screen.

Widgets

Widgets are information elements that can be placed on the home screen on Android devices and in the Today view on iOS devices. Individual channels that require frequent monitoring can be placed as Macula Mobile widgets with moderate or low (from twice per minute down to four times per hour) refresh rate so that you do not have to open the whole app each time you need to check the channel. For channels accessible via Internet, this means you can monitor them even if you are in a remote location on 3G or 4G: relatively low frame refresh frequency does not use much bandwidth. You can also limit widgets to use WiFi connection only.

General steps to add and use a widget are the following:

- add as many widgets as you need, one widget per channel,
- go to Macula Mobile app settings and set widget update and network usage preferences (for details, see the *Settings* section above),
- assign channels to widgets.

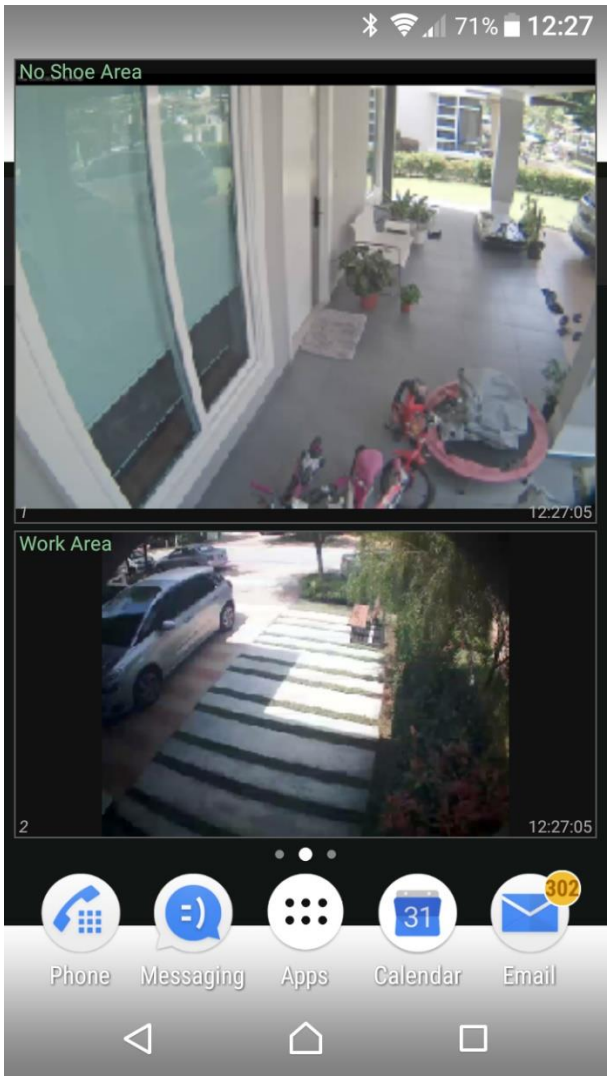
To add a widget on an **Android device**:

- tap on a blank space on the home screen and hold for a couple of seconds until the menus appear,
- tap the *Widgets* menu at the bottom of the screen, locate Macula Mobile widget and then drag to place it onto the desired place. Widget of default size (2x2 cells) will appear with a *Slot not configured* message inside:
    - drag the orange borders to adjust the widget size, then tap outside the widget to exit the adjustment mode (you can change the widget position and size at any time later by long tapping the widget and then moving it)
    - tap the widget once: Macula Mobile application will open, allowing you to choose the channel,
- then, in the Macula Mobile app:
    - go to the app settings before connecting to the server and choose how frequently the widgets will be refreshed, and also their network usage preference (see the *Settings* section above for details),
    - connect to a server of your choice, choose *Camera to widget* from the main menu, then tap a channel to choose it (all channels will be highlighted with blue frames, swipe left or right to load more channels to choose from), and then choose a widget slot from the list by tapping it, too (the slot may be empty or already contain a channel),

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

- go back to your home screen: the assigned channel should now be present in the widget, with the channel name in the top left corner, slot number in the bottom left corner, and last refresh time in the bottom right corner.

To replace the channel, follow the steps 3-4 above; to remove the widget, simply tap and hold it until the menus appear and then drag and drop it onto the Recycle bin icon. Tapping a widget will result in opening the corresponding app, as described above.



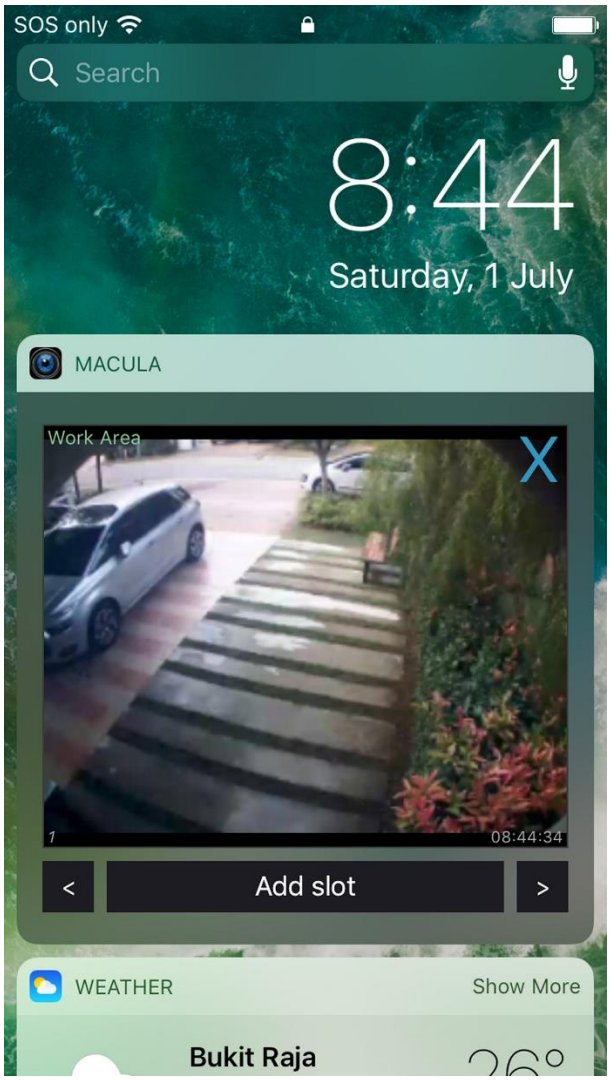
To add a widget on an **iOS device**:

- swipe down over the Home screen, Lock screen or Notification center to bring the Today view screen, scroll to the bottom to reach for the Edit menu, tap *Edit*,
- locate the Macula Mobile app and tap (+) sign to the left of it: the app will be added to the list above,
- tap *Done* when you have finished; the widget will appear under Widgets, allowing you to add and resize the slots - tap any slot to open the Macula Mobile app,
- then, in the Macula Mobile app:
    - go to the app settings before connecting to the server and choose how frequently the widgets will be refreshed, and also their network usage preference (see the *Settings* section above for details),
    - connect to a server of your choice, choose *Camera to widget* from the main menu, then tap a channel to choose it (all channels will be highlighted with blue frames, swipe left or

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

right to load more channels to choose from), and then choose a widget slot from the list by tapping it, too (the slot may be empty or already contain a channel),

- go back to your Today view: the assigned channel should now be present in the widget, with the channel name in the top left corner, slot number in the bottom left corner, and last refresh time in the bottom right corner.

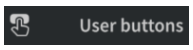


You can drag widgets to rearrange them in the Today view; tapping a widget will open the associated app. To remove a widget, go back to the widget list in the Today view, as described above, and tap the (-) sign next to the Macula Mobile name, then tap the *Remove* button. If you remove the widget and then add it anew, it will retain its view (slots).

User Buttons

User buttons are software buttons, controls used in Macula Monitor and for manual event triggering: upon clicking or tapping a user button, the action associated with it is triggered. The action, the user button itself and the rule that makes the user button work are all pre-configured via Macula Console; see corresponding sections of the server management manual for details.

If you are connected to a server that has configured user buttons and your user account has permissions to use them, the buttons will be available in the app. To access them, tap the main menu and

choose 

.Then, choose the button you want to use and tap it: the associated action will be triggered and you will receive a confirmation in the bottom of the screen.

Events

Macula Mobile app allows you to receive push notifications from the Macula server once they have been set up via Macula Console *Event & Action* management.

In order to do this, create an action of the *Send event to client* type via Macula Console and enable the *Display event in mobile application* option, then attach this action to your desired event in the *Rules* section. When creating the rule, do not forget to set the target channel for it: the notifications will appear for that particular channel and their availability can be controlled via channel access permissions. It is possible to limit the reception of the notifications to certain user profile or user group. You will find more details on how this is done in the *Events & Actions* section, under Actions.

Triggered notifications will immediately appear on the mobile device(s) that have Macula Mobile app installed with the target Macula server configured (connected user account must have permissions for the target channel). The app itself may be not running: events will pop up as regular text message notifications. If the target mobile device is offline, the notifications will arrive shortly after it re-connects to a network that provides required server connection.

Offline Camera

Starting from version 1.7, Macula Mobile allows you to record offline video clips for further upload to the server. The video can be recorded from the device camera in the app and stored as long as required until the server connection is available.

To enable this, you first need to:

- set up the target server connection in the app
- choose your camera preferences
- register your smart device on the Macula server as *External Model* as you would do for live streaming from device camera
- enable Edge Recording for the newly created channel

You only have to do this once for each device (unless you re-install the app). From then on, you will be able to record as many video clips as you wish, and then upload them to the target server.

If you do the have your device paired with the server yet, go to your Macula server configuration via Macula Console, go to the Configuration section and choose Devices from the menu on the left. On the upper panel, click the + *New device* button in order to create a new device; enter your desired name and set the *Model* to (*Generics*) - *External Source*, then save. Note the value appearing in the *Code* field: you will need to enter it into your app.

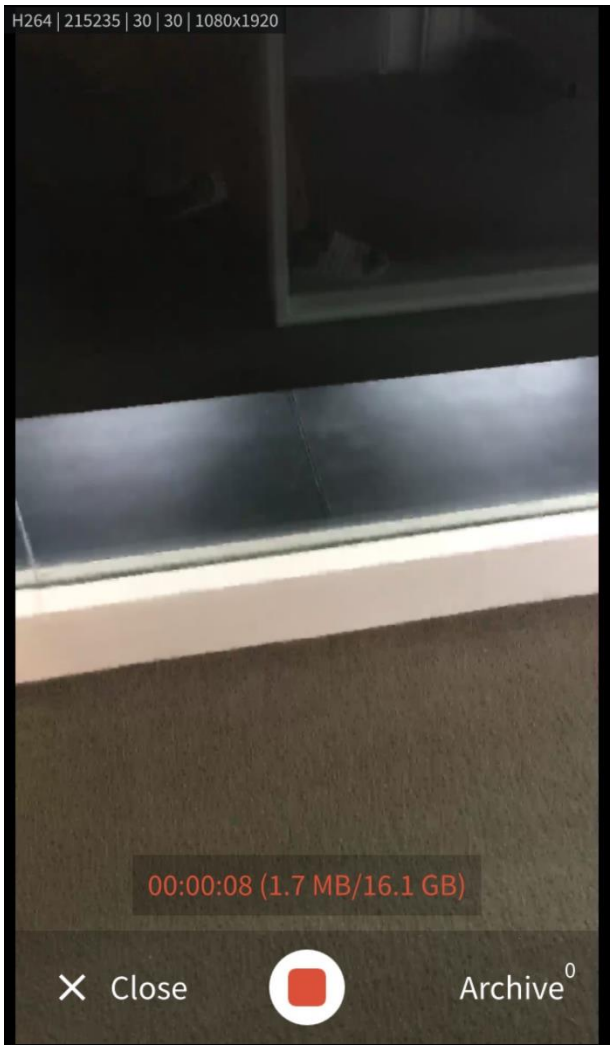
Next, go to your app -> server list -> tap *Settings* in the bottom, find *Camera* in the list and choose your video preferences; the contents of each item may vary depending on your mobile device capabilities:

- **Camera**: back/front (primary/secondary)
- **Resolution**: [the actual list depends on the mobile device capabilities]
- **Bitrate**: Video bitrate
- **FPS**: from 10 up to max allowed by device

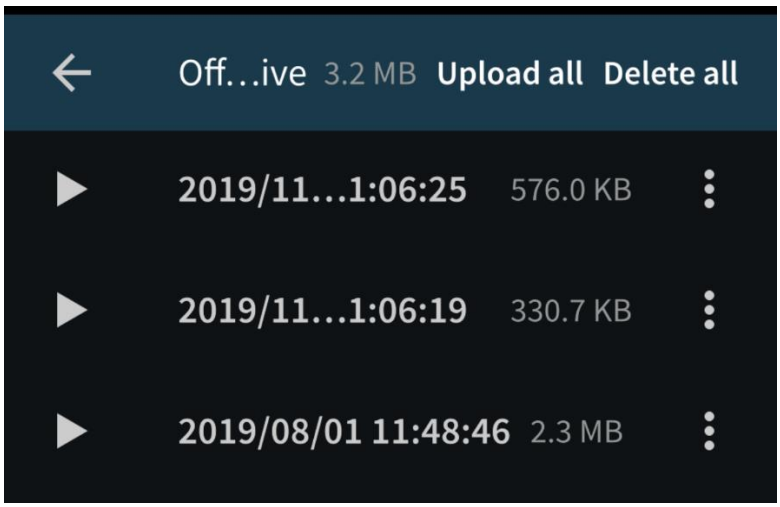
- **Camera Microphone**: disable/enable sound

To start offline recording - go to the Channel list, tap on the top-left corner "hamburger" menu, and select the *Record camera.*

Rotate your device the way you want to hold it during the process and tap the *Start recording* button: it will turn red indicating that the **recording** is happening. Tap it again to **stop**: a **new file** will appear in the list and the camera preview will return to live.

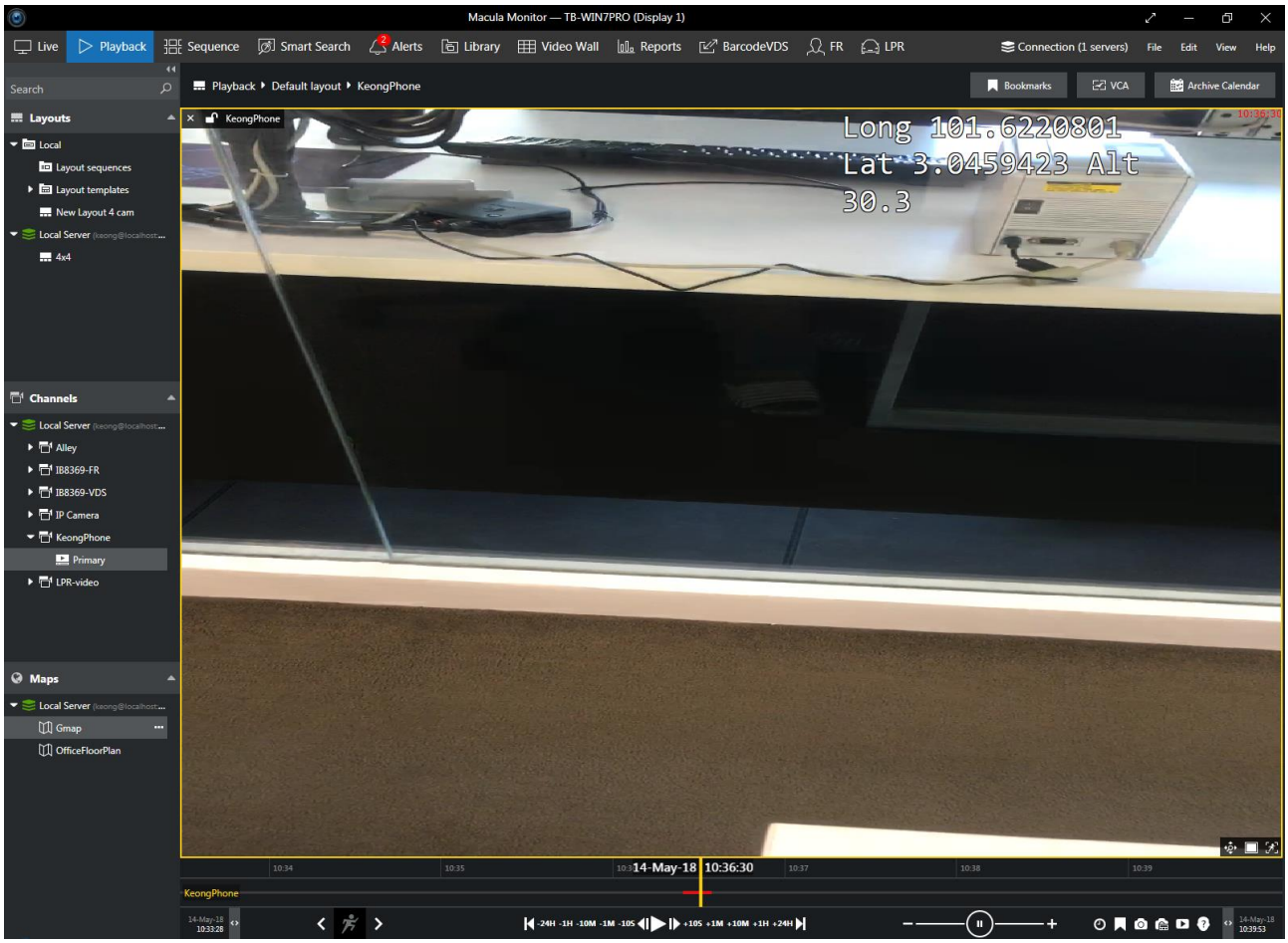


In the right-bottom corner of the screen - tap the *Archive* button. You will find the list of the offline recordings. To replay the recording - tap on the recording you want to replay. The video file(s) will be uploaded to the selected Macula server and stored as an **edge stream** for your device's channel. Do not worry if the upload is interrupted due to network issues: the upload will resume as soon as the connection to the target server is available again.



GPS Tracking

Starting from the Macula Mobile version 1.7 and Macula version 1.8.0, it is possible to send the GPS coordinates of the smart device to the Macula server. The coordinates are then displayed on top of the live and recorded video, and they are also used to trace the device on geo maps.

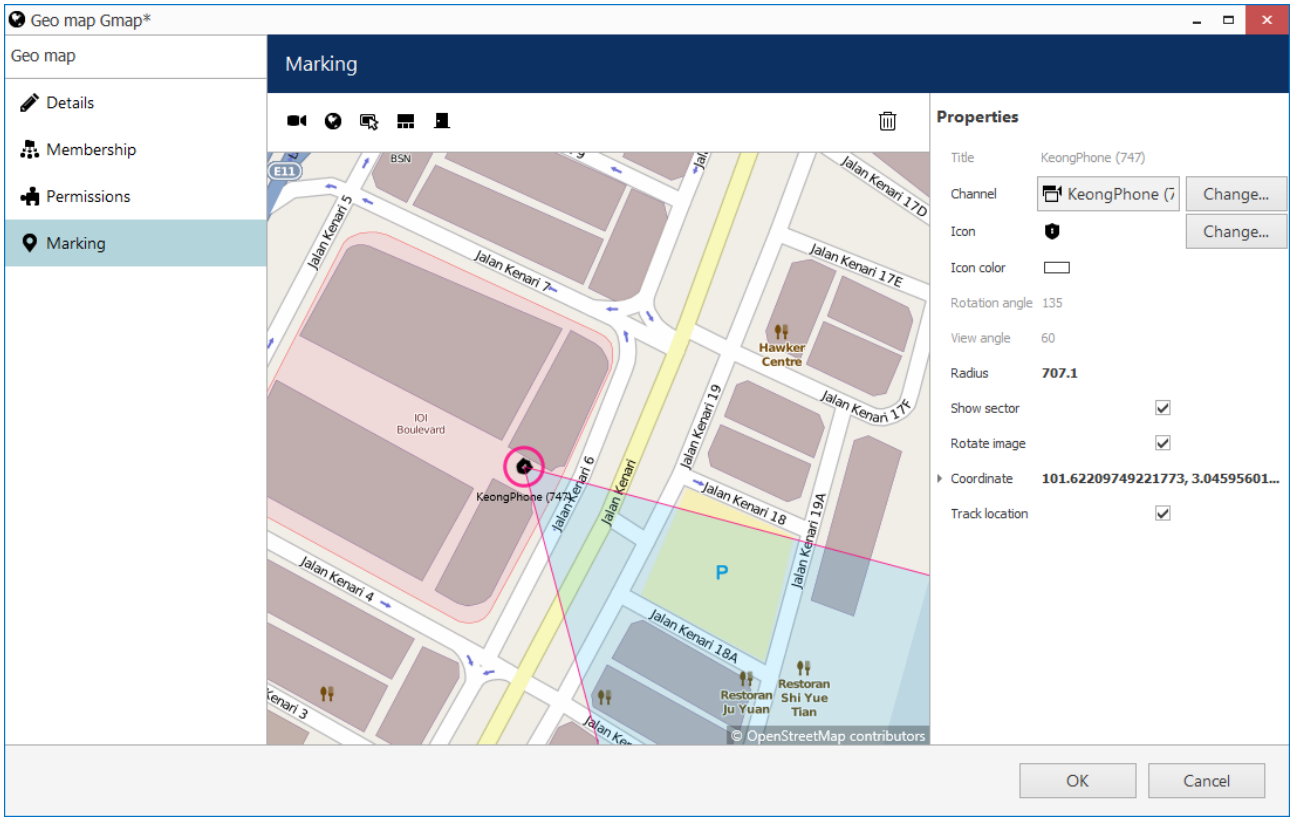


Setup:

- enable sending of GPS data in your app settings
- register your device on the server as described above in the Stream Camera/Offline Camera sections so that it exists in the server device/channel configuration

Macula® Professional Administration Guide

- create a geo map on the server via Macula Console
- place a camera marker on the map, set your smart device as the target channel and enable tracking in the properties



Now, if you move and stream video from your phone to the Macula server, the marker on the map will move as well, displaying your location. GPS coordinates will be also shown on top of the live video stream and also when it is played back. Note that for the offline recorded stream (clips recorded and then uploaded to the server) the coordinates will not be displayed.

8.3 RTSP Streaming Server

Sometimes, you must provide a live stream from the camera to the third-party software or a remote system without giving access to the Macula itself.

It is possible with the Macula RTSP streaming server. This chapter will guide you through enabling the streaming server and setting streaming for the specific channel inside the client.

You will need to:

1. Enable RTSP streaming inside Macula.
2. Add permission for the remote user to access this stream.
3. Provide the correctly formed streaming link to the client.

Enabling the RTSP Streaming Server

The first step is to allow Macula to stream video over RTSP. To do so, go to:

1. *Macula -> Configuration -> Servers*
2. Select the server you want to stream from and double-click it, or locate the *Edit* button at the top of the *Server* subsection and click it - this must bring the selected *Server settings* pop-up window.
3. In the left subsection of that pop-up window, locate and click the *Connections* tab, scroll to the bottom of the right subsection, and find an input field named the *RTSP port* at the very bottom of the subsection.

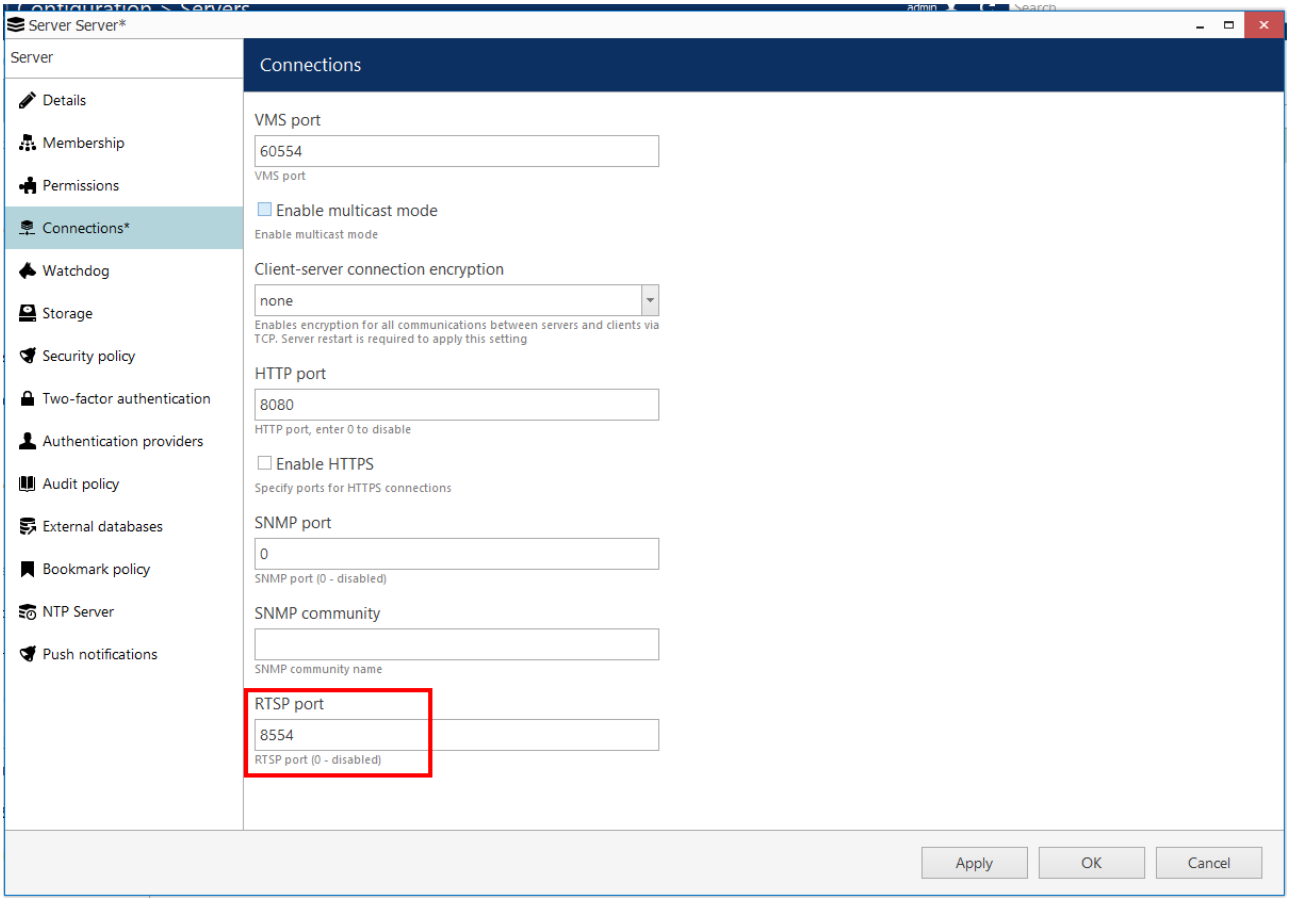
The default value for the *RTSP port* input field is 0, which means streaming is disabled. To enable streaming, you need to provide the port number.

The ports that the Macula may already occupy, so you should avoid them:

- 8080 - standard HTTP port,
- 8082/83 or 8090/92 - may be occupied by external analytics,
- 554 - standard RTSP port may be occupied by the for other purposes

The recommended port is 8554. Since the Macula does not use this port, this must help avoid conflicts.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

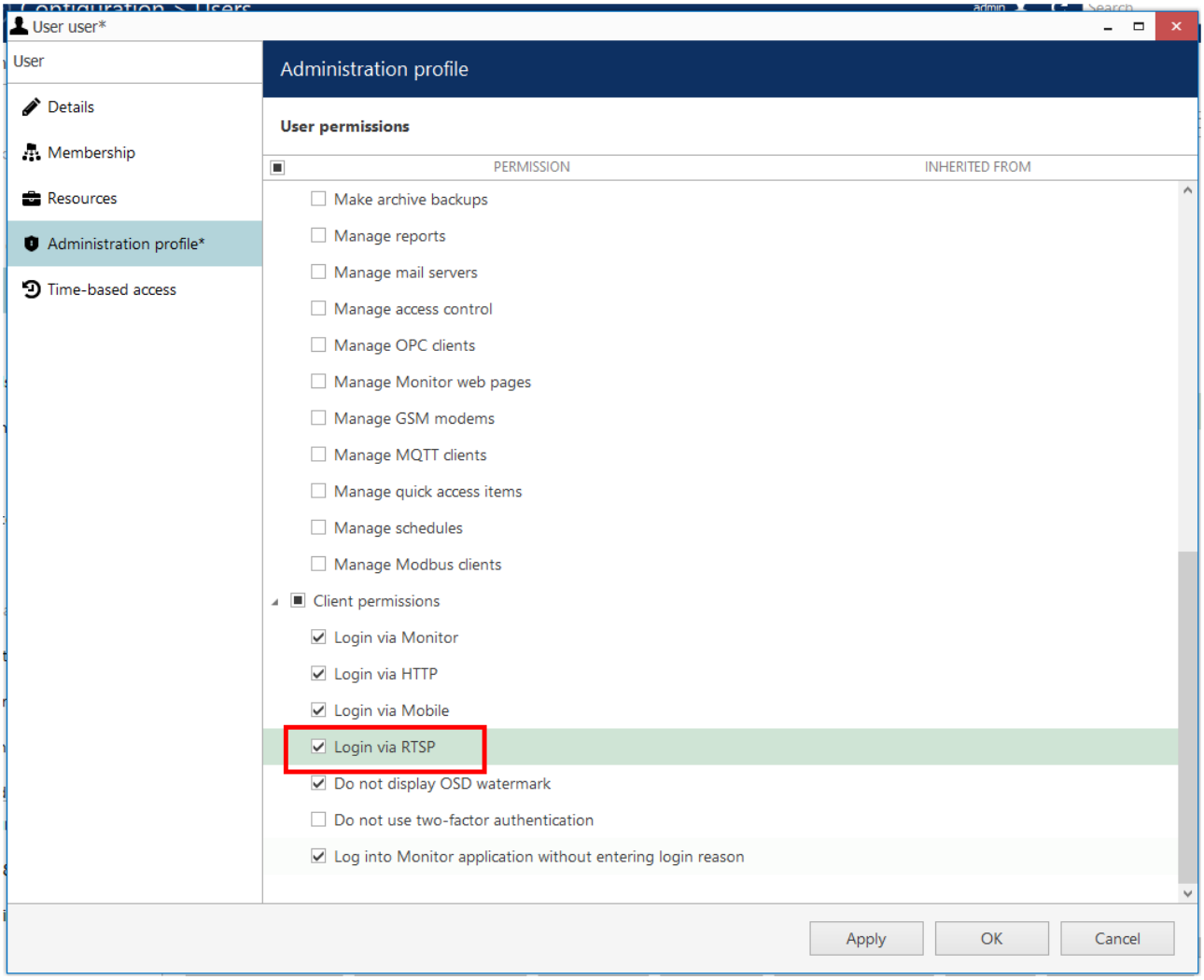


After providing the port, confirm your selection with the *Apply* and *OK* buttons. After that, your *RTSP Streaming Server* is enabled.

Providing Permissions to the Remote User

The server is already streaming, but you must grant permission to access the stream. To do so, go to:

1. *Configuration -> Users*, pick a user you want to provide access to the *RTSP stream* and double click it or locate the *Edit* button on top of the *Users* subsection and click it.
2. Inside the new pop-up window, select *Administration profile*. Find the *Login via RTSP* checkbox under the *Client permissions* section and mark it.

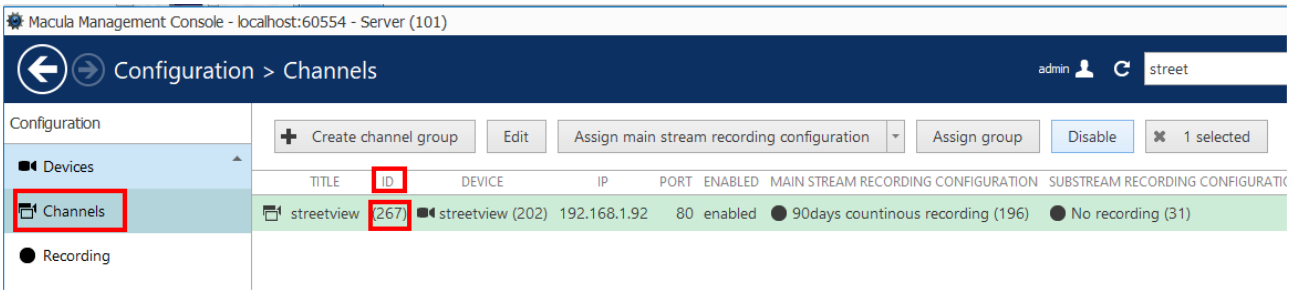


Now, you can access the *RTSP stream* by providing the login and password to the client software you want to use to watch that stream. More details on *Users* can be found in the corresponding manual section.

Forming Streaming Link

The way you form the link to the stream will depend on the client you use to watch the stream, but for any configuration, you will need to know:

1. Streaming server IP address
2. Port, you assigned for the RTSP streaming
3. *Channel ID* you want to stream (You can find it under *Configuration -> Channels*, *ID* column)



⚠ If you do not see the *ID* column inside the *Channels*, find the "hamburger" menu at the top-left side of the *Macula Console*, find the *Settings,* and mark the *Show object's IDs* checkbox.

Link template:

- rtsp://user:password@Server_IP:RTSP_port/channel_ID/live/stream_type (main or substream)

Link examples:

- rtsp://@127.0.0.1:8554/**130**/live/**main**
- rtsp://**user:password**@127.0.0.1:8554/**130**/live/**main**
- rtsp://**user:password**@127.0.0.1:8554/**130**/live/**substream**

If you want to share the stream outside your local network, you must set port forwarding for the port you like to use for streaming. Please consult your network administrator for such cases.

9 Event and Action Overview

Event and action (**E&A**) management is a component of Macula, which provides additional opportunities for handling surveillance system work under certain conditions. The main task is to assign flexible device/server reactions on a user-defined basis. These scenarios may work within a single server, as well as in distributed systems with Macula Enterprise where events originating from one server can trigger actions on one or more different servers.

Events are entities that arise when something happens in the system - namely, when system or system component states changes, for instance, a video stream has been lost, a recording or disk error has appeared etc. These changes can be set up to trigger certain **actions** so that system administrators and/or users are notified and can react to them in a timely fashion. Additionally, there are also extra controlling entities that allow a flexible and advanced setup of event-action rules: conditions, delay times and schedules.

Using event & action management, you can specify your desired outcome for your video surveillance system's operation and determine how software reacts to any event caught on any server and how it turns them into an automated process. Send emails, activate DI/DO, interact with any other software or just bring the attention of the operator to the device that requires their immediate action. The functionality can be used not just for a single event, but on a set of sequenced events to get rid of false alarms and improve the efficiency of the surveillance system.

Possible **E&A scenarios** may be:

- sending alerts through the server based on camera digital input events;
- starting or stopping video recording based on motion in specific regions during specific hours;
- switching to some camera PTZ preset if the door sensors go off at night;
- directing the camera to a specific PTZ preset if another camera registers the same movement;
- etc, etc.

Event & action management offers the following **functionalities**:

- event & action configurator rules
- standard (default) events (available for all servers)
- standard (default) actions (available for all servers)
- custom events of certain types (configurable)
- custom actions of certain types (configurable)
- global events (server-to-server data transmission)
- delay timers
- special conditions
- schedules
- mail server configuration

Each of these components is described in details in the corresponding sections of this document.

Actual setup of E&A depends greatly on your system configuration, E&A usage scenarios, required automation level and other things. However, we recommend that, regardless of system scale and architecture, you stick to the following **order of E&A configuration** steps for optimum results:

1. Preliminary actions

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

   a. Create a plan of your E&A scenarios on paper or in any diagramming/smart draw software - this will ensure you always have a basis to check against
   b. Set up your Macula system so that you have all the servers, devices, channels, users and optional elements pre-created
   c. Pre-configure all the necessary hardware equipment (e.g., camera IO wires, external physical alarms, buttons) and connect it
   d. Pre-configure all third-party programs/scripts/executable files, if necessary
2. Extra setup in Macula Console
   a. Create User Buttons, if you are going to use them
   b. Create Maps, Layouts if necessary
3. E&A Management setup per server
   a. Add mail servers if you are going to use e-mail notifications
   b. Add custom events
   c. Add conditions
   d. Add custom actions
   e. Create rules using all elements; add extra events/rules, if required
   f. Add timers, schedules and conditions to the rules
   g. Check your rule map against your initial plan from 1.1
   h. Test your rules

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

9.1 Rules

All rules defined via *Event & Action Configurator* are listed in the *Rules* section. Click the *Change* button near server name to select a different server from the list: for each server, only relevant rules are displayed. You can perform the following actions from the *Rules* section without opening the *E&A Configurator*:

- **view** the complete list of existing rules, per server, and their properties
- **disable** a specific rule or a set of rules by using the *Disable* button on the upper panel
- **enable** a specific rule or a set of rules by using the *Enable* button on the upper panel
- **test** a specific rule (the rule must be enabled)

In order to **add**, **remove** and **modify** the rules, choose the target server and click the *Open Configurator* button on the top panel.

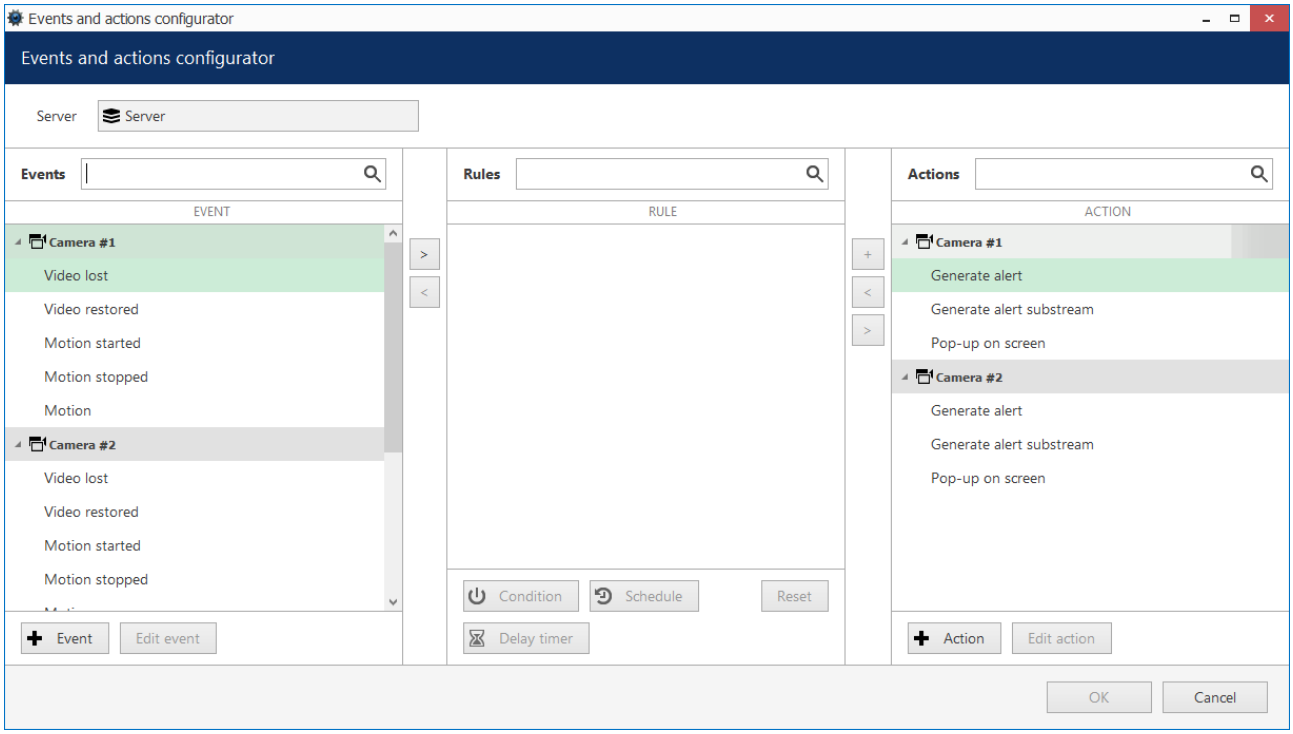
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

9.2 Add Rules

All existing and added entities of E&A can be combined to create **rules** (rule map) for each server, which will define server behavior if events are triggered. This section will guide you through related features, explain the meaning and purpose of used items and provide usage examples.

The rule map is created via the ***Event & Action Configurator***: to open it, go to the *Events & Actions* section in Macula Console and then click *Rules* in the menu on the left, then select the target server for which you wish to add the E&A setup, and then click the *Open configurator* button on the upper panel. To change the target server, click the *Change* button next to the server name and then pick one from the available server list.

The *Event & Action Configurator* will open in a new window; by default, no rules are defined.



You can pre-create all events, actions, conditions and schedules beforehand using the relevant menu sections in Macula Console, or create necessary items as you go from the configurator. Delay timers can only be created as you go for the specified rule and are not saved as independent entities.

Add and Edit Events

Choose the target item from the Events list and then click the + *Event* button below: configuration dialog box will then open with the target device pre-selected. Here you can add alerts from device digital inputs and VCA notifications; see the detailed description of how to create events in the Add Events section.

Events are arranged by sources. Typical event sources are: channels, channel groups, servers, user buttons, video walls, external services.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Built-in (default) types of events - lost/restored video, recording errors etc. - cannot be edited. This is also the case for all built-in actions.

Add and Edit Actions

Choose a target item from the Actions list and then click the *+Action* button below: the configuration dialog box will then open with the target device pre-selected. Here you can add reactions to the following types of events:

- trigger device digital output
- write to OS Application log
- activate target device's PTZ preset
- activate main/secondary stream recording profile
- send an email notification
- run a third-party program
- etc.

See the detailed description of how to create and configure actions in the Add Actions section.

Manage Rules

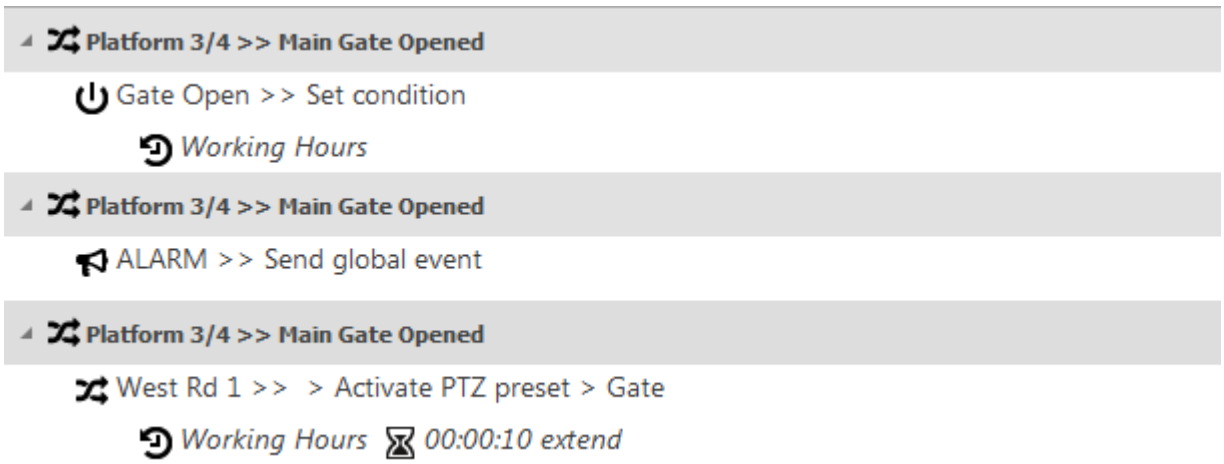
To start combining events, actions and additional controls, simply follow this scheme:

- find your desired **event** in the *Events* list - use search filter on the top panel, if required
- use the < and > arrows or double-click events to add/remove them to/from the *Rules* list
- click free space of the target rule in the *Rules* list (use CTRL or Shift to select multiple ones) - the selected rows will then become highlighted green
- find your desired **action** in the *Actions* list - use search filter on top, if required
- use the < and > arrows or double-click actions to add/remove them to/from the *Rules* list, and the + button to add more than one action for a single event
- select desired actions and add auxiliary controls by clicking buttons on the bottom panel (see description below for details)

Useful tips:

- double-click a device (highlighted grey) to add **all** its events to the rule map
- to **add** an action to an existing rule, use the + button instead of the < button: the original event will be duplicated and new action will be added to the copy
- use the + button between *Rules* and *Actions* lists to add **multiple actions** of the same type to the selected rule(s)
- to clear the *Rules* list, select all rules using Shift or CTRL+A, then press < button on the left to remove all events
- use the *Expand/Collapse list* button on top of each column to hide all contents and only display node titles

The rule header displays the event source and event itself; below, related actions are listed, each with its own set of special controls. Actions of the same type are listed under the same rule header; for all other cases, the events are duplicated, resulting in a separate rule. One condition, one schedule and one delay timer can be attached to **each action**.



Once the rule map has been created, click the *OK* button in the bottom right corner to **save and exit**. Note that simply closing the *Event & Action Configurator* is analogous to clicking *Cancel*: no changes will be saved.

Conditions, Schedules and Delay Timers

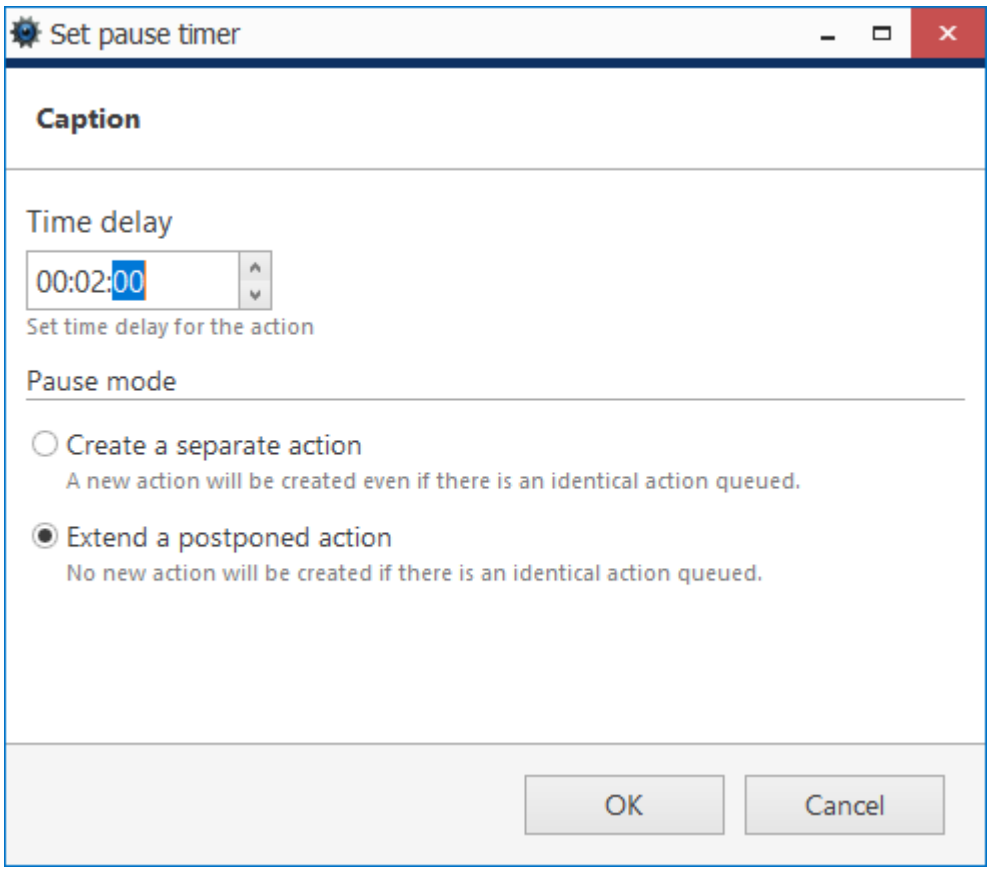
For each event/action pair that is added to the rule map, additional options can be defined in the form of conditions, delays periods and schedules. Select one or multiple target events from the *Rules* list and then click desired control item in the bottom panel.

To remove auxiliary controls from a rule, select it in the *Rules* list and click the *Clear* button on the bottom panel. Note that all defined conditions, timers and schedules will be removed from the target rule, and it is not possible to de-attach them one by one.

Delay Timers

To add a pause timer for specific actions, select one or more of the mapped rules (use *CTRL+click* or *Shift+click* to mark multiple items) subject to delay, and then click the *Delay Timer* button on the bottom panel of the central part of the *Event & Action Configurator*.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Set the delay period for the target timer. Time can be adjusted in the following ways:

- click hours/minutes/seconds and then use the UP and DOWN arrows on the right, or
- click hours/minutes/seconds and use the mouse scroll, while still holding mouse cursor over the relevant timestamp section, or
- enter the time manually using the keyboard numpad.

Next, choose the pause mode:

- **Create a separate action**: new actions of the same type will be created regardless of the acting delay timer, and queued in the same way as the original delayed action
- **Extend a postponed action**: new events of the same type will restart the timer, postponing the resulting action for the specified amount of time

When you have finished, click *OK* to save and exit the dialog box. The newly created delay timer will be assigned to the pre-selected actions.

Extending an action allows you to postpone the action execution repeatedly if more events of the same type arrive within the chosen time period. For example, if incoming events are of a *Recording Error* type, there may come too much of them at once e.g. in case of a major storage issue, causing a lot of triggered actions of the same type, while only a single action may be desirable.

Say, if required action is *Write to application log*, setting a delay timer to *5 minutes + extended action* will postpone the email sending for 5 minutes every time a new recording error appears; when, at a certain point, more than 5 minutes have passed without new incoming events, a single log entry will be eventually created. The **separate action** option, on the contrary, will force logging for every single triggered event.

To remove a delay timer from rule configuration, click the timer to highlight it within the rule, and then click the *Clear* button in the bottom panel. Note that, if there are schedules and/or conditions attached to the same rule, they will be removed as well.

Schedules

Schedules are used when you wish a rule to be active based on a pre-defined itinerary. You can create any number of custom schedules via the *Conditions* section in the Macula Console and then use them for rule control: see Create Schedules section in this document for a detailed explanation of this.

Select one or multiple target events from the *Rules* list and then click *Schedule* button in the bottom panel.

Conditions

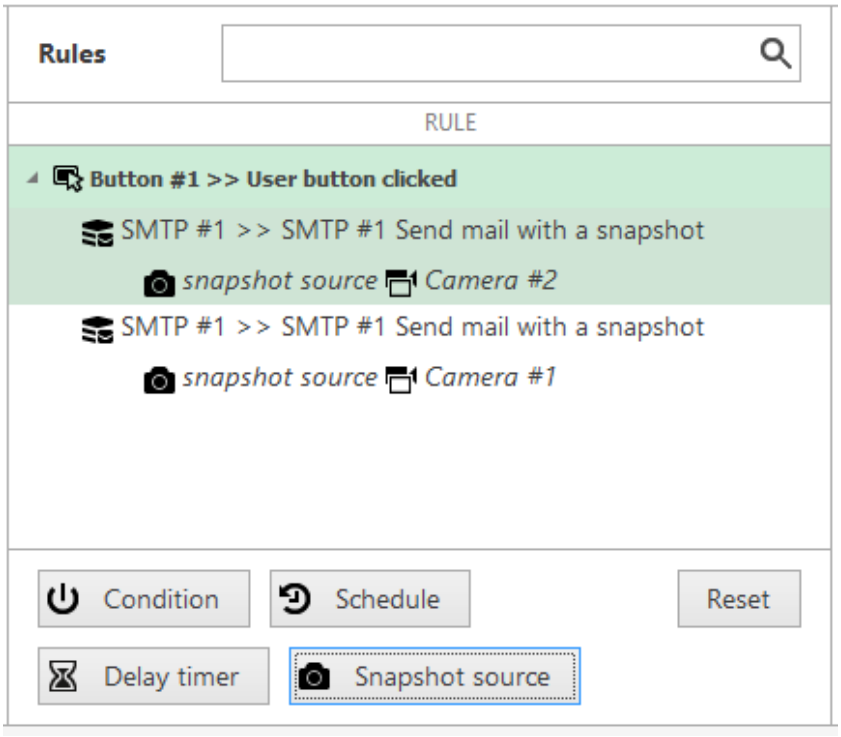
Conditions are supplementary variables that can allow or prevent action execution. The decision is taken based on the condition state: if the condition is **ON**, the planned action will be executed; if the condition is **OFF**, the action will not be performed regardless of the frequency of the triggered event. The condition state can be changed as a result of some other event, so ad additional rule should be added to perform this task; alternatively, you can manually set and unset conditions at your will. Thus, conditions allow the activation and deactivation of rules without requiring them to be entirely deleted.

To assign a condition to the rule, choose one or multiple target events from the *Rules* list and click the *Condition* button on the bottom panel, then either select target condition from the list or create a new one.

Please read the Conditions topic of this document if this feature is new to you: it contains detailed description and usage examples.

Source and Target Channels

Some actions participating in the rule creation need a related channel to be specified so that these rules can be properly executed. For such actions, the source/target channel is specified when you create a rule involving such an action: corresponding additional buttons appear on the bottom panel or the rule map section, next to conditions, schedules and delay timers. Each action allows exactly one related channel; if you need, for instance, two snapshots to be sent via email, just add two actions of the same type and specify different source channels.



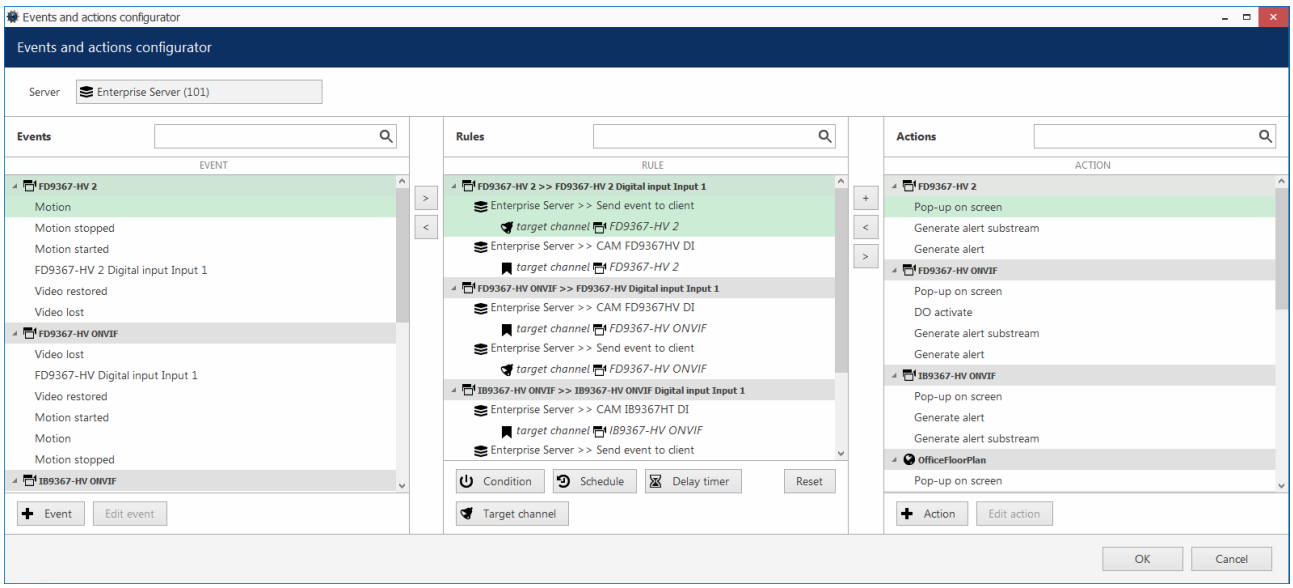
When you combine such actions with events that already are related to some channel (e.g., *Video Lost*, *Motion*, *VCA*, *DI*), that channel is selected automatically for the resulting action. For the rest of events, the channel is not set by default and you need to use the **target/source channel** buttons on the panel below the rules. Also, you can set a different channel instead of the one selected automatically by using the same buttons.

Attaching Snapshots

The *Send Email* action allows you to attach a snapshot from one channel and deliver it together with the email to the recipient. The snapshot can be taken either from the main stream or from the secondary stream (substream), if available. At the action creation time, you just enable the snapshot from either main or secondary stream, and then you will have an option to specify the source channel when creating the rule that involves such an action.

When creating the Send Email action, you can choose to attach a snapshot by selecting the necessary stream option (main/sub) from the drop-down list. The channel itself is not specified at this step as it is not known beforehand, to which channel this action will be applied in future - this makes the action universal, applicable to any target channel.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



The source channel is specified when you attach the *Send Email* action to an event, i.e., create a rule in the *Event & Action Configurator:*

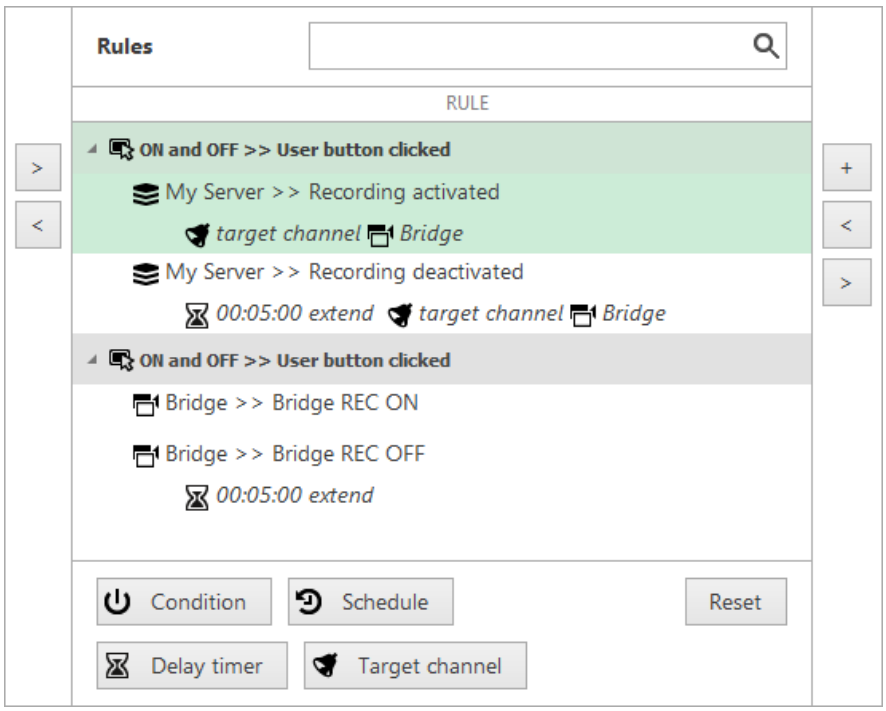
- if the event in the rule has some channel as a source (e.g., motion, VCA, DI), this channel is set automatically as a snapshot source
- for events having sources other than channels (e.g., user buttons, server events), you can specify the source channel by using the *Snapshot source* button on the panel below the rule map
- you can modify the source channel by using the same button, and also disable snapshot attachment by selecting *none* as the source

Email sending rules can accept any extra modifiers just like any other rules - delay timers, conditions and schedules, each of them once.

Adding Target Channels to Rules

There are other actions, apart from *Send Email with a Snapshot*, that are related to channels and may use them as action targets. These are, namely, *Create Bookmark* and *Send Event to Client*.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



The *Create Bookmark* action requires a channel to add the bookmark to. To add bookmarks to multiple channels simultaneously, add several actions of the *Create Bookmark* type and specify different target channels for each.

The *Send Event to Client* action only needs a target channel to be specified in case the action has the *Display event in notification panel* option enabled: as a result, the pre-defined message will appear in the notification area of the specified channel (overlay area in live view, the same place where the stream errors appear - see Macula Monitor user manual for more information). Similarly to bookmarks, you can add more than one action of the same type and add different channels as targets in order to display the message in the notification areas of these channels.

Examples

Here are a few examples of the *Event & Action Configurator* usage. You will find more examples in each of the related topics.

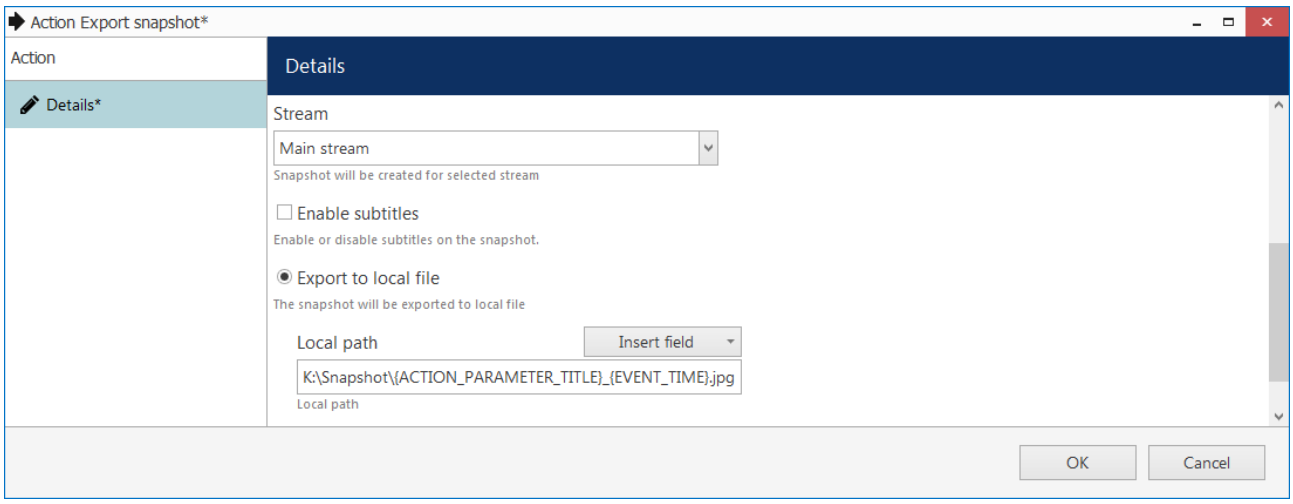
Export Snapshots From All Channels

Task: upon a user button click, save a snapshot from every existing channel on one server.

Preliminary setup:

- create a user button with your desired name
- create an action: export snapshot to a specified location

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



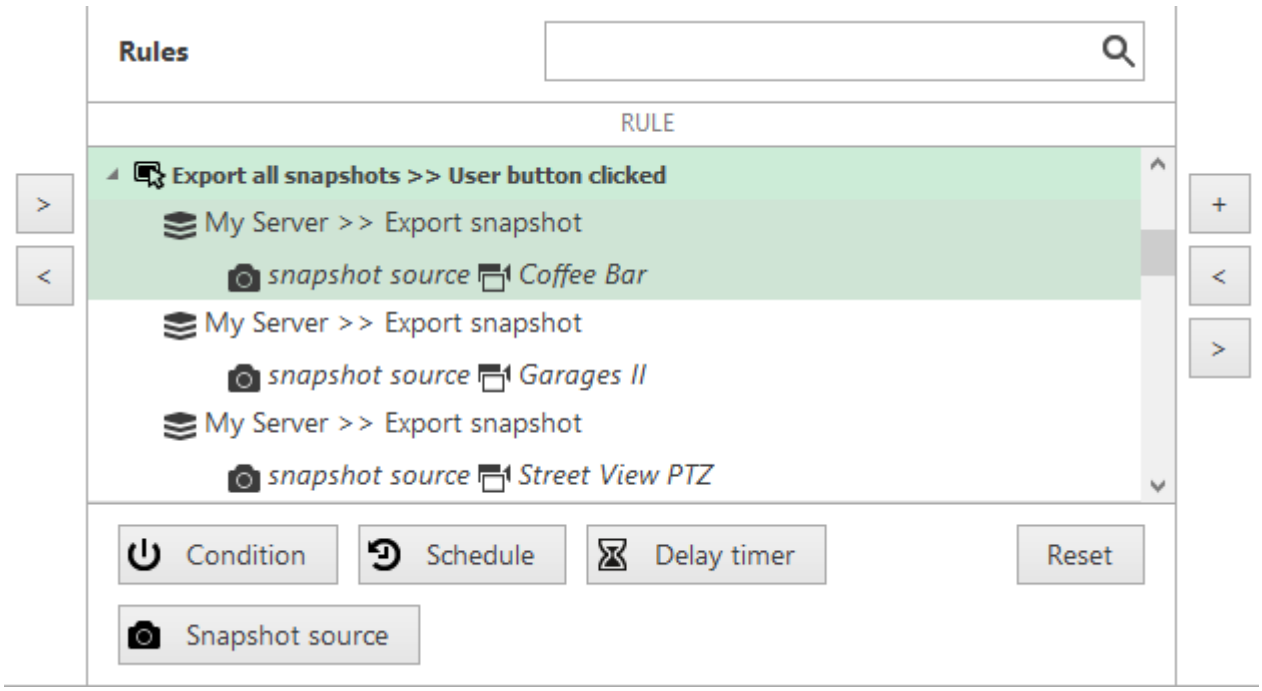
Export snapshot to a specified location using text macros for the file name

Note that the action itself does not contain any fields for the channel to serve as the snapshot source. Thus, the action is universal and can be used repeatedly for many rules; the target channel for the snapshot is then to be specified for each rule in the E&A Configurator.

Use the text macros in the file name and/or path: this is necessary for each snapshot to have a unique name. Otherwise, the snapshots in the same directory will overwrite each other. {ACTION_PARAMETER_TITLE} here is the best option here to differentiate between channels because the originating event (user button clicked) and the action target (server) are the same for all rules. For example, here are two different applications for the same macros:

K:\Snapshot\{ACTION_PARAMETER_TITLE}_{EVENT_TIME}.jpg - each file name contains channel name (snapshot source specified at the rule creation step) and a timestamp

K:\Snapshot\{ACTION_PARAMETER_TITLE\{EVENT_TIME}.jpg - directories with channel names are created, and all snapshots from the same source are put into the same folder and have timestamps as their names



Rules:

- add the *user button click* event once, click it so that it is selected (highlighted green)
- add the *export snapshot* action multiple times for all channels using + button (the rule will be copied automatically)
- define the *snapshot source* (=channel) for each rule using the button in the bottom

As a result, when the user button is clicked in the Macula Monitor or in the Macula Mobile application, snapshots from all available (those having video) channels will be saved into the specified location.

Email Notification on Video Loss

Task: send an email notification when the video stream from certain channel(s) is not available for more than five minutes.

Preliminary setup:

- in the channel settings, set the video loss timeout to 300s (five minutes) for each target channel (select multiple channels and use the *Bulk Edit* button on the upper panel to modify several channels at once)
- configure a mail server with your desired parameters
- create an action: send email to the responsible person using the pre-configured SMTP server

Rules:

the *Video lost* event from each of the target devices triggers the *Send email* action

Note that you do not need to create the *Video lost* event as it is already existed by default for each channel.

Pop Up Channel on Video Analytics Event

Let's see how to pop up video channels if built-in video analytics (VA) trigger a line cross event. Such rules let you efficiently load operators' monitors, so that they only see relevant video instead of tons of static channels.

Task: if video analytics on Channel X detect a person crossing a line, pop up Channel A on all operators' screens.

Preliminary setup:

- Channel A: enable VA, add a crossing line, add a line event of the *Crossed* type with the *Person* class enabled

Rule for Channel A:

- *VCA rule* with the *Line crossed* parameter triggers the *Pop up on screen* action

If you want to limit the popup to a specific video wall display, simply create an additional action of the *Popup object* type. In the action properties, you will be able to specify the video wall display and even viewport index as the channel destination.

Global Handling of Recording Errors

This example will cover a use case with a global event, showing how multiple servers within a single system can be involved in a more sophisticated chain of events and actions.

Task: if there are recording errors on Server A, log this event locally and also add corresponding entry to Windows Application log on the central server. The *Recording error* event is there by default and so there is no need to create it.

Preliminary setup:

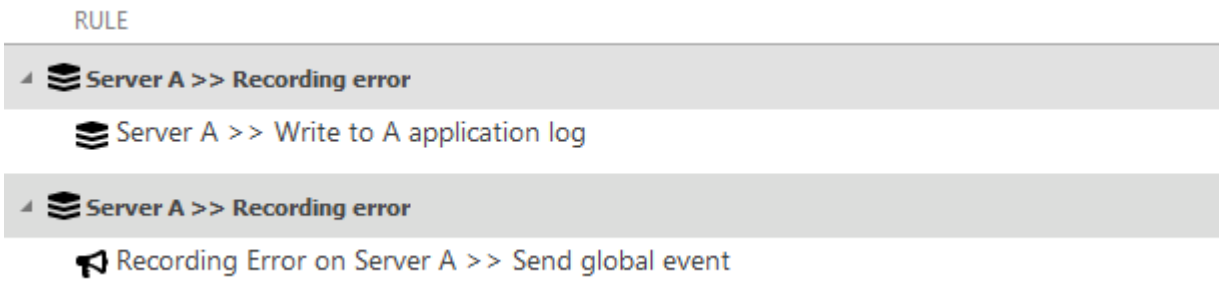
- Server A: *Write to A Application log* action
- Central Server: *Write to CS Application log* action
- Global event *Recording Error on Server A*

Rules for Server A:

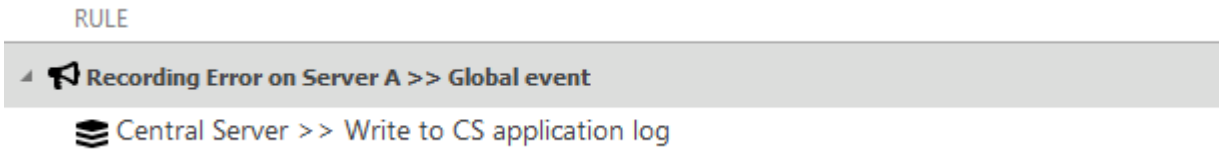
- *Recording error* event triggers local *Write to A Application log* action
- *Recording error* event triggers *Send global event* action for the *Recording Error on Server A* event

Central Server rules:

- *Recording Error on Server A* global event triggers its own *Write to CS Application log* action



Server A generates a global alert and sends it to all servers in the system.



The Central Server is subscribed to the global alert and therefore reacts with the assigned action.

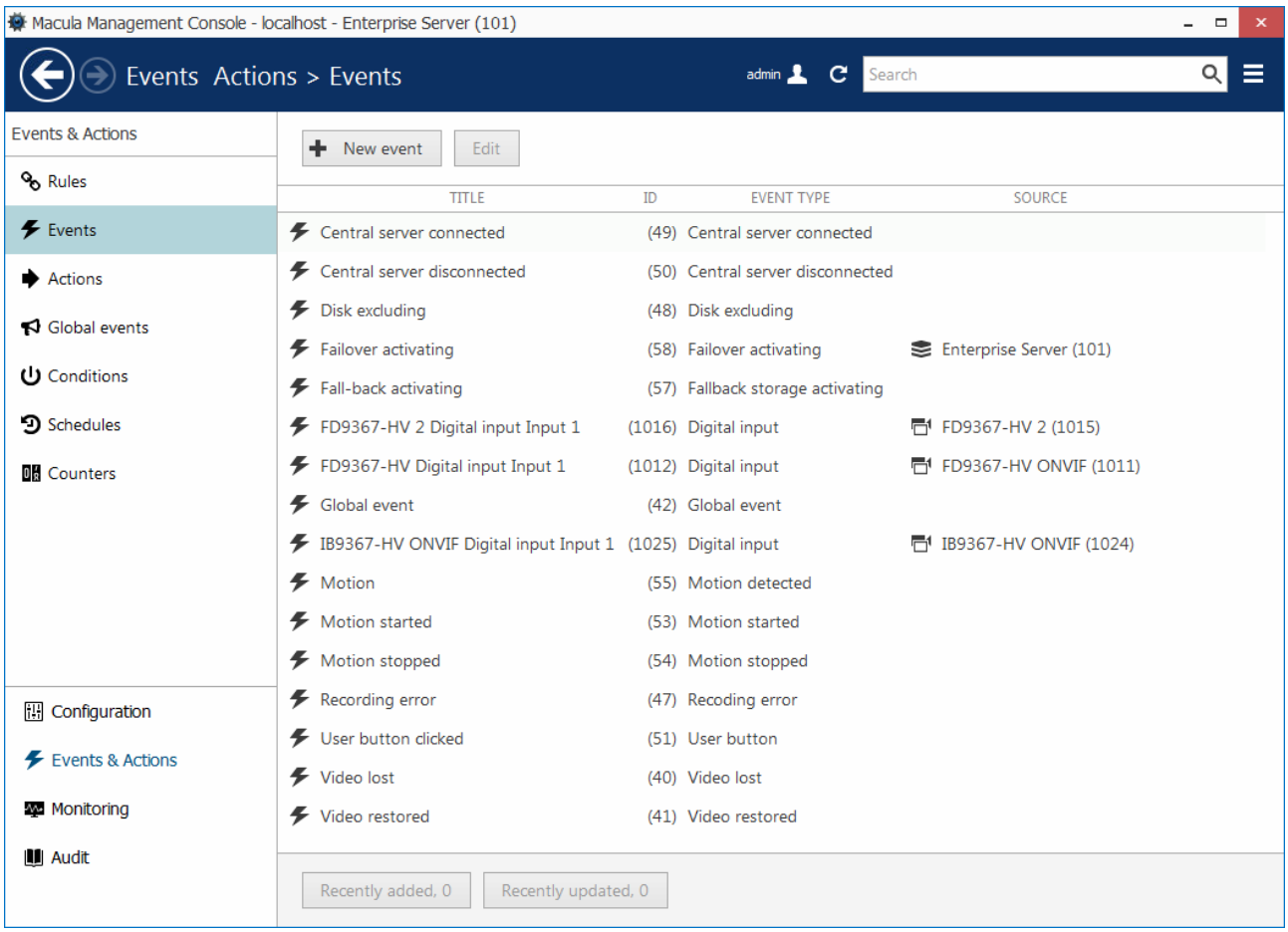
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

9.3 Default Events

Events are entities that appear when something happens in the surveillance system - namely, when the system or system component state changes. These changes can be set up to trigger certain actions so that system administrators and/or users can react to them in a timely fashion.

For each Macula server, there are a set of default events, which behave in an identical way on all servers and cannot be altered or deleted. These are:

- **Central Server Connected**: the connection with central server has been restored; event is available for non-central **servers**
- **Central Server Disconnected**: the connection with central server marked as unavailable because the timeout defined in the server settings has been reached; event is available for non-central **servers**
- **Disk Excluding**: one of the storage locations has been marked as unusable and has been excluded from the recording configuration; event is available for every **server**
- **Failover Activating**: a recording server has failed and has been automatically replaced by a failover node
- **Fallback Activating**: main storage has failed, server has automatically switched to fallback storage; event is available for each **server**
- **Global Event**: global (system-wide) event from one of the servers has been fired; event is available for all defined global events and on all servers with Macula Enterprise
- **Motion**: motion has been detected; event is available for each **channel**
- **Motion Started**: some motion has been detected (single motion event has occurred); event is available for each **channel**
- **Motion Stopped**: no more motion is being detected; event is available for each **channel**
- **Recording Error**: problem encountered while recording video data to the storage; event is available for each **server** and for each **channel**
- **Recording Recovered**: server has recovered from the recording error; available for each **channel**
- **User Button Clicked**: user button was pressed; event is available for all created **user buttons**
- **Video Lost**: no video stream available for this specific channel for the defined amount of time, which is set in the channel settings; event is available for each **channel**
- **Video Restored**: video stream connection re-established; event is available for each **channel**
- **External Event**: for each **channel**, three custom events are available (see details below)



Default events are available in the *Event & Action Configurator* and can be used in the same way as user-defined events, except for they cannot be edited. Events are arranged by **sources**. Typical event sources are: channels, channel groups, servers, user buttons, video walls, external services.

External Channel Events

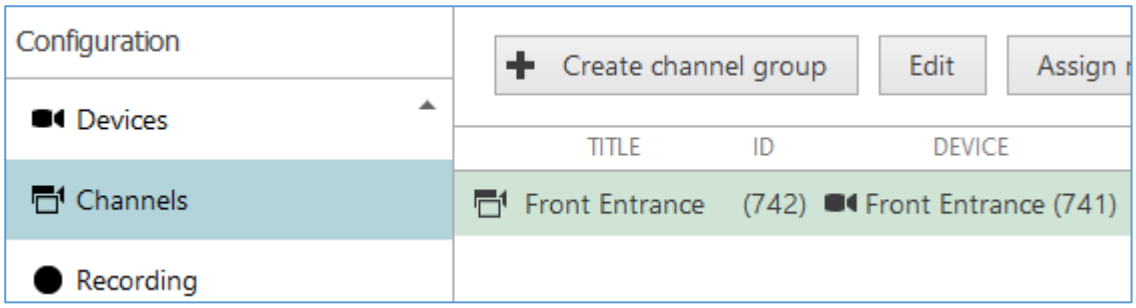
External (custom) channel events are reserved for the cases when you need Macula to react to an event that originates in any third-party system, which is not connected to Macula. Each of these three available events is triggered via **HTTP API** by sending a HTTP request; the channel events exist by default, meaning that all you have to do is to build the URLs and then use them externally. There is also an option to add up non-channel external events with a configurable ID (see *External events* below).

Custom events use the following URL tags:

/event/<resource_id>/external1/activate
/event/<resource_id>/external2/activate
/event/<resource_id>/external3/activate

where <resource_id> is the channel ID. You can look up the channel ID in Macula Console, in the resource table of the *Channels* tab, provided that your Macula Console settings have object IDs enabled. If they are not, enable *Object IDs* via main menu > *Settings* > *General* tab.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

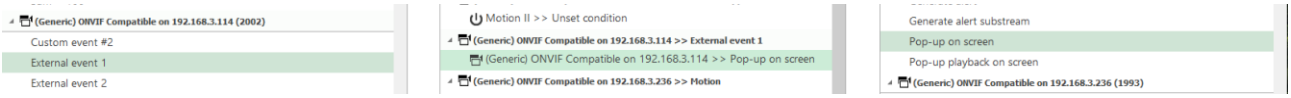


Use the Macula server IP and HTTP port to build the full URLs. For the default HTTP port setting and IP equal to 10.10.10.1, the URLs will look as follows for a channel with its ID equal to 115:

http://10.10.10.1:8080/event/115/external1/activate
http://10.10.10.1:8080/event/115/external2/activate
http://10.10.10.1:8080/event/115/external3/activate

The authentication type should be **digest**, and the method must be **GET**, for example:

curl -v --digest -u admin:password http://10.10.10.1:8080/event/1257/external1/activate



In Macula Enterprise systems:

- use the IP and port of the server, where the target channel is configured
- if the main recording server has switched to failover, use the IP and port of the failover node (channel ID remains the same)

When triggering the event over the Internet, make sure that the HTTP port of the target Macula server is reachable (open on the firewall(s) and forwarded, if required).

9.4 Add Events

Events are entities that appear when something happens in the system - namely, when system or system component state changes. These changes can be set up to trigger certain actions so that system administrators and/or users can react to them in a timely fashion.

In addition to the default set of events, certain types of events can be added manually.

To access event management in Macula Console, select the *Events & Actions* section and then select *Events* from the menu on the left.

To create an event, click *+ New event* button on the upper panel; event configuration dialog box will open. It is also possible to add events as you go, from the *Event & Action Configurator*. Fill in the settings, then click *OK* to save and close the dialog box. The newly created event will appear in the item list under *Events* and will be available for setup in the *Event & Action Configurator*.

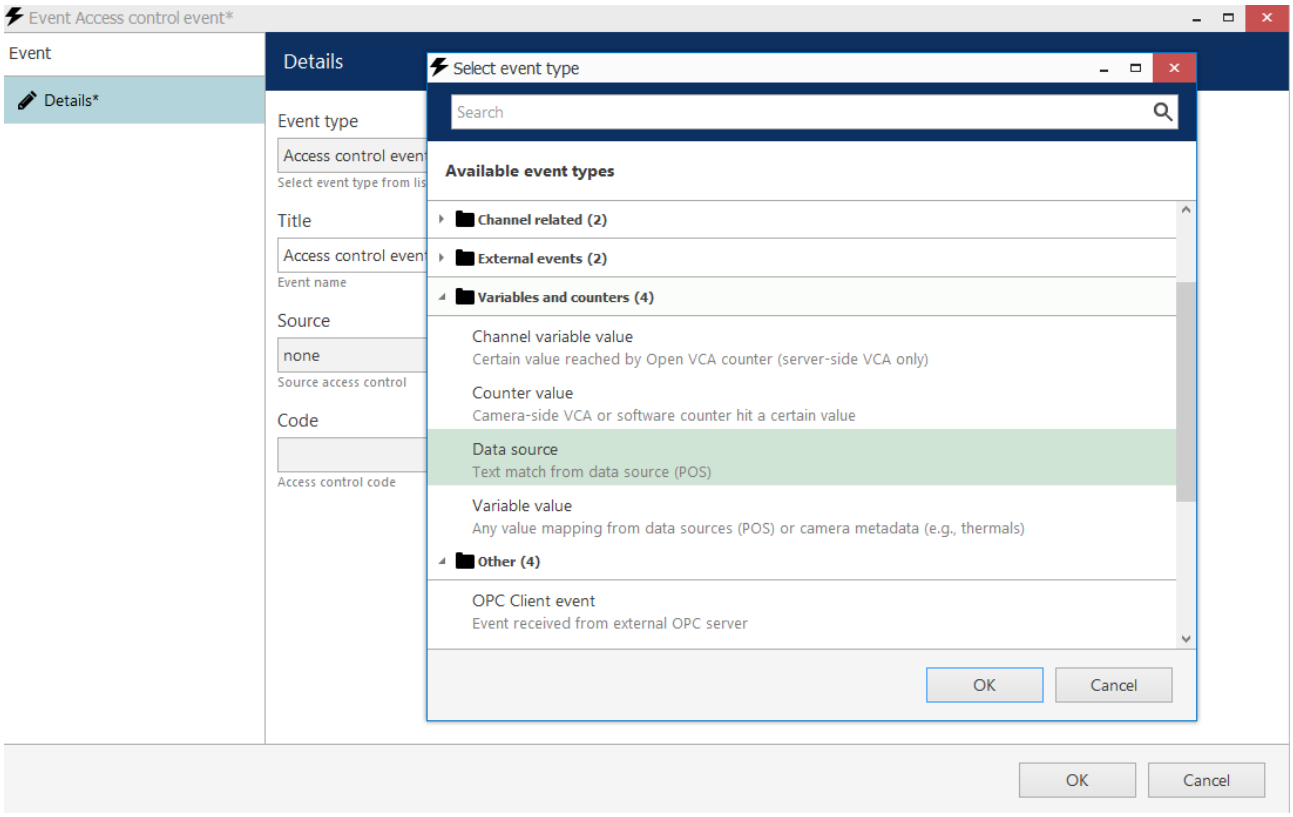
Once you have created an event, it is impossible to change its type, only its source and properties.

Below, you will find explanations about every available event type.

Before creating events from camera DI, VCA source, GSM modem, or external service make sure to:

- add the resource (channel, modem, etc.) to the server configuration;
- enable alert generation in channel settings via Macula Console for device digital inputs (DI);
- enable and set up rules via camera Web interface for edge VCA and set up rules via channel settings for software-side Open VCA;
- set up the External Service event generation logic for external services (license plate recognition, face recognition etc.)

Without this preparation, you will be unable to create the events.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Prior to software version 1.17.0, events and actions were simply listed alphabetically. Starting with v.1.17.0, events and action are additionally grouped for your convenience. Start typing a keyword to quickly find a specific event.

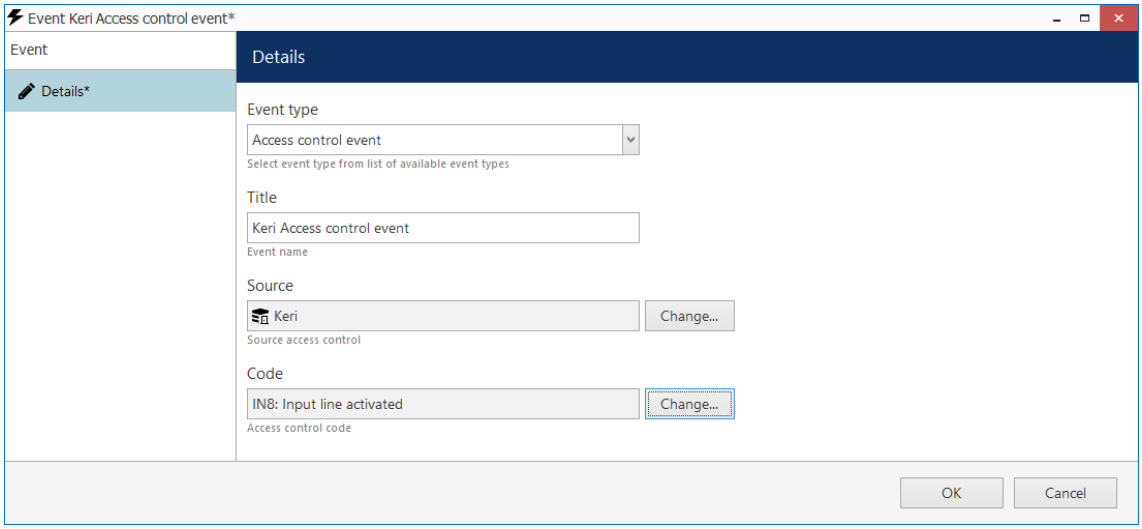
Access Control Events

Events in this group originate from connected access control systems.

Access Control Event

This type of event is triggered by the status code coming from the access control integration, whenever the status code is not related to any door (making it impossible to use *Door event*). The codes are vendor-specific and will vary depending on the access control suite type.

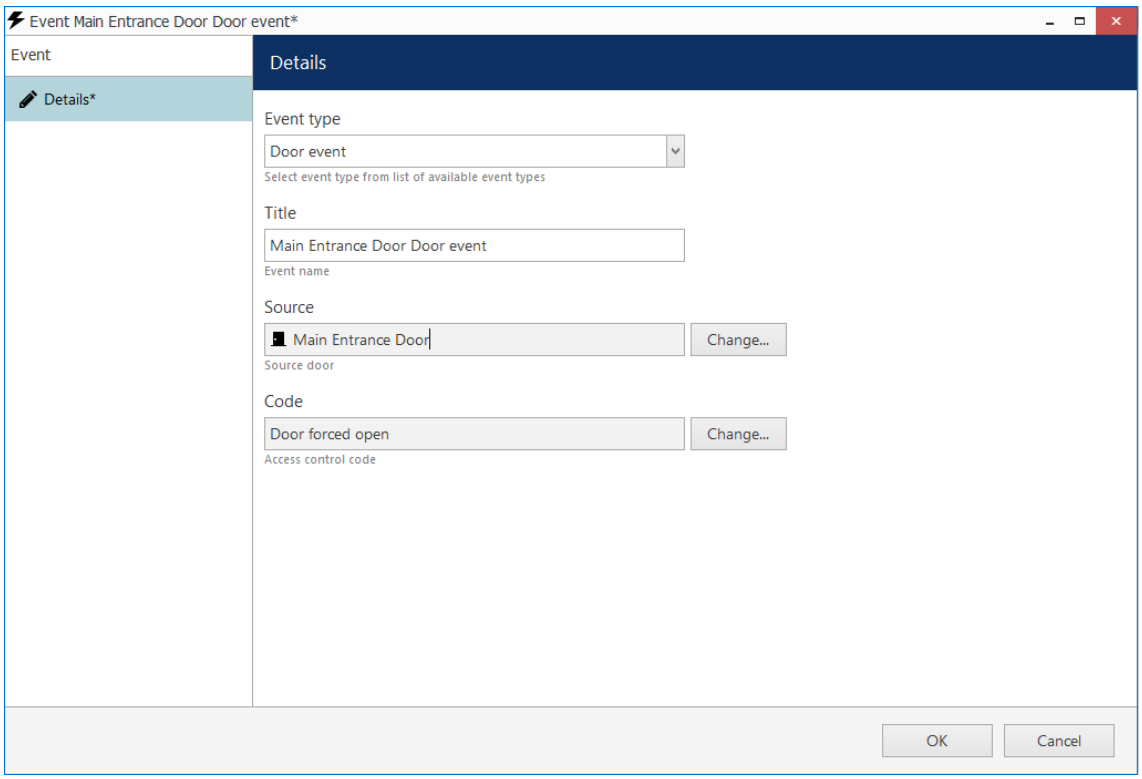
- **Title**: user-defined event name, as it will appear in the *E&A Configurator*
- **Source**: access control server that will send the status changes
- **Code**: vendor-specific event code



Door Event

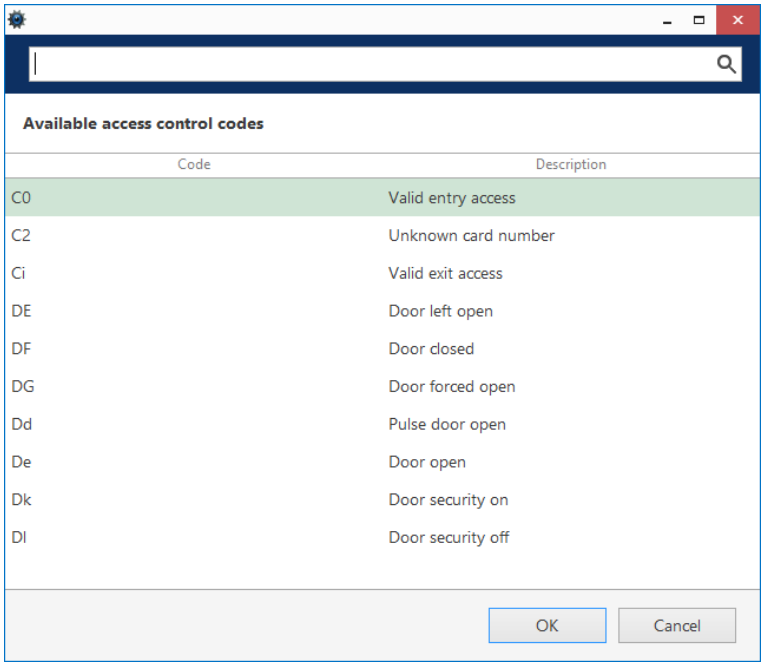
This type of event is used to set up Macula server reactions based on door status changes, which are received from the integrated third-party access control software.

Macula® Professional Administration Guide



Settings:

- **Title**: user-defined event title
- **Source**: a door from the access control module (choose from list)
- **Code**: received status or error code from the access control module (choose from list)



The list of codes will differ depending on the access control type. For details about each code, please refer to your access control software documentation.

Channel Related Events

Events in this category have channels as sources.

Before creating such events - from camera DI or VCA source - make sure to:

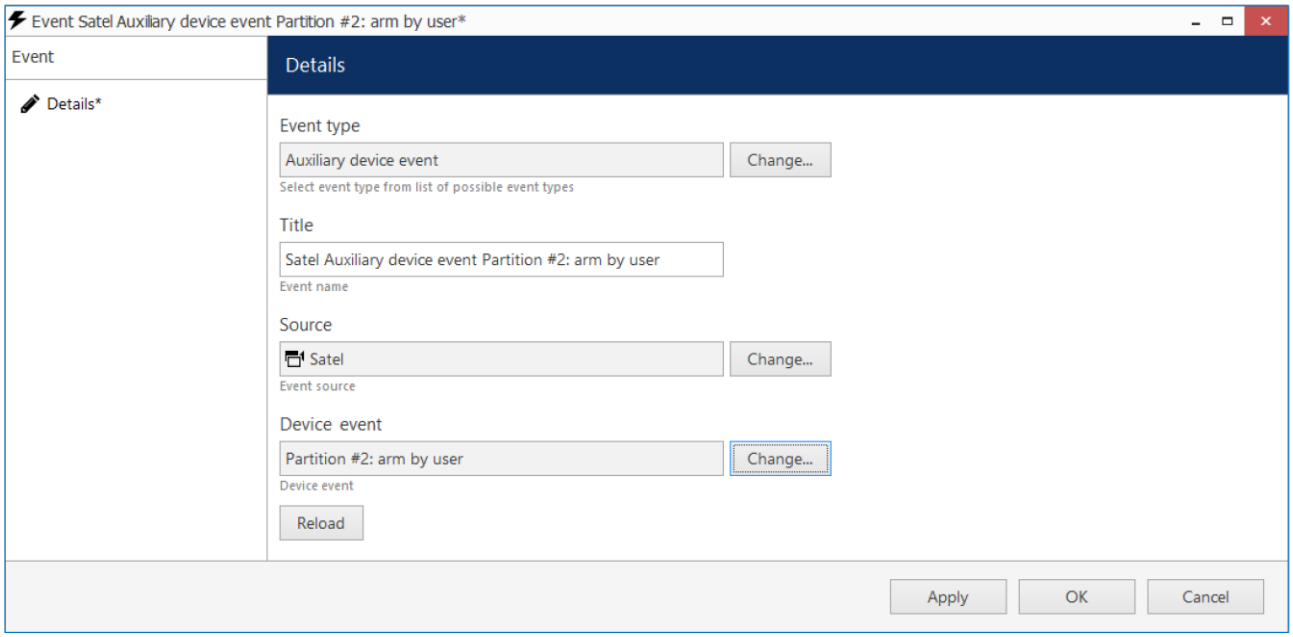
- enable alert generation in channel settings via Macula Console for device digital inputs (DI)
- enable and set up rules via camera Web interface for edge VCA, or set up Open VCA rules (Open VCA must be activated)

Without these settings, the target channel will not have corresponding DI or VCA items available in the event settings (the item list will be empty).

Auxiliary Device Event

This type of event is similar to *VCA Event* and designates some event that happens on the device side, with the difference that the auxiliary device event comes from a non-video device. Auxiliary device events may come from alarm control panels, various sensors, audio detectors etc. These events are received directly via device integration (not via OPC/MQTT/...) and are not directly reported as DI/DO events either.

If your device falls into this category but the auxiliary event list is empty, try the *VCA event* type.



Available settings:

- **Title**: user-defined event name that will appear in the E&A Configurator
- **Source**: source device (e.g. Satel alarm control panel)
- **Device event**: event type on the device side

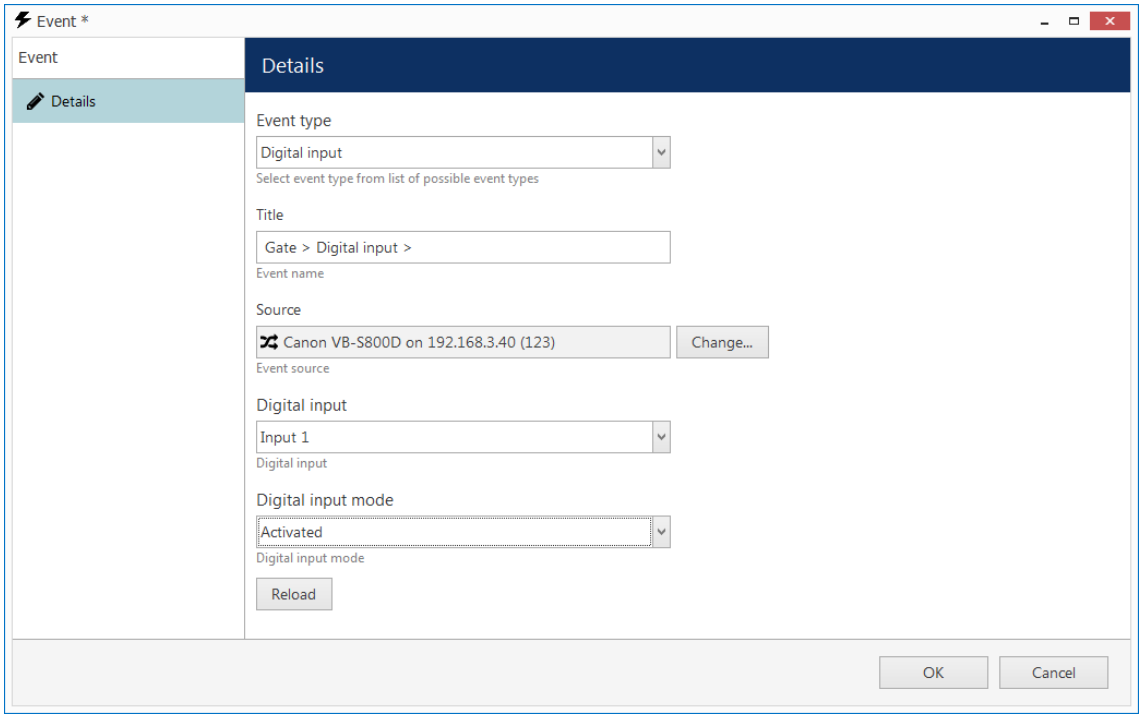
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Digital Input

This event is triggered when a device's DI state is changed. Before creating the event, make sure you have enabled DI event generation in the device channel's properties.

The following settings are available for *Digital Input* event:

- **Title**: a user-defined event name
- **Source**: choose the device from which the DI event originates; event generation must be enabled in the channel settings
- **Digital Input**: select one of the DIs of the target device to serve as event trigger; the number of inputs depends on the total available and configured inputs
- **Digital Input Mode**: the binary input state to trigger alert; must conform with the DI state set up in the channel settings

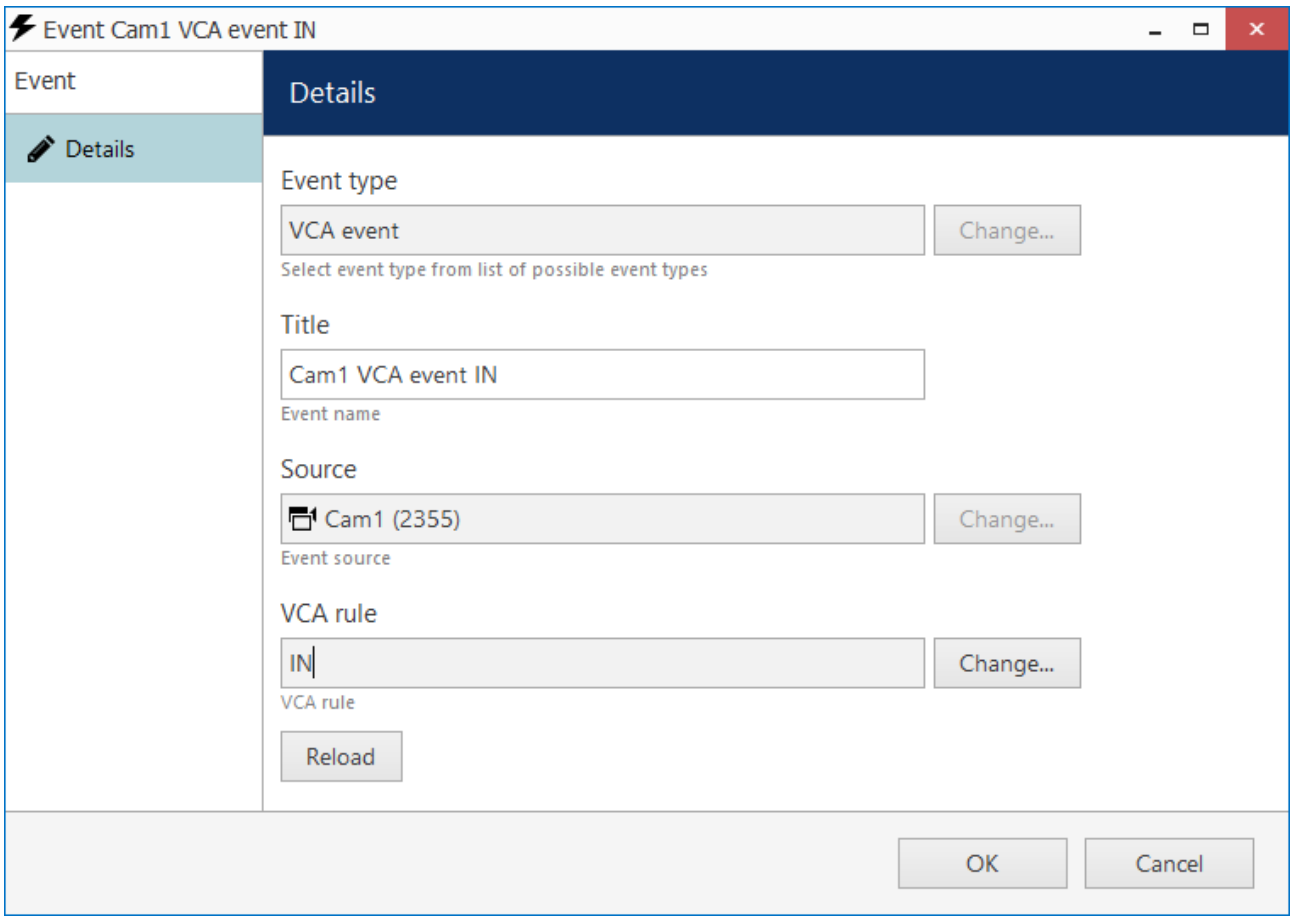


VCA Event

For **camera-side VCA** and software-side **Open VCA** events. Note that this event only covers triggered VCA **rules**, and not counters. In order to set up reactions for VCA counter changes, use the *Channel variable value* event (for Open VCA) or *Counter value* event (for camera-side counters).

The available settings are:

- **Title**: user-defined event name
- **Source**: choose a channel from which the video analytics event originates; analytics rules must be enabled via the camera Web interface (some cameras have basic VCA events enabled by default, e.g. volume detection) or pre-configured using the Macula Console for the software-side Open VCA module (see corresponding documentation for configuration details)
- **VCA Rule**: video analytics rule to trigger event alert; may come from the camera side, Open VCA engine, or built-in VA engine; available rules depend on device model, capabilities and VCA configuration



If you do not see a recently created VCA event in the drop-down list, try clicking the *Reload* button: this will refresh the source event list. For guidelines on how to enable and configure Open VCA, please see the related document.

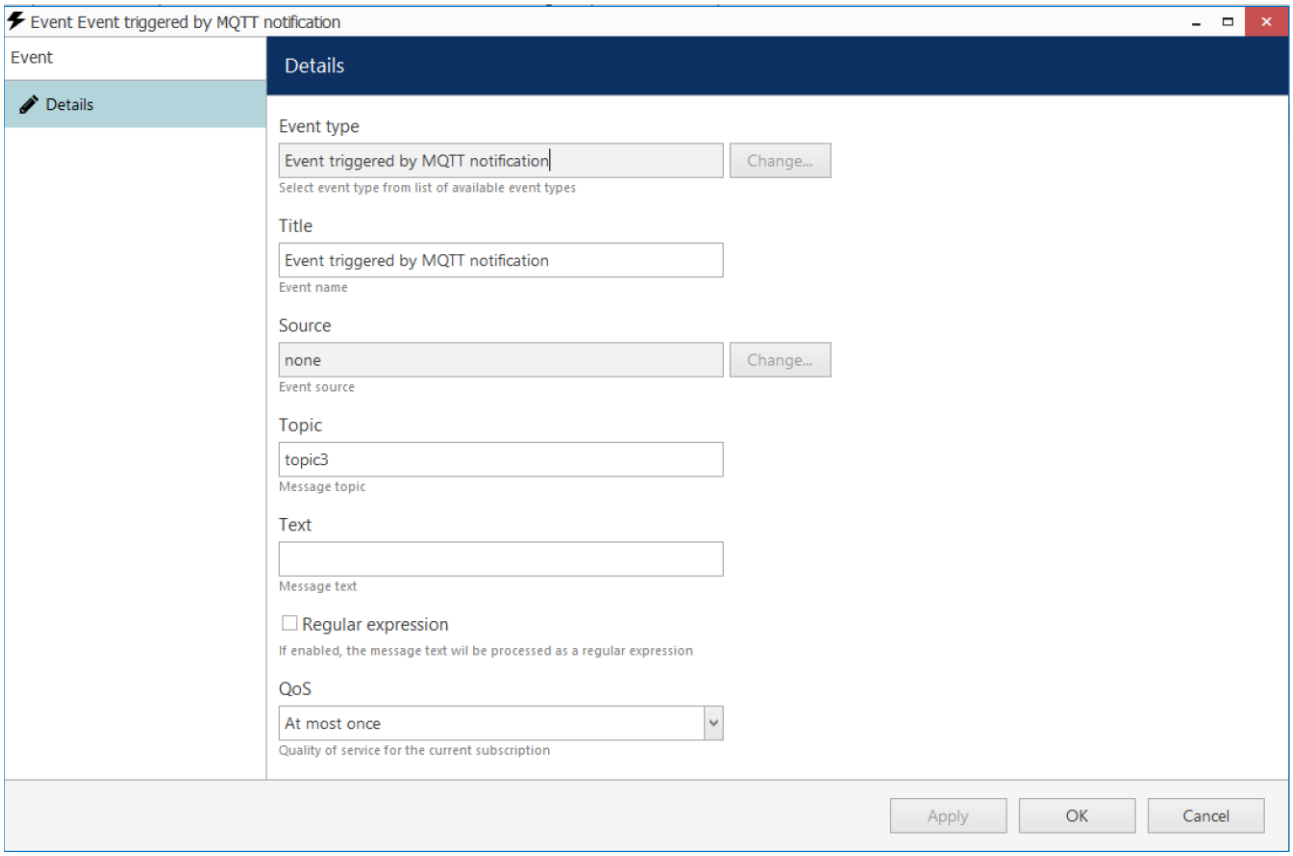
External Events

These events come from all kinds of external systems.

Event Triggered by MQTT Notification

This event is triggered by incoming MQTT messages from a third-party broker. The message may be an exact text match, or you can evaluate it using a regular expression (regex) and catch a keyword or a part of the message.

- **Title**: event name that will appear in the E&A Configurator, corresponds to the macro {EVENT_TITLE}
- **Source**: MQTT client that will subscribe to the current topic and act as event source. Leave empty if you want the event to be visible for all existing MQTT clients
- **Topic**: MQTT topic to subscribe to
- **Text**: incoming message that will trigger the E&A event. If empty, any message will trigger the event. The field cannot be empty if marked as regular expression!
- **Regular expression**: enable this option to enter a regular expression in the Text filed instead of plain text
- **QoS**: required level of quality of service



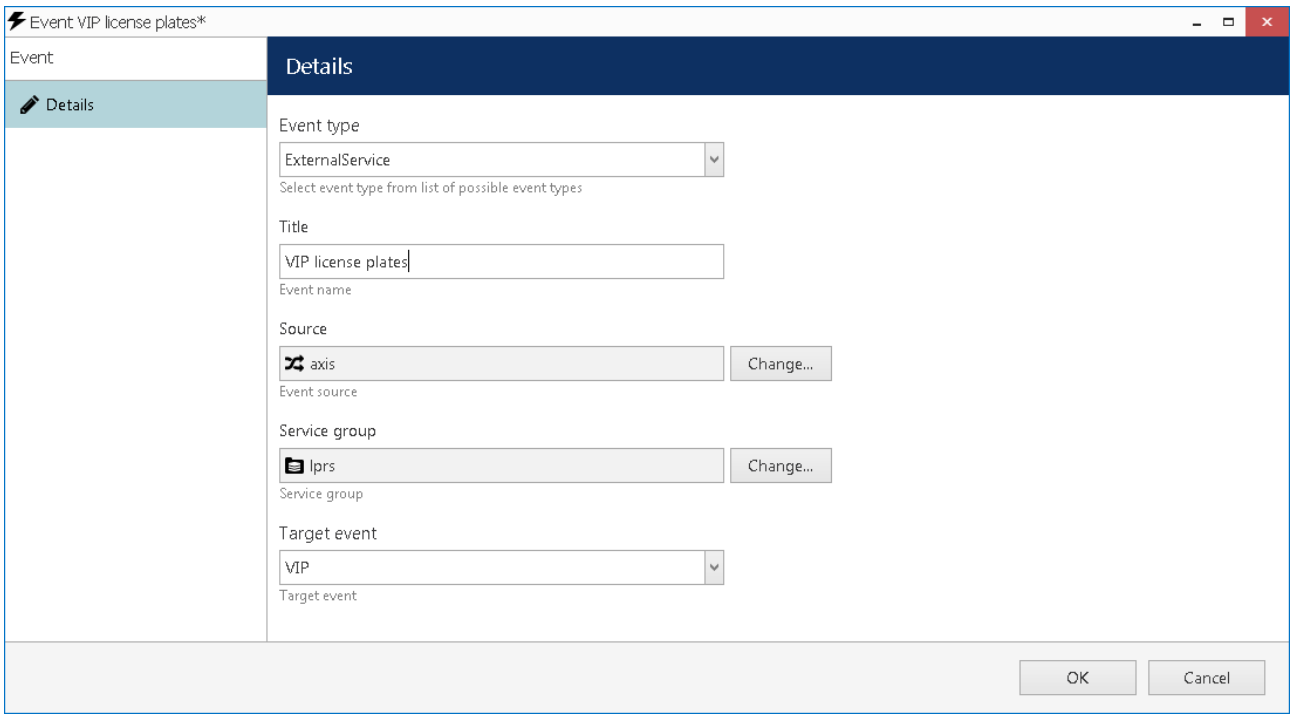
Fields *Source* and *Text* may be left empty. Empty source means that the event will be created for every existing MQTT client. Empty message text means that the event will be triggered by any message having the defined topic; however, you cannot leave this field empty if you wish to use regex. If the Regular expression option is enabled, the Text field must contain an evaluating expression to analyze the message text.

External Service

External Service type events are messages from modules that are operating via Macula HTTP API and are listed in Macula Console as external services. By default, license plate recognition and face recognition services are integrated.

The following settings should be defined:

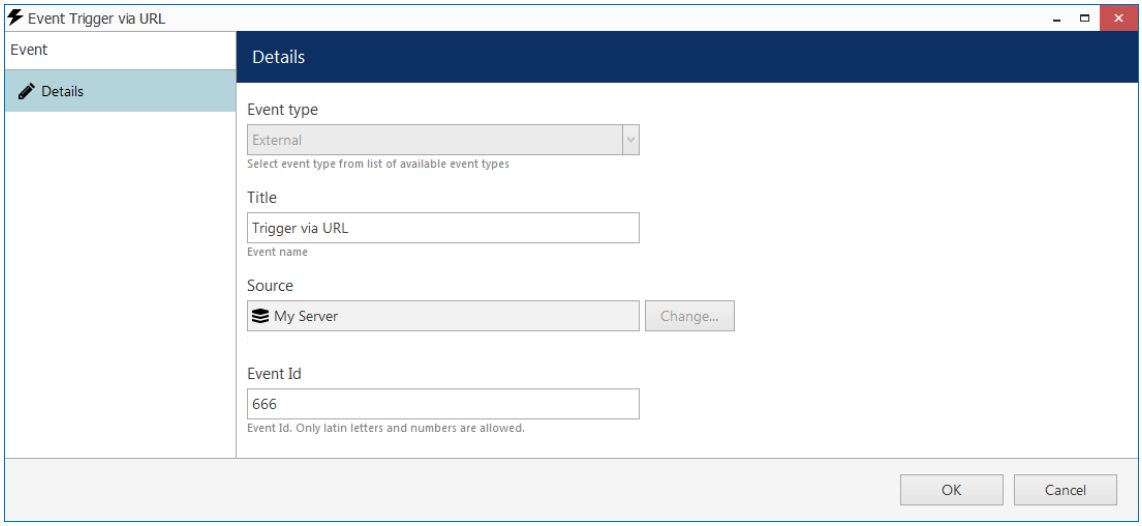
- **Title**: user-defined event name
- **Source**: the channel that is used by the target external service
- **Service group**: the group the external service belongs to in Macula Console settings
- **Target event**: service-specific result type, e.g., recognition result
    - *Known*: recognition result has a match within the external service database (black/white list in LPR, subjects' database in FR), matching any tag
    - *Unknown*: recognition result has no matches within the external service database
    - *Tags*: recognition result was found in the external service database and it has a specific tag assigned to it



The example event here accepts events from the License Plate Recognition (LPR) module and will report plates recognized from the specified source channel if these results are present in the known plates' list with a *VIP* tag.

External

External events are HTTP requests from third-party software: integrations, scripts, Web browsers etc. These are a basic example of Macula HTTP API: an **URL** is used to trigger the event.



For the external request to trigger an event, create the event on your desired Macula server:

- **Title**: user-defined event name
- **Source**: Macula server that will accept the HTTP request
- **Event ID**: alphanumeric event identifier, **only** Latin letters [a-zA-Z] and digits [0-9] allowed

The request link is built as follows:

http://<server_address>:<http_port>/externalEvent/activate?id=<event_id>, where

- <**server_address**> is the target server's IP address or hostname (in Macula Enterprise systems, use the exact Macula Recording Server address, not Macula Enterprise server address)
- <**http_port**> is the server's HTTP port (8080 by default)
- <**event_id**> is an alphanumeric identifier of the event, which is defined at the event creation step

Example: *http://192.168.1.99:8080/externalEvent/activate?id=666*

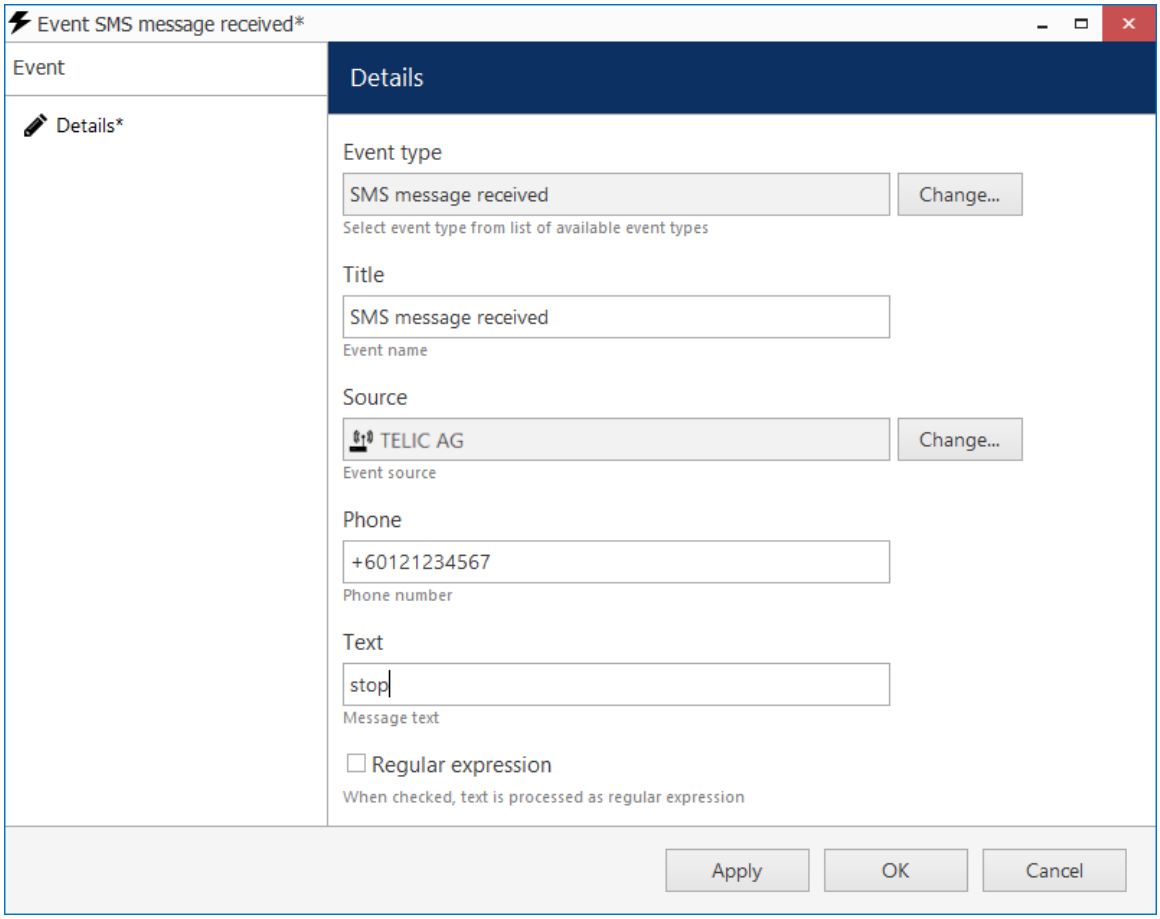
SMS Message Received

SMS events are events triggered by short messages, which are received by SMS (GSM) modems. You need to connect the hardware (modem) to the Macula server, insert a SIM card, and add the modem into Macula Console in order to receive this type of events.

Available settings:

- Title: user-defined event name
- Source: existing modem hardware to accept the message
- Phone: sender's full phone number; if empty, the event will be triggered by SMS from any number
- Text: SMS text to trigger the event, case-sensitive; leave empty for any text to trigger the event
- Regular expression: enable if you wish to evaluate the incoming text with regex, e.g., use placeholders

⚠ The phone number must be in the international format (with leading + or 00 and a country code) for ALL numbers, even local ones. The event will not work properly without the country code.



In this event type, you can use certain keywords in your messages, or set up regular expression rules to catch patterns.

Variables and Counters

Events in this category are triggered by certain **value changes**. These values can be text variables, software or VCA counters, mappings from data sources (POS or other serial text), channel metadata etc. Each event is dedicated to a specific kind of variable or counter.

- *Counter value*: for camera-side VCA counters and also software counters
- *Data source*: text match from Data sources
- *Open VCA counter value*: server-side VCA (Open VCA) counters
- *Variable value*: pre-defined variable value analysis

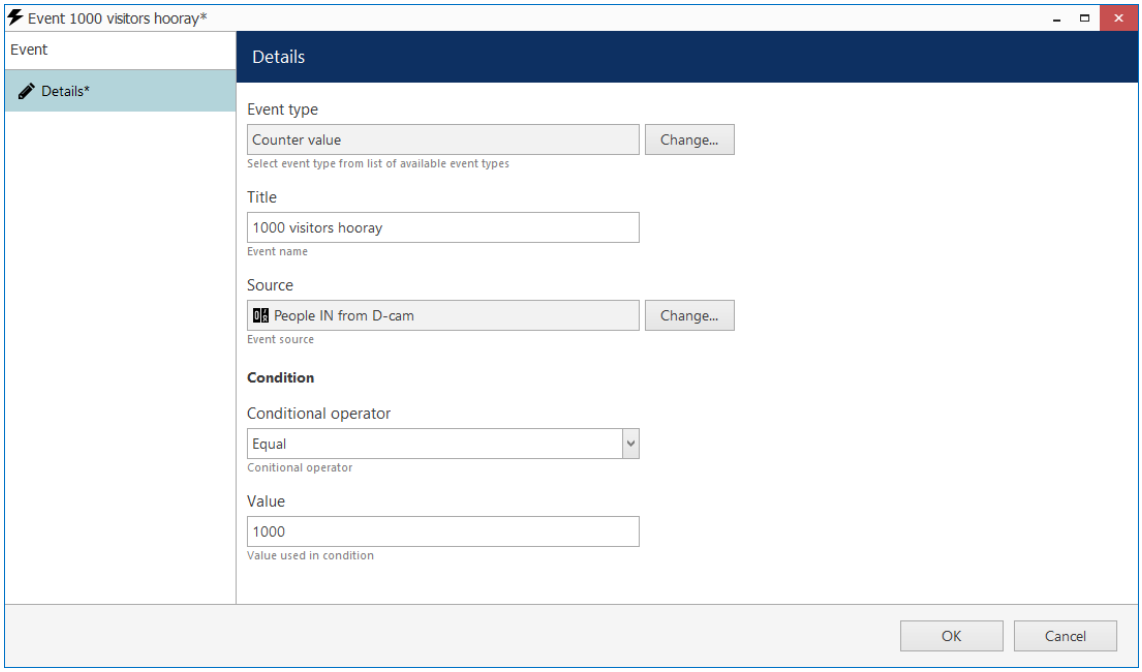
Counter Value

Solely for **camera-side counters** and **software counters** (server-side, NOT VCA).

Software counters can be created in Macula Console to count any events in the system. Camera-side counters are only available for certain integrations (e.g., Dahua with smart tools).

This event is similar to the previous one, with the difference that you do not have to set the data type, but rather simply select a pre-created counter. Counters from the cameras must be also explicitly added in Macula Console under *E&A* > *Counters* > *New VCA Counter*.

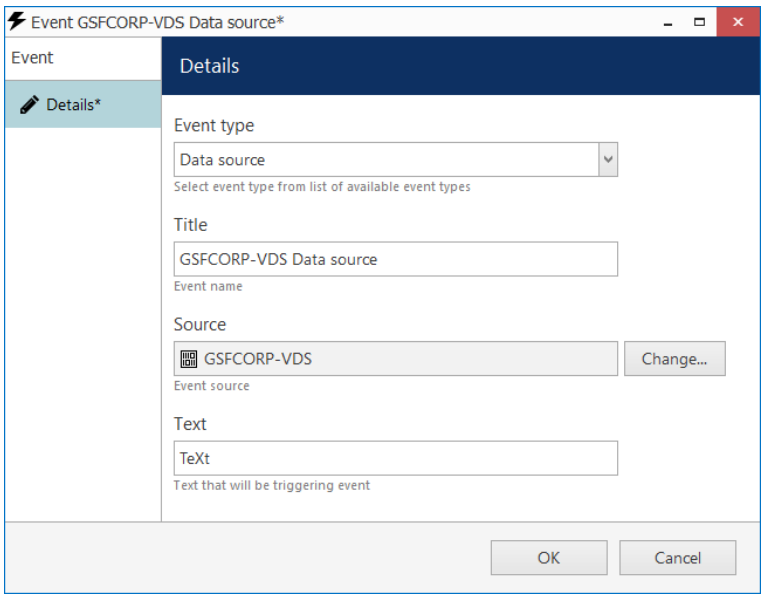
- **Title**: user-defined event name
- **Source**: choose one of the pre-created software or camera-side counters
- Condition: define what the counter value will be compared to
    - **Conditional operator**: choose the comparison type - greater, less, equal, etc.
    - **Value**: an integer value for the counter to be compared to



For actions further linked to this event, you can **pass the counter value** by using the **text macro** (field) *{ADDITION_INFORMATION}* (you can insert it in any textual action by right-clicking the text area or by clicking the *Insert field* button). The format will be [counter_name]=[counter_value]. For example, for a counter named *Total* hitting a value of five, the macro will show *Total=5*.

Data Source

The server will monitor incoming text from Data sources, triggering an event in case the specified string is received. This can be used to react to certain keywords from POS terminals and any other serial data sources. The string for comparison is defined in free **text** form (not regex). The server will be looking for an **exact match**, i.e., the field is case-sensitive and all extra symbols (commas, spaces) are accounted for.



Available settings:

- **Title**: user-defined event name
- **Source**: data source to be used as event source; text from data provider will be analyzed for matches
- **Text**: case-sensitive keyword or key phrase; when an exact match is found in the text, the event will be triggered

For the event to operate, it is **not necessary** for the target data source to be bound to any channel. Associating data sources with channels only affects video overlay in the Macula Monitor application; text detection will work on the server side, and therefore the data source may be independent.

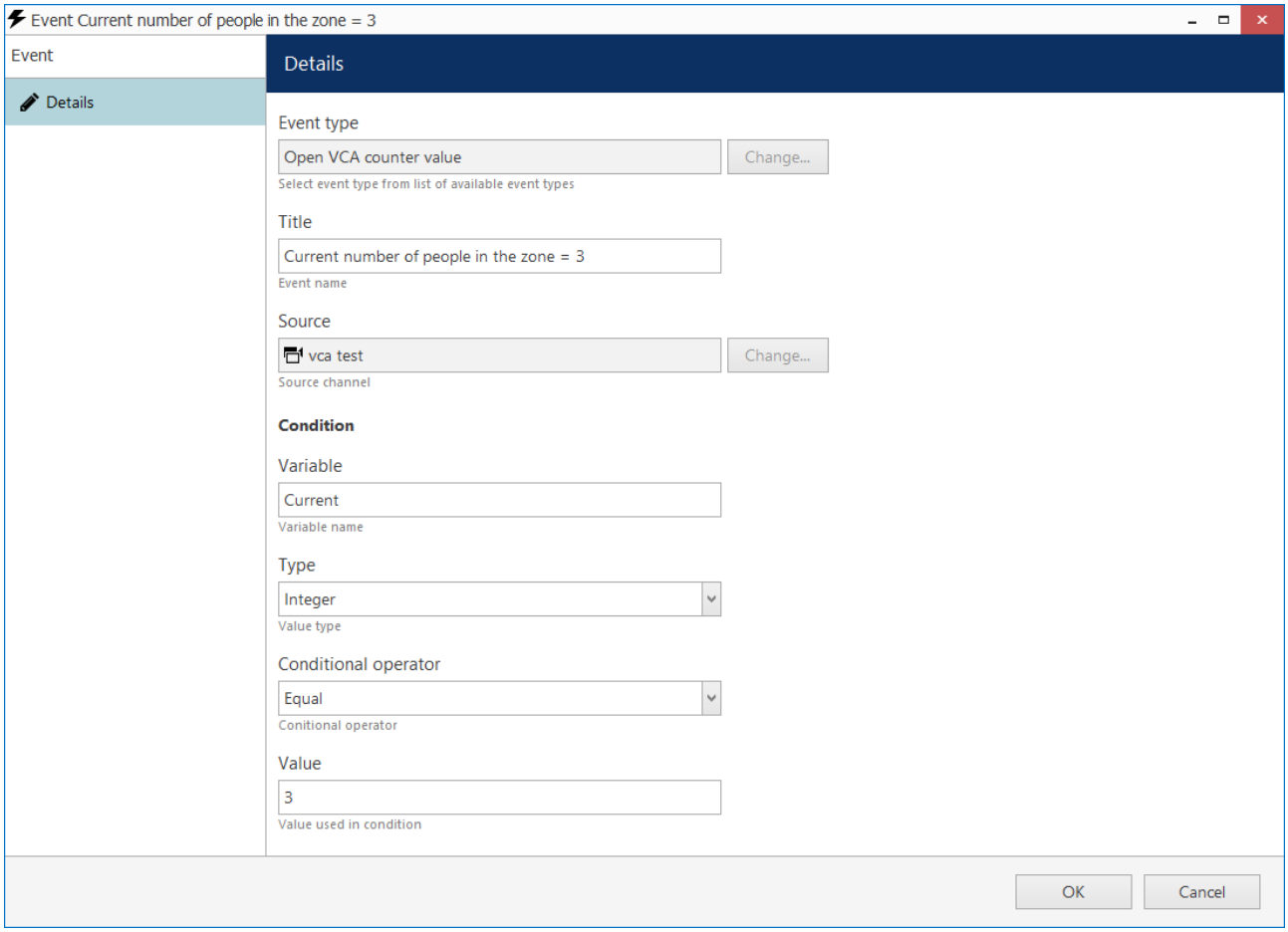
Open VCA Counter Value

This event is dedicated to Open VCA **counters** (those set up on the server side for a specific channel). Each counter value update triggers a comparison of the integer counter value to the pre-defined value. The comparison operation is carried out using two integer data types and returns true (event is triggered) if the condition is true. The available conditions are: equal/not equal, greater/less, greater/less or equal.

To react to Open VCA rules, use the *VCA Event* under channel-related events.

- **Title**: user-defined event name

- **Source**: a channel that has Open VCA enabled and at least one counter set up
- Condition: define what the counter value will be compared to
    - **Variable**: Open VCA counter name
    - **Type**: must be **integer** (other types are listed to ensure event compatibility with older software versions)
    - **Conditional operator**: choose type of comparison - greater, less, equal, etc.
    - **Value**: an integer value for the counter to be compared to

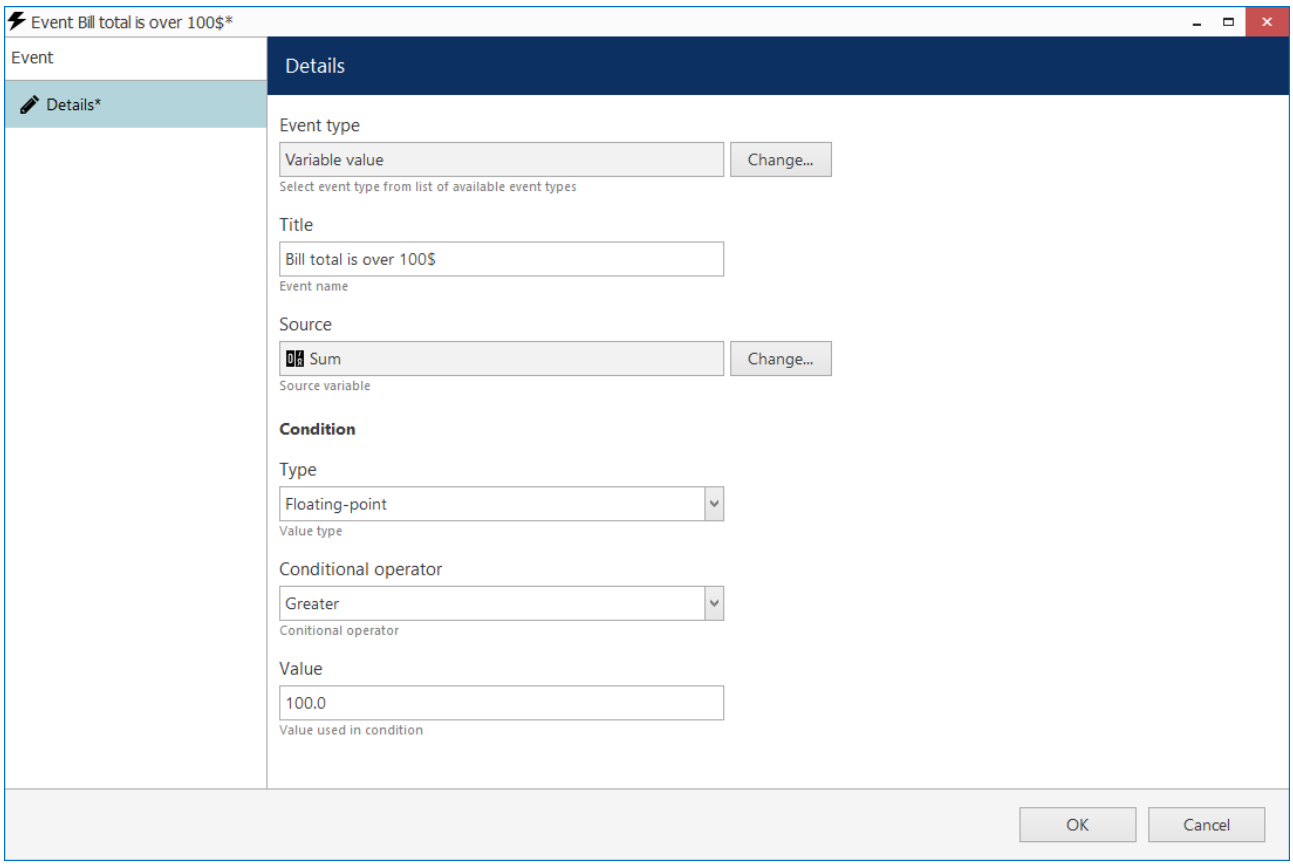


For actions further linked to this event, you can **pass the counter value** by using the **text macro** (field) *{ADDITION_INFORMATION}* (you can insert it in any textual action by right-clicking the text area or by clicking the *Insert field* button). The format will be [counter_name]=[counter_value]. For example, for a counter named *Total* hitting a value of five, the macro will show *Total=5*.

Variable Value

If you have some **variables** set up in the E&A section, you can use E&A manager to trigger events when these variables meet some specific condition. Mostly, these variables are mappings from Data sources: thus, this event supplements the previous *Data Source* event by matching **any data type** (not just text).

The second purpose of this event is analysis of **metadata** received **from cameras** (or other devices). A typical example of this is variables from **thermal cameras** containing exact temperature measurement. To use this feature, first create channel variables under *Variables* in the E&A section. Then, use them as



This event has the following settings:

- **Title**: user-defined event name
- **Source**: a channel to be analyzed for the variable (which is set in the corresponding data source profile or has VCA configured); if none selected, the event will be visible for all channels
- **Variable**: variable name, must match the mapping name in the data sources profile or the VCA counter name
- **Type**: variable type; may be integer, double or string for a data source mapping, and integer for VCA counters
- **Conditional operator**: depends on the variable type
- **Value**: value that will be compared with the variable value

⚠ For VCA counters, there are a few special requirements:
- type must be **integer**
- **event source** must be selected (the channel that has VCA configured, either camera-side or software side)

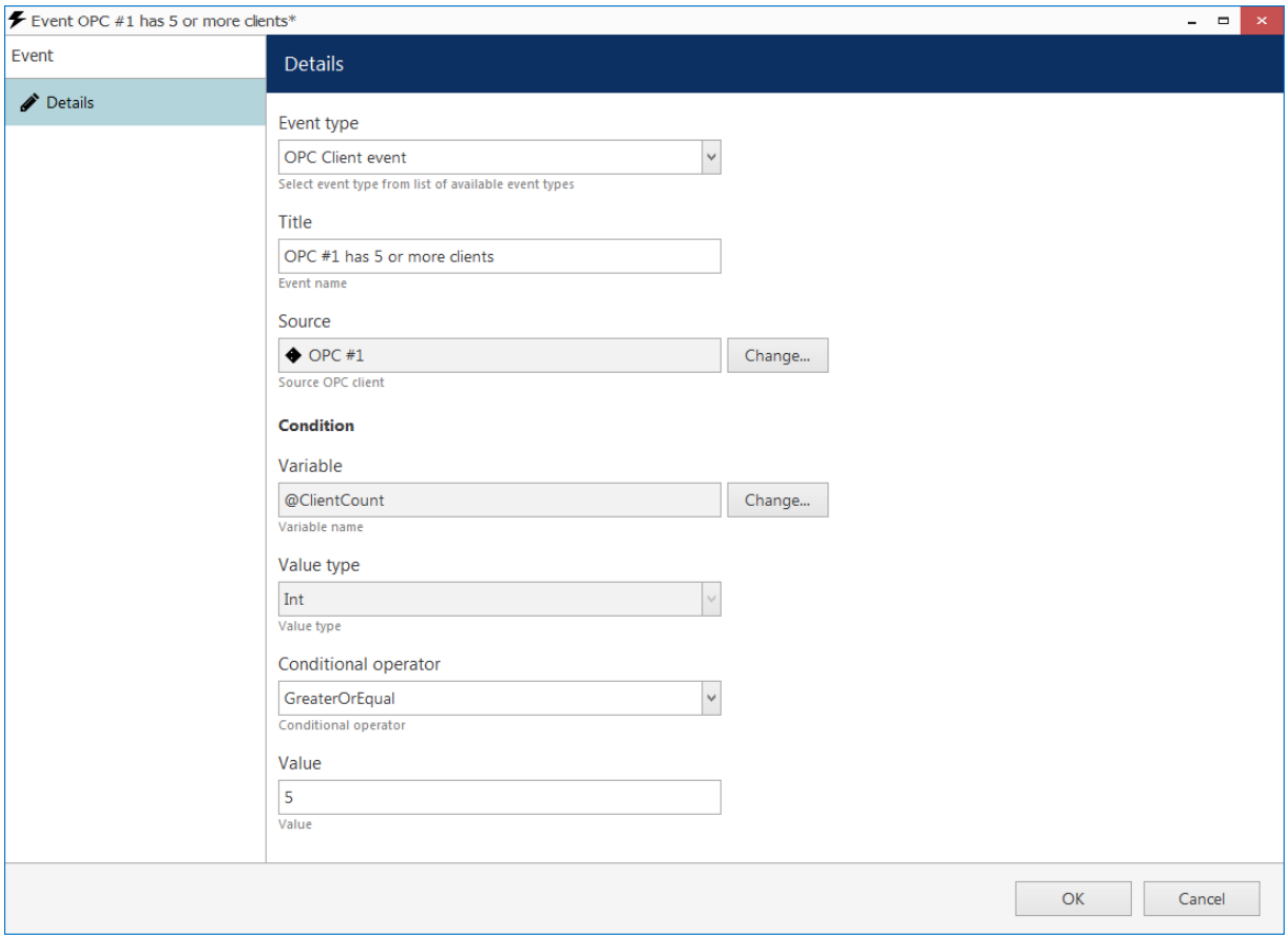
Other Events

Events having no special category (or, at this point, unique), are grouped under *Other events*.

OPC Client Event

Data received from OPC servers can be analyzed - compared to specified values using conditional operators - so that an event is triggered when the target OPC node value meets the defined condition.

For this type of event to work, there should be at least one OPC server configuration available with at least one data node.



Settings:

- **Title**: user-defined event name
- **Source**: OPC client configuration (connection to an OPC server)
- **Condition**: defines a requirement for the OPC data item that will trigger the event
  - **Variable**: OPC data node, must be of compatible type and have a read permission
  - **Value type**: one of the standard data types, auto detected
  - **Conditional** operator: list of possible conditional operators, depends on the data type
  - **Value**: value to compare the variable to, must match the variable value type

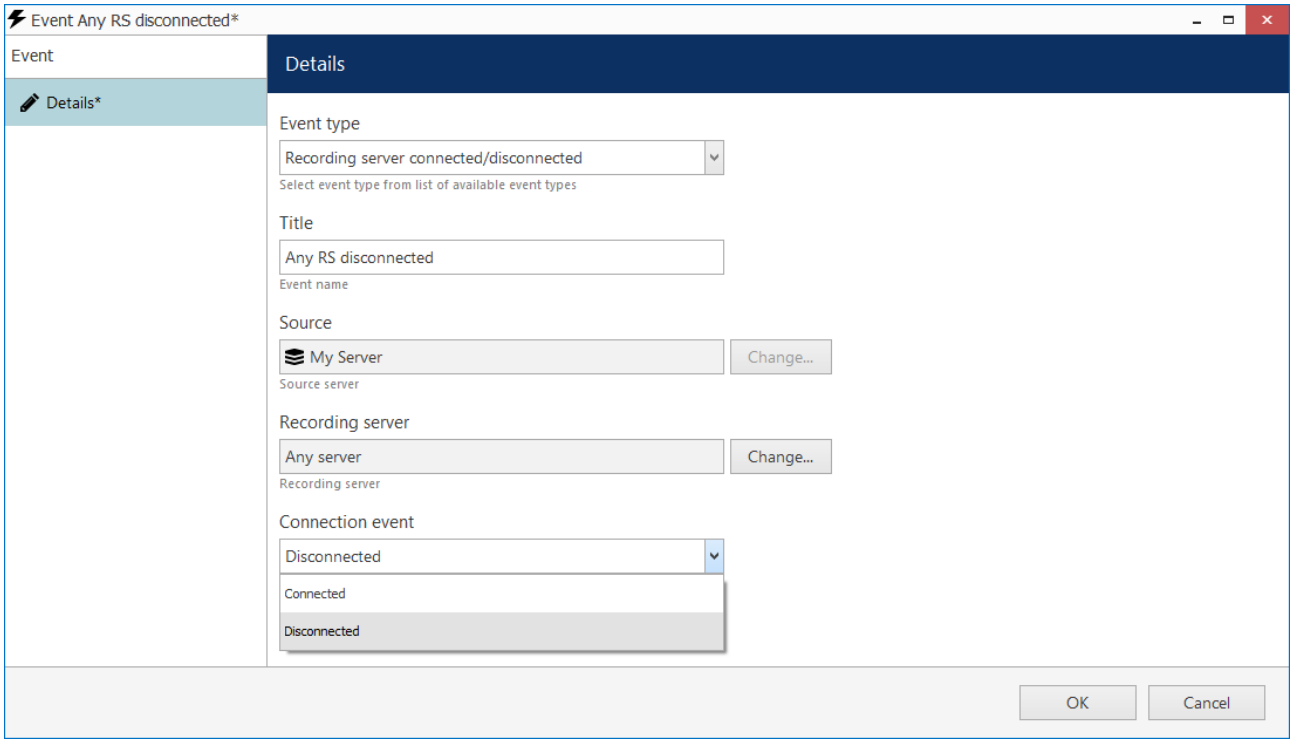
For some conditional operators, the *Value* field may be different, e.g., represent a range, a regular expression, or a bit mask. This depends on the selected data type and conditional operators available for it.

Recording Server Connected/Disconnected*

In the Macula Enterprise system, when a recording server goes down, this event will be triggered on the central management server. (Built-in events only include central server disconnection and failover activation events.) You can add both connection and disconnection events, or either one, for every recording server in the system.

Settings:

- **Title**: user-defined event name
- **Source**: central management server (unchangeable)
- **Recording server**: target secondary server to trigger the event, or Any to enable this event for all recording servers
- **Connection event**: connected/disconnected (one at a time)



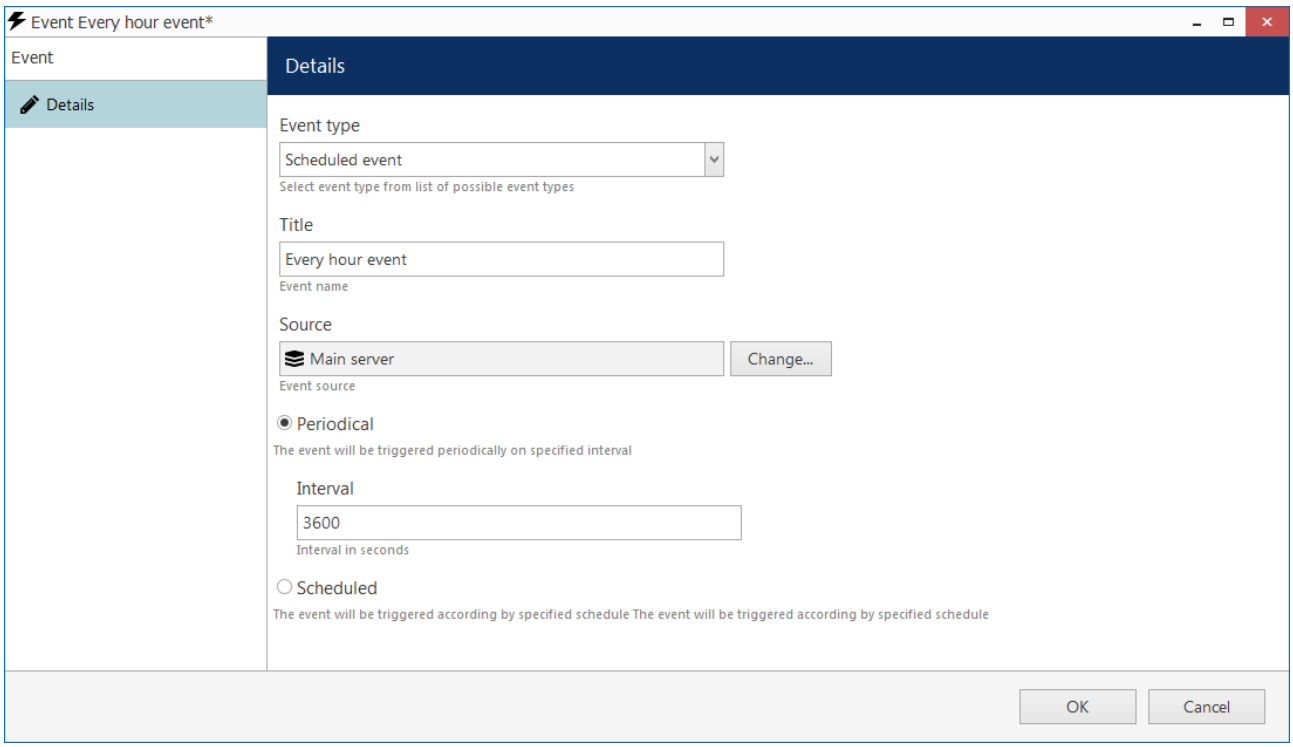
So, if you need to get a notification about a particular server going offline or online, choose that server in the event properties. To cover all recording servers with a single event, choose Any in the Recording server field: if your associated action is textual (email, alert, etc.), use the {ADDITION_INFORMATION} macro to display the name of the recording server in question.

From each recording server's side, there also exist two default (built-in) events: *Central server connected* and *Central server disconnected*. You do not need to add them manually, they will appear for each existing recording server.

*This feature is only available in Macula Enterprise edition.

Scheduled Event

The server can create automatic events on a daily or weekly basis, or at certain intervals. Such an event does not have any underlying source to originate from, it is simply generated by the system in the specified moment(s) of time. Note that the time defined here is server time.



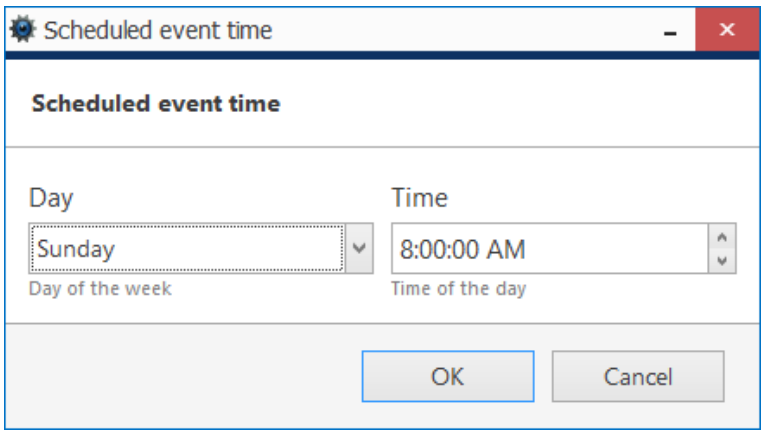
There are two types of automatic events: periodical and scheduled. Periodical events arise at the specified intervals, e.g., every hour or every ten minutes. Scheduled events follow the specified timetable, e.g., are triggered at 8AM every day.

For a scheduled event, you need to define:

- **Title**: user-defined event name
- **Source**: target server to generate the event on
- **Periodical**: choose this type if you need the events to be generated every N seconds
    - **Interval**: time interval in seconds between two automatically generated events, minimum interval is fifteen seconds
- **Scheduled**: choose this mode if you wish to build a timetable to serve as a basis for the event generation
    - **Event schedule**: weekly timetable for the event generation

Minimum time interval for the periodic event is 15 seconds and maximum is 86400 seconds (which is equal to 24 hours).

To add a schedule, simply click the *Add* button below and append as many items as you like. You can add multiple moments per day as well.



Remember that you can enter the time either manually from the keyboard or by clicking the timestamp elements and then using your mouse wheel, while still hovering your mouse cursor over the element that is being adjusted. To edit any of the items, select one and click *Edit*, or simply double-click an item; to remove, select one or many (use *CTRL+click* or *Shift+click* to select multiple items, or also *CTRL+A* to select all) and then click *Remove*.

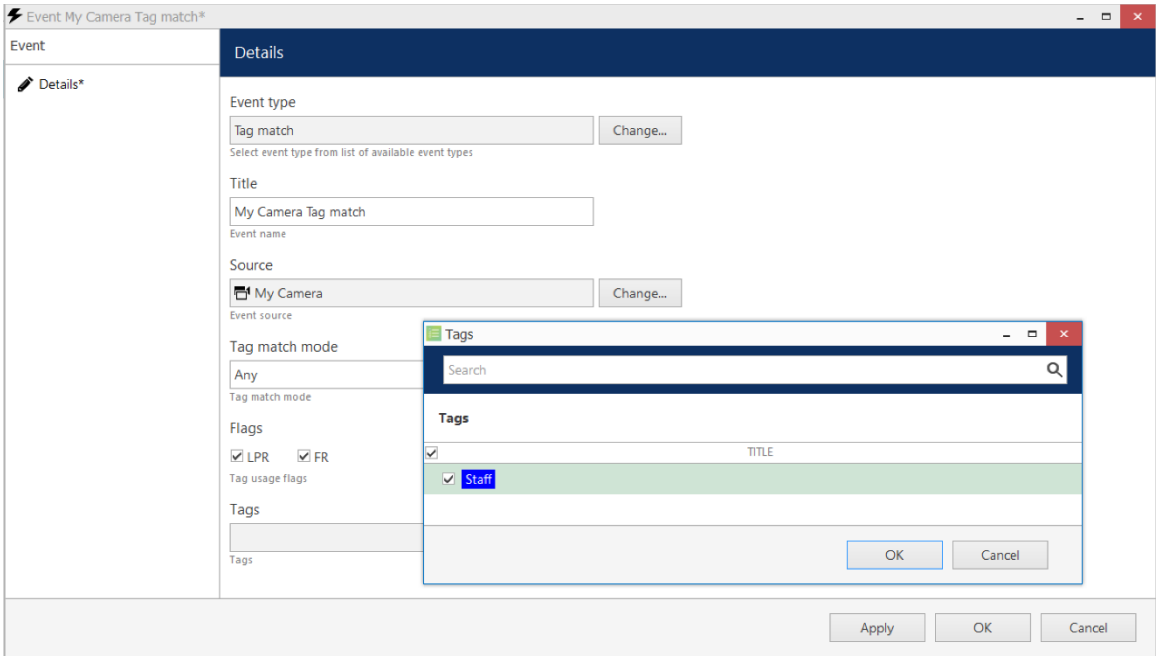
Tag Match

This event occurs when the Macula server receives a recognized car **number plate** or a **face** that matches one or more internal tags.

Settings:

- **Title**: user-defined event name
- **Source**: the video channel that serves as the event source (the one being analyzed)
- **Tag match mode**:
  - **No tags**: event will be triggered by items that are not tagged
  - **Any**: the item matches one or more (at least one) of the tags selected below
  - **All**: the recognition results must match all tags specified below
  - **Not any**: the event is triggered if the recognition results do not match any of the specified tags
- **Flags**: choose if you want to use LPR, FR, or both recognition results to trigger the events
- **Tags**: define the tag list, if required

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



You can use as many tags as you need in each event.

Video Wall*

This type of event is raised when the **video wall state is changed**. This happens, when objects are sent to video wall from the resources' menu in Macula Monitor, when they pop up automatically based on another event, or when users manage the video wall via dedicated tab in the Macula Monitor application. Note that events of this type are **not generated** if screen contents are changed directly via **local** screen management - drag-and-drop or double-click.

Advanced options let you specifically define the nature of that change, the video wall screen and even the target viewport.

This event can happen on three levels, depending on the defined scope:

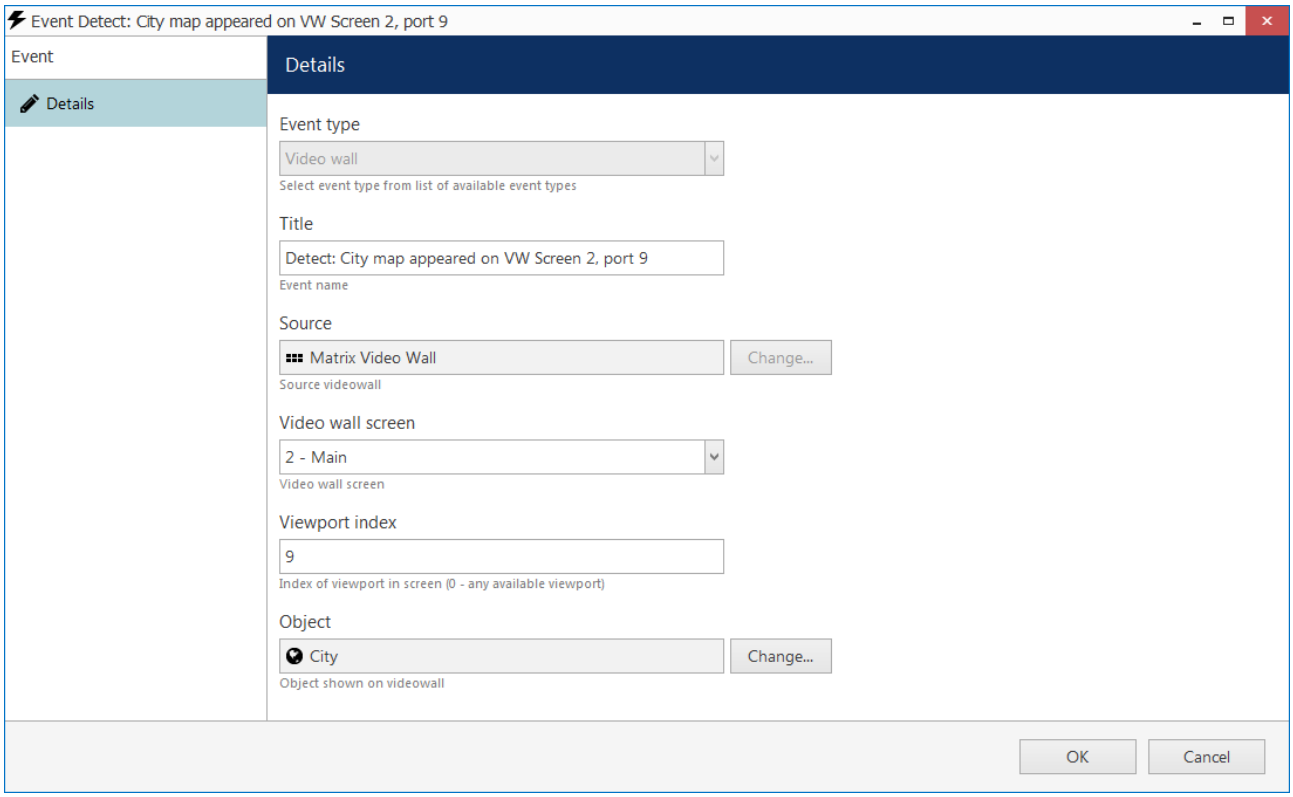
- any part of the video wall (video wall is defined, other settings set to *any*)
- specific video wall screen (video wall and its screen are defined, leaving viewport choice to *any*)
- specific viewport in the video wall screen (all settings defined)

The triggered events for all these areas will differ slightly (see examples below).

Available settings:

- **Title**: user-defined event name
- **Source**: video wall
- **Mode**: the type of changes
  - *Updated*: **any change** in the specified location (any or a specific object has been placed on or removed from the target location)
  - *Added*: the target object has been added to the specified location for the very **first time**
  - *Removed*: the target object has been **completely removed** from the target location
- **Video wall screen:** target video wall display
- **Viewport index:** number of the port to trigger the event, set 0 (zero) for any viewport
- **Object:** any object (if *updated*), or a specific map/channel (*updated/added/removed*)

Note that the target object must be specified for *added/removed* modes: there are no events for "any object added" or "any object removed". These two modes are intended to be used with concrete objects. If you do not care, which object was added or removed, use the *updated* mode.



The viewports are numbered starting from 1, from top to bottom and from left to right. Zero index means the event will be triggered, when the target object appears in any viewport of the target video wall display.

Event Examples:

1) An event is set to be produced when Channel S is *removed*. Depending on the defined settings, the event triggering will differ in the following way:

- if only **video wall** is defined without any details: event will be triggered after all instances of Channel S are removed. In other words, if Channel S is present several times on different video wall screens, the *Removed* event will only be triggered after the last instance of Channel S is removed, and the exact video wall screen or viewport do not matter.
- if a **video wall screen** is defined: same behavior but limited to this specific screen. If Channel S is currently displayed on other video wall screens, its presence is ignored. The last Channel S instance removed from the target screen will trigger the event.
- if a specific **viewport** is defined: the event will be triggered every time Channel S is removed or replaced by any other channel.

2) Event settings are set to maximum precision: video wall, video wall screen, and viewport are specified. In this case, the event area is limited to the **viewport**, and replacing Channel E with Channel X will trigger the following events (if they have been set up):

- *Removed* event for Channel E
- *Added* event for Channel X

- *Updated* event (no object needs to be specified)

3) The event is set to be generated when Channel Y is *added*. Consider the following scenarios:

- only video wall or video wall screen is defined for the event; the target video wall screen has a 2x2 layout, and:
    - Channel Y pops up in any viewport, filling in an empty space or replacing any other channel: event is **triggered**
    - Channel Y pops up again in the same viewport, replacing itself (so there are no changes): event is **not triggered**
    - Channel Y is then displayed in another viewport (so that it now appear in two viewports): event is **not triggered**
- video wall, its screen and a viewport index are defined:
    - every time Channel Y pops up or is placed into the target viewport, the event is **triggered**

*****This feature is only available in Macula Enterprise edition.

⚠ Removing and adding event sources again (e.g., deleting and creating edge VCA rule with the same name) may render them **unusable** if they are already included in the *Event & Action* configuration. Make sure to verify the event operability and then re-create and re-insert the event after modifying it, if necessary.

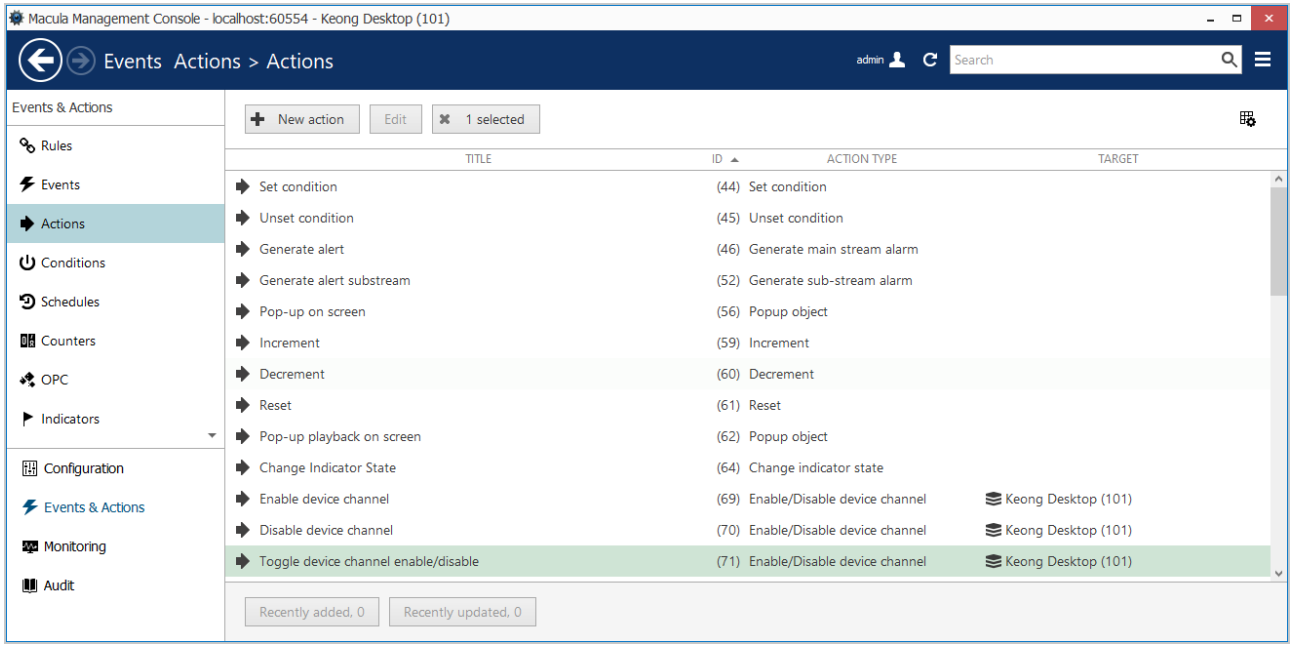
9.5 Defaults Actions

Each item - server, channel, or other resource - has a set of default actions that have identical behavior on all servers and cannot be altered (edited) or deleted. These are:

- **Generate Alert**: generate an alarm that can be used as recording basis in recording profiles; this action is available for each channel
- **Generate Alert Substream**: generate an alarm that can be used as recording basis in recording profiles; this action is available for each channel substream
- **Send Global Event**: send a global event notification to all servers; this action is available for each defined global event
- **Pop-up On Screen**: display the object on all Macula Monitor windows that accept pop-ups of the target object type; action is available for channels, maps and shared layouts
- **Pop-up Playback On Screen**: display instant playback for a channel in Macula Monitor application while keeping the live view mode; action is available for all channels
- **Disable channel**: change the target channel state by disabling it; the action is visible on each server, allowing you to choose the target channel when creating the event rule
- **Enable channel**: change the target channel state by enabling it*; the action is visible on each server, allowing you to choose the target channel when creating the event rule
- **Enable device channel VA:** Turn on the Video Analytics attached to the device Channels. You must preconfigure VA inside the Channel settings to trigger this Action with the particular Channel.
- **Disable device channel VA:** Turn off the Video Analytics attached to the device Channels. You must preconfigure VA inside the Channel settings to trigger this Action with the particular Channel.
- **Set Condition**: change the target condition state to *ON*; this action is available for each condition
- **Unset Condition**: change the target condition state to *OFF*; this action is available for each condition
- **Increment/Decrement/Reset**: change counter value; this action is available for each software counter
- **Send global event**: broadcast a global notification to all servers; this action is available for every global event

*Make sure your license has enough free channels for this action to work properly.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



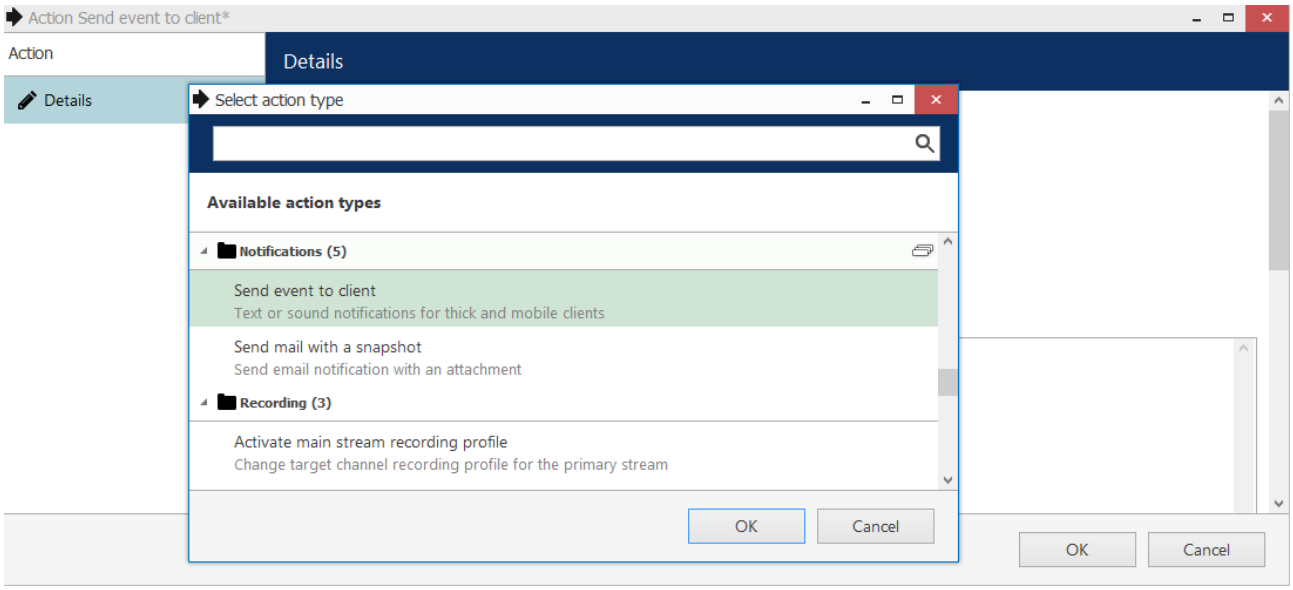
When you generate an **alert** for main stream or substream, all channels having alert-based recording enabled will start recording for the duration of time period defined in the profile as **post-recording time**; after that, the profile operation will be terminated and target channel will return to its normal recording configuration.

Default actions are available in the *Event & Action Configurator* and can be used in the same way as the user-defined actions. These actions are not listed under Actions as they are not configurable.

9.6 Add Actions

In addition to the default actions, certain types of actions can be added manually and customized.

To access action management in Macula Console, choose the *Events & Actions* section and select *Actions* from the menu on the left. In order to create an action, click the + *New action* button on the upper panel; an action configuration dialog box will open. It is also possible to add actions as you go using the *Event & Action Configurator*.



All available actions are grouped according to their purpose. Choose your desired action type from the list to see action-specific settings.

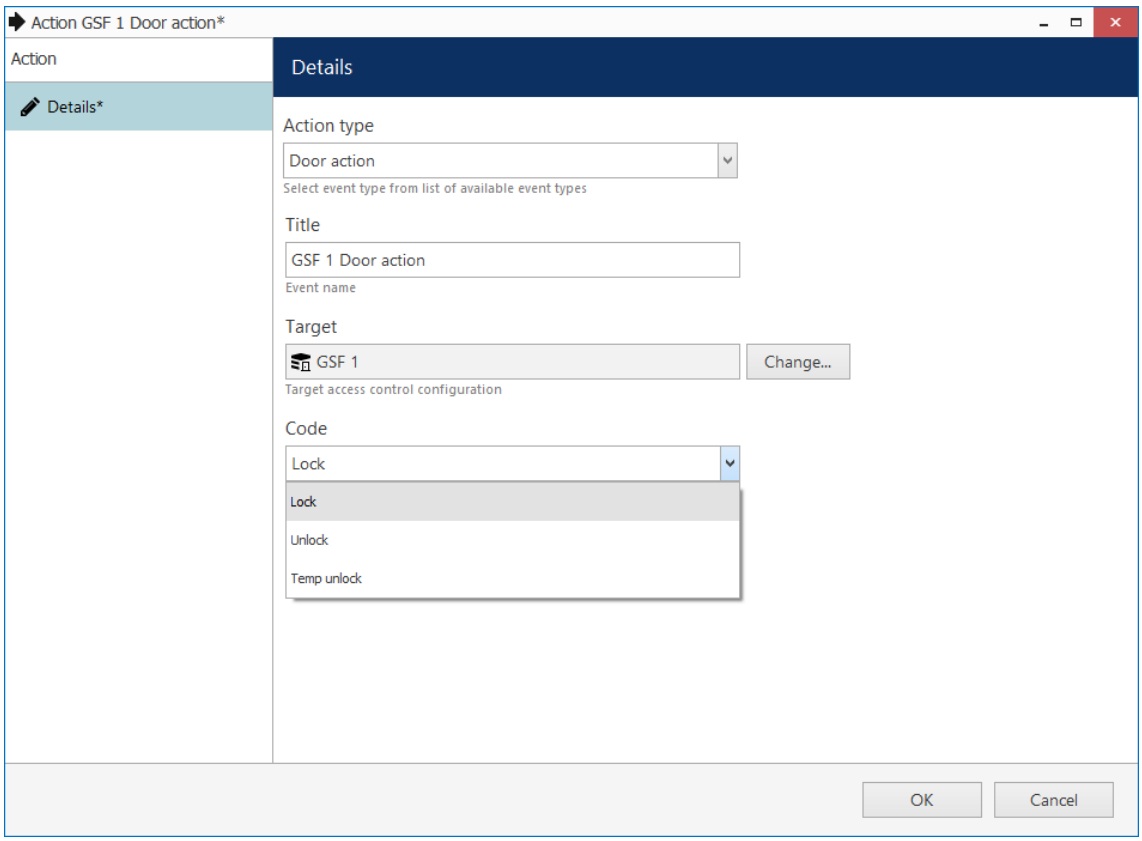
Access Control Actions

Actions in these sections are related to the access control integrations. Typically, these are used to control the door state.

Door Action

If you have a third-party access control module connected, you can change the door state from here.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



As a **target**, specify the access control configuration added earlier. The specific door for this action will be chosen at the rule creation step, allowing you to use this action for many different doors within the same Visual Access System configuration.

Available **action codes** here are: lock, unlock, and temporarily unlock (standard access control door states). Once the action is triggered, the corresponding command will be sent to the access control software.

Channel Related Actions

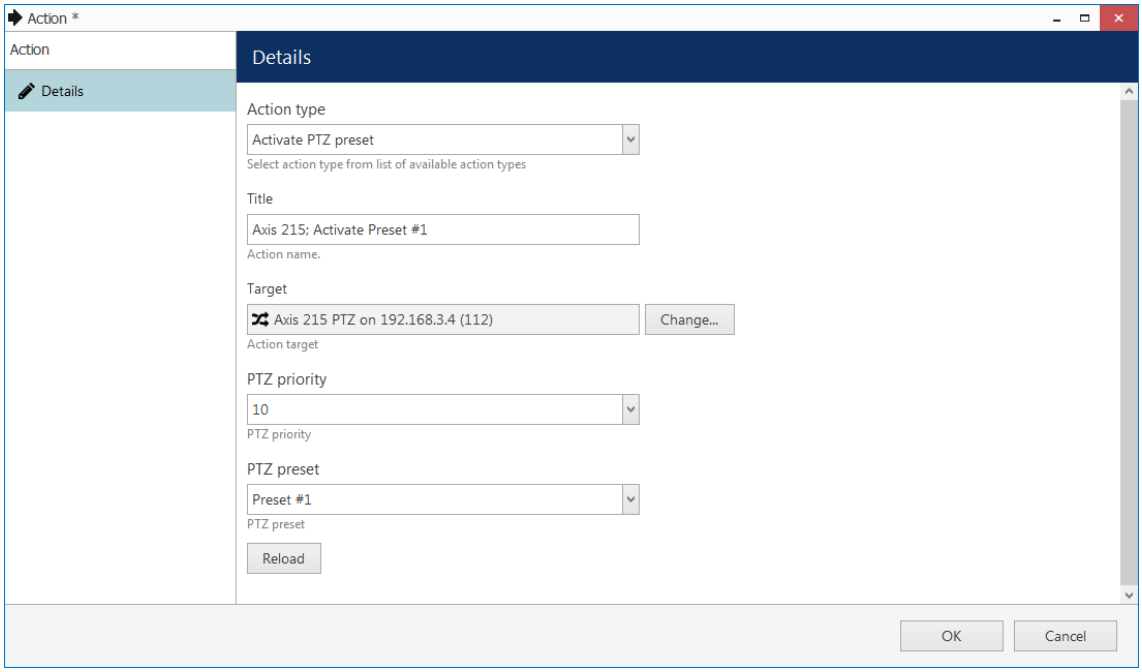
Actions in this category have direct relation to channels, e.g., PTZ presets and tours, digital output (DO) state change etc.

Activate PTZ Preset

This action type allows you to make a PTZ camera go to a specific pre-configured preset. You just need to specify:

- **Title**: a user-defined action name
- **Target**: the target device which is to accept the PTZ command
- **PTZ priority**: priority to execute PTZ action with (0 = lowest, 10 = highest, higher priority will override tours and user commands*)
- **Preset**: pick one of the automatically loaded target device presets from the drop-down list (you might need to create some first via Macula Monitor)

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

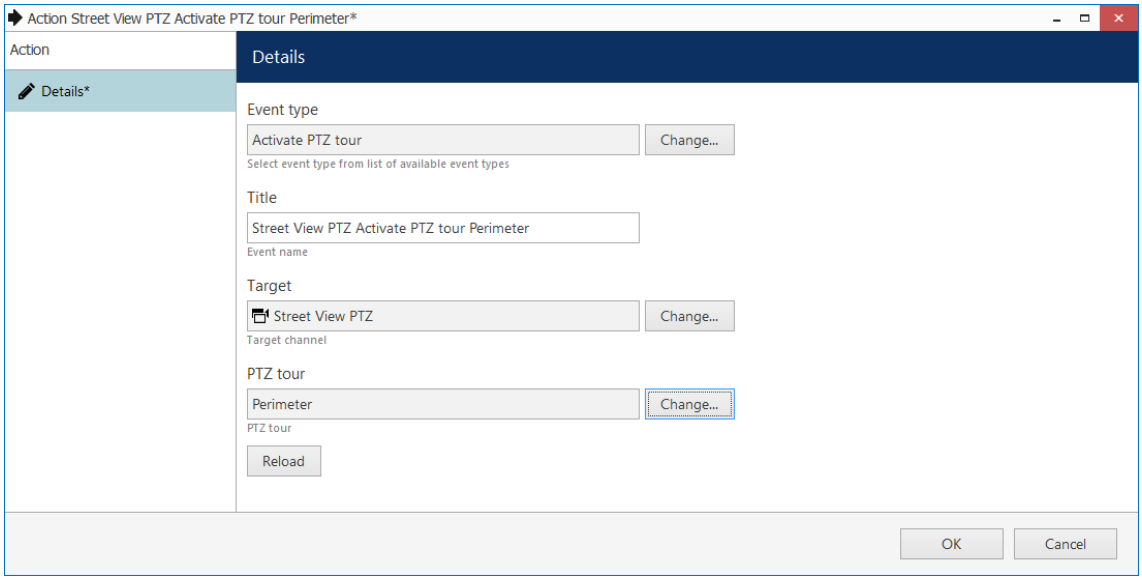


*PTZ priority parameter is used when two or more simultaneous PTZ command requests (either from action or from direct user input) are sent at the same time. When this happens, request with a higher priority is fulfilled while request with a lower priority is delayed for ten seconds. Default **PTZ priority** for all actions is equal to **five** (medium priority), which also coincides with the **default per-user** PTZ priority. You can assign any action a higher PTZ priority (six to ten) or a lower one (four to zero) by editing the *Activate PTZ Preset* action properties. All PTZ tours have zero priority.

Use the *Reload* button to refresh the list of presets: this will be useful if you have created new presets while keeping the action creation dialog box open.

Activate PTZ Tour

This action is similar to the previous one but instead of activating a single PTZ profile you run a series of presets called a PTZ tour. PTZ tours must be pre-created via Macula Monitor application. For each tour, you define the order of presets and their duration.



Action: activate a custom pre-configured PTZ tour

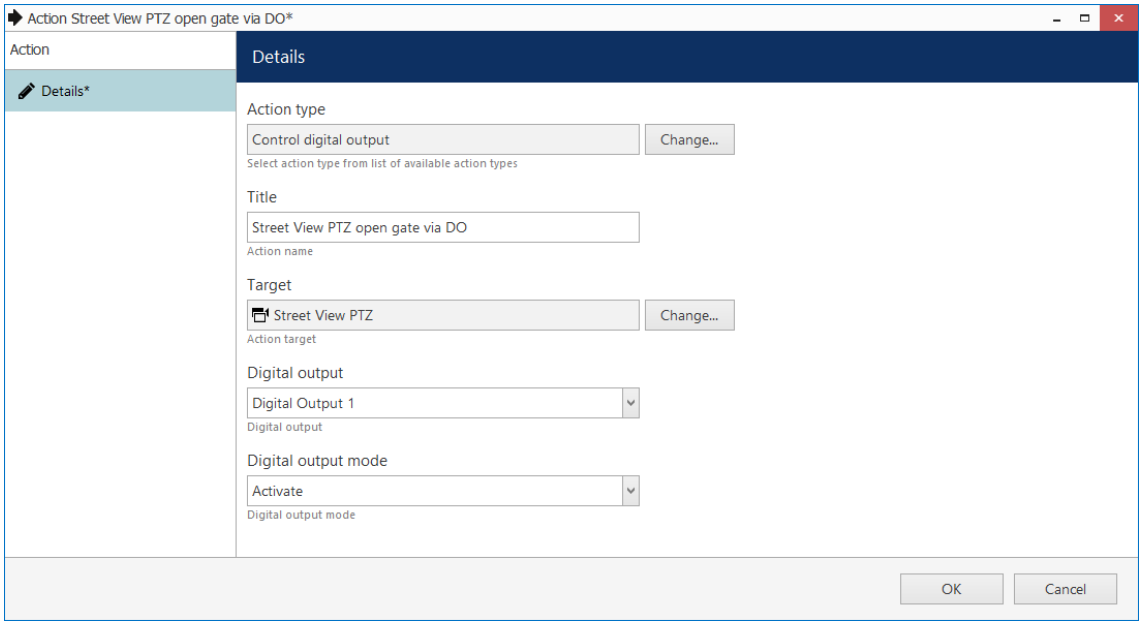
- **Title**: the user-defined action name
- **Target**: the target channel that has a pre-configured PTZ tour
- **PTZ tour**: the target PTZ preset sequence to be activated

When this action is executed, the target PTZ tour is activated and looped endlessly. You can stop the tour manually via Macula Monitor or Macula Mobile application. Tours that do not have the autostart property will also be stopped when the Macula server is restarted.

Control Digital Output

Devices having relay (digital) outputs (Dos) can have them triggered as a result of the *Control digital output* action. You are asked to enter the following details for this action type:

- **Title**: user-defined action name, by default it is >*Activate PTZ preset*>, suggesting that before and after >> arrows you can insert the camera name and DO number/target – or, alternatively, re-define the whole title according to your own naming convention
- **Target**: the target device which is to accept the digital input control command
- **Digital Output**: pick one of the available Dos of the target device to be triggered
- **Digital Output Mode**: choose whether an activation or deactivation command is sent to the target relay output



Digital output(s) must be enabled in channel settings for the target camera; otherwise, you not will see any available Dos in the drop-down list after selecting the target device. Also, make sure that digital output operation has been allowed via device Web interface.

Device Action

This action is reserved for special device-side actions like wiper control, arm/disarm, lights ON/OFF etc. This functionality depends on the device integration.

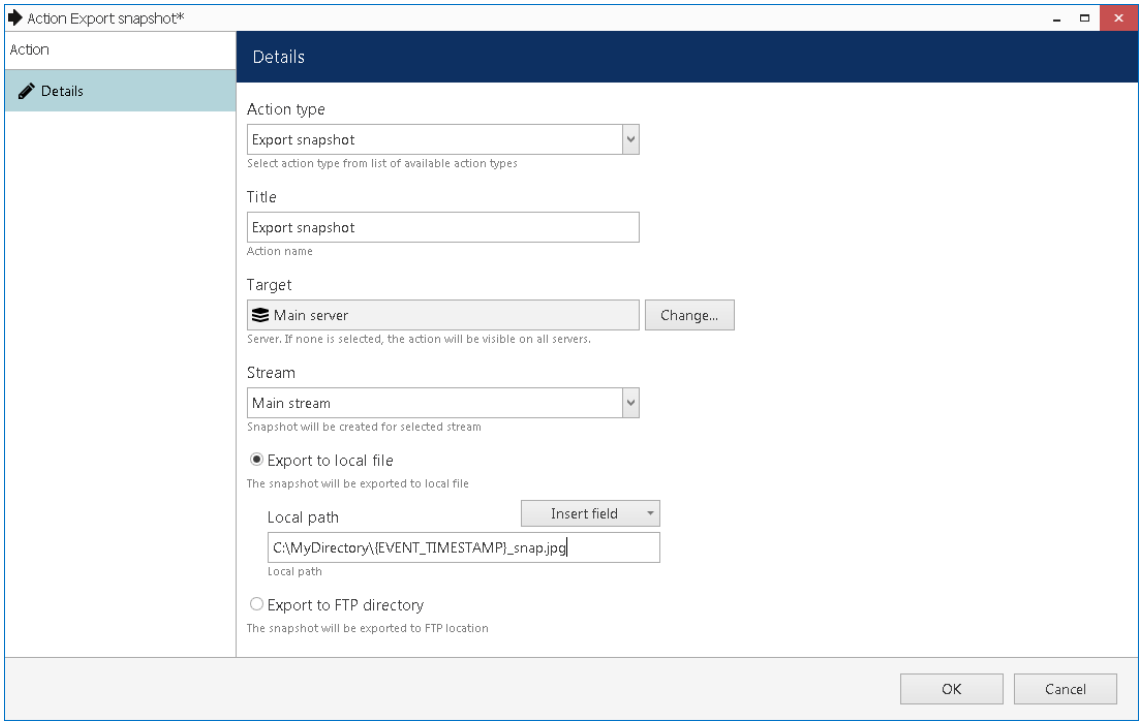
- **Title**: the user-defined action name
- **Target**: the target channel to accept the command
- **Device action**: integration-specific device action
- **Parameter**: command-specific parameter, if required (e.g., alarm code for arming/disarming alarm panels)

Currently, device actions are only supported for few devices. If you do not see any available action for your camera, try using the *Send HTTP Request* action described further: that action allows you to enter a CGI/HTTP command from device API.

The *Parameter* field is integration-specific. For example, when working with Satel devices, you can use device action to arm/disarm the panel, providing the code in the *Parameter* field.

Export Snapshot

A snapshot from the main or secondary stream of any channel can be saved as a result of an action. The file can be saved either locally (on the target server) or to a remote server (FTP).



The following settings are to be defined here:

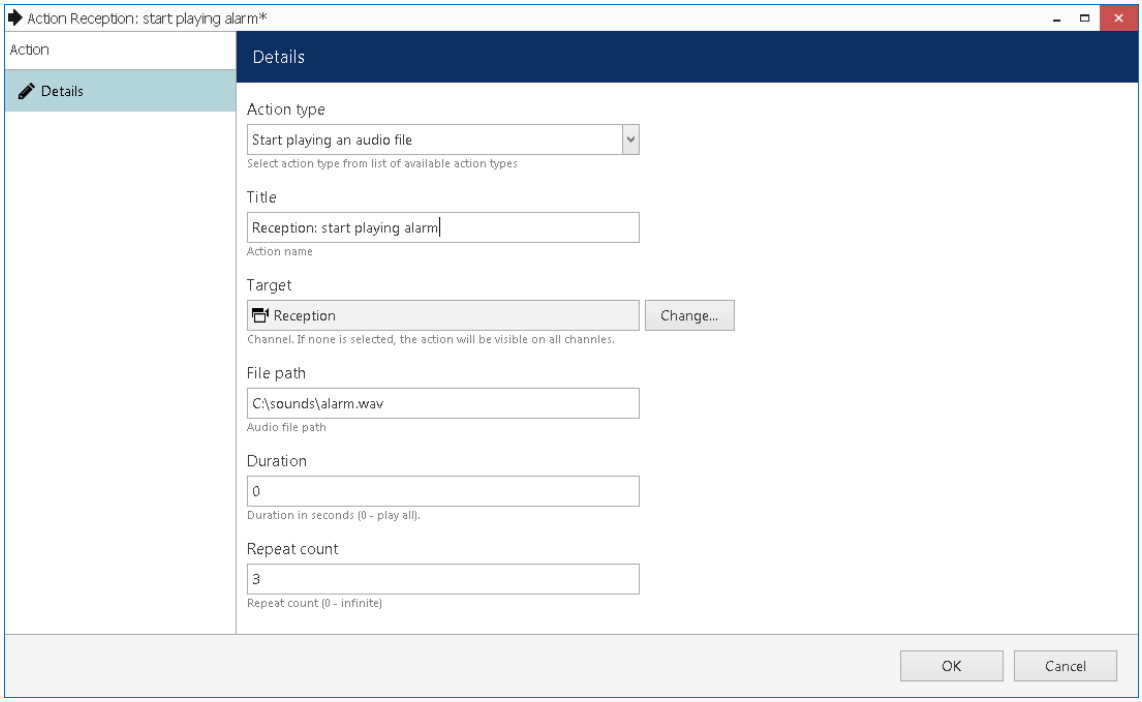
- **Title**: user-defined action name
- **Target**: the server to execute this action on
- **Stream**: main stream or substream of the target channel (the channel is to be defined at the action rule creation step)
- **Enable subtitles**: enable this setting to activate subtitles and expand additional settings
  - **Text**: subtitle text (plain text and/or macros)
  - **Position**: subtitle alignment (top/bottom, left/right, corners)
  - **Font**: subtitle font (choose from the system dialog)
  - **Colors**: background (transparent by default), foreground (text itself), shadow (text shadow)
- **Export to local file**: the snapshot will be saved to the target server chosen above using the specified path

    - **Local path**: full path and filename, e.g., C:\MyDirectory\{EVENT_SOURCE_TITLE}_{EVENT_TIMESTAMP}.jpg
- **Export to FTP directory**: the snapshot will be saved onto a different machine that is not a part of the system
    - **FTP path**: full path and filename
    - **Host**: target machine's IP address or domain name
    - **Port**: port to be used for FTP connection
    - **Username**: user account name to connect to the remote server
    - **Set password**: specify a password, if required to log into the remote server

You can include text macros in the filename, for example, insert timestamps and event source title automatically to create files with different names every time the action is executed.

Start Playing an Audio File

It is possible to send an audio file to the connected device in case it has a built-in or a connected speaker: Macula server can use a .wav file to send audio to the remote camera or video server.



You need to specify:

- **Title**: user-defined action name
- **Target**: the channel for the sound to be sent to (if none selected, the action will be available for all channels)
- **File path**: full path to the local ***.wav** file that should be used for audio output
- **Duration**: the amount of time for the audio to be played (set zero to play the whole file)
- **Repeat count**: the number of times for the audio file to be repeated (set zero for the file to played non-stop)

If you need the audio to be played continuously until another event stops it, set the *Repeat count* parameter to zero and use the *Stop playing an audio file* action to terminate the playback.

Stop Playing an Audio File

This action is used as a complement for the *Start playing an audio* file action: it stops the audio transmission in case you need to force stop it earlier than specified in the *Start playing an audio file* action, e.g., if the starting action lets the audio file to be played infinitely.

The following settings are available here:

- **Title**: user-defined action name
- **Target**: target channel (leave *none* for the action to be available for any channel)

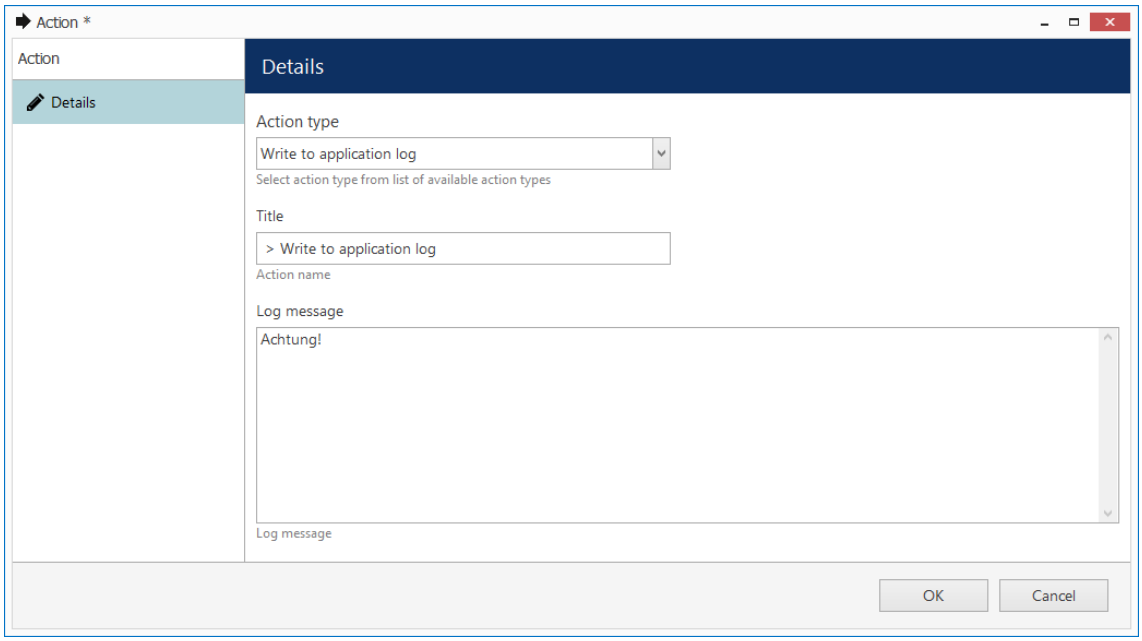
Logging

In addition to default audit log, you can choose custom events to be appended to the Macula server audit log or to Windows application log.

Write to Application Log

The *Application log* action type allows you to write a log entry into the Windows Application log, which will be accessible via Windows Event Viewer. The log entry level is *Information* and entry source is Macula Server. You can define:

- **Title**: a use-defined action name inside the Macula Console; by default it is *Write to Application log*
- **Log Message**: the message text to appear in Windows Application log



Use the *Insert Field* button on the right-hand side (it appears when you have clicked inside the text area) or right-click the text area and choose *Insert* to add a text macro (see *Action Parameters* further in this topic for details).

Write to Audit Log

The *Audit log* action type is similar to that of *Application log*: it allows you to write a log entry into the Macula own Audit log, which will be accessible via Macula Console, in the *Audit* section. The log entry is added in the Server audio section and its event type will be *User defined*. You can set:

- **Title**: a use-defined action name inside to be used in E&A; by default it is *Write to Audit log*
- **Log Message**: the message text to appear in the Audit log

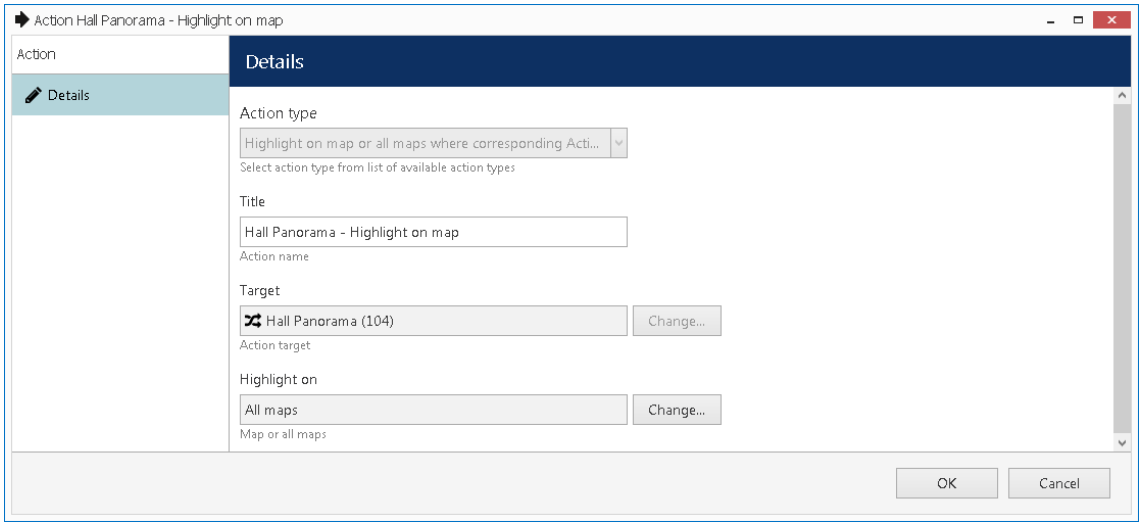
Use the *Insert Field* button on the right-hand side (it appears when you have clicked inside the text area) or right-click the text area and choose *Insert* to add a text macro (see *Action Parameters* further in this topic for details).

Notifications

Actions in this section allow you to send all kinds of alerts to clients and also email notifications.

Highlight On Map

If your target device appears on one or more maps, you can visually accent it on the map as a result of the triggered event. It is possible to define one particular map or make the device become highlighted on all maps where is has been placed.



The following objects are supported for this action as targets:

- **Channels** (channel markers will be highlighted)
- **User buttons** (user button markers will be highlighted)

Pop Up Object On Screen

You can set up individual channels, maps and layouts to appear on a specific **video wall** display as a result of some triggered event, e.g. motion detected in certain regions. If you wish an object to pop up in all connected Macula Monitor applications without using video walls, use the built-in (default) event of the *Pop up on screen* type.

Additional setup is required from the Macula Monitor application side:
- shared layouts should be pre-created in order to be used in action creation
- target Macula Monitor window must be allowed to accept either channels/maps or layouts

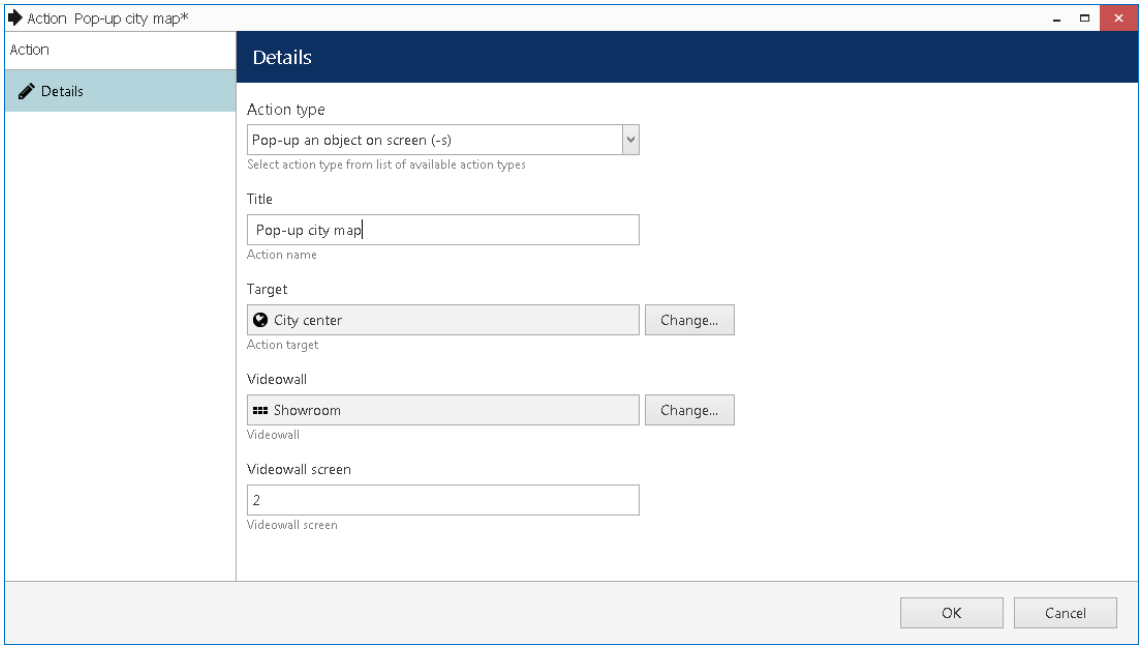
- target Macula Monitor window must be set to be a part of the target video wall

What you need to specify in the action properties is:

- **Title**: user-defined action name, by default it is *[channel] Pop up and object on screen [Video wall name]*
- **Target**: a channel, map or a pre-created shared layout to appear on the screen
- **Video wall**: target video wall for the object to appear on
- **Video wall screen**: a specific display in the video wall layout for your object to appear on
- **Viewport index**: the exact position of the video output cell in the grid (starting from 1, left to right, top to bottom), leave 0 to use the first available viewport

If you do not care, which viewport is used for popup, leave the viewport index parameter equal to 0. This will send the popup object to the first empty viewport; if all viewports are occupied, the object will pop up to the first non-locked one. When all viewports are occupied and locked and the viewport index is set to 0 (=any viewport), the popup will not work on that screen.

If the target viewport is set (is different from 0) but it is occupied and locked on the Macula Monitor side, the target channel will force pop up anyway, and the viewport state will stay locked.



You can create new maps right from the object selection dialog in case you have not created them beforehand.

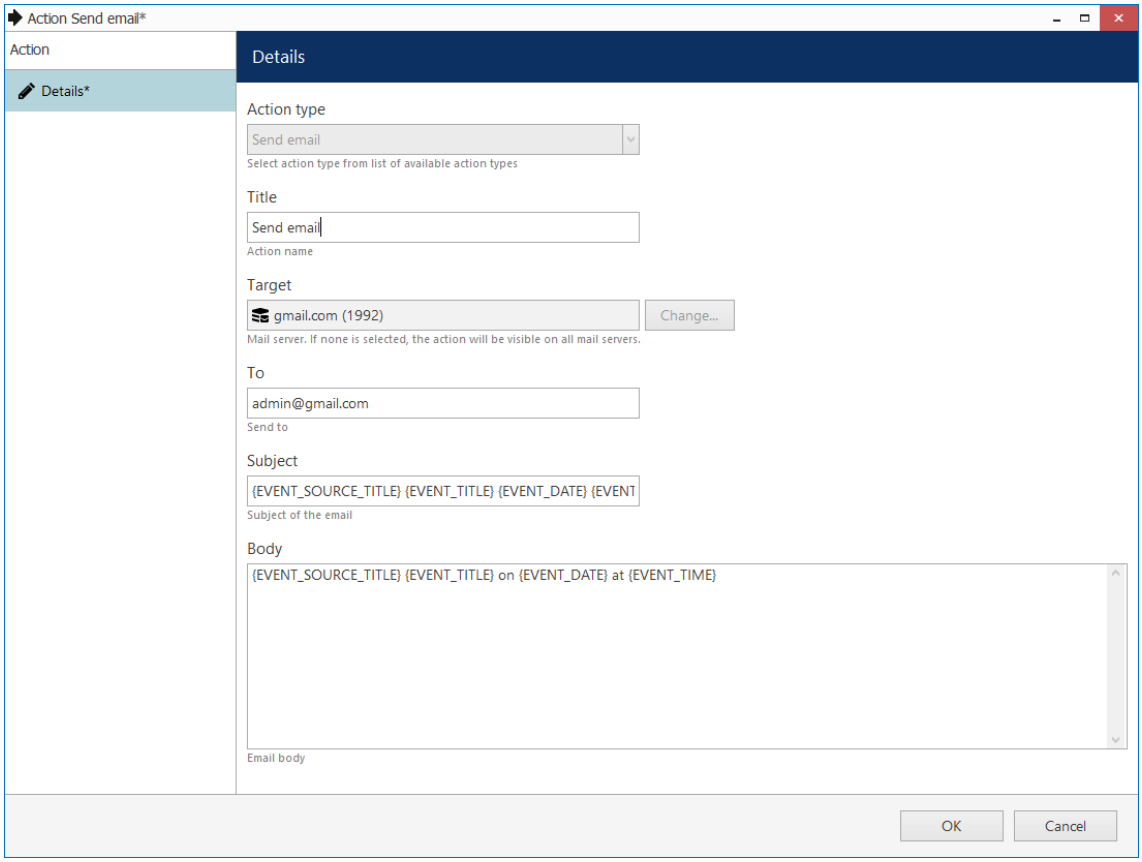
Send Email

In order to send an email notification, you are requested to define the following values in the action settings:

- **Title**: a user-defined action name; by default it is *<mailserver> Send email*, you can insert the device name and target email address - or, alternatively, you can re-define the whole title according to your own naming convention

- **Target**: specify the SMTP server to be used for email sending; if none are selected, the action will be available for selection on any of the existing configured mail servers when creating a rule
- **To**: notification recipient email address
- **Subject**: email notification subject (use the *Insert field* button to add text macros)
- **Body**: email notification body text (use the *Insert field* button to add text macros)

Configure your SMTP server(s) before creating email-related actions.



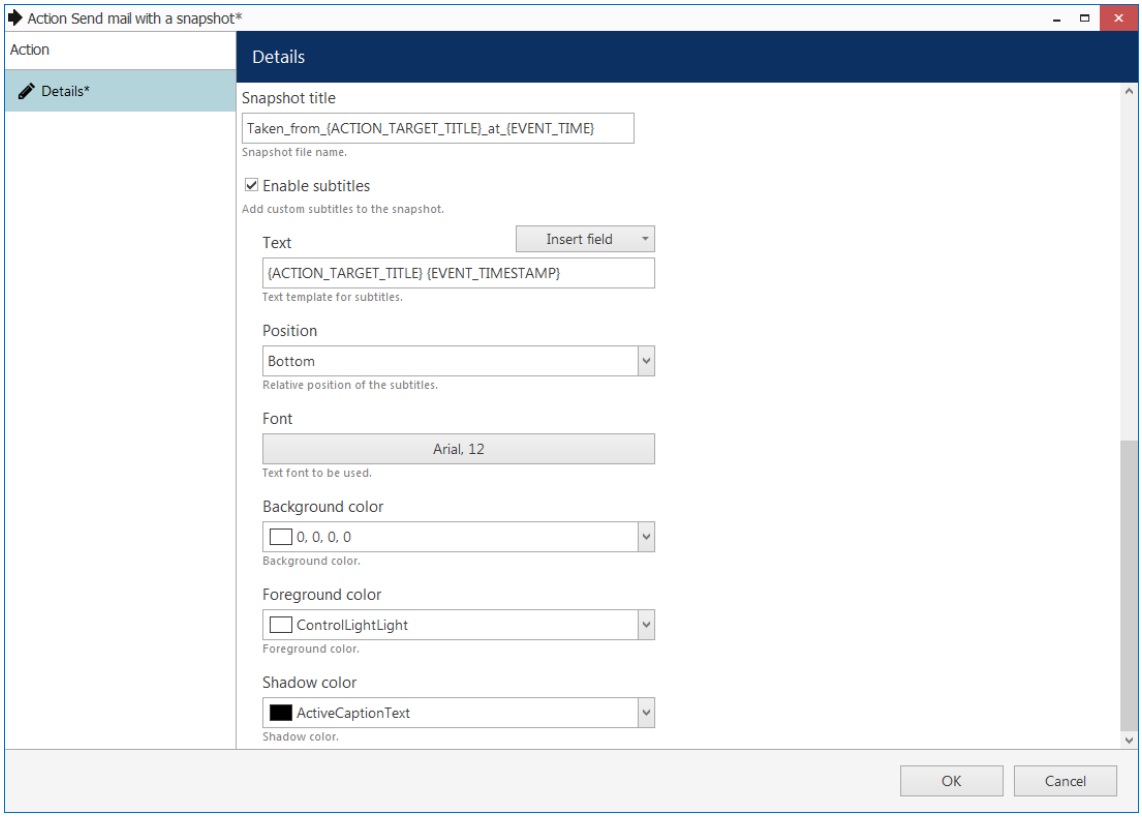
Send Email with a Snapshot

This action is similar to the *Send Email* action described above, with all the settings being the same except for one: it allows to attach a snapshot from a channel and send it together with the email. The channel is specified when creating a rule with this action.

Additional setting:

- **Attach snapshot**: choose if you want to take a snapshot of main stream or substream of a channel and deliver it together with the message
- **Snapshot title**: user-defined file name, e.g., Snap.jpg, or Snap_{EVENT_TIME}_from_{ACTION_PARAMETER_TITLE}.jpg
- **Enable subtitles**: enable this setting to activate subtitles and expand additional settings
  - **Text**: subtitle text (plain text and/or macros)
  - **Position**: subtitle alignment (top/bottom, left/right, corners)
  - **Font**: subtitle font (choose from the system dialog)
  - **Colors**: background (transparent by default), foreground (text itself), shadow (text shadow)

The subtitles will be hard merged with the exported image.



In the *Send Email with a Snapshot* action, you only need to define whether this specific action will take a snapshot from the main or from the secondary stream. Actual channel for the snapshot to be taken from will be defined when you create a rule involving this action:

- if the source event originates from some channel, that channel will be automatically used as a snapshot source; you will be able to change the target channel using the *Snapshot source* button below the rule map in the E&A Configurator
- if the source event does not come from a channel (e.g., user button click event), you will have an option to define the target channel using the *Snapshot source* button below the rule map in the E&A Configurator

If you specify no snapshot source when creating the rule, a regular email will be sent. You will find more details on attaching the snapshot in the Rules section of this document.

Send MQTT Notification

This action uses a pre-configured MQTT Client to publish MQTT messages. You must have at least one MQTT Client in your server configuration, and a running MQTT broker to accept and broadcast the message. Message/connection settings are typical MQTT message properties; make sure your broker supports the settings you enter here.

Available settings:

- **Title**: action name that will appear in the E&A Configurator
- **Target**: pre-configured MQTT client; leave empty for the action to be available for all existing MQTT clients
- **Topic**: MQTT topic to be published

- **Text**: MQTT message text to be published
- **QoS**: required level of the MQTT quality of service

You can use macros in all text fields to pass parameters like {EVENT_TIMESTAMP} or {EVENT_TITLE}. To insert those, right-click the text field or use the *Insert text field* button.

Send SMS

Using this action, you can send short messages to the pre-defined numbers. GMS modems must be present in the server configuration for this action to work.

- You have to fill in the following:
- Title: user-defined action name
- Source: existing modem hardware to send the message
- Phone: the recipient's phone number in international format (cannot be left empty)
- Text: SMS text to be sent, right-click to insert text macros like {EVENT_SOURCE_TITLE}

Keep in mind the maximum possible SMS length when composing the message. Longer messages will be split into multiple SMS.

Send Event to Client

This action allows to send a push notification to all or specific client applications. This may be just a pop-up message, or an event in the channel notification area with a sound, or all of these combined.

Available settings:

- **Title**: user-defined (custom) action name that will appear in the E&A Configurator
- **Message**: notification body text (use the *Insert field* button to add text macros)
- **Display event in alerts**: mark this if you want a message to be appended to the Macula Monitor log in the *Alerts* section
- **Display a warning message box**: mark this if you want a **dialog box to pop up** on the Macula Monitor side (to be closed by the user)
- **Display event in notification panel**: the message will be shown in the **notification panel** of the live view of a specific channel (you will have to set the channel when creating the rule)
- **Display event in mobile application**: the message will be sent as a push notification to all **Macula Mobile clients** that have the target server configured
- **Play audio notification**: play a sound on the Macula Monitor side; sounds themselves are defined in each Macula Monitor application
    - **Audio notification**: sound notification number, from 1 to 10 (here, you just specify the number, actual sound is defined per client and may not coincide in different application instances)
- **Send event to specific user or user group**: show the notification only to a specific user or user group

Recording Related Actions

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Several actions are related to recording: these can change main and secondary stream recording profiles, as well as append new items into the archive, such as bookmarks.

Activate Recording Profile

Any of the existing recording profiles can be activated for the device of your choice as a result of a triggered event. You can separately activate **main** stream and **substream** recording: use the *Activate Recording Profile* action for main stream and the *Activate Substream Recording Profile* action for secondary stream. Enter action details as follows:

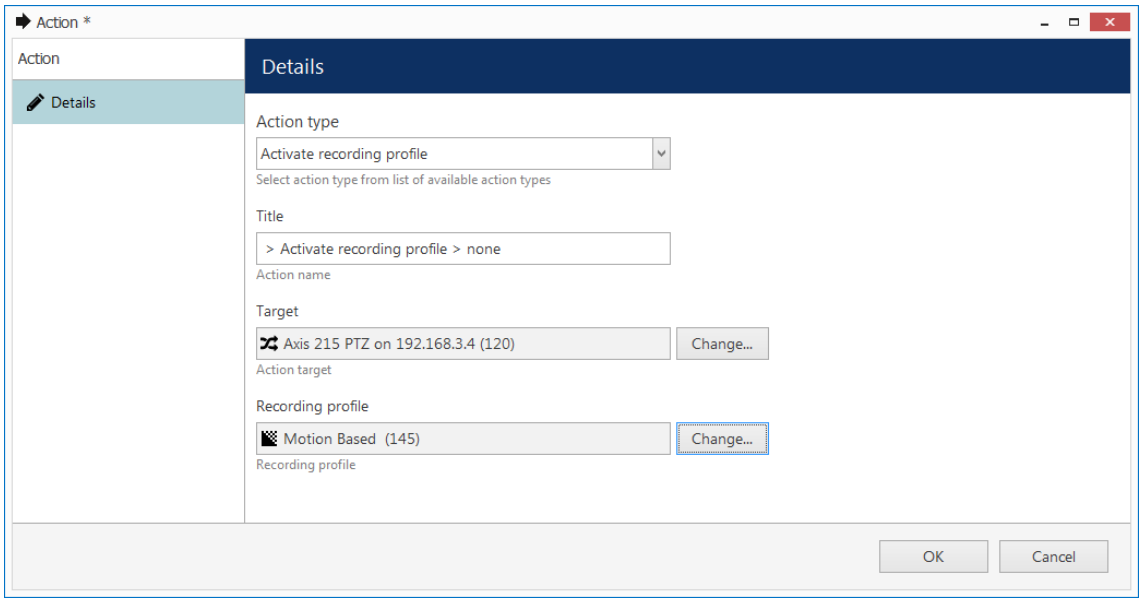
- **Title**: the user-defined action name
- **Target**: the target device for which recording is to be activate
- **Recording profile**: the pre-configured recording profile to be activated as an action; you will find profile configuration tips further in this section of the manual

The recording profiles are changed within the channel's recording configuration. Thus, for example, if the channel's recording configuration has a 3-second pre-recording duration, it will stay 3s for any recording profile you activate via E&A.

The recording profile is activated permanently; to switch to a different recording profile, use another action of the same type and different target profile.

Recording profile activation **cannot call off** the default recording configuration (the one currently assigned to the target channel); rather, **this action can only add more** recordings. Thus, channel default recording configuration must define the minimum required recording scheme (based on a single profile or on a schedule) and E&A scenarios will add to that.

Example: a channel is set to record based on motion. There are two user buttons: one of them sets the channel to *Constant recording*, and the other sets the *No recording* profile. Triggering the first button will activate constant recording, and triggering the second button will return channel recording to its default state (which is *Recording by motion*) instead of disabling the recording at all.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Recording profile activation **cannot call off** the default recording configuration (the one currently assigned to the target channel); rather, **this action can only add more** recordings. Thus, channel default recording configuration must define the minimum required recording scheme (based on a single profile or on a schedule) and E&A scenarios will add to that.

Example: a channel is set to record based on motion. There are two user buttons: one of them sets the channel to *Constant recording*, and the other sets the *No recording* profile. Triggering the first button will activate constant recording, and triggering the second button will return channel recording to its default state (which is *Recording by motion*) instead of disabling the recording at all.

Recording Triggering Examples

When channel recording profile includes **alert-based** recording, recording can be activated as a result of a *Generate Alert* type action and its engagement time is determined by the profile's *post-recording time* parameter. In this case, actual recording profile is not changed and the current recording profile is used (the one assigned to the channel through its recording configuration). The default (built-in) recording profiles have post-recording intervals of 10 seconds, which may be fine when conducting, e.g., motion-based recording (video is recorded for 10s after motion event), but may not be suitable for other types of events. In such case, you can pre-configure any number of different recording profiles and use them for action setup.

If a recording profile is triggered by an *Activate Recording Profile* type action, the recording profile used for the target channel is complemented with the profile triggered from E&A, and recording duration can be controlled using action delay timers.

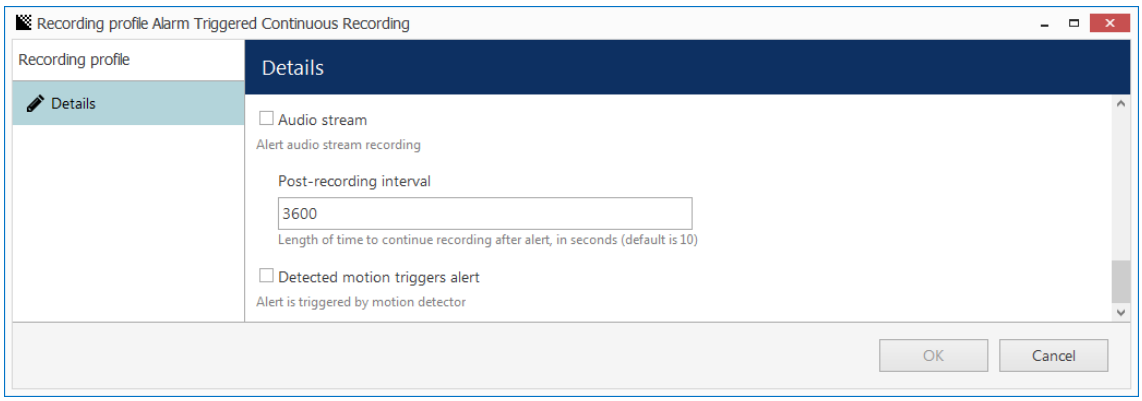
Scenario 1. The camera's recording configuration is normally motion-based. The action is intended to be used for recording based on digital input events, which are triggered when someone opens main entrance door; starting from that point, the video and audio streams will be recorded continuously for one minute.

- channel base recording configuration: motion-based video recording
- actions triggering recording profiles:
    - action #1 triggers a recording profile with continuous video + audio (e.g., built-in Continuous Recording profile)
    - action #2 triggers the built-in *No Recording* profile: as a result, channel recording is returned to its default (configured) state
    - action #2 is delayed for one minute using a Delay Timer

Scenario 2. The camera normally records continuous video with low FPS during the daytime, and does not record anything at night and during weekends. If camera VCA detects fire or smoke in the area, continuous recording at full frame rate will be conducted for 30 minutes.

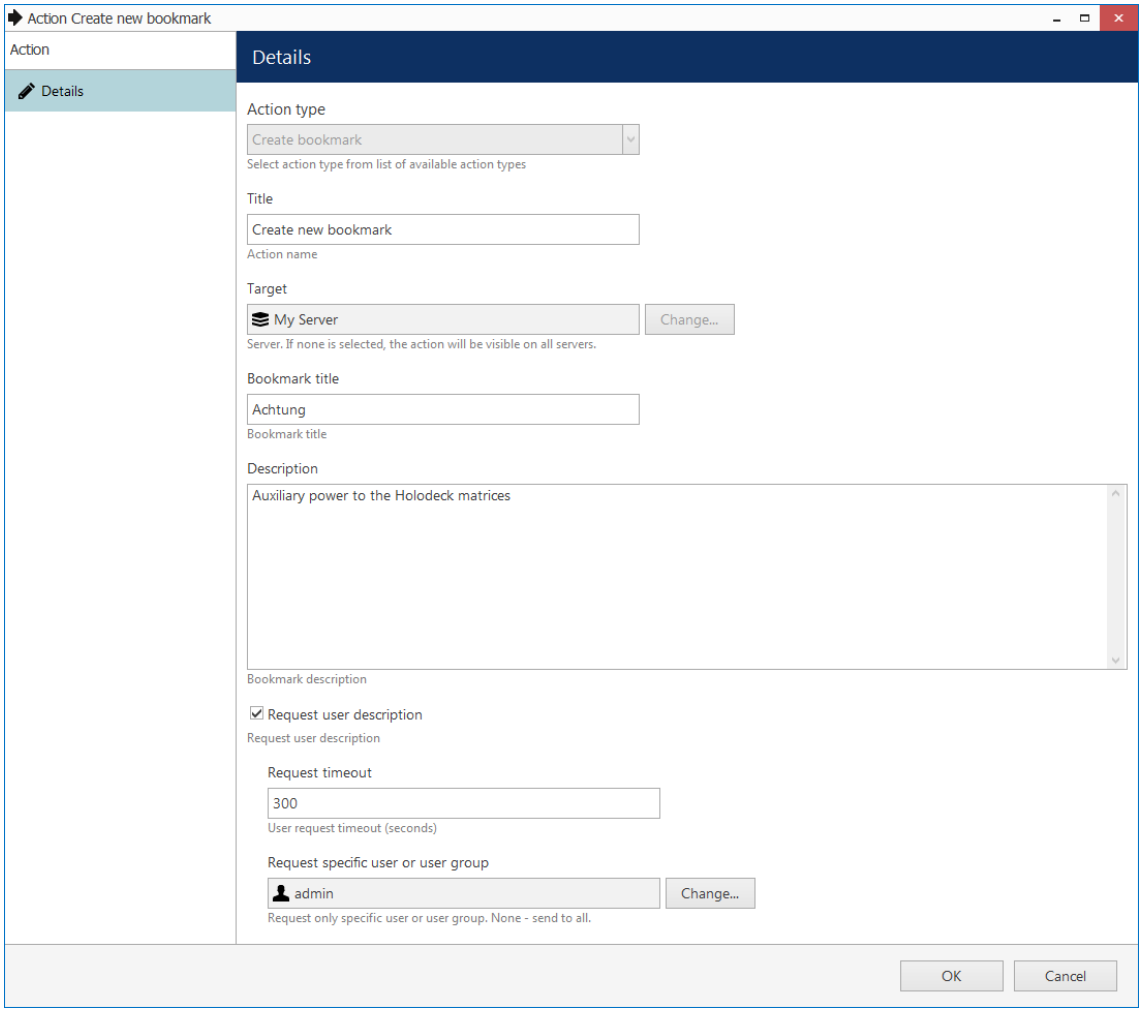
- channel base recording configuration: based on schedule, continuous recording at restricted FPS + no recording
- action triggering recording profiles:
    - action #1 triggers continuous video recording without frame rate limitation
    - action #2 triggers the built-in *No Recording* profile: as a result, channel recording is returned to its default (configured) state
    - action #2 is delayed for thirty minutes using a Delay Timer

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Create Bookmark

Bookmarks can be created by the server, based on any available event. This can be done either completely automatically or complemented with user input - from the users who are connected via Macula Monitor application.



Available settings:

- **Title**: custom (user-defined) action name
- **Target**: server to add the bookmark on (select *none* to make the action visible on all servers in the system)

- **Bookmark title**: name that will appear in the archive and also displayed to users, if user description is requested (use the *Insert field* button to add text macros)
- **Description**: extra information to be stored with the bookmark (use the *Insert field* button to add text macros)
- **Severity**: bookmark severity level (info = lowest, critical = highest); you can change the severity level colors via server settings, *Bookmark policy* tab
- **Request user description**: enable this if you want to obtain bookmark description from Macula Monitor users - this comes useful when you require feedback from users and/or when the description may differ from time to time
    - **Request timeout**: defines for how long the description request will be displayed on the Macula Monitor side
    - **Request specific user or user group**: display confirmation dialog box only to the target user or user group; if not defined, the request will be sent to all connected users

Note that the target channel is not specified at this step: you will have an option to specify it using the *Target Channel* button when you create a rule with this particular *Add Bookmark* action. If the source event of such a rule is channel-specific (e.g., *Video Lost*, *Motion*), the channel will be set automatically. Please see the *Add Rules* section for examples.

Scenario 1: fully automated

In the *Add Bookmark* action settings, do not enable the *Request user description* option. Instead, specify desired bookmark title and description. Now, when you use this action in a rule, a bookmark will be added automatically with the pre-defined description.

Scenario 2: bookmark with user confirmation

Enable the *Request user description* option and specify the bookmark title: make sure to make the title comprehensible as it will be displayed to the Macula Monitor user when prompting for the comment. Optionally, you can specify the description - it will be used when no user input is specified (users ignored or missed the description dialog box).

After you have added the action, you can go ahead and use it in the E&A Configurator: there, upon adding a rule, you will have an option to specify the **target channel** for the bookmark to be added to.

Other Actions

Actions having no special category are listed here.

External Service

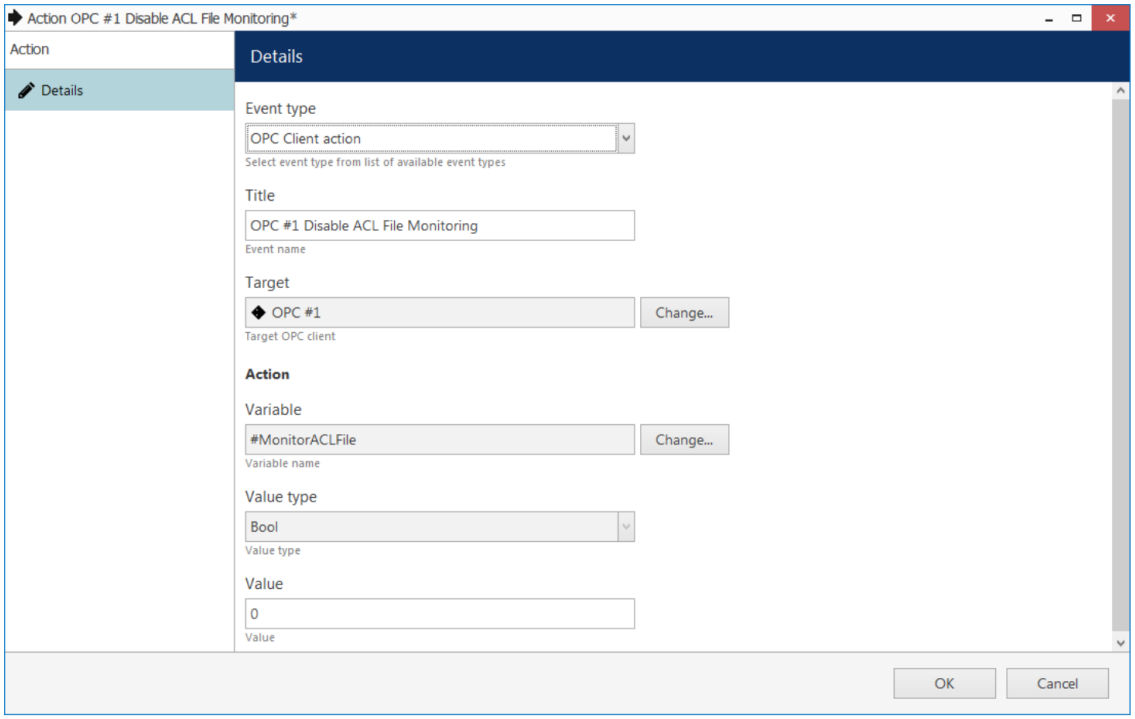
For external services that have their own events, it is possible to trigger these as actions from Macula servers. You need to specify:

- **Title**: user-defined action title
- **External service**: external service (connected to the Macula system via HTTP API) to accept the data
- **Target action**: choose one from the list of available items (availability is ensured on the external service side)

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

OPC Client Action

This action type uses an existing OPC client configuration to send write commands to an OPC server, thus changing values of its nodes.



You need to define:

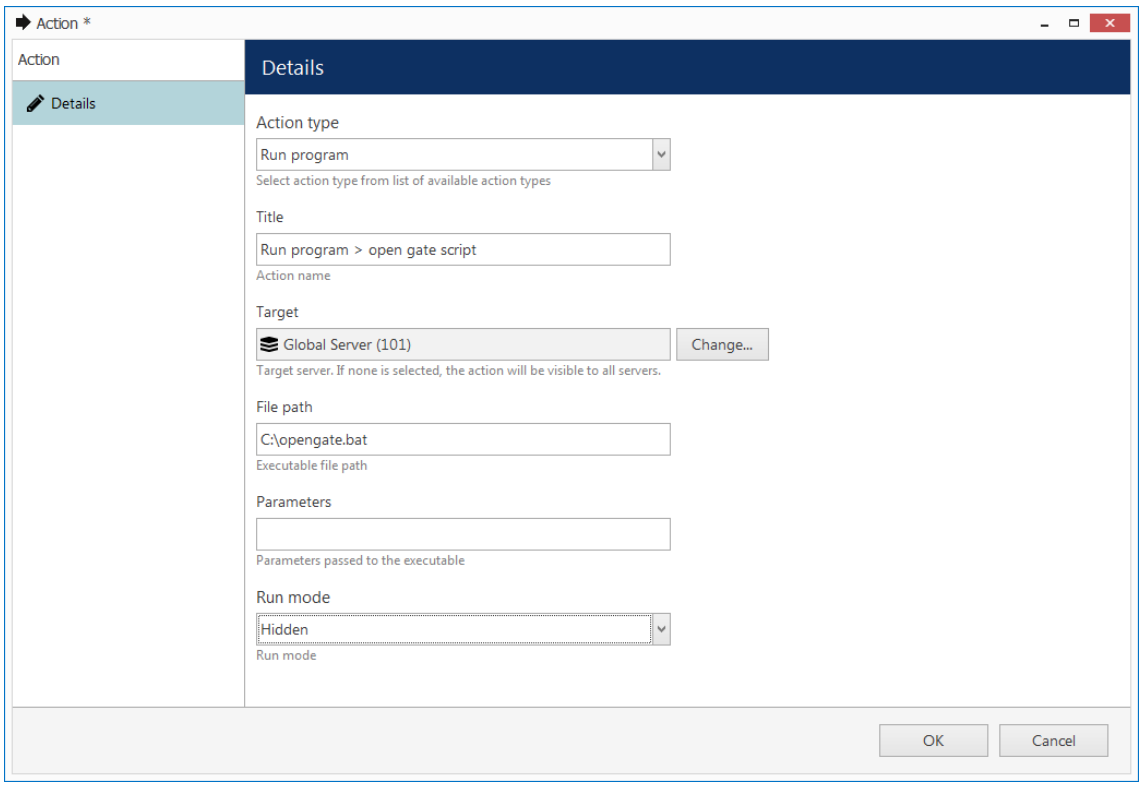
- **Title**: user-defined action name
- **Target**: OPC client configuration (connection to an OPC server)
- **Action**: operation to be performed with the data node value
  - **Variable**: target OPC server data node (choose one from the list), must be of compatible type and have a write permission
  - **Value type**: one of the standard data types, auto detected
  - **Value**: new value to be assigned to the variable, must match the variable value type

Run Program

The *Run program* option gives you the opportunity to define a third-party application (script, batch or a GUI application) that will be launched as a reaction to defined camera events. The following parameters should be specified:

- **Title**: a user-defined action name
- **Target**: target Macula server to execute program on
- **File Path**: full path to the executable file
- **Parameters**: input parameters, if the program launched accepts any (e.g., a batch file) (use the *Insert field* button to add text macros)
- **Run Mode**: execution mode - hidden (silent, invisible to server user), minimized (minimized to taskbar) or normal (program will run in its default state)

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

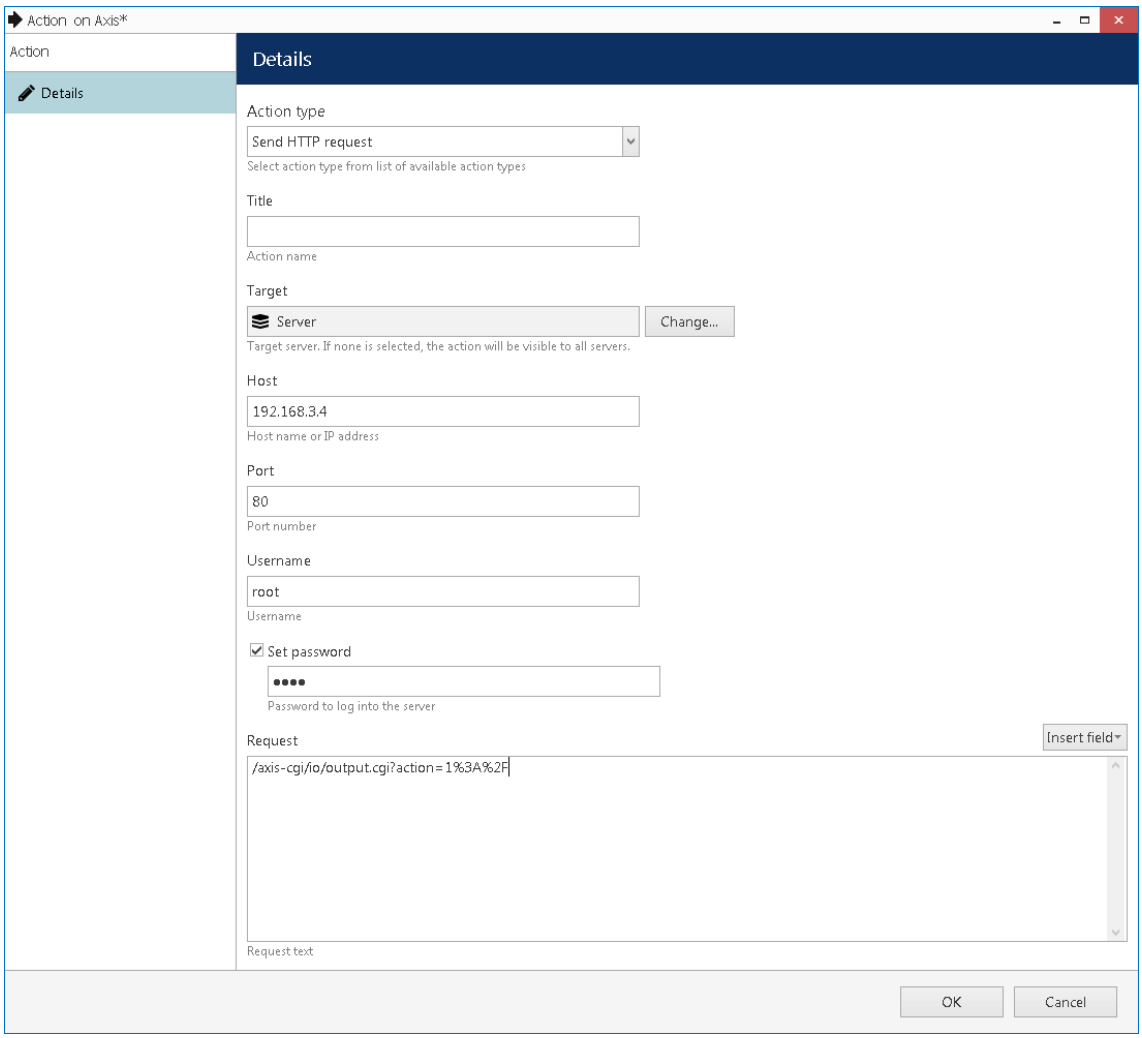


Use the *Insert Field* button on the right-hand side (it appears when you have clicked inside the text area) or right-click the text area and choose *Insert* to add a text macro (see *Action Parameters* further in this topic for details) into the *Parameters* field.

Send HTTP Request

As a result of a triggered event, HTTP/CGI requests can be sent from Macula servers to any third-party servers or devices that can accept such commands. The target devices can be third-party software, Web servers, cameras or any access control hardware. This event is similar to the previous one, with the difference that here there is a single HTTP request, while using the *Run Program* action you can program multiple requests with necessary delays and internal logic.

This action supports both HTTP and HTTPS. For secure HTTP, use port 443 as default, or whichever port is configured on the remote service.



Things to be defined:

- **Title**: user-defined action name, by default it is *Send HTTP request [target host]*
- **Target server**: a server for the action to be available on; if no server is defined, the action will be available on all servers
- **Host**: an IP or hostname that will be accepting the HTTP request
- **Port**: port number to accept the request, port 80 is default
- **Username**: a username to log into the target host, if necessary
- **Password**: a password to log into the target host, if necessary; to change the password when editing the action, put a check mark on the *Set password* and define a password below
- **Request**: HTTP command string

The resulting request link will be formed as a combination of the host and request fields with the specified port, plus username and password, if specified.

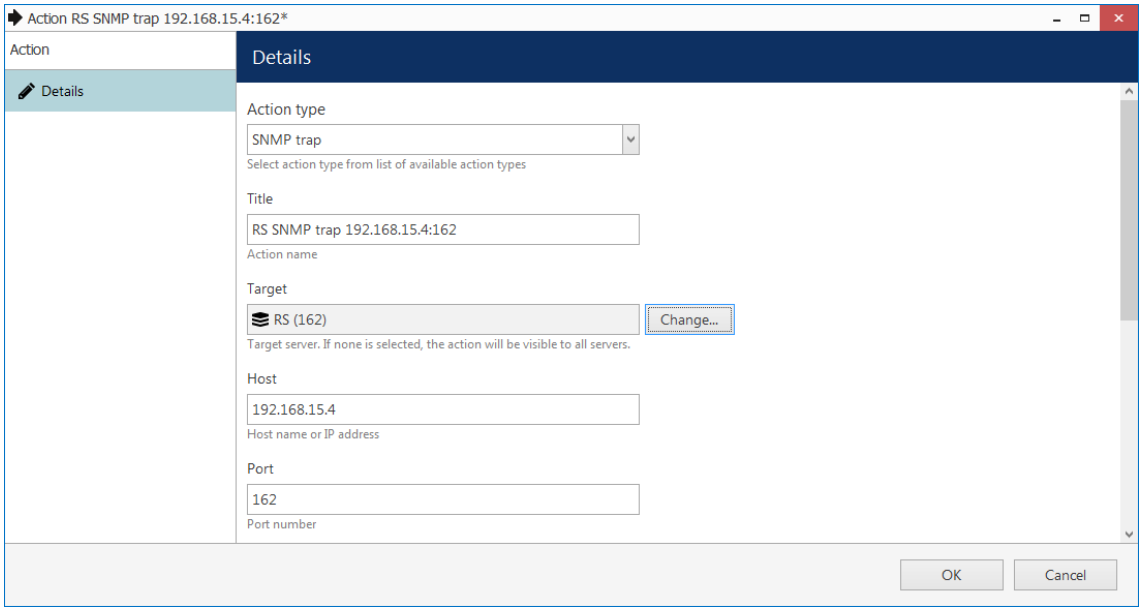
Use default port 80 for HTTP and 443 for HTTPS.

Use the *Insert Field* button on the right-hand side (it appears when you have clicked inside the text area) or right-click the text area and choose *Insert* to add a text macro (see *Action Parameters* further in this topic for details) to be passed as a parameter in the HTTP request.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

SNMP Trap

This event allows Macula server to act as an SNMP agent and generate and send trap messages to a **third-party SNMP manager**.



You need to define:

- **Title**: user-defined action name, by default it is *[server] SNMP trap [host] [port]*
- **Target**: Macula server for the action to exist on; if none selected, the action will be visible on all servers
- **Host**: target SMTP manager address
- **Port**: target port
- **Community**: SMTP community expected by the SMTP manager
- **Trap ID**: automatically generated ID
- **Message**: text message to be sent

Use the *Insert Field* button on the right-hand side (it appears when you have clicked inside the text area) or right-click the text area and choose *Insert* to add a text macro (see *Action Parameters* further in this topic for details) to be passed as a parameter.

Action Parameters (Macros)

Actions that handle text information (log messages, send emails and run third-party program) can accept macro commands. Currently, the available parameters are:

- {EVENT_ID} - internal identifier of the triggered event
- {EVENT_TITLE} - user-defined name of the triggered event
- {EVENT_SOURCE_ID} - internal identifier of the event source
- {EVENT_SOURCE_TITLE} - user-defined name of the event source
- {EVENT_UTIME} - event UTC time
- {EVENT_UDATE} - event UTC date
- {EVENT_TIME} - event local time
- {EVENT_DATE} - event local date

- {EVENT_TIMESTAMP} - event UTC timestamp in a system-independent format YYYY-MM-DD hh:mm:ss.ms
- {EVENT_TIMESTAMP_UNIX_MS} - event timestamp as Unix Epoch time
- {ADDITION_INFORMATION} - extra information for *Disk Excluding, Fallback activating* and *Recording Error* events
- {ACTION_ID} - internal identifier of the action
- {ACTION_TITLE} - user-defined name of the action
- {ACTION_TARGET_ID} - internal identifier of the action target (usually, a server)
- {ACTION_TARGET_TITLE} - user-defined name of the action target (usually, a server)
- {ACTION_PARAMETER_ID} -internal identifier of the additional action parameter (e.g., target channel defined in the rule)
- {ACTION_PARAMETER_TITLE} - user-defined name of the additional action parameter (e.g., target channel defined in the rule)
- {VALUE} - number plate value from the Tag Matched event
- {CHANNEL_RECORDING_ID} - channel recording identifier, as displayed in the channel details when IDs are enabled in the Macula Console app settings; channel ID is used

Example of a text string containing a macro: "{EVENT_TITLE} event occurred on {EVENT_UDATE} at {EVENT_UTIME}".

Event sources are listed for every rule in the *Rules* section of *Events & Actions*; typically, these are servers, devices and other resources capable of generating events (e.g., user buttons). **Action parameter** is a supplementary item added to the rule, e.g., *target channel* for the text notification, *source snapshot* for the attaching snapshots to emails or exporting them.

The {ADDITION_INFORMATION} macro has support for parameters. These depend on the originating event. For example, for **LPR events**, try the following ones:

- {ADDITION_INFORMATION:Plate} for the license plate number;
- similarly, use Speed for the estimated vehicle speed
- and Confidence to get the recognition accuracy,
- Info1/Info2 fields are available for the Macula LPR external service.

For the **face recognition** events, additional parameters may be equal to Subject and Tag, as well as SubjectSimilarity (if a person was found in the DB)

When you have finished, click *OK* to save and close the dialog box. The newly created action will appear in the item list under *Actions* and will be available for configuration.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

9.7 Understanding Conditions

Conditions are auxiliary controls for event/action rule operation: these are **condition variables**, 'locks' for the defined event/action mappings.

Each condition can only be in one of two states: **OFF** or **ON** (0 or 1, *false* or *true*, to put it in terms of formal logic). When applied to a rule, the condition serves as an additional clause for the action execution: the action will only be performed if attached condition is ON, and is never performed if condition is OFF - regardless of whether the event has been triggered. The condition **state** can be manipulated using the *Set condition* and *Unset condition* **actions** (these exist by default for each and every created condition), which, in their turn, can be set off by some other events.

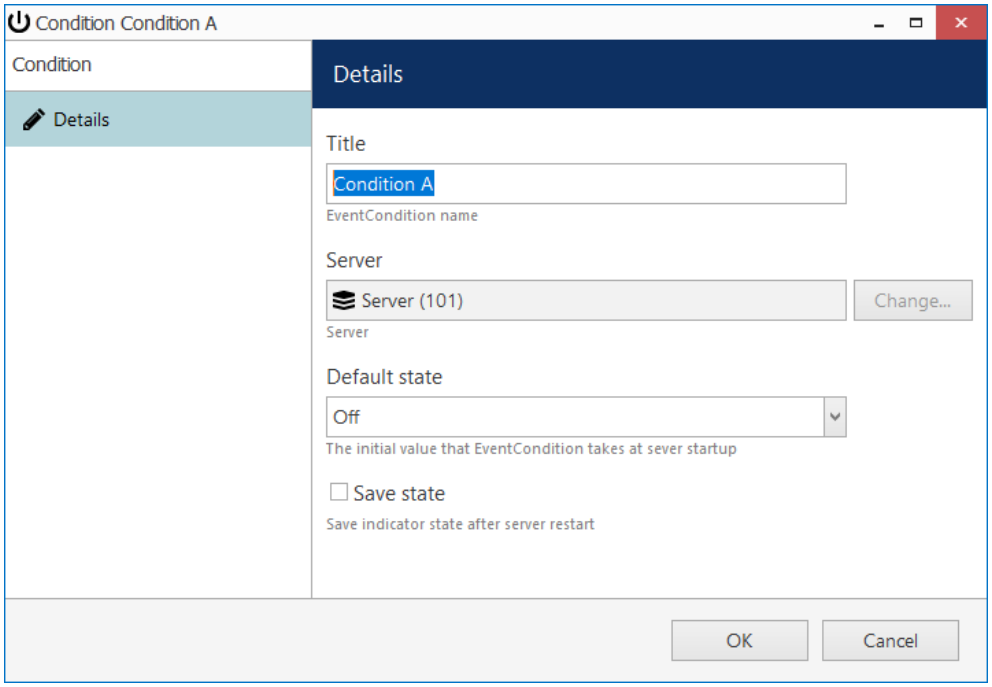
The conditions are available in the *Event & Action Configurator*: click the *Conditions* button in the bottom part of the *Rules* section to load the existing condition list or create a new one.

Add Condition

To add, remove and manage the conditions in the Macula Console, go to the *Events & Actions* section and choose *Conditions* from the menu on the left. Conditions can be also added as you go from the Event & Action Configurator.

Click the + *New condition* button on the upper panel to bring up the condition configuration dialog box. Here you have to:

- enter an comprehensible **title** for the condition - usually, the best ones are those which express a state, e.g., camera offline, motion present, door opened etc.
- choose the **target server** - conditions, as non-global events, are local and operate within a single server
- set condition **default state**, i.e., the state it is in before it is set or unset for the first time; this can be either ON or OFF
- **Save State**: Save condition state after server restart



When you have finished, click *OK* to save and close the dialog box; the newly created condition will appear in the item list and will become available in the *Event & Action Configurator*.

Use the buttons on the upper panel to edit and remove the conditions; the filters on the bottom panel will help you load recently added or recently edited items.

Condition Usage Examples

Consider a system that has three cameras installed: *Camera A* overlooking area A, *Camera B* overlooking area B that is just next to area A, and *Camera C,* which is a supplementary PTZ device and can be turned to view both areas and even more, and overlooks area C by default. If a person walks into area A, he/she will be detected by *Camera A's* video analytics; if he moves on, he will enter area B and the security guard will see him on *Camera B*.

Now, imagine that *Camera B* suddenly goes offline. The security guard is OK with that, until there is someone in area B; he notices some motion in area A and takes control of *Camera C*, and makes it overlook area B, but the person of interest is long gone by that time, and there is no footage of him being present in area B. So, the task is to automate the process so that *Camera 3* serves as a backup while *Camera B* is offline; the configuration in such a case may look as follows:

- Event 1: *VCA*, source: *Camera A*
- Event 2: *Video Lost*, source: *Camera B*
- Condition: *Camera B Offline,* default state: *OFF*
- Action 1: make *Camera C* go to preset *Area B*
- Action 2*: Set Condition,* target: condition *Camera B Offline*

Rules:

- Event 2 triggers Action 2 (that switches the state of condition *Camera B Offline* to ON)
- Event 1 triggers Action 1 upon the condition *Camera B Offline*

Thus, Action 1 (go to the PTZ preset) is only actually triggered then and then only if *Camera B Offline* condition state is ON, which is not possible while *Camera B* is online.

Now, we need this to work both ways, i.e., we want to return *Camera C* to its home position and reset condition state back to *OFF* when *Camera B* comes online again. New configuration elements will be added:

- Event 3: *Video Restored*, source: *Camera B*
- Action 3: *Unset Condition*, target: condition *Camera B Offline*
- Action 4: make *Camera C* go to preset *Area C*

Rules:

- Event 3 triggers Action 3 (that switches condition state to OFF)
- Event 3 triggers Action 4

These new rules ensure that, once *Camera B* is streaming again, *Camera C* will go back to its original position, thus terminating it as a backup device; and the condition is *OFF*, meaning that the triggering of VCA rules in area A will not make *Camera C* move.

The whole setup in *Event & Action Configurator* is as follows:

RULE

Camera A >> VCA: motion in Zone1

Camera C >> Activate PTZ preset > Area B

Camera B Offline

Camera B >> Video lost

Camera B Offline >> Set condition

Camera B >> Video restored

Camera B Offline >> Unset condition

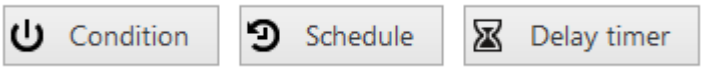
Camera B >> Video restored

Camera C >> Activate PTZ preset > Area C

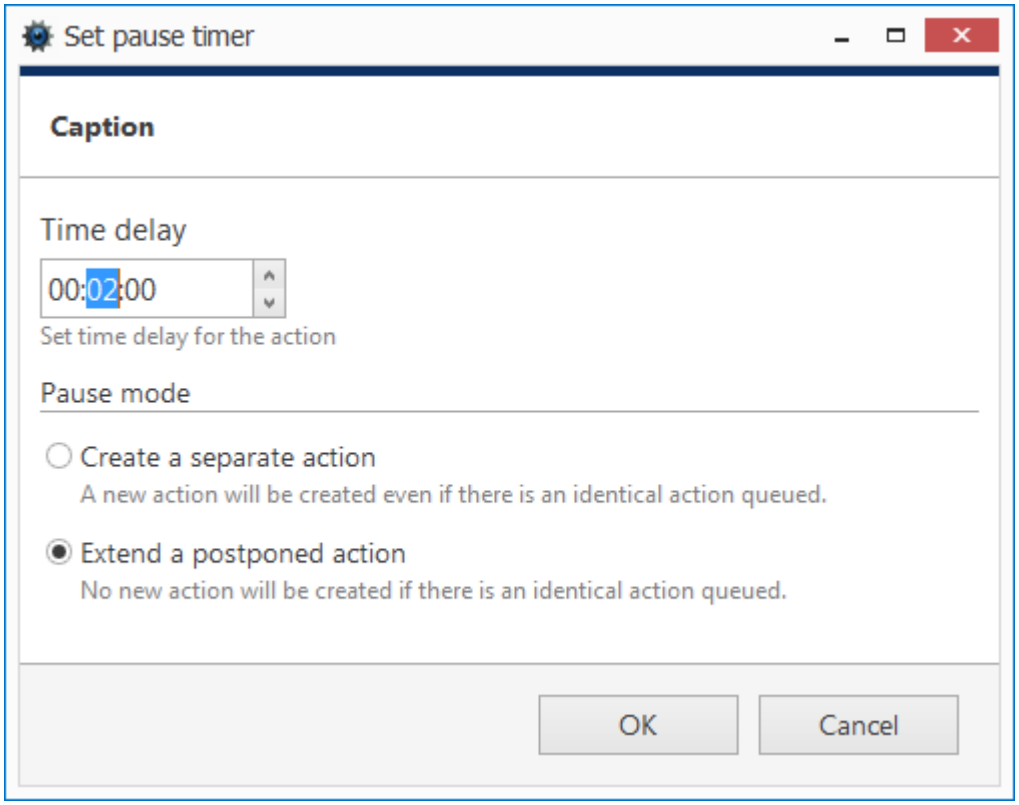
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

9.8 Delay Timers

Delay timers are supplementary entities for controlling action launching. Unlike conditions and schedules, timers cannot be pre-created in the main Macula Console *Events & Actions* section, but rather are defined as you go for each rule with the *Event & Action Configurator*, which is available via the *Rules* section.



To add a pause timer for specific actions, select one or more of the mapped rules (use *CTRL+click* or *Shift+click* to mark multiple items) subject to delay, and then click the *Delay Timer* button on the bottom panel of the central part of the *Event & Action Configurator*.



Set the delay period for the target timer. Time can be adjusted in the following ways:

- click hours/minutes/seconds and then use the UP and DOWN arrows on the right, or
- click hours/minutes/seconds and use the mouse scroll, while still holding mouse cursor over the relevant timestamp section, or
- enter the time manually using the keyboard numpad.

Next, choose the pause mode:

- **Create a separate action**: new actions of the same type will be created regardless of the acting delay timer, and queued in the same way as the original delayed action
- **Extend a postponed action**: new events of the same type will restart the timer, postponing the resulting action for the specified amount of time

When you have finished, click *OK* to save and exit the dialog box. The newly created delay timer will be assigned to the pre-selected actions.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Extending an action allows you to postpone the action execution repeatedly if more events of the same type arrive within the chosen time period. For example, if incoming events are of a *Recording Error* type, there may come too much of them at once e.g. in case of a major storage issue, causing a lot of triggered actions of the same type, while only a single action may be desirable.

Say, if required action is *Write to application log*, setting a delay timer to *5 minutes + extended action* will postpone the email sending for 5 minutes every time a new recording error appears; when, at a certain point, more than 5 minutes have passed without new incoming events, a single log entry will be eventually created. The **separate action** option, on the contrary, will force logging for every single triggered event.

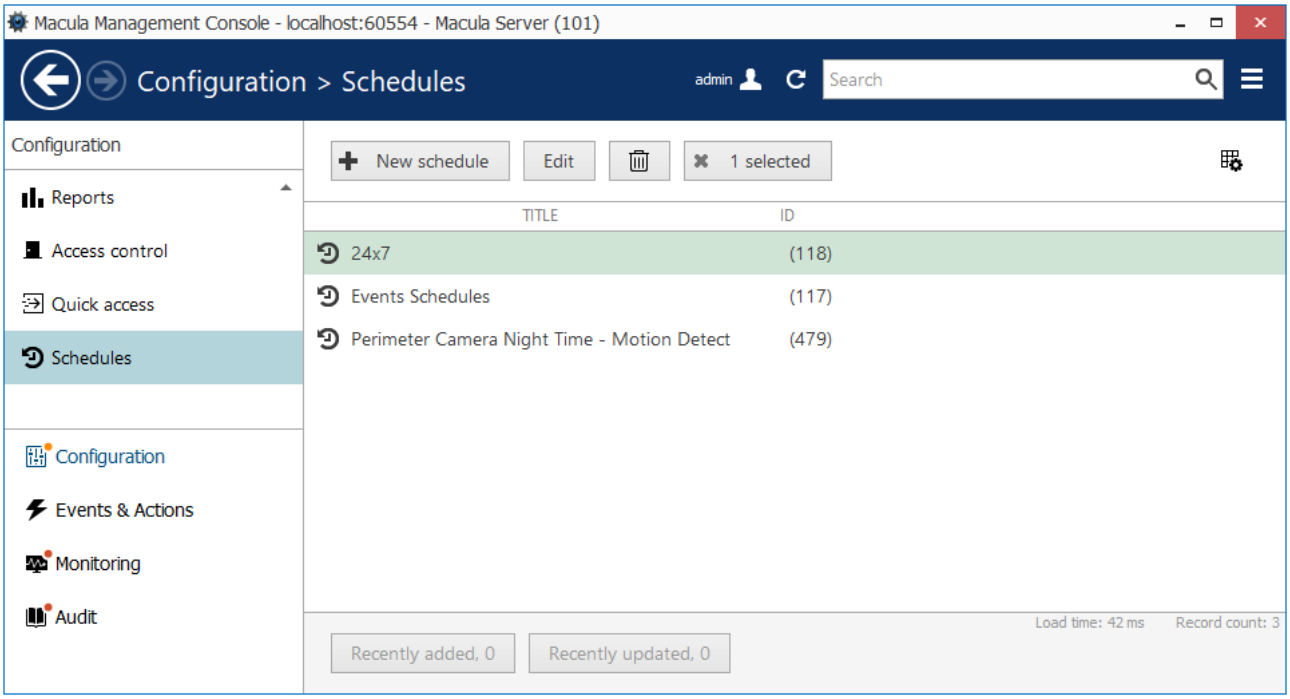
To remove a delay timer from rule configuration, click the timer to highlight it within the rule, and then click the *Clear* button in the bottom panel. Note that, if there are schedules and/or conditions attached to the same rule, they will be removed as well.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

9.9 Create Schedules

Starting with version 1.26, you can find **Schedules** at the bottom of the **Configuration** section. You can create your Schedules and use them for the **Users** and **User groups** or **Events & Actions** schedules later. In previous Macula versions, You can find Schedules under the Events & Actions section.

You can also create or reuse existing *User-defined calendars* for special days based on the particular calendar date and override the regular schedule with exclusive scenarios.



Please be aware that *Recording Schedules* use their **own schedule type**. How to create *Recording Schedules* is described in the corresponding manual section.

Create new schedule

To create a new schedule, go to:

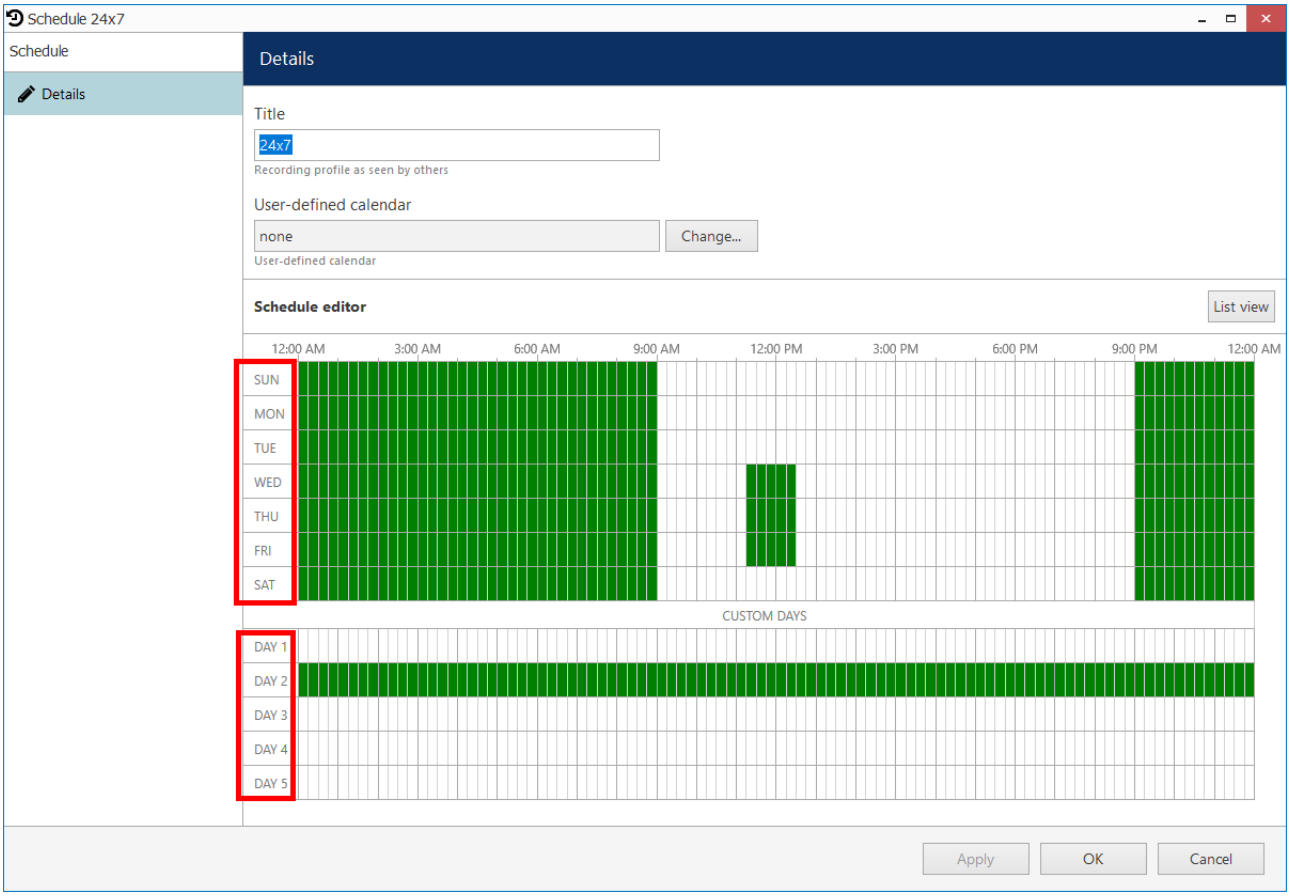
1. *Configuration -> Schedules -> New schedule* button. A *Schedule* pop-up window will appear.
2. Fill in the *Title* field to identify your newly created schedule later.

You will see the *Grid View* in the *Schedule Editor* field by default. The grid view has two separate sections - **Weekdays** and **Custom days**.

You can mark the table by clicking and holding your mouse button while moving the mouse inside the table with the step of 15 minutes. Marked time means that the schedule is active on those days at that particular time.

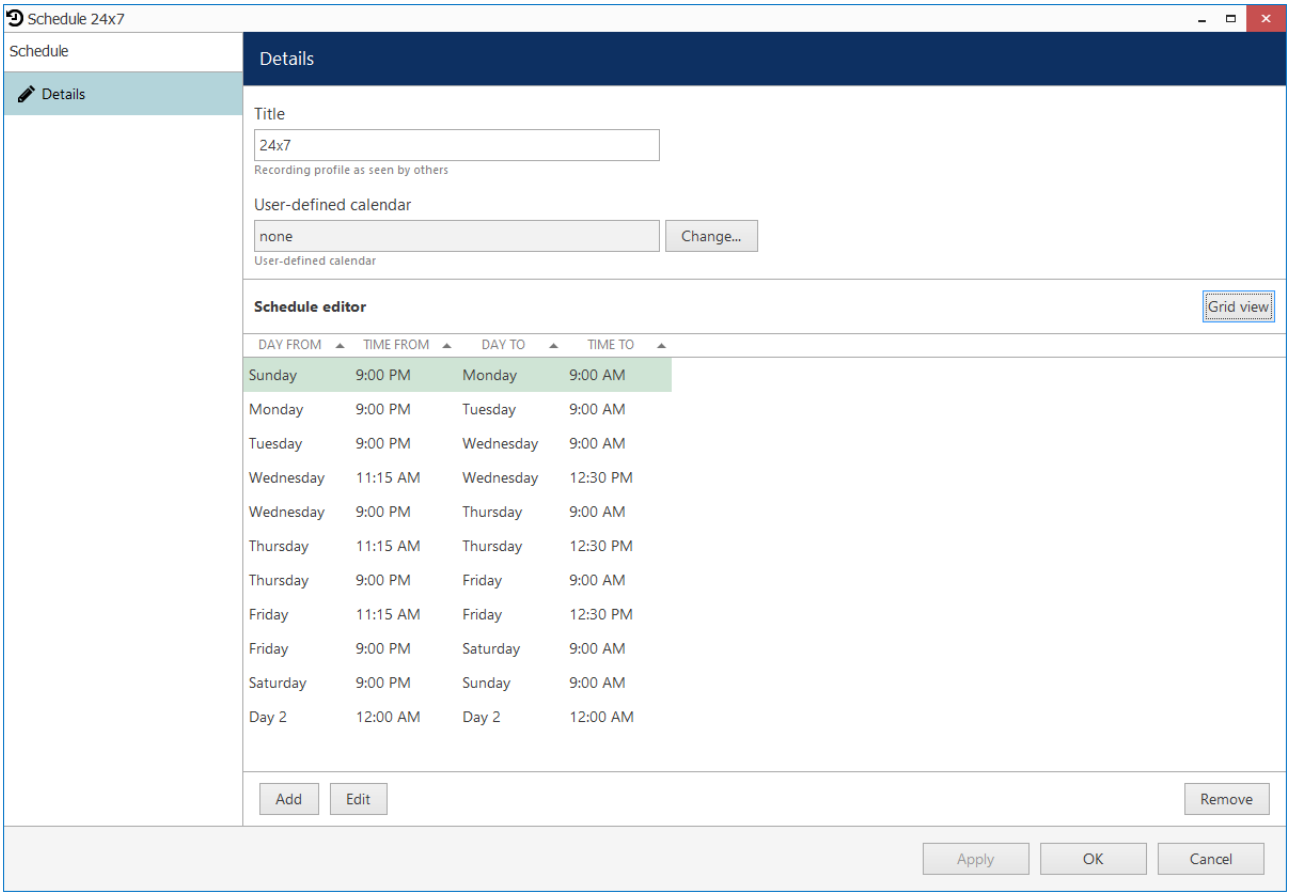
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



You also can switch to the List view by pressing the button *List view* from the right side over the *Schedule editor* field. You can create multiple entries inside the *List view* and edit details later inside the *Grid view* by selecting the particular entry and clicking the *Grid view* button.

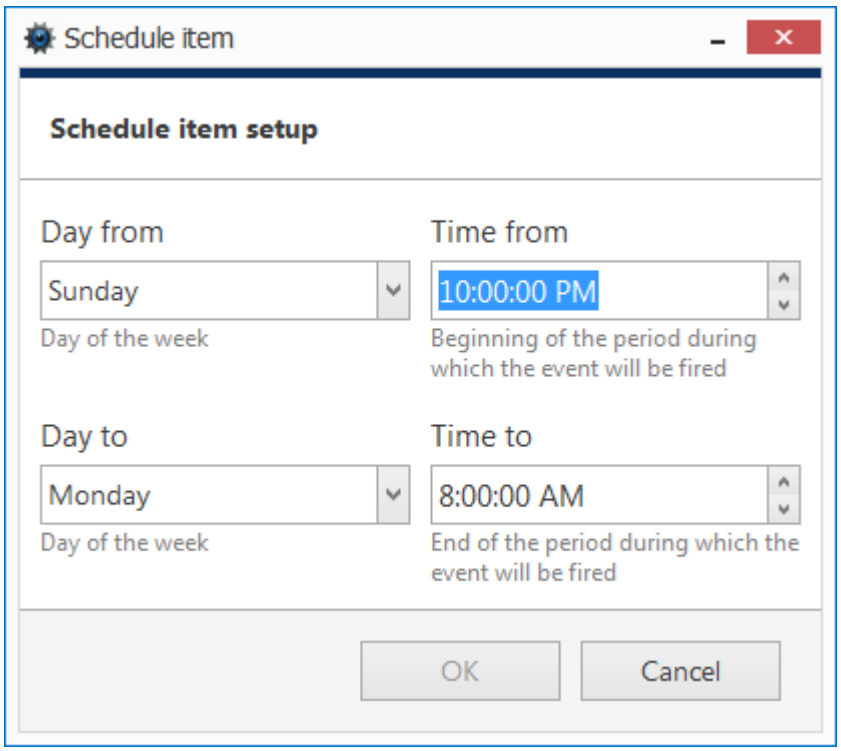
Macula® Professional Administration Guide



To add a schedule scenario using the *List view:*

1. Find the *Add* and *Edit* buttons on the bottom-left side inside the *Schedule editor* field. Click on the *Add* button. One more pop-up window named *Schedule item* must appear.
2. Inside the *Schedule item* pop-up window, you find dropdowns: *Day from* and *Day to*, and the Time input fields: *Time from* and *Time to*.
3. Select the **weekday** you want to start your scenario and the day you want to set as the endpoint of the schedule using dropdowns.
4. Setup the "*Time from*" and "*Time To*" in your new schedule scenario, and press the *OK* button to confirm. Time settings apply to each day selected from the dropdowns.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



You also can set a *Custom day* inside the *Schedule item* pop-up window. Pick Day 1, 2, 3, 4, or 5 from the "*Day from*" dropdown menu, set the timeframe, and press the *OK* button to confirm.

Weekday schedule

The **weekday** schedule will repeat itself indefinitely, based on days of the week, unless you override it by the *User-defined calendar*.

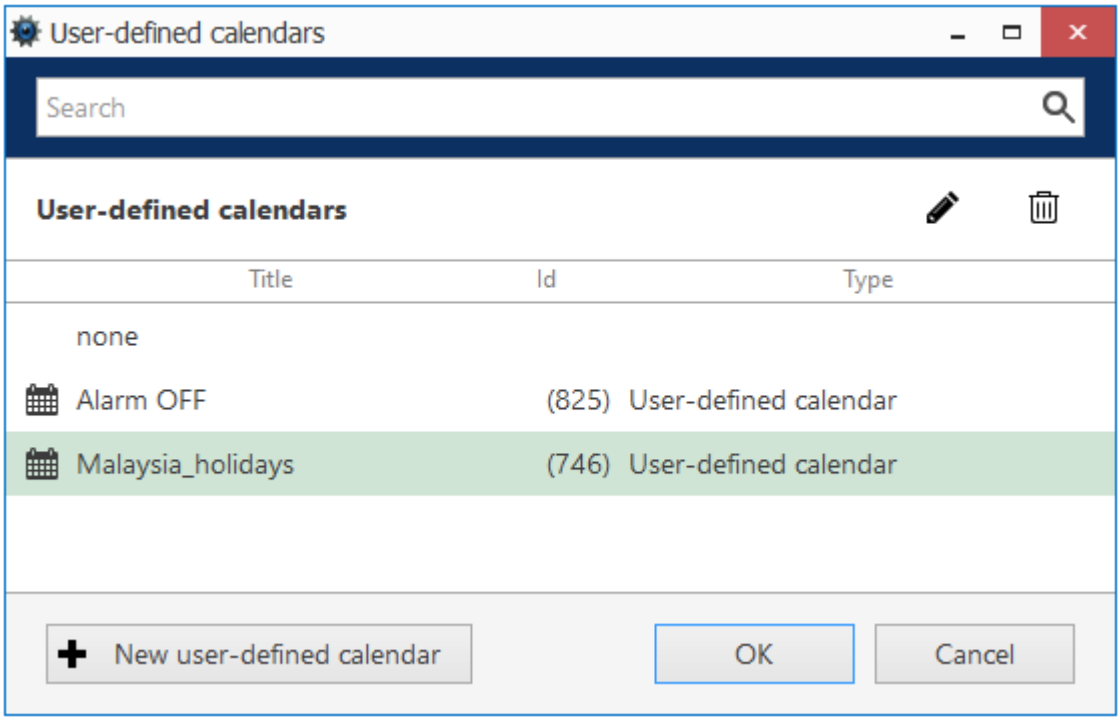
Custom days Schedule

Section **Custom Days** works differently. You can create five different schedule scenarios that later on can be applied to override the regular schedule. You can utilize it with *User-defined calendars*.

User-defined calendars

There may be special calendar dates that don't fall into the regular schedule scenario. For such occasions, create or reuse a *User-defined calendar*.

1. Inside the *Schedule* pop-up window, click the "*Change...*" button from the right side of the *User-defined calendar* field.
2. "*User-defined calendars*" pop-up window will appear. If you already have some predefined calendar - you can reuse it by selecting it from the list and confirming with the OK button.



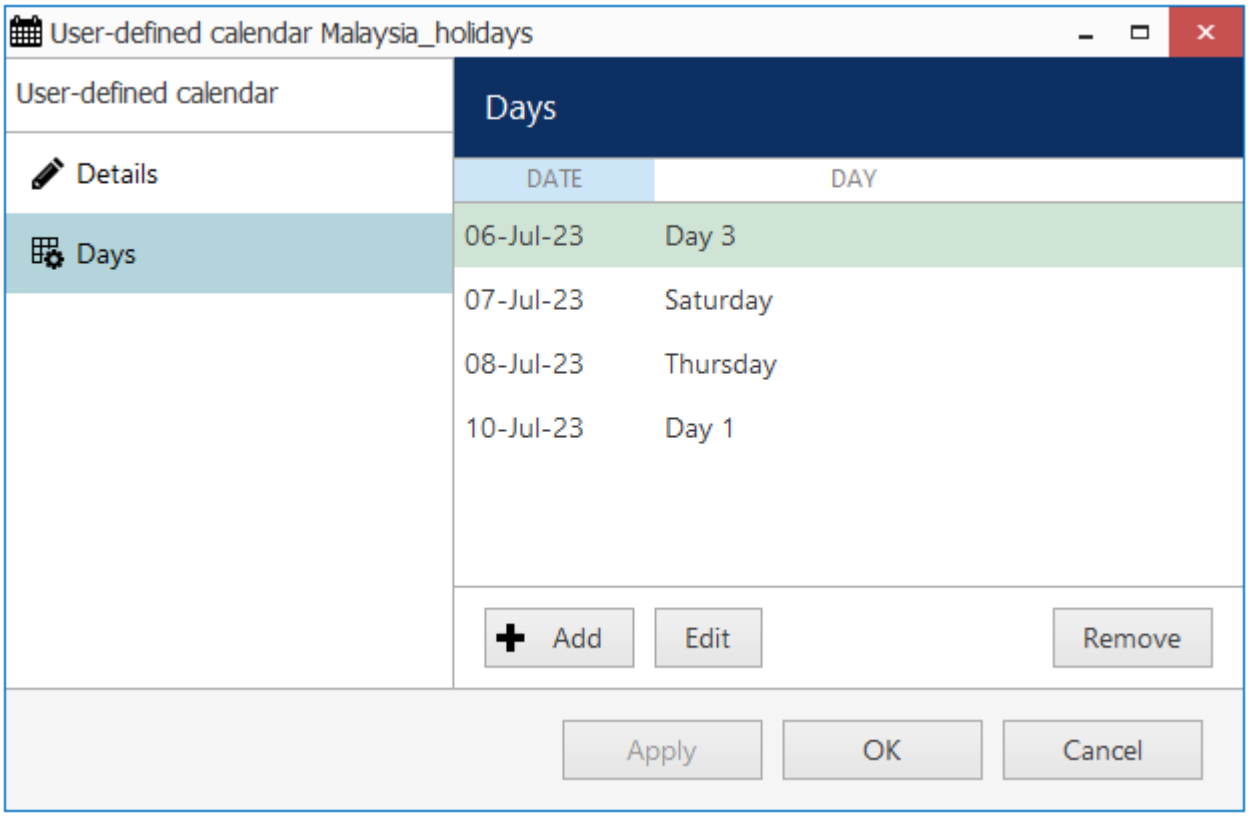
⚠ This calendar will override your regular schedule on the dates you have set up inside the calendar. All other dates will be executed on your weekday schedule scenario.

To create the new User-defined calendar:

1. Click on the +New user-defined calendar button on the bottom-left of the pop-up window. The new pop-up window will appear.
2. Add the Title to identify the created calendar later.
3. In the left panel of the User-defined calendar window, select the Days tab and click the +Add button.
4. Select the Date from the dropdown menu inside the Day window. Click on the Day field and find the day from the list.
5. Confirm your choice with the OK button.

You can select days from the regular schedule (for example, to make a particular Saturday a working day, pick any working day schedule scenario) or use the five custom days we saw earlier. We can use **Custom days** inside the calendar to create five different custom scenarios to override our regular schedule on a calendar basis.

When you complete setting up your custom scenarios for the calendar-based schedule, confirm your new calendar inside the parent pop-up window with the Apply and OK buttons.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

9.10 Counters, Indicators and Variables

Apart from actions, events and rules, the Event & Action section of Macula Console contains additional resources, which can be used for building even more versatile automated scenarios.

Software Counters

Software **counters** are entities that can contain a certain integer value, which can be altered based on some occurred event. These can be used in Macula, for example, to count events that do not originate from VCA and therefore cannot be accounted for using VCA counters.

Counters can be created in the Events & Actions section of Macula Console, under the *Counters* subsection. Each one has a title and a server where it resides (as the *Event & Action* scenarios are defined per server; use global events to transfer events from one server to another - for Macula Enterprise installations).

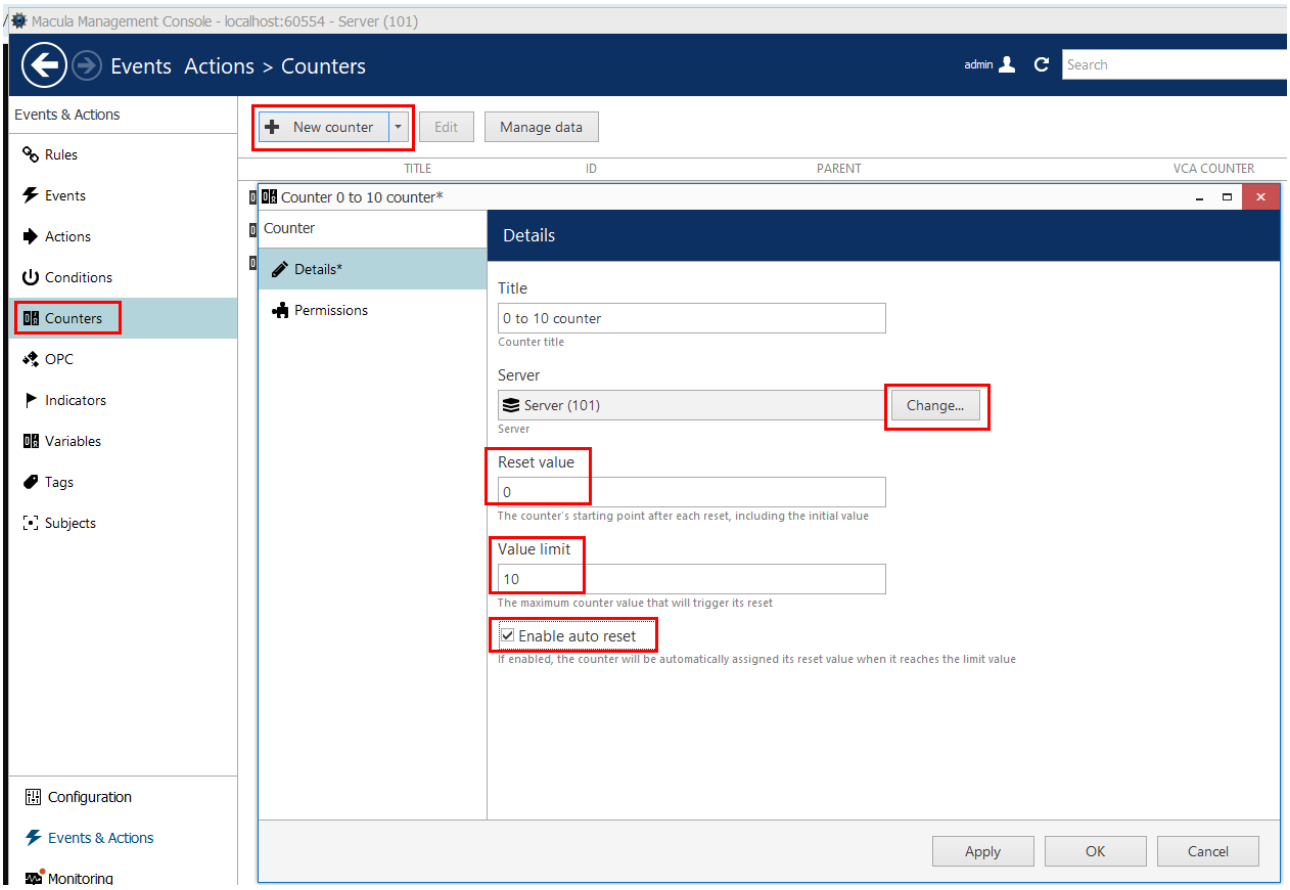
Reports can be then built based on the software counter values, along with VCA counters: automatic reports are available for configuration in Macula Console, and manual reports can be created in the Macula Monitor application. Both modes also permit report export in PDF format.

Add and Remove Counters

To add, remove and manage the software counters in the Macula Console, go to the *Events & Actions* section of Macula Console and choose *Conditions* from the menu on the left. Click the + *New counter* button on the upper panel to bring up the counter configuration dialog box. Here you have to:

- The *Title* field: Provide a meaningful name to your counter
- The *Server* field: counters are non-global entities, so select the server you wish the counter being attached
- The *Reset Value* field: You can input here the initial value for the counter after reset
- The *Value Limit* field: You can limit counter value with this field
- The *Enable Auto Reset* checkbox: By marking this checkbox, you enable automatic counter reset when it reaches the value from the *Value Limit* field

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



In the *Permissions* tab, you can grant **access** to this counter's **data** to individual users and user groups. Anyone with the rights to access archived VCA metadata for the target counter will have it in the Macula Monitor application in the *Reports* section. If the *Access archived VCA metadata* permission has been granted for the **whole server**, the target user or user group will have access to **all counters** on that server, regardless of the individual counter permissions.

When you have finished, click *OK* to save and close the dialog box; the newly created counter will appear in the item list and will become available in the *Event & Action Configurator*. You can create any number of software counters.

Use the buttons on the upper panel to edit and remove the counters; the filters on the bottom panel will help you load recently added or recently edited items.

How to Change Counter Values

Counter values can be changed based on any event in the Event & Action scenarios, when building rules. Counter value changes can be a separate action or an additional one to serve for counting the number of times when the rule was triggered.

There are three **built-in actions** that are available by default for any created counter:

- **Increment**: increase counter value by one
- **Decrement**: decrease counter value by one
- **Reset**: set the counter state back to zero

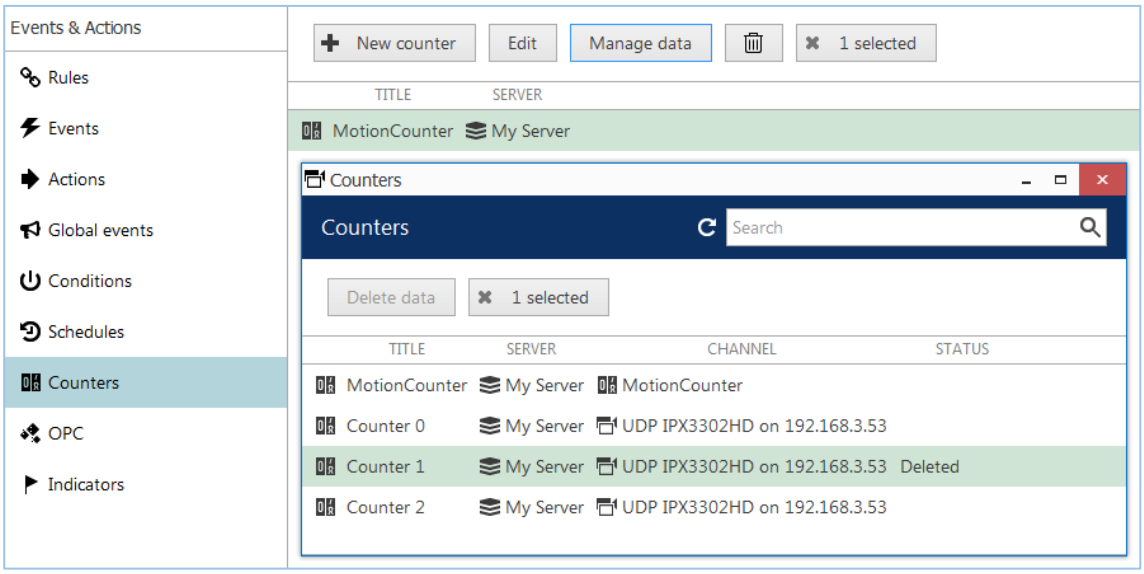
The **initial value** of any counter is **zero**.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Manage Counter Data

Internal Macula counters can be removed at will at any point: select all redundant counters and click the *Recycle bin* button on the upper panel.

However, only software (user-created) counters can be deleted in this way. Counters originating from VCA cannot be deleted in this way, as they exist in the VCA configuration (either camera-side or server-side video analytics). Those entities do not even appear in the list in the *Counters* section. To view them, press the *Manage data* button on the upper panel: an additional dialog box will pop up, displaying **all counters**, both user-defined and VCA imported.



Here, you will see **all counters** with **some value**, including those, which have been removed from VCA configuration and are therefore out-of-date. Select the unnecessary items and press *Delete data* above: all information about the target counter will be then removed from the database:

- for software counters, this means that only the past counter values are wiped out; the counter itself stays in the list (you can remove it from the list as described above)
- for VCA counters, the counter itself is deleted from the database, too (but not from the VCA configuration)

> Removing the software counter's data reset it to zero.
>
> Removing VCA counter's data will reset only counter state on the server. Camera counter's value will not be reset!

If there are no new incoming data for the removed counter, it will disappear from *Reports* shortly - both in Macula Console and Macula Monitor. If it still exists and Macula continues receiving data from the target counter, it will re-appear in this list automatically. So, in other words, the Manage data dialog box reflects the current state of the counter's database.

Usage Example

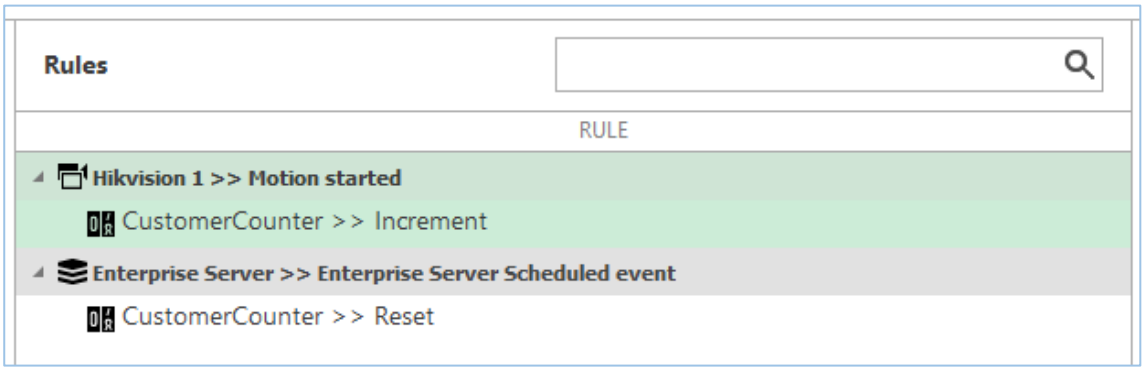
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Consider a use case where it is required to count how many times during the day the office door was unlocked; the door is opened by an access control module, which is also wired to the digital input of a camera so that the system is notified when the door is unlocked.

Required E&A items in this case are:

- Event 1: *Digital Input*, source: corridor camera
- Event 2: *Scheduled event*, type: scheduled, every day 12:00AM
- Counters: *HowManyTimesDoorWasOpened*
- Action 1: *Increment*, target: counter *HowManyTimesDoorWasOpened*
- Action 2: *Reset*, target: counter *HowManyTimesDoorWasOpened*

Events 1&2 are not default and should be made, and the counter has to be created as well. Actions associated with the counter will be added automatically so there is no need to create these.



The final set of rules for this scenario looks as follows:

- Rule 1: Event 1 triggers Action 1
- Rule 2: Event 2 triggers Action 2

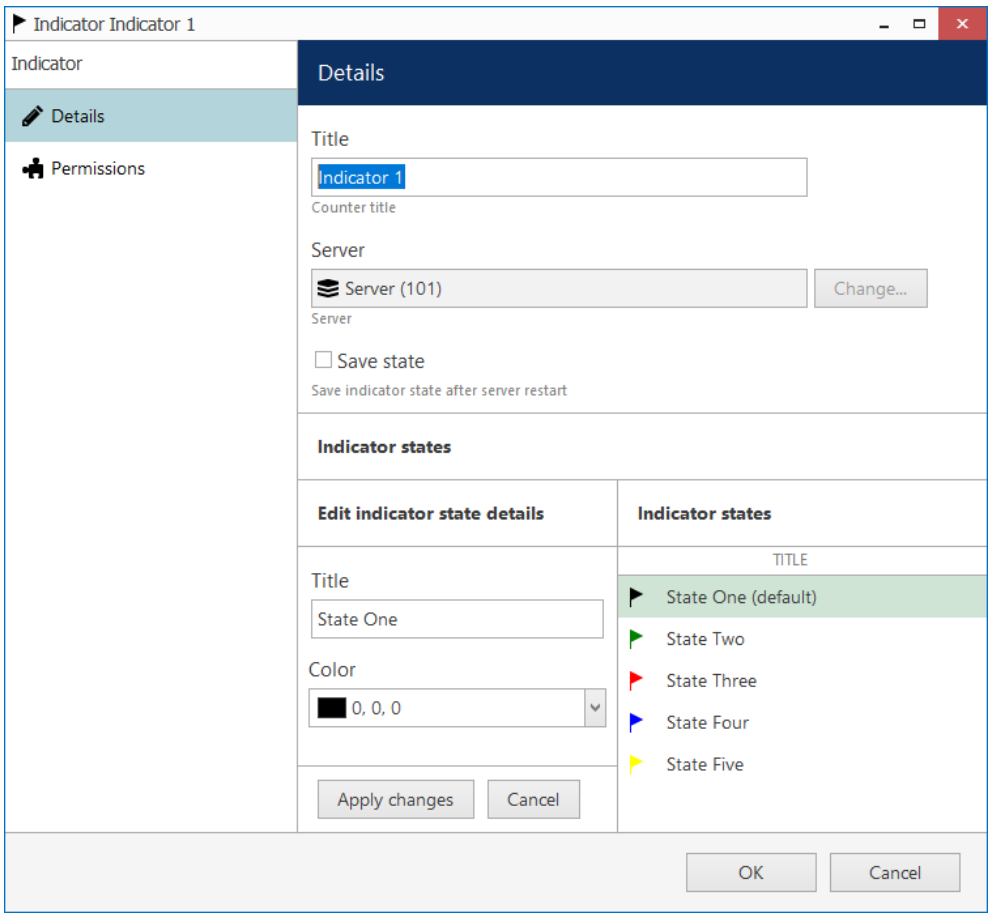
Thus, every time the door is opened, this event is accounted for by the software counter; the counter is reset based on schedule every midnight. Using the counter data, it is possible to build a report and see, for example, most and least popular times, the average number per week etc.

Indicators

Indicators are objects with several **states**. These states (conditions) can be changed based on any events in the *Event&Action Configurator*. Indicators can be placed on **maps**, thus helping you build an interactive dashboard.

You can create indicators in the Events & Actions section of Macula Console, under *Indicators*, then place them onto maps - either regular or geo maps. The indicator state and color can be then changed based on E&A events: once you create an indicator, it is automatically added to the Actions section of the E&A Configurator and actions for changing its state are created.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Create and Manage Indicators

To add, remove and manage the indicators in the Macula Console, go to the *Events & Actions* section of Macula Console and choose *Indicators* from the menu on the left. Click the + *New indicator* button on the upper panel to bring up the counter configuration dialog box.

The following settings are available here:

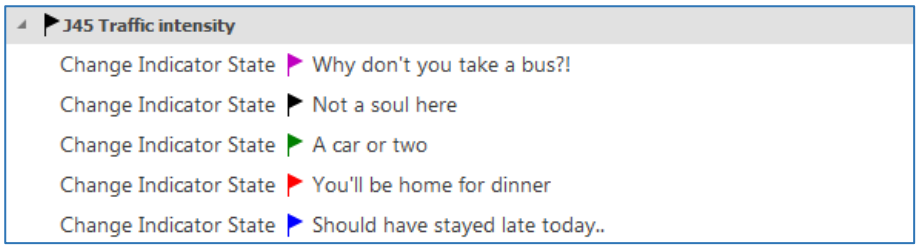
- **Title**: user-defined name
- **Server**: Macula server, to which the indicator belongs (related actions will be only available in the target server E&A Configurator)
- **Save state**: Save indicator states after server restart
- **States**: 5 different indicator conditions with custom names and colors

When adjusting the state details, do not forget to hit the *Apply* button for the changes to take effect.

Change Indicator State

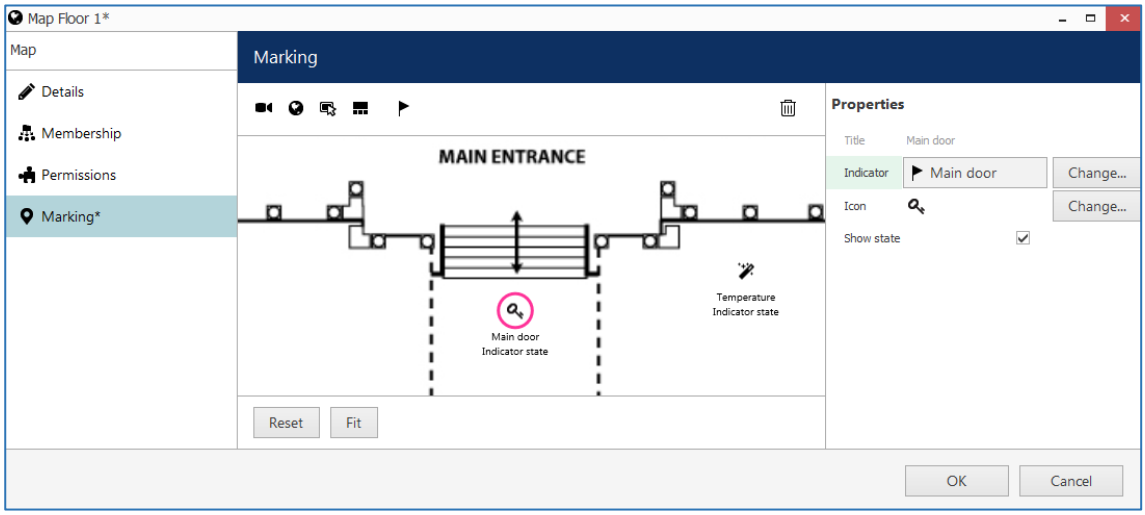
The indicator state can be changed based on any event in the Event & Action scenarios, when creating rules. The indicator state can be changed as a separate action, or it can be combined with any other one, thus helping visualize the state of other items.

There are five **built-in actions** for every indicator that allow to set the indicator to any of its states. If you only need two or three, simply do not trigger other conditions. The actions will appear automatically after you create the indicator.



Maps

When placed onto maps, indicators change their color and display the comment according to their state. Both regular and geographic maps have an **indicator marker** available on the panel above the map, alongside with other markers. Thus, you can build interactive panels that will reflect the condition of the system.



Usage examples

Depending on your needs, indicators can help in many different scenarios.

Use case #1: external sensors are sending temperature data. Based on the value, the indicator state is set to very low / low / normal / high / very high.

Use case #2: conditions are used throughout the system for door status (open/locked). The indicator is used to visualize the condition state (in this case, only 2 out of 5 states are involved).

Variables

Variables in Macula are entities having a certain value that changes over time. Create variables if you wish to set up reactions (via E&A) to certain variable values, e.g., certain temperature readings from thermal cameras.

To access the variables management in Macula Console, choose the *Events & Actions* section and switch to *Variables* in the menu on the left.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Variables differ by source. Currently, there are two groups of sources: devices (IP cameras or other) and data sources.

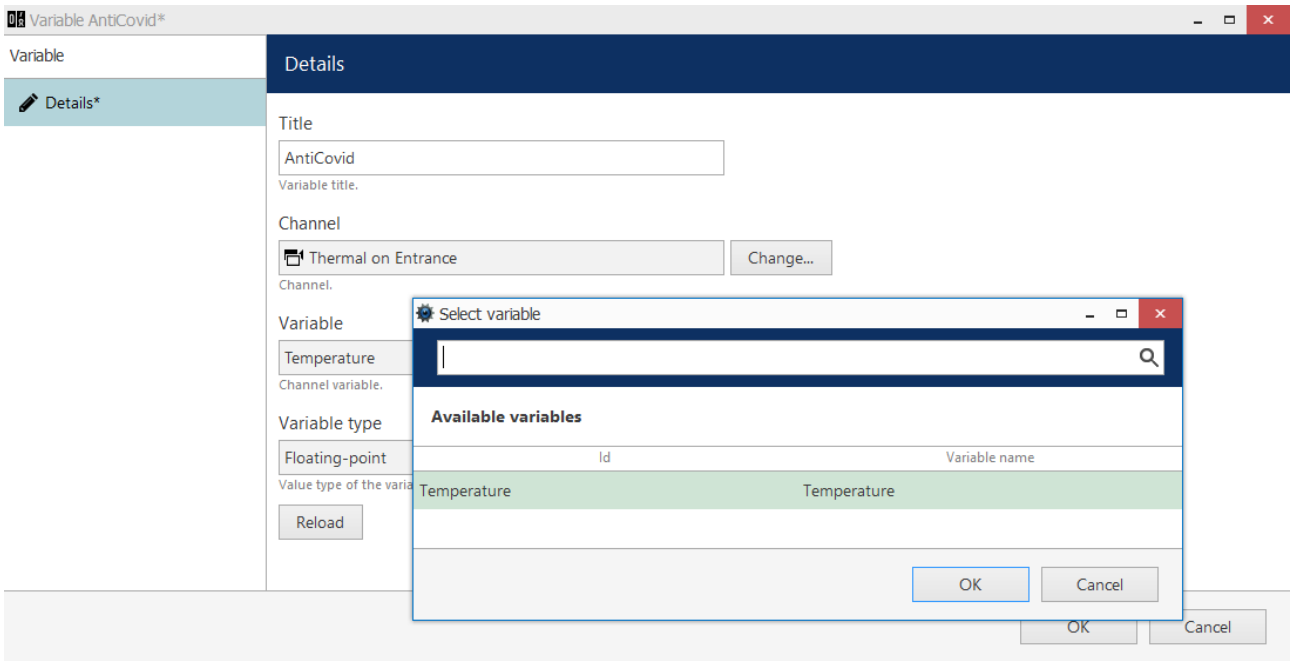
Channel Variables

Some device integrations support receiving certain variable values from cameras. For example, some thermal devices send the temperature measurements as floating-point numbers. In order to "catch" the data on the server side, simply create variables for these cases. Afterwards, you will be able to use these variables in events: for example, trigger events if the value is greater or less than certain threshold.

To create a new item, click the + *New channel variable* button on the upper panel. In the dialog box, choose the source channel and fill in the settings.

- **Title**: user-defined variable name
- **Channel**: source channel (device integration must be supporting variables, please contact support@gsfcorp.com for details)
- **Variable**: choose one from the list of available items (if none are available, the device has none or the integration does not support variables)
- **Variable type**: variable data type

For most variables, the data type is fixed, so you only need to choose the variable source and give it a name.



Click *OK* when done; the newly created variable will be appended to the list.

After you have added the channel variable, use the *Variable value* event to define the value range you want to trigger the event-action rules.

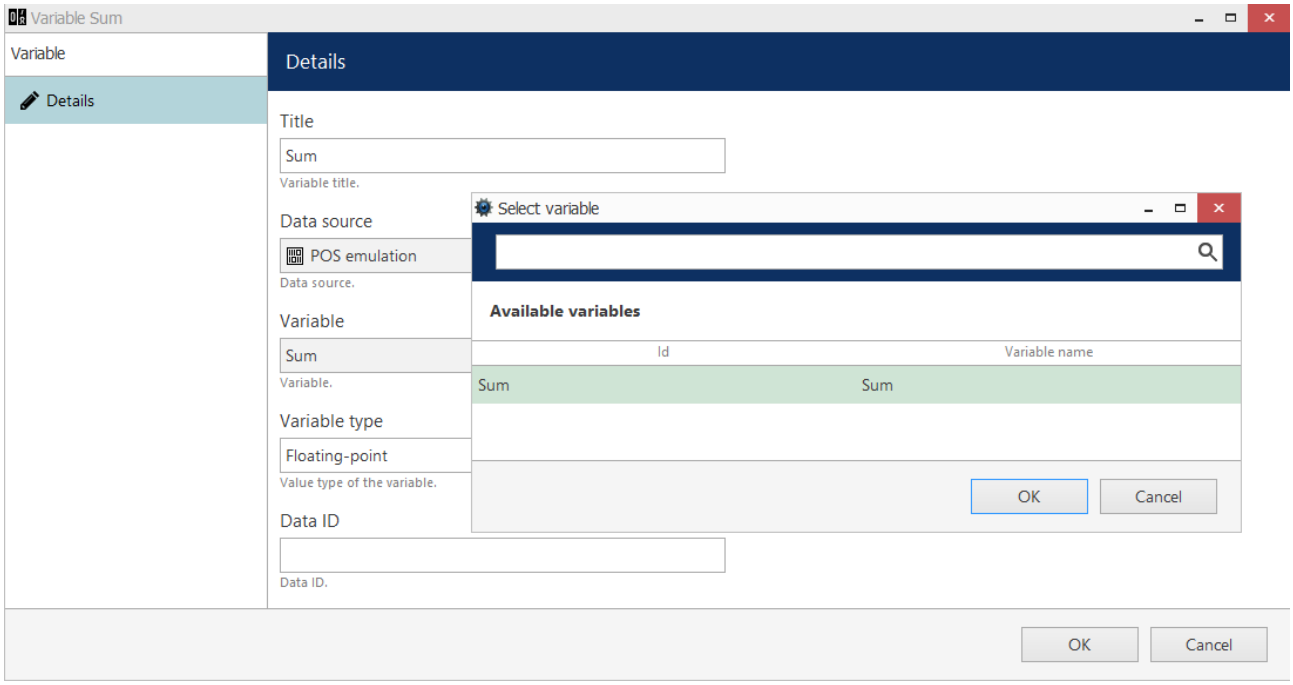
Data Source Variables

Data source variables are based on the pre-defined data source mappings. First, create some regex mappings for your data sources as described in the corresponding section of this document. Then, create a data source variable in the *Variables* subsection by clicking the drop-down arrow un the upper panel and selecting the + *New data source variable* option.

The following settings are to be defined:

- **Title**: user-defined variable name
- **Data source**: choose one of your existing (pre-configured) data sources
- **Variable**: choose one of the pre-configured mappings
- **Variable type**: choose the data type of the selected variable (for further comparison in events)
- **Data ID**: enter your POS identifier in case the data source delivers data from multiple terminals or other sources

The *Data ID* field is optional and is only required if your data source has combined streams from multiple sources. If there is only one data stream, leave the *Data ID* field empty.



Click *OK* when done; the newly created variable will be appended to the list.

After you have added the data source variable, use the *Variable value* event to define the value range you want to trigger the event-action rules.

9.11 Tags and Subjects

Macula offers a possibility to create **tags and subjects** for LPR and FR black/white lists, respectively. You can use these in combination with the Event&Action rules to roll our desired automated scenarios. Tags and subjects in Macula Console are not exported or imported to/from tags and subjects in LPR/FR services; they can act as a supplement or a replacement of these.

> Tags and subjects here are not synchronized or somehow related to those in Macula LPR or FR modules. If you already have tag lists in the LPR module, you can continue using it with E&A events.

> At this point, it is only possible to add tags and subjects from Macula Console. The option to add tags from the Macula Monitor application only refers to external LPR/FR service tags.

The recognition itself may run on an edge device (e.g., ANPR camera) or be provided by an external service. The idea is that the recognition results are received by Macula and then matched with the local tag/subject database.

Subjects are expected license plate or facial recognition results. For ANPR, a subject is a car number plate, and for FR each subject is a person.

Tags are used as marks for the LPR/FR subjects. One or more subjects with the same tag form a **list**, and you can use tags to trigger events and event chains. Each tag can be used for all types of services, which is convenient, for example, to handle access for a group of people and their cars.

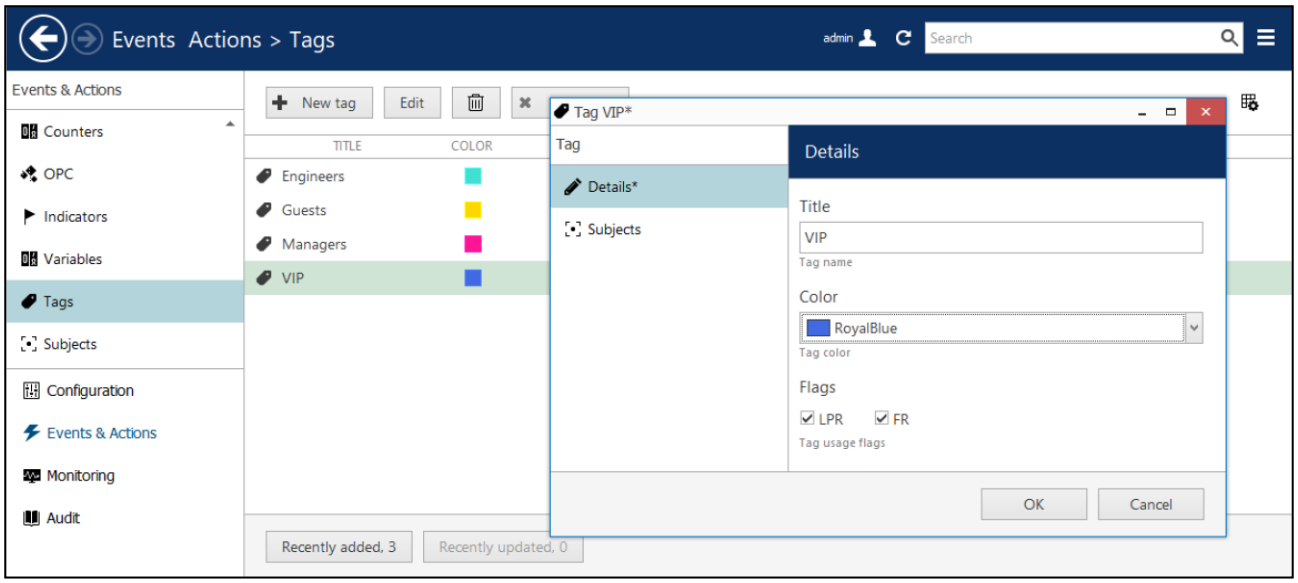
Create Tags

To create tags in Macula Console, switch to the *Events&Actions* section. Choose *Tags* on the left, then click the *+New tag* button on the upper panel.

For each tag, you can choose:

- **Title**: user-defined tag name that will appear in rules and in Macula Monitor
- **Color**: will also appear in Macula Monitor to mark entries with this tag
- **Flags**: choose if you want to use this tag for FR lists, LPR lists, or both

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



When finished, click *OK* to save and close the dialog box. The newly created tag will appear in the item list; you can edit any tag by double-clicking it in the list, or by selecting a tag and clicking the *Edit* button on the upper panel. Remove tags by selecting one or more items and then clicking the *Recycle bin* icon on the upper panel.

Create Subjects

Creating subjects is similar. To create subjects in Macula Console, switch to the *Events&Actions* section. Choose *Subjects* on the left, then click the *+New LPR subject* or *+New FR subject* button on the upper panel.

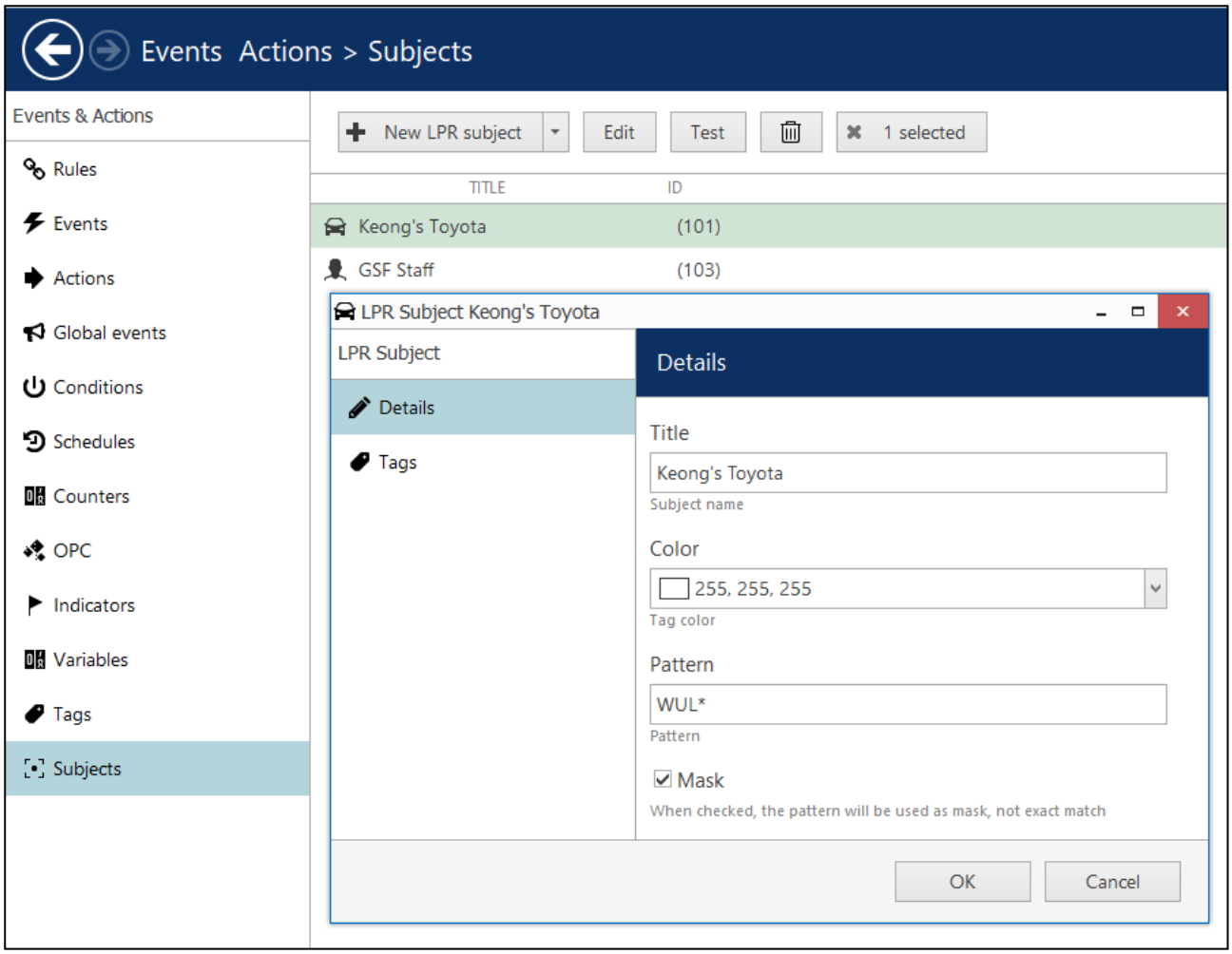
For each subject, the following settings are available:

- **Title**: user-defined tag name that will appear in rules and in Macula Monitor
- **Color**: will also appear in Macula Monitor to mark this subject's recognitions (if the subject is tagged,
  the subject color will be replaced by tag color)
- **Pattern**: exact plate number or a mask (e.g., D* to match all plates starting with D and having any length)
- **Mask**: enable this to enter a mask instead of the exact match in the pattern field above

Patterns for masks: use * for any number of unknown characters, and ? for exactly one unknown character. For example:

- F* will match all license plates of any length starting with F
- F????? will match all license plates starting with F with a total length of 6 characters
- F?* means there's F and then one or more unknown characters

Use query **testing** (see below) to check if an expected recognition value is "caught" by the mask.



When finished, click *OK* to save and close the dialog box. The newly created subject will appear in the item list; you can edit any subject by double-clicking it in the list, or by selecting a subject and clicking the *Edit* button on the upper panel. Remove subjects by selecting one or more items and then clicking the *Recycle bin* button on the upper panel.

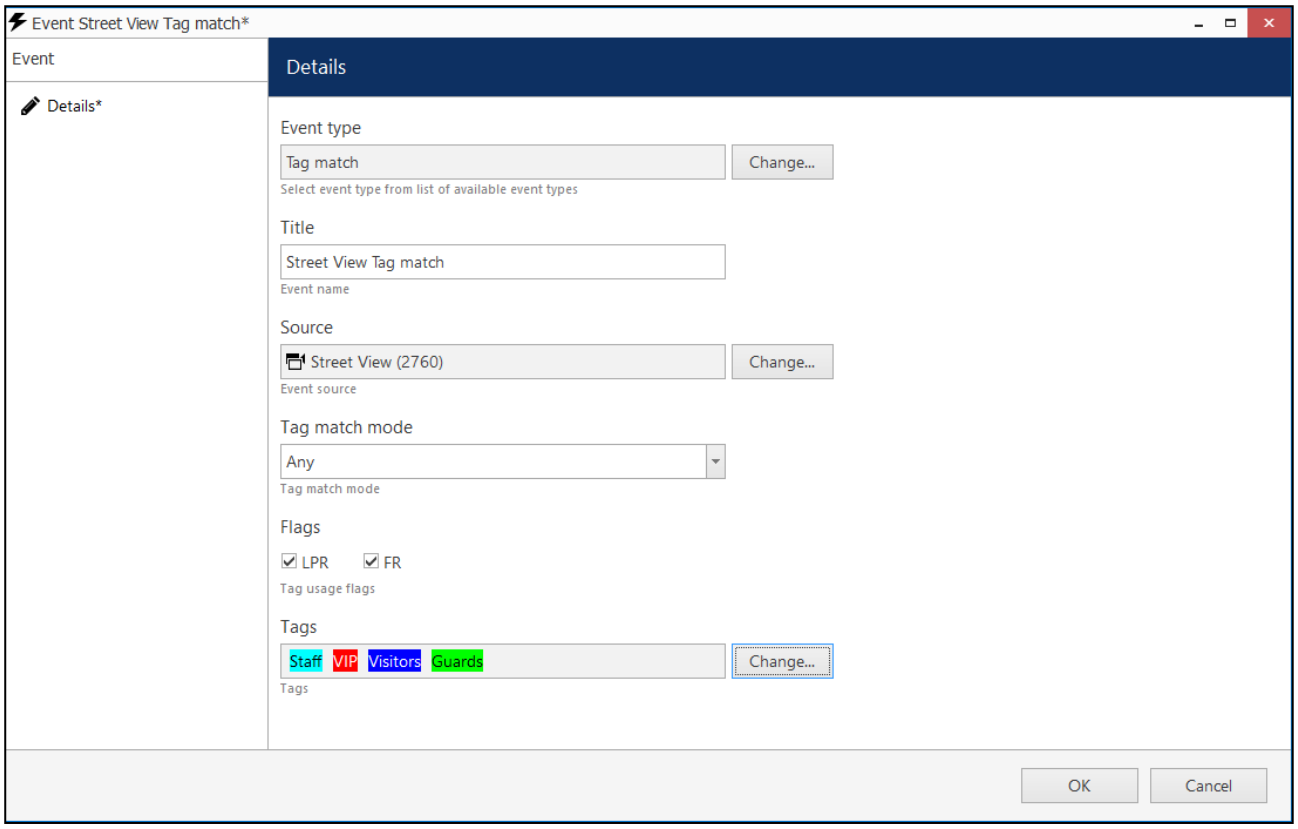
Add Tag Matching Events

A special event type is available for the built-in tags. This event is triggered **when a recognition result has a matching tag** profile: this may mean one of the required tags is present or absent, and other scenarios.

To add the **tag matching event**, switch to the *Events* subsection and click + *New event* button on the upper panel. Set the event type to *Tag match*. The following settings are available:

- **Title**: user-defined event title that will appear in the *E&A Configurator*
- **Source**: a channel that will serve as a recognition source
- **Tag match mode**: choose what kind of match you want (see more detailed explanation below)
- **Flags**: choose one or more if you want this tag event to be triggered for specific recognition type
- **Tags**: choose a set of tags that will be used for comparison

Recognition may be LPR or FR and it may run on the camera side or as an external service.



Possible tag **match modes**: event will be triggered if..

- **NoTags**: recognition result does not have any tags (the license plate/subject is not present in the database)
- **Any**: recognition result tag matches one or more tags in the list (at least one)
- **All**: recognition result matches all defined tags (possibly more, but at least those listed)
- **NotAny**: doesn't match any of the specified tags

For example: in the snapshot above, the event is triggered when recognition result matches *Staff*, *VIP*, *Visitors*, or *Guards* tag.

Create Rules

As soon as you have created tag-based events, you can match them with any actions to create automated scenarios in the *Event & Action Configurator*.

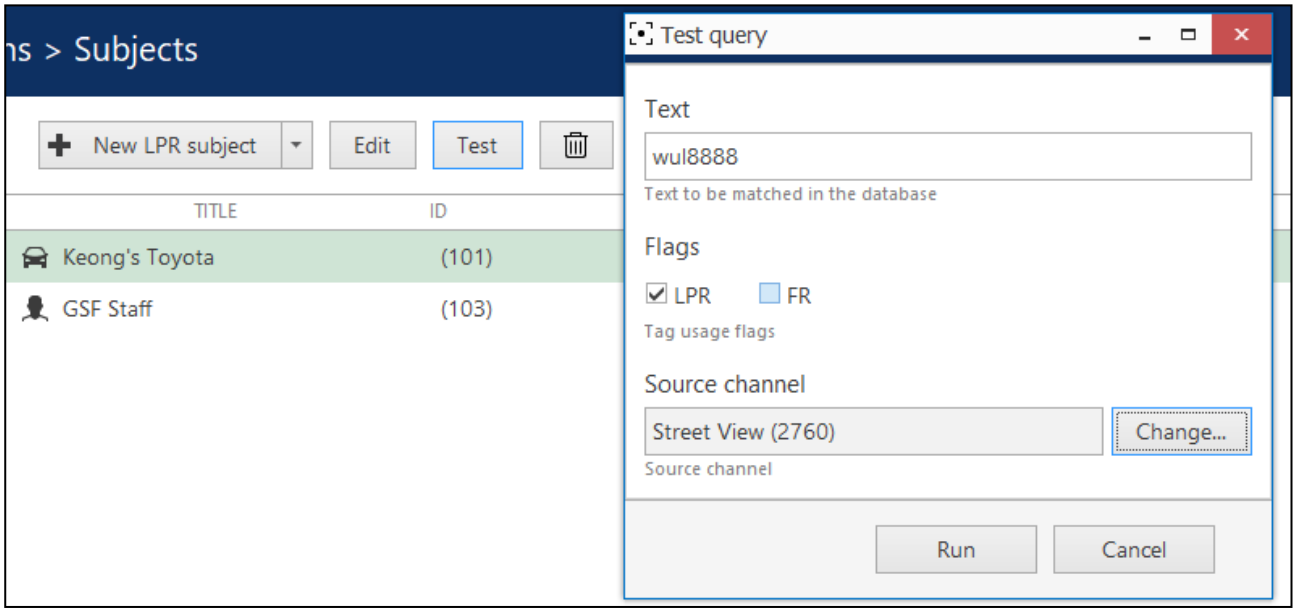
Rule examples:

- open a gate based on staff car entering (action: change DO state, prerequisite: DO wired to the gate)
- notify operators with a sound (action: send event to client, option: play audio notification, prerequisite: audio notifications enabled on the client side)

Test Tags and Subjects

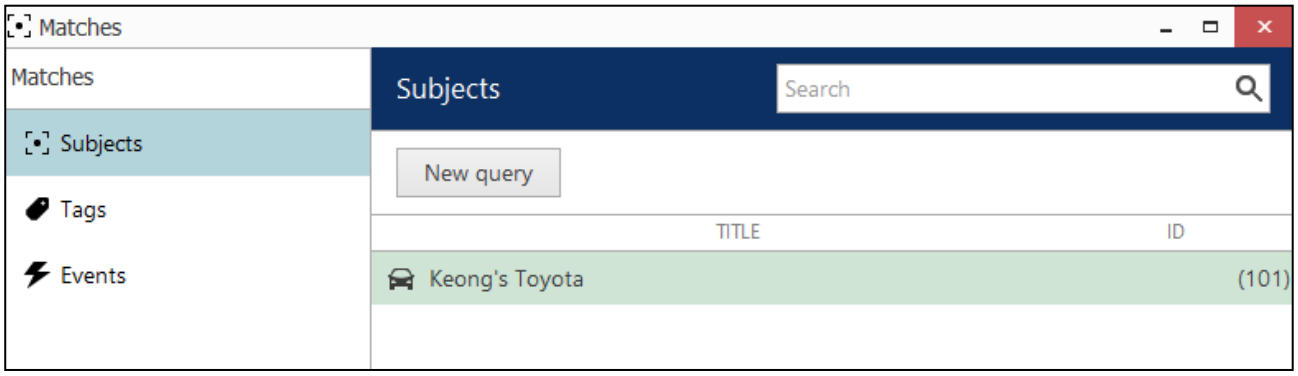
From the *Subjects* section, you can **check if the whole scenario works** for a specific **recognition result**. Simply click the *Test* button on the upper panel, enter the desired parameters, and click *Run*. The test query is not bound to any specific subject entry so it does not matter which item is selected in the item list.

The test validates if the entered recognition value has any matching subjects and, therefore, tags, and also checks if it triggers any events. Events are only checked if there are active rules using these events!

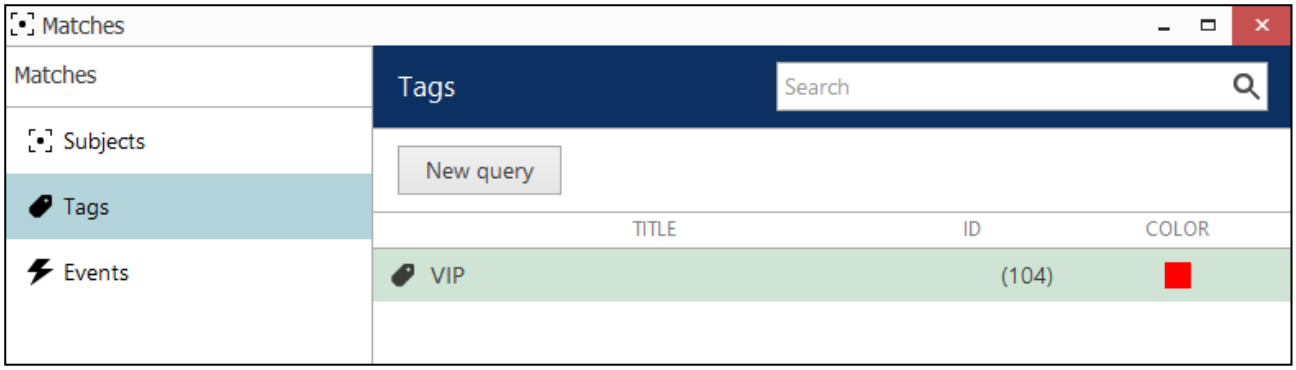


As an example, let's see the test results for the test above. The dialog box with the results will have several tabs.

In the *Subjects* tab, all matching **subjects** will be listed. In the example here, E-plate matches the recognition result because this subject is defined as a mask WUL*, matching any license plate starting with WUL.

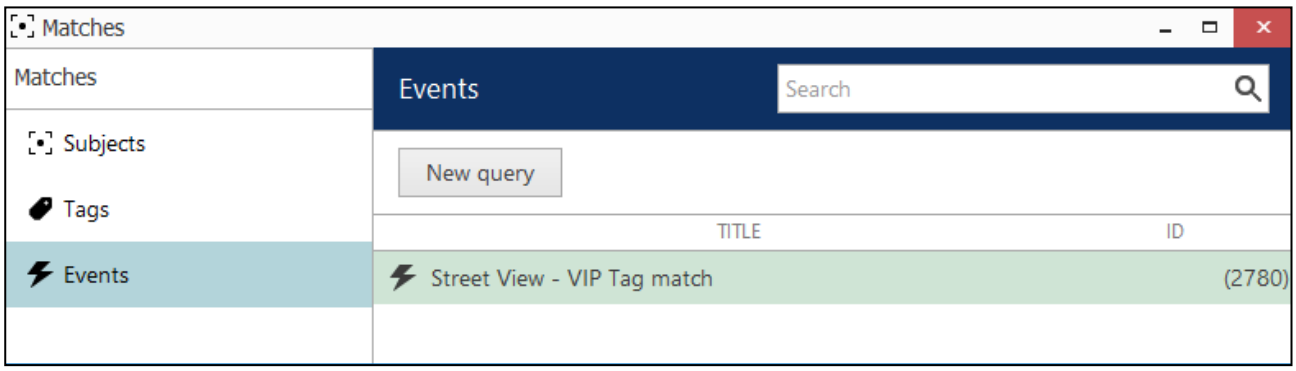


In the *Tags* tab, all matching **tags** will be listed with their corresponding colors.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Finally, in the *Events* tab, you will see, which **events** would be triggered by the test pattern.



Note that the event list will be empty if there exist some relevant events but there are no rules using them!

9.12 ONVIF Generic Events

Custom ONVIF Events

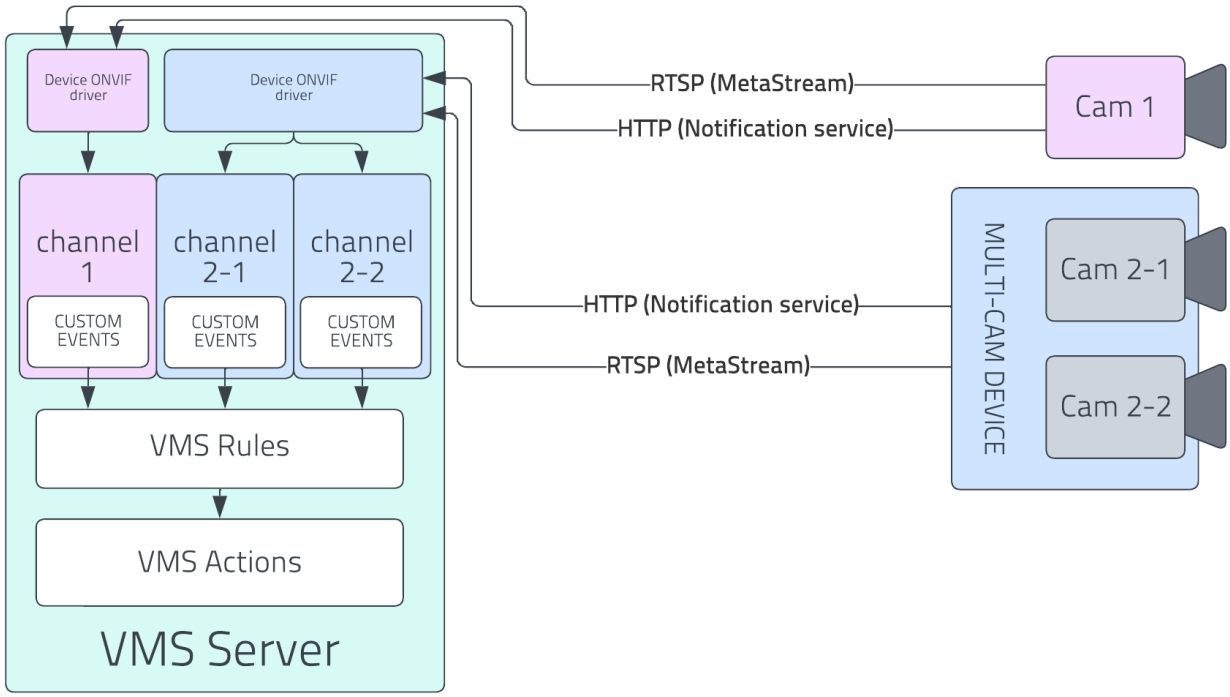
Introduction

You can create custom rules based on ONVIF camera-generated events inside Macula Console *Events & Actions*. To do so, you need:

1. ONVIF compatible camera connected via ONVIF driver to the Macula,
2. Understanding of the camera events,
3. Basic knowledge of the ONVIF standard XML responses generated by your cameras.

Although ONVIF is a set of rules that standardizes video monitoring hardware and software - the range of available options is extensive, and different cameras may have very different capabilities. In the context of this manual, we will focus on integrating this wide range of varying camera capabilities into the Macula and fully utilize your camera potential.

The scheme below represents the cameras sending Event data to the Macula server.



This event data is sent via RTSP and HTTP in XML format and adheres to the ONVIF-defined standard. Both streams may represent the same or different events, and you must invest your attention to get out the most from your setup.

User Defined Events

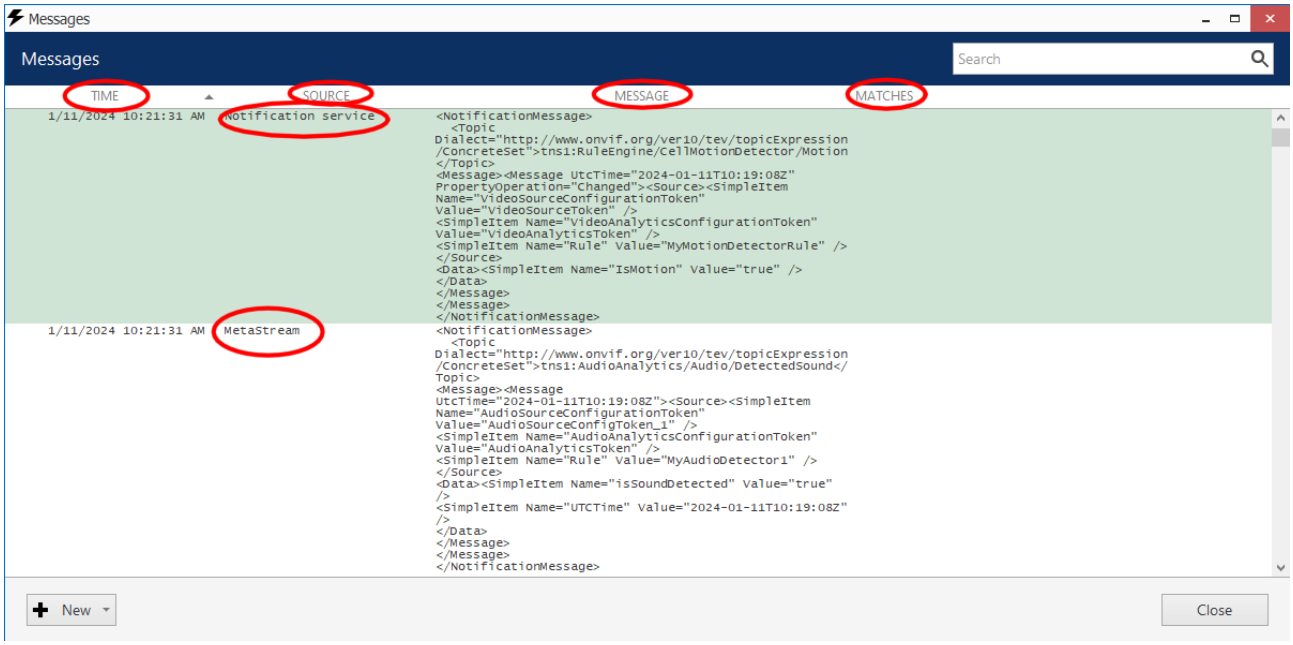
To begin with the ONVIF-based custom event creation, you must add a camera via the Generic ONVIF driver. You can find how to add your devices in a corresponding part of this manual.

1. After adding a device, find the *Channels* inside *Macula Console -> Configuration* sub-section.

2. Find the corresponding channel and open it in a pop-up window by double-clicking on its name or selecting it and pressing the *Edit* button on the top of the channel list subsection.
3. Find the *User defined events* in the pop-up window at the bottom of the right subsection.

You will see the empty subsection with three buttons on the top. *+New* drop-down button, grayed-out *Edit* button, and *Notification messages* button. You can create a New generic event by clicking the *+New* or *Notification Messages* buttons. Both options will bring the new *Messages* pop-up window with the list of received notification messages in XML format. Received data represented in a table-like form with columns:

- **Time** - Received notification server timestamp (MM/DD/YYYY HH:MM:SS)
- **Source:**
  - **Notification service -** data stream received via HTTP
  - **MetaStream -** data stream received via RTSP
- **Message** - Received data in XML format. The Message column is updated in real-time as the data is received.
- **Matches** - if you have already created a generic event filter, you will see an indication for the events with exact matches for that existing filter.



Locate the event you want to use as the prototype for the filter, click on it, and then click on the *+New* button on the bottom-left part of the pop-up window. You may find the same event inside both - *Notification service* and *MetaStream* data. For such cases, our recommendation is to use *MetaStream*. This stream is sent together with the video stream, so it is easier to notice any instability the third-party factors may cause.

> ⚠ N.B. You can find your camera capabilities in the manufacturer's manual or the Conformant Products - ONVIF webpage.

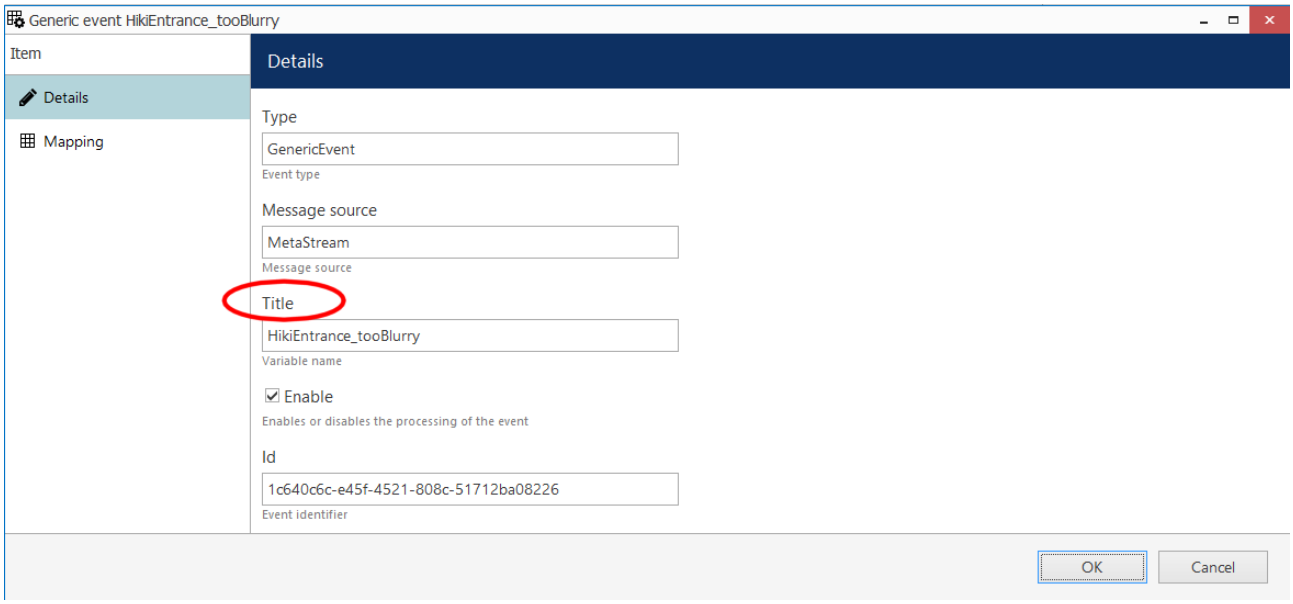
This will bring the Generic event pop-up window.

You will see the following fields inside the Details tab:

- **Type -** Event type (in this case - *GenericEvent*), non-editable.

- **Message source** - *Notification service/MetaStream*, non-editable
- **Title** - the only field that the user should fill in. The display name of the created event. Editable.
- **Id** - Event identifier. The field will be completed automatically after the event is saved. You can identify the event inside log files by this ID.
- **Enable** checkbox - enable event processing. Uncheck it to stop processing the event.

The only field you should fill inside the *Details* subsection is the *Title* field - add a meaningful name that will allow you to recognize this event inside the *Events & Actions Configurator*.

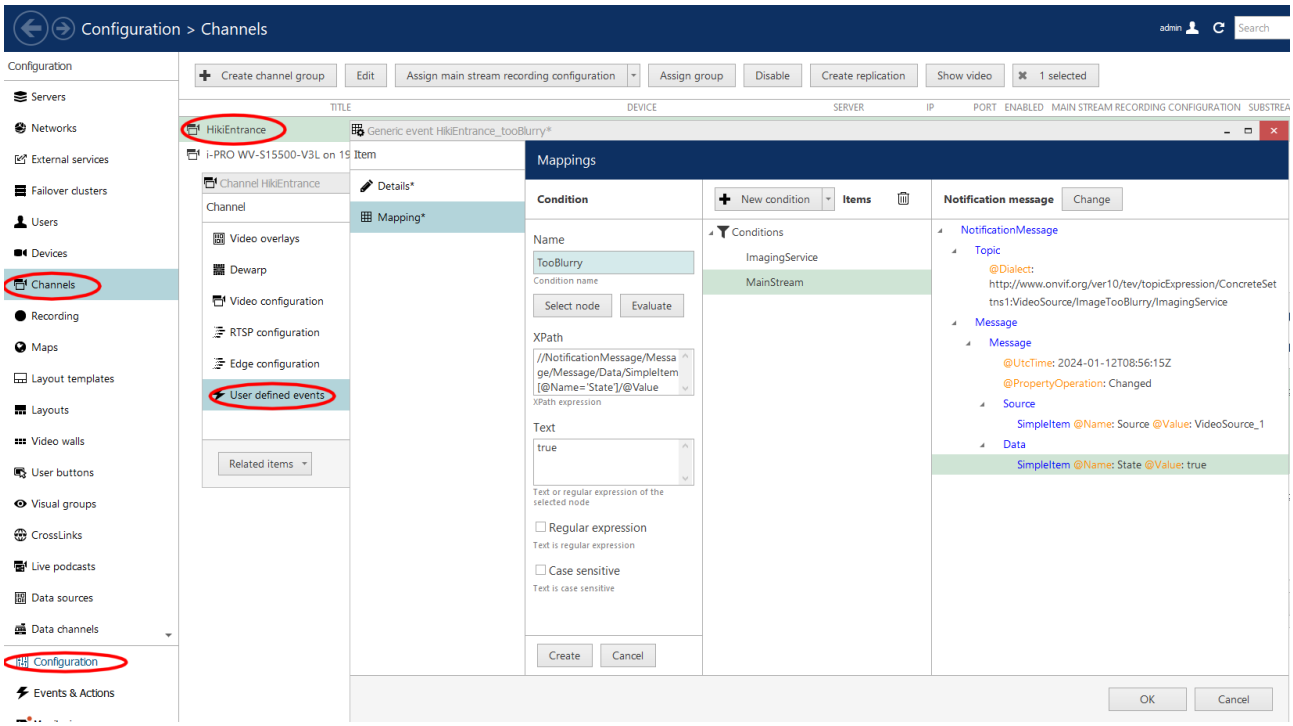


VCA event mapping

The next step is to map data. Inside the Item subsection, locate the *Mapping*; this will bring the *Mapping* options. You will see three subsections:

- **Notifications message** - the most-right subsection of the *Mapping* section. Provide a detailed view of the selected message.
- **Items** - represents the mapped portions of the *Notification message*. You may create multiple items - only exact matches will be processed (similar to the && conditional operation).
- **Condition** - the left subsection of the *Mapping* section. This subsection allows adjustments to the *Items* created in the *Items* subsection. You will find the following interface elements:
    - **Name** field - You can edit this to make the Items subsection more readable. Provide a meaningful name for the *Condition* Item.
    - **Select node** button - which will bring a pop-up screen with the notification message. Use it if you want to change the part of the message your item is based on.
    - **Evaluate** button - Evaluate if the created *Item* matches the current condition. Use it if you manually adjusted *XPath* or *Text* fields to avoid errors. Values: "true" - if the Item condition matches the Notification message; "false" - if *XPath* value or *Text* does not have an exact match.
    - **XPath** input field - represents the path to the *Item* conditional value in the context of the *Notification message* tree; may contain variables.
    - **Text** input field - represents the value that must match to meet the event's trigger condition.
    - **Regular Expression** checkbox - mark it if REGEX is used for conditioning.

- **Case sensitive** checkbox - by default, condition matching is registry case-independent. Mark this checkbox only if you need registry case-dependent conditioning.
- **Save/Apply changes** button - Save changes before switching to the next *Item* or confirming event with the *OK* button at the bottom-right corner of the *Mappings* subsection.
- **Cancel button** - Cancel current changes made to the selected Item.

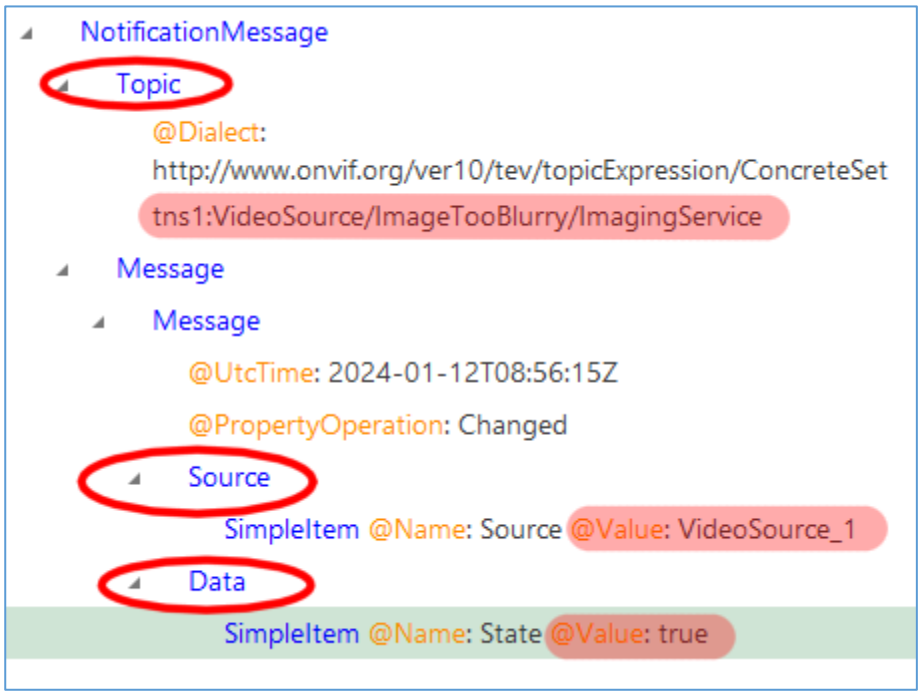


Blurry mainstream Custom VCA Event scenario

At first glance, Generic events may seem complicated, but they provide an unprecedented level of elasticity if needed or allow the creation of simple event triggers from otherwise incompatible devices. The example below will create a generic event based on the ONVIF camera's mainstream blurriness.

1. Ensure the camera is connected via the ONVIF driver and the Camera analytics is up and running.
2. Go to *Configuration -> Channels* -> 'Your Channel' and double-click on it.
3. At the bottom of the right section, find *User defined events*, select it, then on the top of the right subsection, click the *+New* button -> *New generic event*.
4. Locate relevant event. In the example case, this will be an event sent via Metastream containing information on the image quality. Click on the *+New* button at the *Messages* window's bottom-left side.
5. In the provided example the event is named "HikiEntrance_tooBlurry." Click on the *Mapping*. You will see already created *Item* based on the event topic.
6. For Example, the camera has both mainstream and substream, and the mainstream is found under the *Message/Source/VideoSource_1*. To evaluate only mainstream, you need to create one more *Item*.
7. At the *Notification Message* subsection, locate *Message/Source* and click on the node; then, in the *Items* subsection (the one in the middle), click the *+New condition* button. You can change the *Item name* to something more meaningful, like in the provided example, "MainStream," and confirm the adjustment with the *Create* button..

8. Now, the system knows "where to look." All that's left is to tell the system what it must look for. Create one more *Item* from the *Message/Data* node. In the provided example, you need to evaluate if the image is blurry, so you are looking for the value - "true." Select the Data node, Click the *+New condition* button, rename the *Item* as "TooBlurry," and confirm it with the *Create* button.
9. Confirm Generic Event with the *OK* button, then confirm it again with the *Apply* button under the *User defined events* subsection.

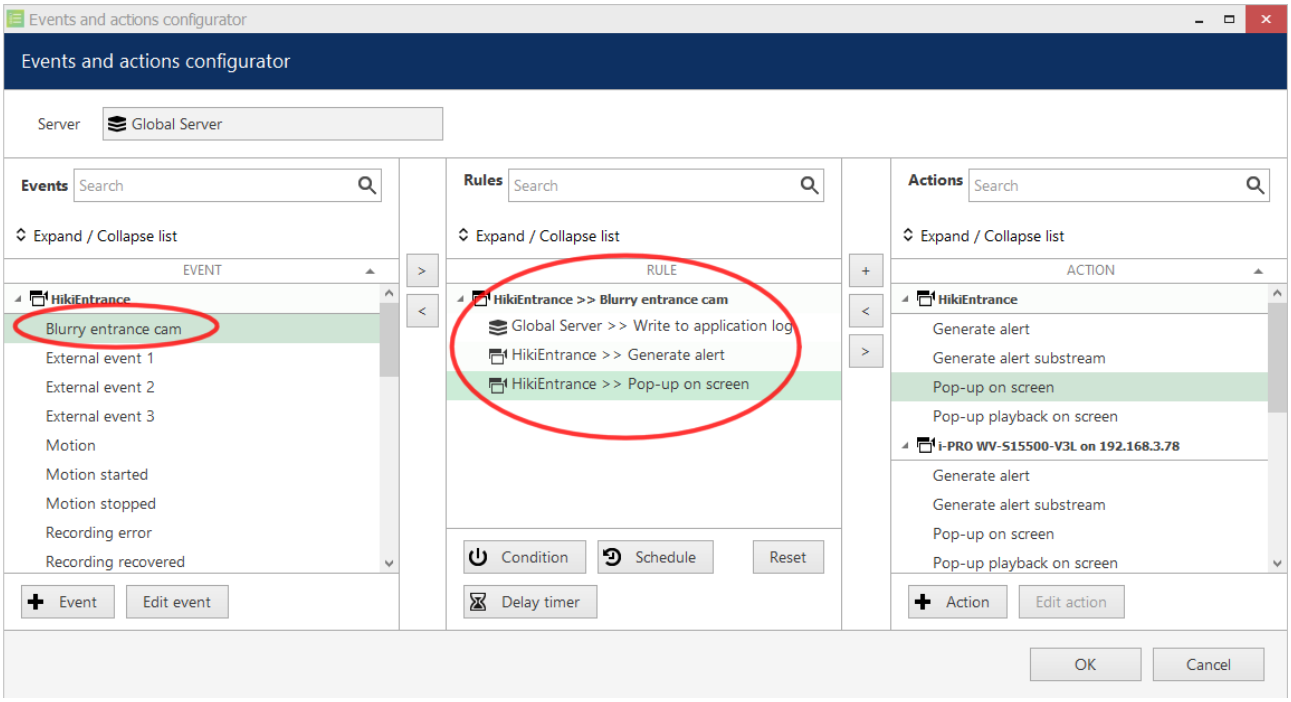


From now on, you are ready to build *Actions* based on the blurriness of the camera mainstream. To do so:

1. Go to the *Macula Console -> Events & Actions -> Events*
2. At the top-left part of the *Events* subsection, find the *+New event* button and click it.
3. Find the *VCA event* (Stands for Video Camera Analytics) from the pop-up window and confirm with the *OK* button.
4. Add the *Event Title*, which will be displayed inside the configurator. Name it "blurry entrance cam."
5. Click the *Change* button on the right side from the *Source* field and select the camera you used to create that generic event.
6. To bring a custom event to its full potential, you must add the *VCA rule*. Click the *Change* button and find your generic event name in the pop-up window. It will likely be at the bottom of the list. Confirm your selection with the OK button, then click the *Apply* and the OK buttons to save your event.
7. Go to the *Rules* subsection and open the configurator. The goal is to log this event to the server, generate an alert, and pop up the channel inside the Macula Monitor.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



That's it. All the Actions are now available for your event. This way, very complicated scenarios might be created, starting with basic notifications for the simple analytics event and up to very specific conditioning for the VCA value for the particular case.

10 Other Resources and Functionality

Apart from the main video management system resources - video channels - Macula provides miscellaneous types of auxiliary resources and object types like maps and user buttons, and video walls for Macula Enterprise edition.

This chapter contains documentation on additional resource types, their properties, and related tools.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.1 Webpages and CrossLink Channels

Macula servers can work with several types of **interactive resources** - meaning that the user can not just watch and record the feed, but also control its contents from the Macula Monitor application. These resources are called CrossLink channels. CrossLinks can provide a direct interactive interface to SCADA, access and flight control, radars and lidars, other VMS software, and other applications. This means a straight-away front-end integration without any additional implementation.

CrossLinks require a special license and are represented by **interactive webpages** and by interactive **desktop applications**. Depending on the setup, these allow capturing, recording, and controlling the remote contents in an intuitive manner.

CrossLink Types

How to choose the required resource type based on your use case scenario:

- webpage device: the interactive device is created on the server side (like for any camera) to allow live & recording
- direct webpage: there is no device on the server side, live Web contents goes directly to Macula Monitor, allowing multiple independent sessions
- remote desktop: the device is created on the server side (like for any camera) to allow live & recording
- non-interactive webpage device: static video feed to the server for recording and non-interactive display (does not require CrossLink license, just a regular channel)

Basically, you need to determine whether you want to

1. Have a remote **Web interface** (website, Web server) or a **workstation**.
2. In case it is a Web application, choose if
    a. The user should be able to **control** the remote contents,
    b. It needs it to be **recorded** on the server side.

Below, you fill find more detailed information about each type and step-by-step configuration guidelines.

Prerequisites

For all interactive contents, you need a special license channel type called **CrossLink**. The required number of CrossLink channels is added to your license alongside regular channels and VA channels. There are two different types of **CrossLink licences**:

- **Basic**: interactive Web with or without recording
- **Advanced**: interactive Remote Desktop (server-side device)

Advanced CrossLink license includes Basic CrossLink options as well, meaning you can use an Advanced CL license for creating a Basic CL item (webpage). For non-interactive Web devices, a regular channel license is used, and there is no need to obtain a CL license of any kind.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Feature	Regular Channel	CrossLink Basic	CrossLink Advanced
Display and record live web pages without user interaction	Yes	Yes	Yes
Display interactive webpages	-	Yes	Yes
Record interactive webpages as channels	-	Yes	Yes
Display and record interactive desktop applications as channels	-	-	Yes

For every remote **workstation** you wish to add under CrossLink Advanced, you need to install any **VNC server software** on the remote side and ensure its accessibility via given IP/host and port. (For Mac computers, simply enable it in the settings.)

We strongly recommend using visual groups for CrossLink Advanced channels, so that the users can differentiate between video streams and interactive contents.

CrossLink Basic: Interactive Web Device

CrossLink Basic provides access and interaction with **Web applications**. These may be websites, device interfaces, or Web services, and you can stream and record any of these. Special device model, *(CrossLink) Interactive URL*, is reserved for this. Each device of this kind uses 1 (one) CrossLink Basic channel license.

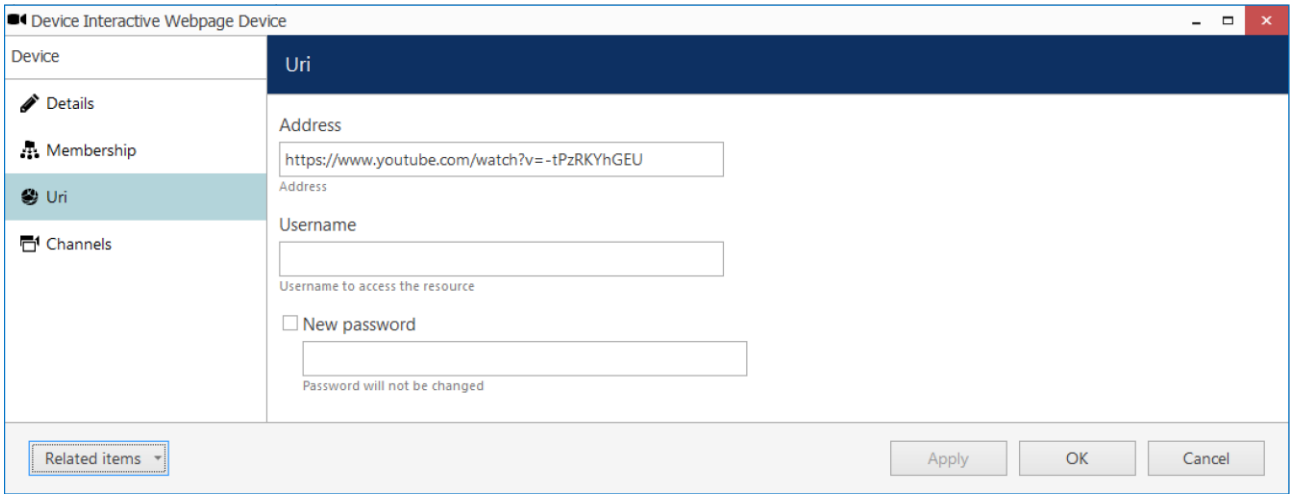
To create an interactive web device in Macula Console, go to the *Configuration* section in the bottom left panel, choose *Devices* on the left, then click the + *New device* button in the upper panel to bring up the item creation dialog box.

In the model list, choose the **(CrossLink) Interactive URL** model**.** Then, switch to the *Uri* tab and fill in the settings:

- **Address***: full target URL
- **Username**: if required
- **Password**: if required

***Note that redirects from the specified domain are not allowed. Therefore, the specified link must not be a shortened URL (e.g., youtu.be, or goo.gl)

⚠ No redirects from the specified domain are allowed for security reasons.



Click *Apply* to save the settings, then switch to the corresponding channel using the *Related items* button in the bottom left corner or the dialog box.

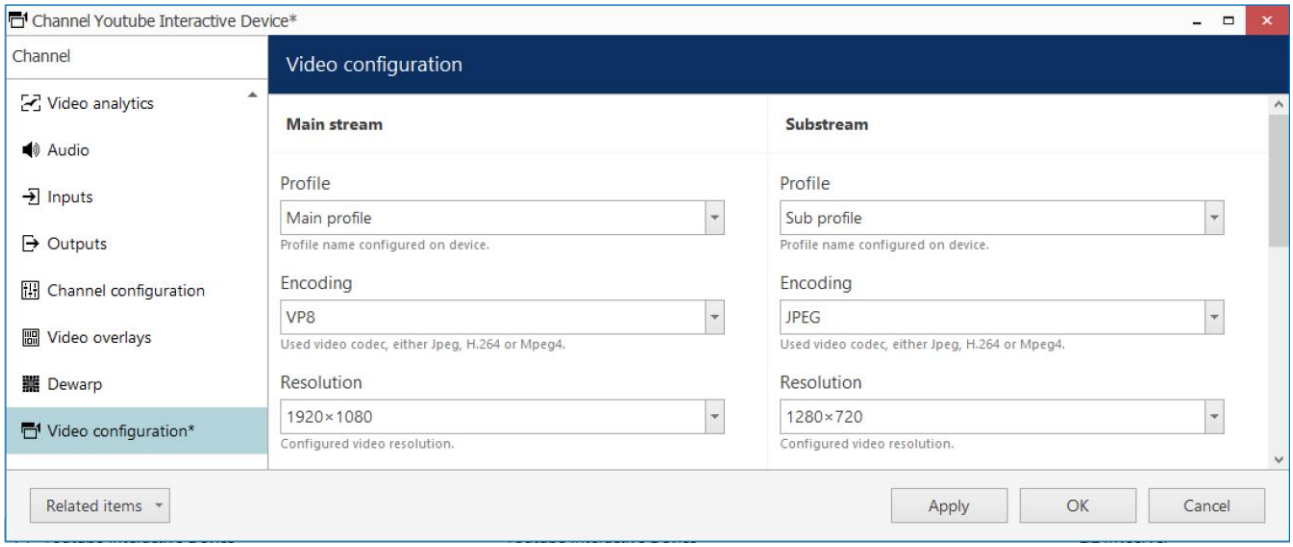
Basic channel settings are the same as for the traditional channels with the following elaboration:

- recording can be configured for **both main and secondary** streams
- **audio** is not available
- remote control **permission** is granted using *PTZ Control* permission
- **video parameters** can be set up in the *Video configuration* tab:
  - choose between JPEG (higher quality, bigger size) and VP8 (smaller recording size at the expense of picture quality) **compression**
  - select **resolution** (but be careful when combining VP8 with lo-res and low bitrate, it may make the text unreadable)
  - set bitrate and target frame rate

Use VP8 cautiously as it may decrease image quality dramatically, and render the text unreadable on smaller resolutions. Larger resolutions will increase CPU usage on the server side and may produce sluggish image display. The main advantage of using VP8 is that it uses much less storage space thanks to compression, so the recommended usage profile would be to use one stream with VP8 for recording, and another one with JPEG for live view and interaction. You will be able to switch between streams in the Macula Monitor application.

When setting VP8 with a specific bitrate, keep in mind that it will be the maximum possible bitrate, not the target bitrate.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



There is also a **dedicated tab** with CrossLink-specific settings. The following settings are available here:

- **Ignore certificate errors**: if enabled, invalid certificates will be ignored, and the page will be opened even if something is wrong with the site certificate (only do this if you trust the page certificate!)
- **Auto refresh interval**: enable this if the remote Web contents is dynamic and you want the page to be refreshed without user interaction

As Web contents poses certain threats, we do not recommend ignoring certificate errors unless you trust the page completely. Also, the following **rules** will apply to **browsing**:

- **no redirects** from the specified **domain** (sub-domains are allowed)
- **no pop ups** (including floating windows and new pages opened in a new tab)
- **no downloads** or **copy-paste**

Keep this in mind when configuring your interactive URL device. You will get a corresponding error message in the **channel's notification panel** in Macula Monitor if some of these restrictions are activated.

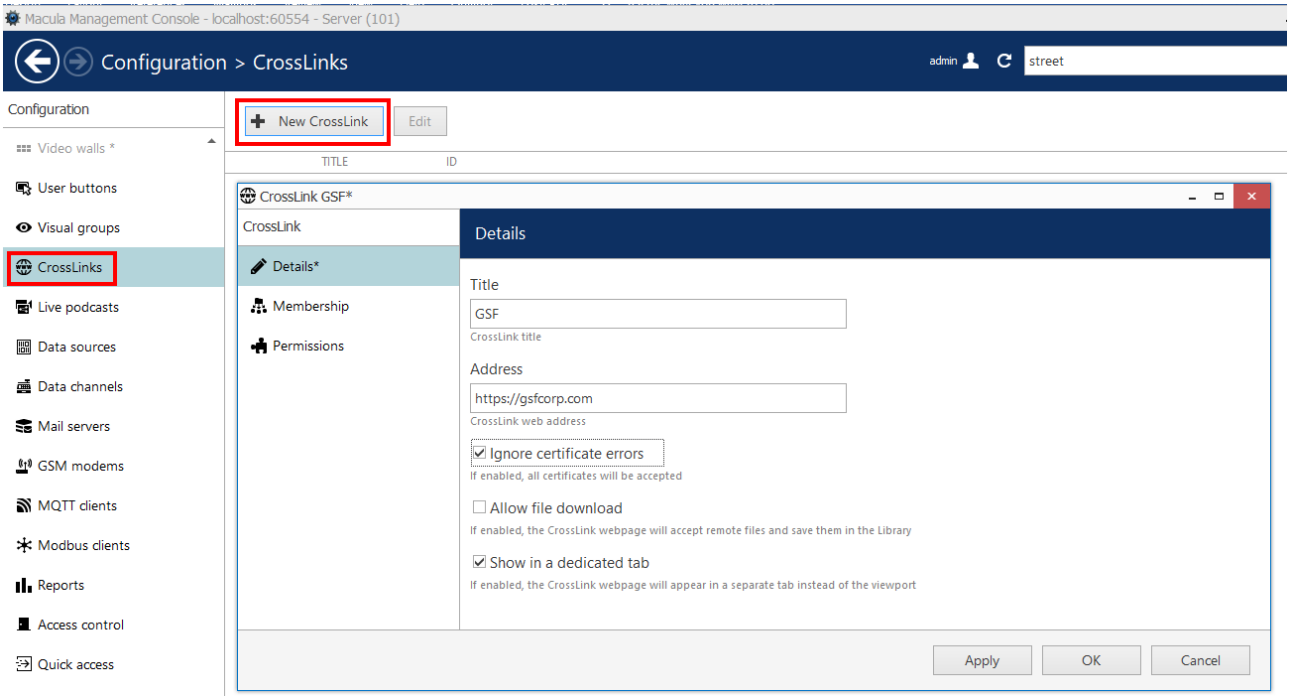
Example: the link to *youtu.be* will not work as it is a shortened link and it redirects to another domain, *youtube.com*. Use the full URL in the device configuration.

CrossLink Basic: Interactive Web

If you do not need to record the web contents, but would rather like to **access the Web page directly** from Macula Monitor, you do not need to add a device: instead, simply create a Webpage in Macula Console, and it will go directly to the Macula Monitor application. This item requires one CrossLink Basic license.

You can use this type of resource for:

- configuration of IP cameras
- configuration of Web services
- remote control of any non-integrated, or advanced setup of integrated devices
- providing variety of resources while in kiosk mode (operator instructions etc.)
- To create the webpage, go to the *Configuration* section of Macula Console, choose *CrossLinks* on the left, then click the *+ New CrossLink* button on the upper panel.



Settings:

- **Title:** webpage name that will appear in Macula Monitor
- **Address**: full webpage URL (no shortened links!)
- **Ignore certificate errors**: if enabled, invalid certificates will be ignored, and the page will be opened even if something is wrong with the site certificate
- **Allow file download**: the webpage will accept remote file downloads and save them in the Library if the checkbox is marked.
- **Show in a dedicated tab**: Show in a dedicated tab: if the checkbox is marked - the webpage will disappear from the viewport, and the new item in the Main menu will appear.

Click *OK* to save and close the window. The newly created webpage will appear in the list. Your Macula Monitor application will now have an extra section in the *Resources* panel (on the left) containing webpages.

As Web contents poses certain threats, we do not recommend ignoring certificate errors unless you trust the page completely. Also, the following **rules** will apply to **browsing**:

- **no redirects** from the specified **domain** (sub-domains are allowed)
- **no pop ups** (including floating windows and new pages opened in a new tab)
- **no downloads** or **copy-paste**

Keep this in mind when configuring your webpage. You will get a corresponding error message in the ***Alerts* tab** in Macula Monitor if some of these restrictions are activated.

Example 1: you cannot configure the webpage to google.com and let the user search: they will be unable to navigate to a specific result as it involves domain change.

Example 2: you can add a Wiki webpage and let user choose the language, as it will redirect them to the third-level domain (say, en.wikipedia.org or de.wikipedia.org), which is OK.

CrossLink Advanced: Remote Desktop

On top of the previous features, CrossLink Advanced adds the opportunity to remotely control any workstation from Macula Monitor. The target machine may run Linux or macOS, the one requirement is that the remote party must have VNC server software (any) up and running.

Using one CrossLink Advanced license, you can configure any of the interactive channels - be it a webpage, webpage channel, or a remote workstation channel.

> ⚠ Be careful when you grant access to this kind of device, as it gives the user **full control** of the remote PC. You may want to use **additional security**, e.g., ask user for a password on behalf of the OS.

Usage examples:

- remote access to Linux workstations with non-integrated software
- access to other VMS software running on an older or embedded version of Windows
- recording of operator workstations running Macula Monitor or any other software

Each Remote Desktop channel will use one CrossLink Advanced license. If your license only includes Basic CrossLink channels, you will not be able to add a new device of this kind.

Add Device

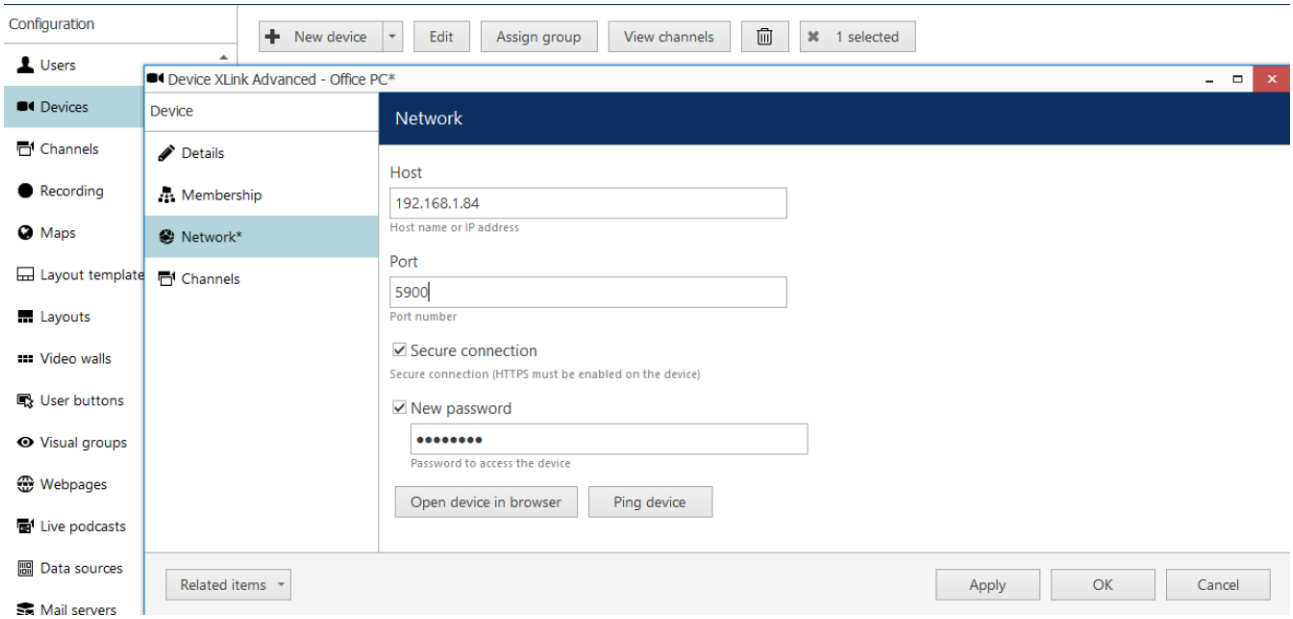
To create a **remote desktop** controlling device in Macula Console, go to the *Configuration* section in the bottom left panel, choose *Devices* on the left, then click the + *New device* button in the upper panel to bring up the item creation dialog box.

In the model list, choose the **(CrossLink) Remote Desktop** model**.** Then, switch to the *Network* tab and fill in the settings:

- **Host**: target machine IP or hostname
- **Port**: the port for VNC connection (5900 by default)
- **Secure connection**: enable to use HTTPS (must be enabled in the VNC server settings), or leave empty for insecure connection
- **Password**: enter the password, as defined on the remote side

Use the *Ping device* button below to check the remote workstation availability.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



When you have finished, click *OK* to save and exit; the newly created device share will appear in the item list, and its channel also immediately appear in the Macula Monitor application(s) for eligible users.

> ⚠ If your created *Remote Desktop* device does not work and you think all settings are correct, install a local VNC client on the Macula server and see if you can reach the remote machine this way.

To edit any of the previously created devices, double-click it in the item list or select any with single mouse click and then hit the *Edit* button on the upper panel. Use the *Search* field in the upper-right-hand corner to quickly find the existing items, and the *Disable* button to **disable and enable** channel sharing. Use the 🗑 recycle bin button in the upper-right-hand corner to remove one or multiple items: hold *CTRL* or *Shift* to select several items at once, or *CTRL+A* to select all.

Filters in the bottom panel allow you to load recently added/modified items.

Channel Configuration

Most of the channel settings are the same as for the traditional channels with the following elaboration:

- recording can be configured for **main stream** only, as there is no secondary stream
- **audio** is not available but you can combine the video with audio stream from a camera (use the *External* option in the *Audio* tab and choose the source channel)
- remote control **permission** is granted using *PTZ Control* permission
- **video parameters** can be set up in the *Video configuration* tab:
    - choose between JPEG (higher quality, bigger size) and VP8 (smaller size at the expense of picture quality) compression
    - select resolution (but be careful when combining VP8 with lo-res and low bitrate, it may make the text unreadable)
    - set bitrate and target frame rate

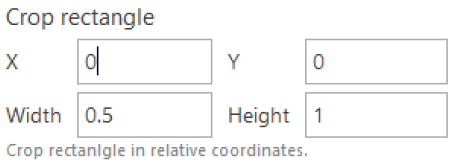
Frame rate will be **dynamic** during remote control and recording, meaning that FPS will be low while nothing happens, but it will grow if the remote user starts doing something or if there is video playback.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Optimal interactive video configuration for most use cases is JPEG @1080p.

Output Area

CrossLink Configuration is a dedicated tab for CrossLink-specific settings. Currently available settings include **cropping** setup, which allows you to select the region that will be displayed in the Macula Monitor application. In other words, you can crop the whole incoming image and only show/record a specific area. This comes useful, for example, when the remote workstation has multiple displays. Cropping affects both Macula Monitor **display and recording**.



By default, the output area is full - X=0, Y=0, Width=Height=1. The coordinates and size are relative. Crop examples:

- Full image: X=0, Y=0, Width=1, Height=1
- Display 1 of 2: X=0, Y=0, Width=0.5, Height=1
- Display 2 of 2: X=0.5, Y=0, Width=0.5, Height=1

If the remote workstation is configured to ask for a **password**, and you intend to control it remotely from Macula Monitor (not just record), make sure you can see the right display.

Remote control does not allow to send **system key combinations** (e.g., CTRL+Alt+DELETE) to the remote workstation; local OS will catch these key combinations. Therefore, make sure to disable the “Press Ctrl+Alt+Del to Log on” option on remote Windows workstations.

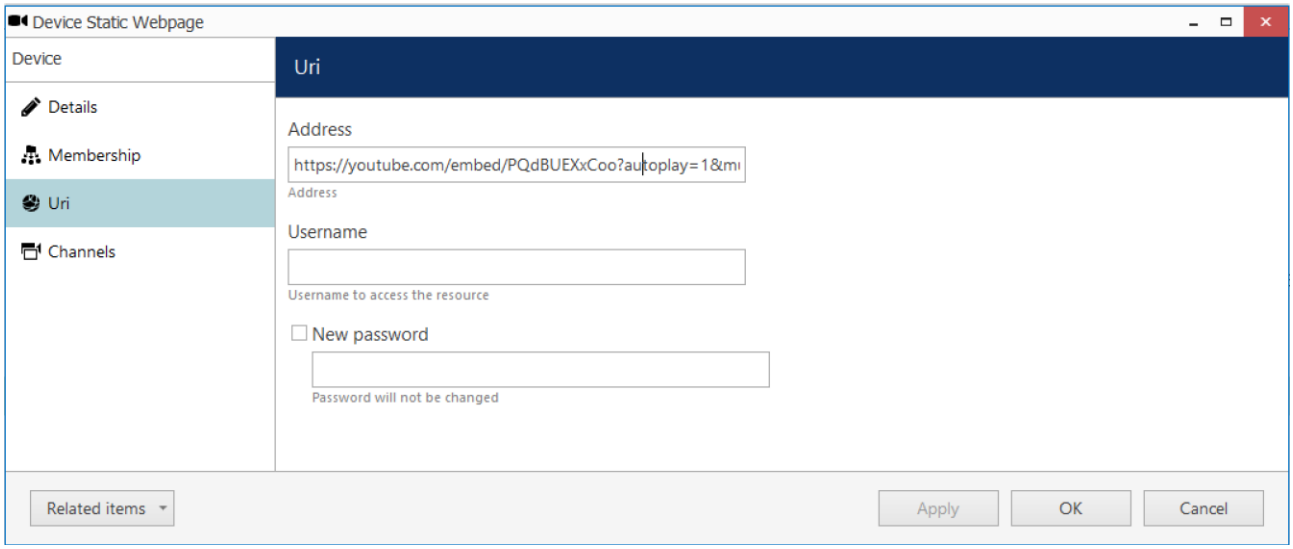
Non-Interactive Web Device

If you want to record and use non-interactive webpages in Macula Monitor, use a special device driver type called HTML Source. These represent static webpages, which are available for recording as any other channels, and are visible in the Macula Monitor application. As this type of device is non-interactive, no CrossLink license is used: HTML source devices require a **regular channel license**.

Usage examples:

- Display media contents for marketing purposes
- Digital signage
- Statistics and dashboards

To create a non-interactive page, create a new device and set its model to **HTML Source (view only)**, then assign it to the desired server. Similarly to interactive webpage, set the **target address** in the *Uri* tab. The user will be unable to navigate away from this address, so make sure you specify the full and exact URL. If the target page requires **authentication**, enter the username and password in the device properties.



Next, click the *Related items* button and switch to the channel edit dialog box.

As the webpage contents will be static in the Macula Monitor application, you need to take care of the **contents transition**. To force refresh contents from the Macula side, use the auto refresh parameter in the channel properties.

In the *HTML source configuration* tab, you can edit the following **settings**:

- **Ignore certificate errors**: if enabled, invalid certificates will be ignored, and the page will be opened even if something is wrong with the site certificate
- **Auto refresh interval**: enable this if the remote Web contents is dynamic (e.g., graphs) and you want the page to be refreshed without user interaction (set 0 to disable auto-refresh)

There is no need to set auto-refresh for video contents; however, you may wish to enable video auto-replay.

In the example here with YouTube streaming, the video is looped by adding URL parameters; the final link will look as follows:

https://www.youtube.com/embed/VIDEOID?autoplay=1&mute=1&loop=1&playlist=VIDEOID – video added in such a way will be played on repeat indefinitely.

This link is formed by clicking the *Share* button next to the YouTube video and adding the parameters. This ensures that nothing but the video is displayed in the viewport (no comments or other stuff present in the regular YouTube page). Similarly, if you wish to use video from other websites, make sure to provide the exact link to the video itself, not to the whole page containing the video.

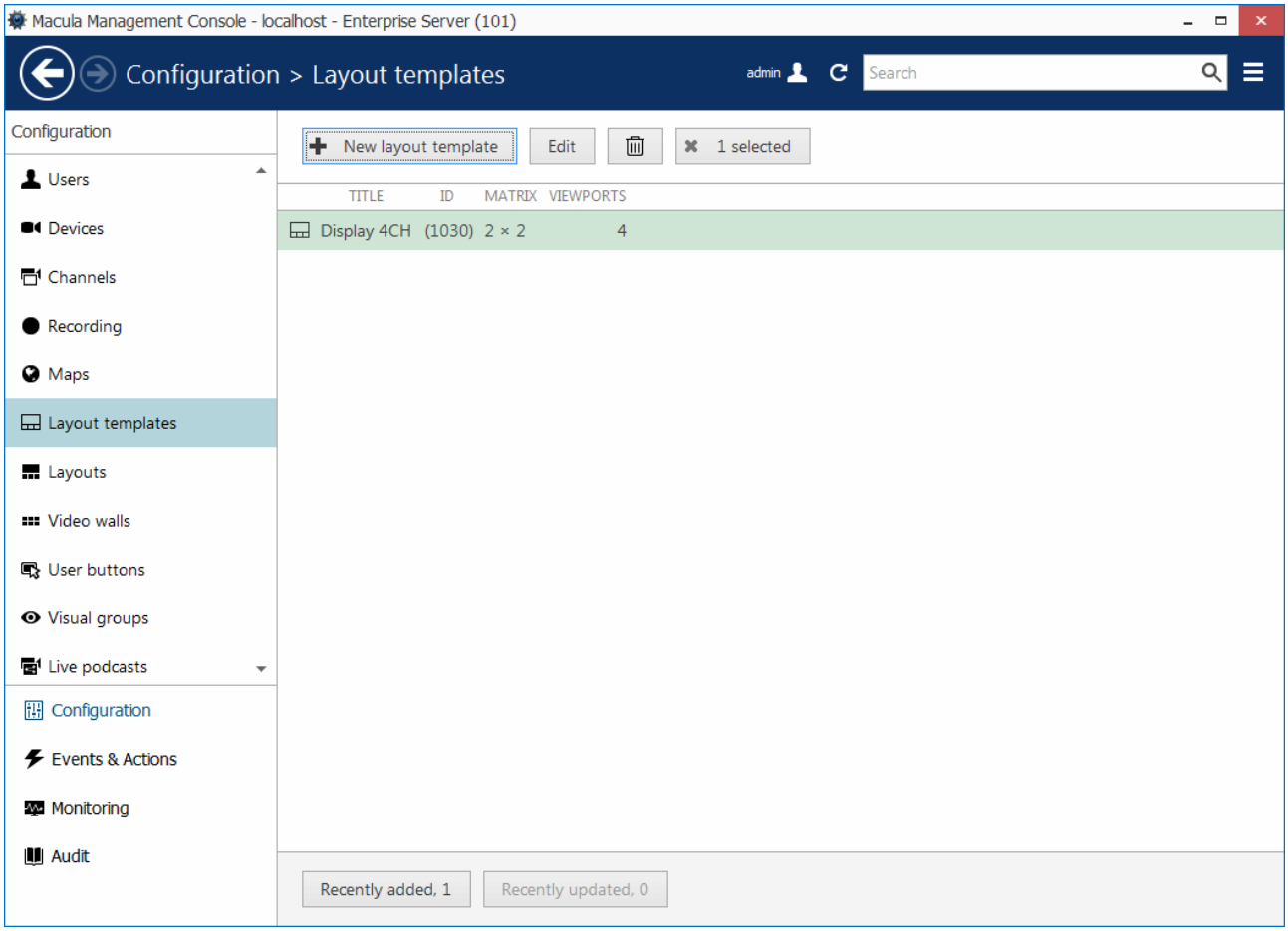
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.2 Layout Templates

Layout templates are arrangements of empty viewports. These can be later filled with channels and maps in your Macula Monitor application and later saved as layouts. Each template can be used any number of times for creating both local or shared layouts.

You can create your own, **custom layout templates** and then use them in any Macula Monitor applications connected to the target server.

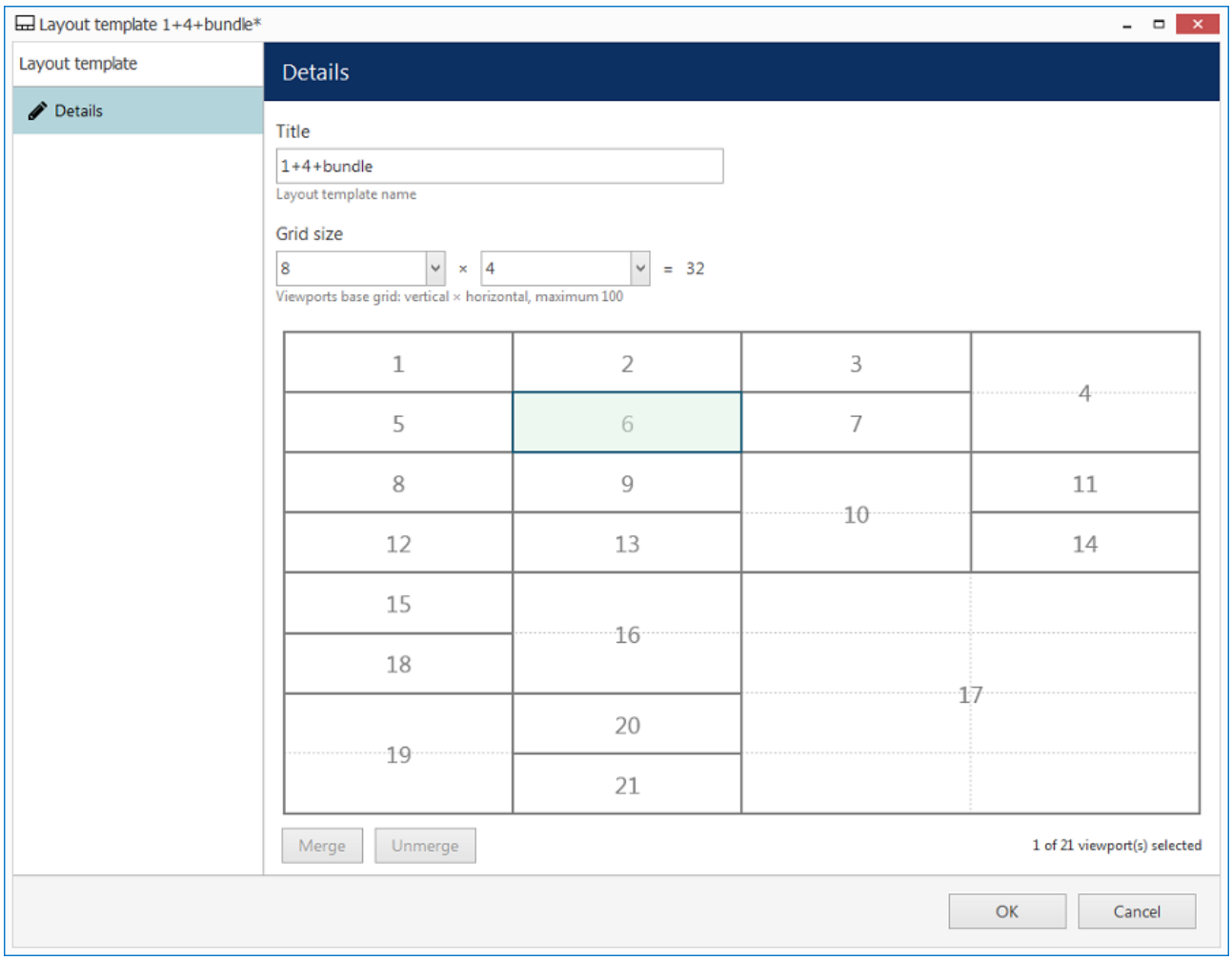
To access layout templates via Macula Console, go to the *Configuration* section in the bottom left panel and select the *Layout templates* component in the menu on the left. Use the *Search* field in the upper-right-hand corner to filter existing items; press *Refresh* button to reload the item list.



Click the + *New layout template* button on the upper panel to bring up the configuration dialog box.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



Enter the template **name**, choose **grid size** and then **modify the grid**, if desired: you can select multiple cells at once with your mouse and then use the *Merge* and *Unmerge* buttons below to create custom cell combinations. Note that you can only create rectangular regions, not just any polygonal areas.

- For corridor view cameras, merge several cells vertically, so that the image fits the target viewport without much stretching/distortion
- For surround view cameras or 180/360-degree dewarp, merge a row of cells

When you have finished, click the *OK* button; the newly created layout template will appear in the item list and it will also appear in any connected Macula Monitor applications after synchronization.

Use the *Edit* button to alter any template at any time: modifications will immediately be synchronized with Macula Monitor after you save the changes and modified templates will be available for use. However, if the modified layout was already in use, its current output will not be altered, allowing you to save the old layout in Macula Monitor. Drag and drop the new layout template to the Macula Monitor live view display to load the updated template version.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.3 Shared Layouts

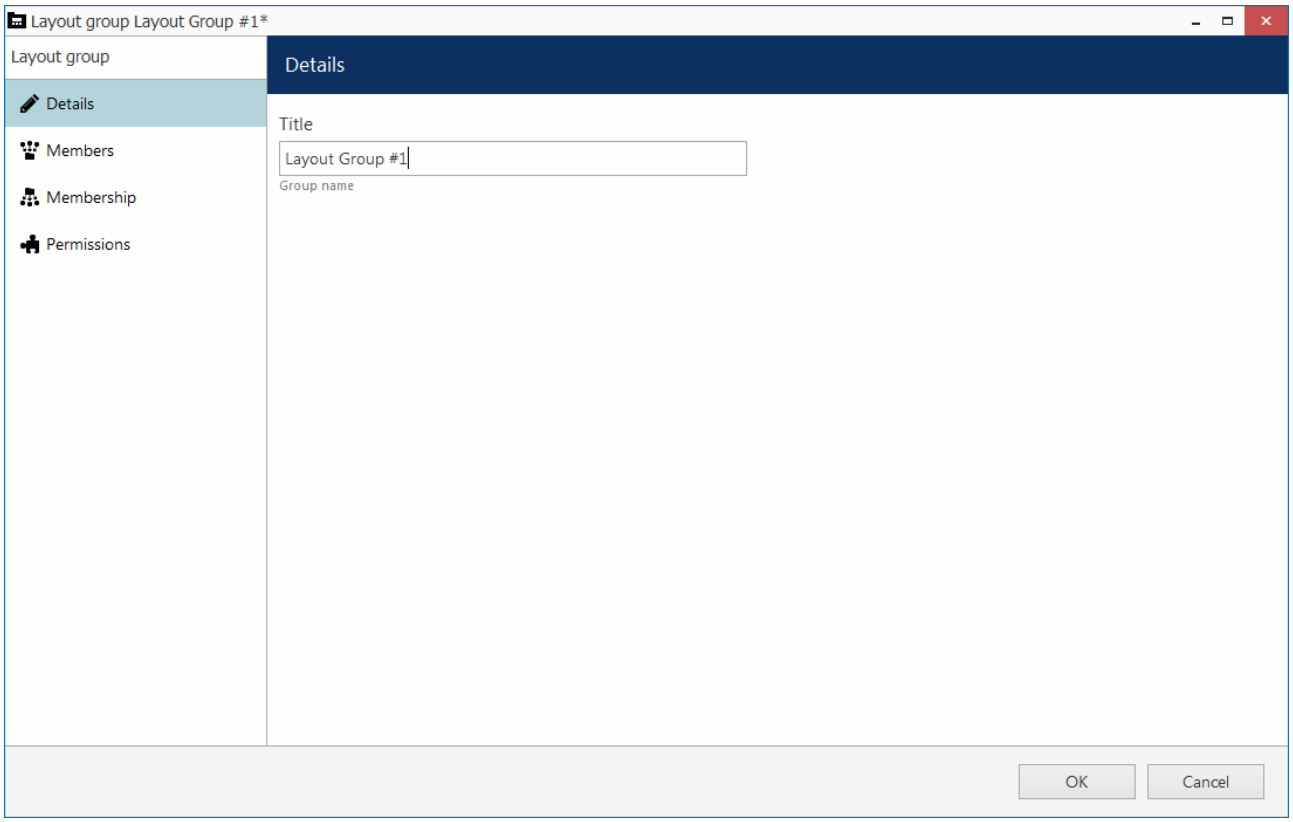
Layout is a pre-configured viewport configuration with channels assigned for live view and archive playback.

Layouts are created in the Macula Monitor application by filling a layout template with video channels. There are two main groups of layouts: **local**, which are created and stored locally on the same computer where the Macula Monitor is installed, and **shared**, server-side layouts, which are kept on each server and are available for all users that are connected to the same server from other client computers. If the license or server policy limits the number of max client connections to 1, layouts can still be shared between non-concurrent client connections from different machines.

Layouts themselves are created via Macula Monitor application but layout sharing should be pre-enabled from Macula Console. In order to make server users able to share and access this resource, **shared layout groups** should be pre-created on the server side. Groups are used for handling user permissions and also for logical arrangement of the shared layouts.

> If **no layout groups** exist in the server configuration, layout sharing will be disabled for the target server from the Macula Monitor side.

To create a new group in Macula Console, open the *Configuration* section and *choose Layouts* from the menu on the left. Click the *+ New layout group* button in the upper panel to bring up the shared layout group creation dialog box.



In the *Details* tab, enter a user-defined name for the target layout group. This name will appear in all connected Macula Monitor applications when creating a shared layout.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Use the *Members* and *Membership* tabs to create nested groups; *Members* tab will also allow you to manage group contents after some layouts have already been created.

In order to **allow access** to specific shared layout groups for selected users, go to the *Permissions* tab:

- Administer permission grants access to the layout group in Macula Console and allows the user to share layouts via this group (put new layouts into target group)
- *View* permission allows users to see the contents of the group, i.e., shared layouts, when they connect to the target server from the Macula Monitor application, and use these layouts in Macula Monitor

> All users with the View permission will be able to see and use the shared layouts from the target layout group. However, visibility of the contents of each layout will depend on each user's channel and map permissions.

Shared layouts can be used in Layout Sequences in Macula Monitor independently or combined with regular layouts as well.

10.4 Maps

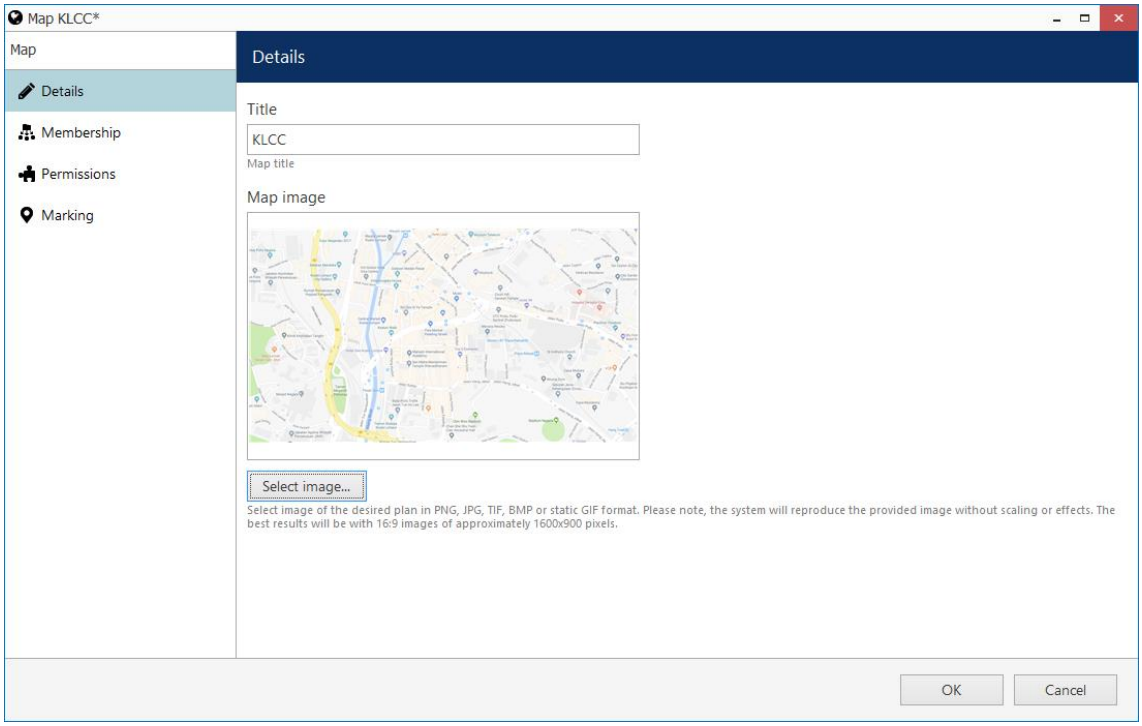
Maps are resources that allow you to use an image of the building **plan** or some **area** and place **interactive markers** on it. Cameras, doors, user buttons, and other items put on maps can then be clicked in the Macula Monitor application to provide the desired interaction and facilitate the operators' work. Links to other maps help create multi-layered building plans for better navigation.

To access map management via Macula Console, select the *Configuration* section from the bottom-left-hand menu and then click *Maps* in the menu on the left.

Two types of maps are available at this point: **maps** based on user image, and **geo maps**.

Create Map

Click the + *New map* button on the upper panel to bring up the map configuration dialog box.



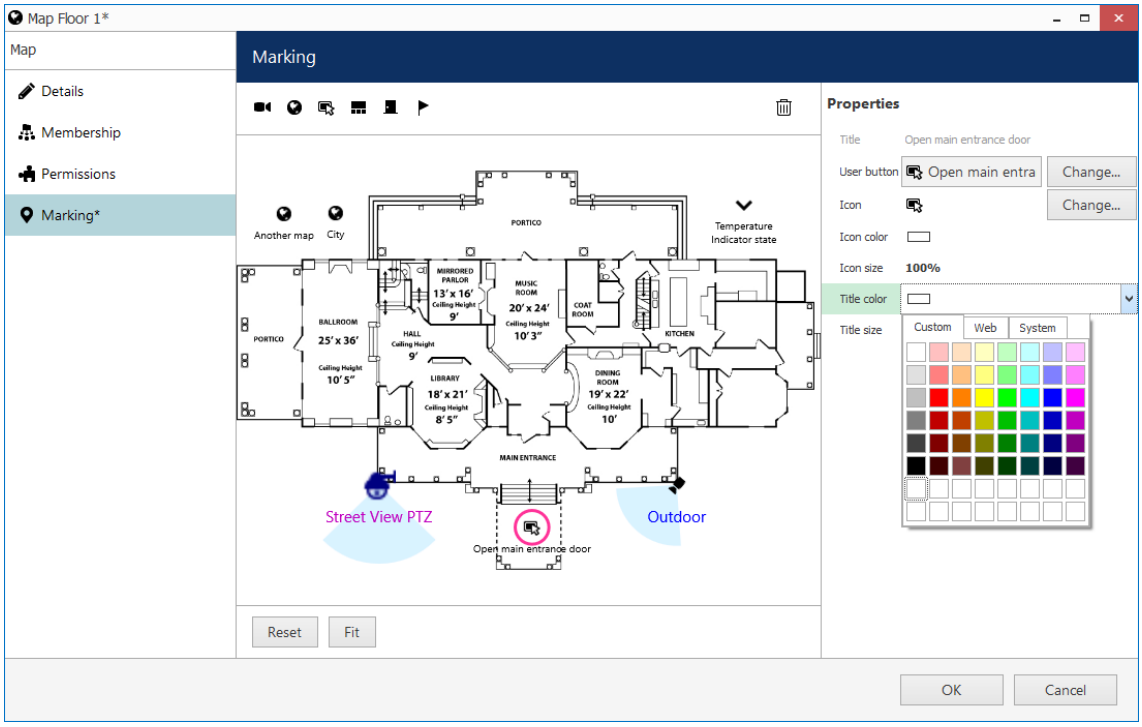
On the map *Details* tab, enter a user-friendly name for your new map, then select the Organization it represents, if applicable, and upload a picture that will be used as plan basis. All major raster picture formats are supported: JPG/JPEG, BMP, PNG, TIF/TIFF and GIF.

> ⚠ There are the following limitative requirements for the pictures loaded as maps:
> - picture resolution should be less than **8.25MP**
> - file size should be less than **5MB**
>
> Files not meeting these limitations will not be uploaded.

Place Camera Markings

Switch to the *Marking* tab to place cameras on the map.

Macula® Professional Administration Guide



Manipulate your map picture by zooming IN and OUT with the mouse wheel, dragging the picture with the left mouse button and using the *Reset* and *Fit* buttons below. *Reset* a show non-zoomed 100% size picture (or a picture fragment, if it is larger than the window), and *Fit* zooms your picture so that it fits into the preview window.

To place a **camera marker**, drag the camera icon from the upper-left-hand corner and drop it on the scene. Camera markers will allow you to pop up channels by double-clicking the markers in Macula Monitor. They will also have a **red mark** on them in the Macula Monitor application if the target channel is **offline** (if the Video lost event has been triggered): the channel's *Video loss* parameter is used as a timeout, which is 15s by default. The following actions are possible:

- select the camera by clicking the camera icon on the plan (and **not** the blue sector representing the viewing area)
- move the camera around by dragging it (the sensitive area is within the pink circle)
- change coverage sector by dragging two pink dots on the sides of the blue sector: drag to the sides to adjust the vertical angle up to fisheye (full circle)
- correct camera position: drag central pink dot to the sides to rotate camera, drag to/from the center to change radius
- remove the marking by selecting it and pressing the *Delete* button on your keyboard or the recycle bin button on the upper panel

The properties window on the right enables you to:

- choose target device for the currently selected marking
- view information about marking angles and radius
- turn ON/OFF displaying of coverage area
- change the marker icon color and size
- adjust the marker title color and size

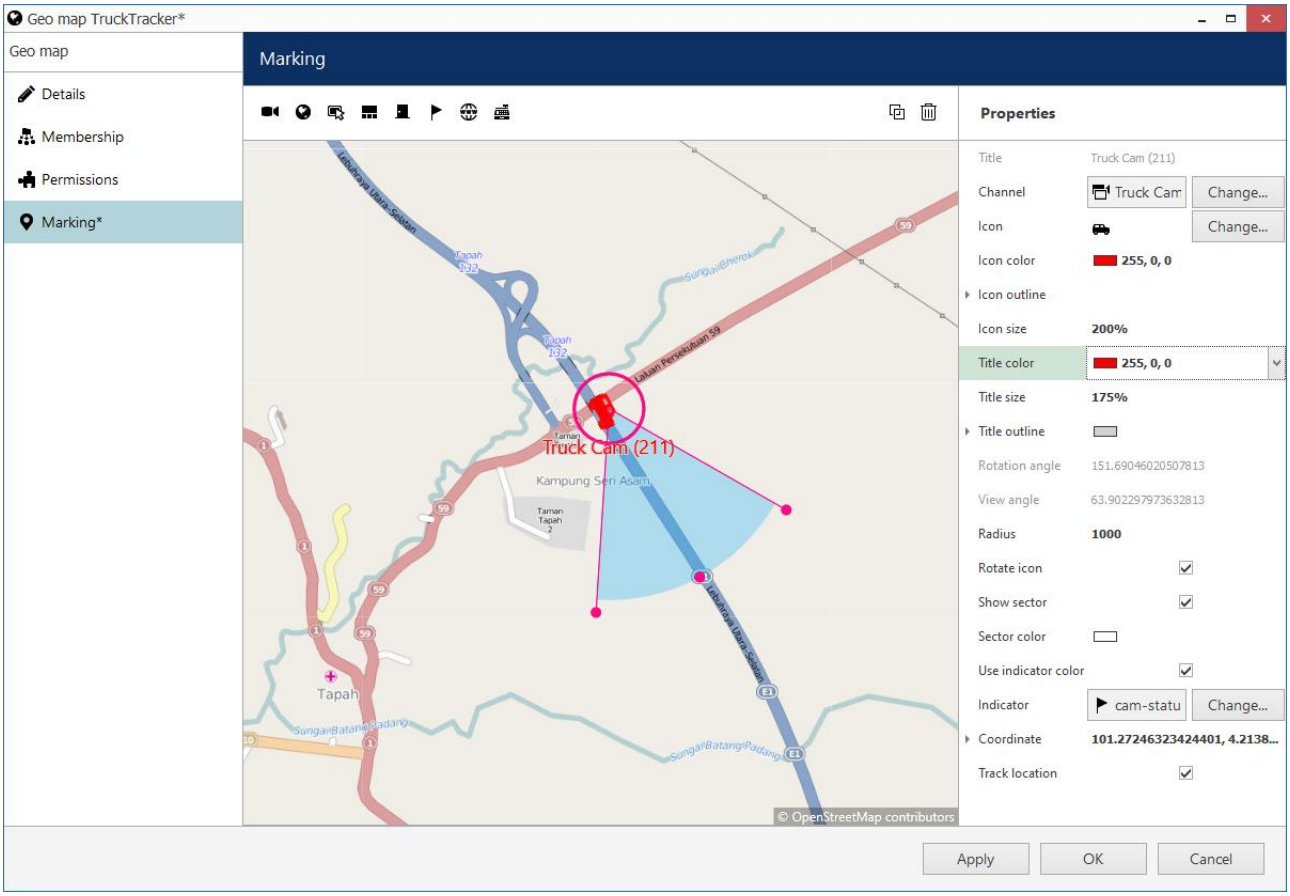
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Camera Marker Binding with Indicators

You can attach indicators to cameras in order to change the **camera icon color** on the map's viewport according to the preset **Indicator**.

First, you need to create the Indicator itself, then set up **rules** for the **previously created Indicator**, and then you can attach the **previously created Indicator** to the camera. After that, your Camera cone color will change according to your rules set for the Indicator.

1. Go to *Configuration* -> *Maps* -> Your particular map
2. In the *map* window, select *Marking* from the left menu
3. Drag and drop the camera icon from the menu over the viewport
4. On the top of the *Properties* menu, select the *Channel* you want to attach to the already placed camera icon.
5. At the bottom of the *Properties* menu, select the previously created Indicator.



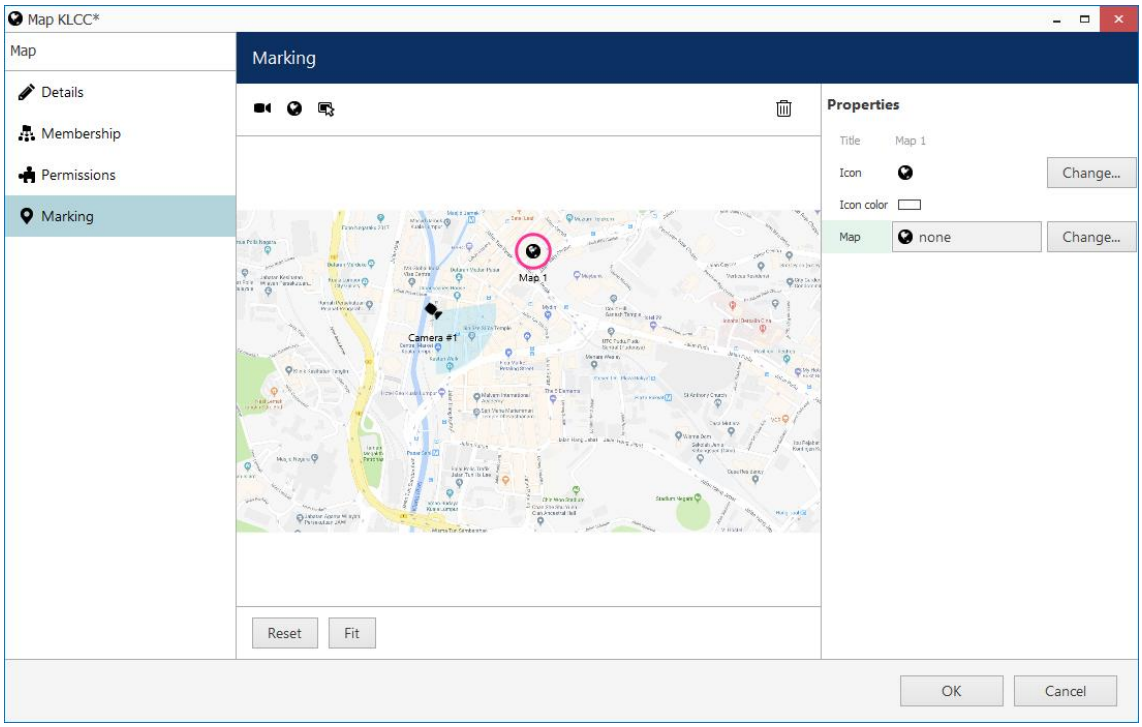
Other Markers

Several other marker types turn your map into a fully featured control panel. To place any marker, drag the corresponding icon from the upper-left-hand corner and drop it onto the scene.

Macula® Professional Administration Guide

It is also possible to add **map markers** and use them as shortcuts to other maps: target maps will pop up when corresponding map markers are double-clicked in Macula Monitor. To place a map marker, drag the map icon from the upper-left-hand corner and drop it onto the scene.

Click a map marking and use the properties window on the right to browse for a map that you wish to be a target for the current shortcut. Remove markers by selecting them and then hitting the *Delete* button on the keyboard.



In the same way you can also add **user buttons** to your map and trigger assigned actions by double-clicking the buttons in Macula Monitor. Select your desired user button on the map and then use the properties section on the right to bind a user button to the marking.

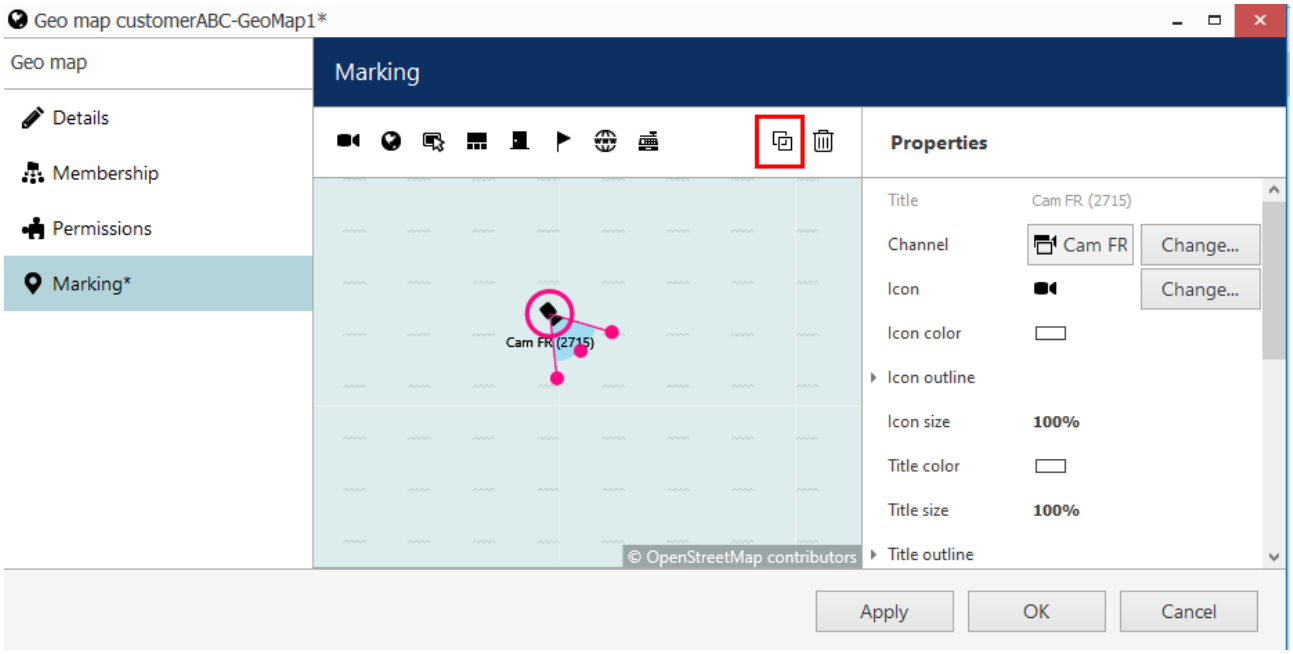
Similarly to individual channels, it is possible to place **layout markers** for shared layouts to be displayed when double-clicked on the map in Macula Monitor. The target shared layout and the icon style can be defined in the properties section on the right.

Door markers are intended to be bound to doors from the access control integration: door statuses are then displayed on the map in the Macula Monitor application. The target door and icon styles for different door stated is to be defined in the properties section on the right.

Finally, **indicators** are multi-state entities that can change their state - and, therefore, their colors on the maps - based on events. These may be temperature ranges, condition states, or any other system component states that have related events.

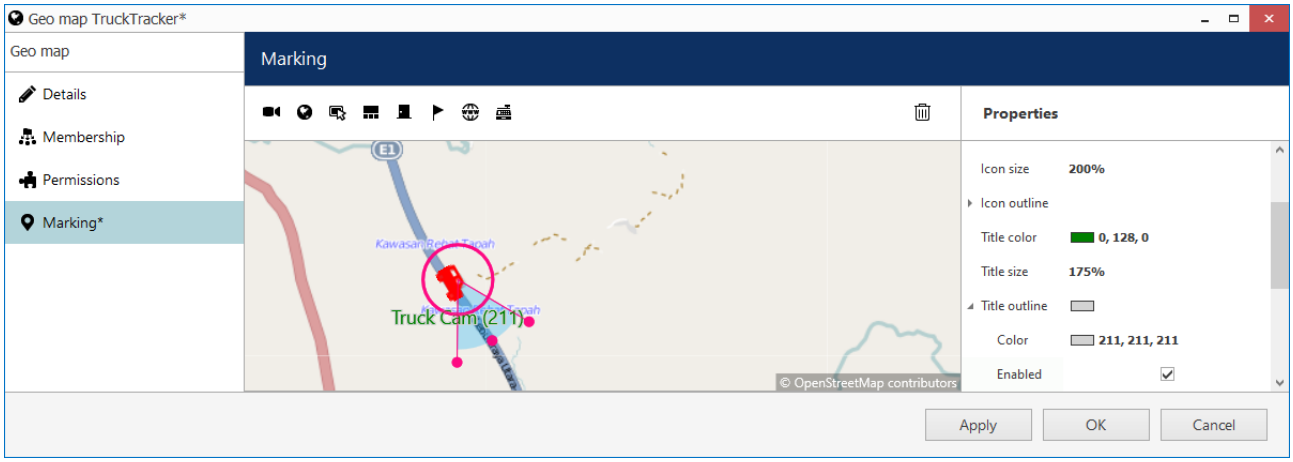
Copy Markings/Indicators

You can duplicate any indicator on Maps. To do so, select the indicator/marking you want to copy. At the top-right corner of the Marking section, you will find two buttons: one for deleting the indicator/marking and the second for duplicating. Click on the duplicate button. This will create a copy of the selected overlay.



Marker Customization

Each marker has a customizable icon, size, color, outline, and the same options are available for its text label. To edit the marker, click the marker on the map: its properties will appear on the right. As you change the properties, the changes will be immediately reflected.



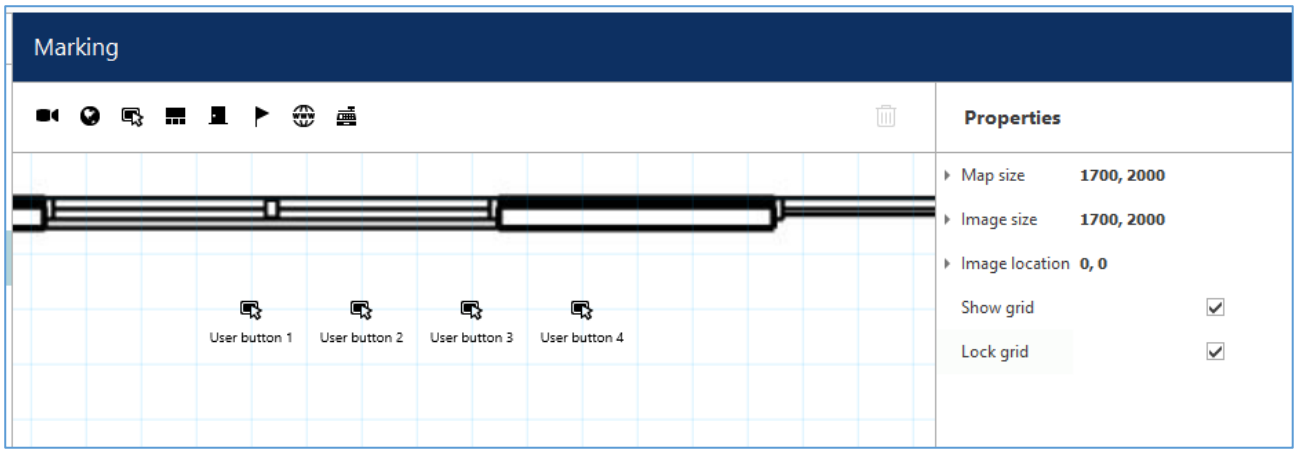
Marking Arrangement

By default, you can place camera markings and other icons freely. But, for some purposes, using a **grid** for marker arrangement can be useful. For example, when you do not use an actual map but rather create a **control panel** with action buttons, and when the number of markers is big, use grid arrangement to facilitate the creation process.

While in the *Markings* section of the map management, click anywhere on the background (not an icon). If a marker was selected, the selection will disappear, and you will see map properties on the right. In the properties section, mark the corresponding option to enable it:

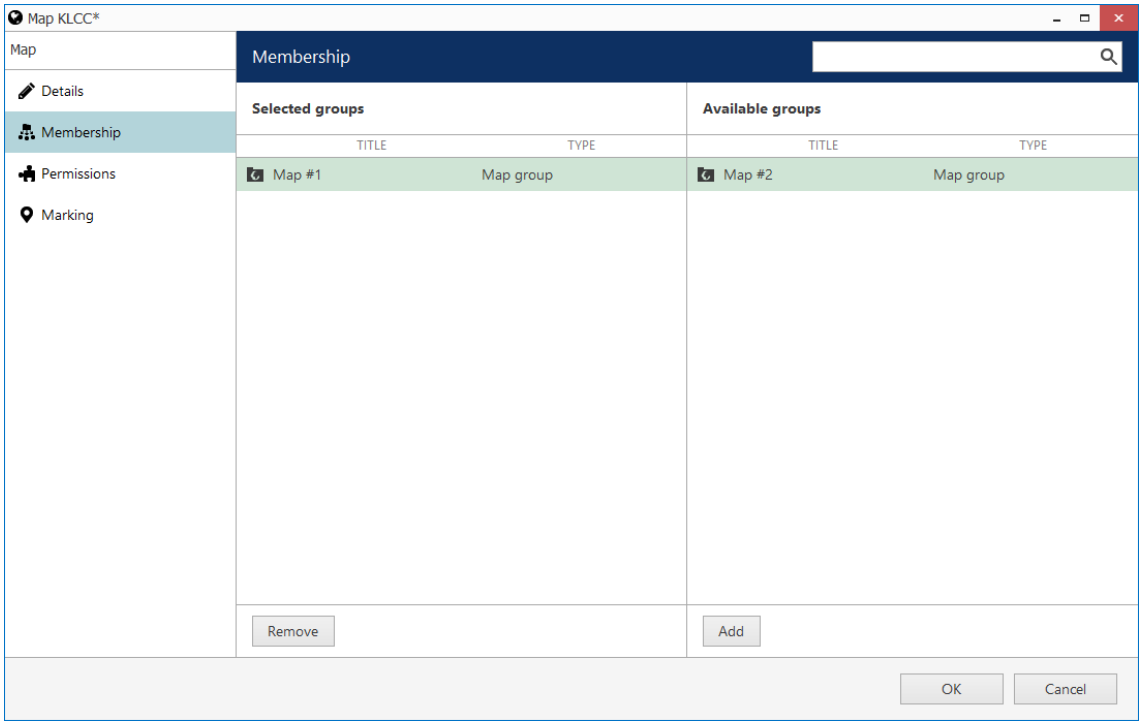
Show grid: will show the grid lines; all added markers can only be placed at intersections

Lock grid: if enabled, the grid size will be locked at the current zoom level, and zooming the image in/out will zoom the grid as well



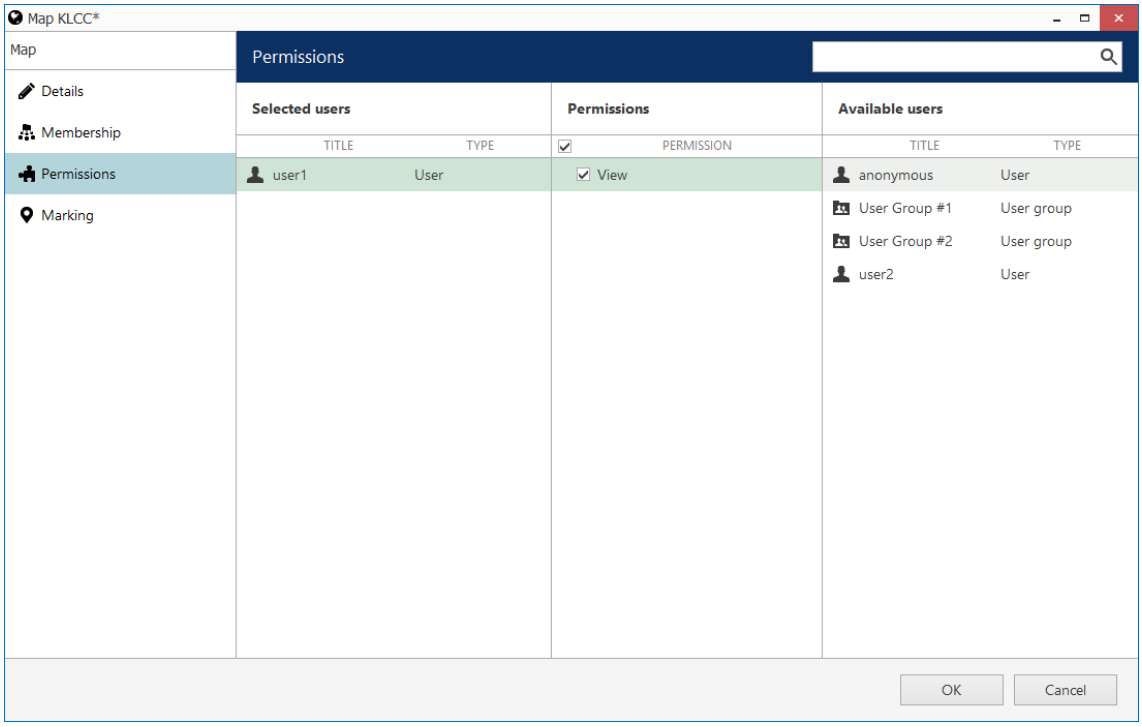
Membership and Permissions

Just as other resources, maps can be grouped and assigned user permissions.



In the *Membership* tab, you choose groups for this map to become a member of: select groups by double-clicking items in both columns or by using the *Add/Remove* buttons below.

Macula® Professional Administration Guide



Permissions tab enables you to choose the users and user groups that will have access to this resource. Select at least one permission to select a user/user group; uncheck all manually or using *Clear* button below to deselect. *Administer* permission means user will be able to see, open and edit map via Macula Console, and *View* only allows user to load the map in Macula Monitor.

When you have finished, click *OK* to save and close the dialog box. The newly created map will appear in the item list of the *Maps* section.

Use the buttons on the upper panels to perform item-specific actions: remove, edit and quickly assign map group; the filters on the bottom panel will help you switch between recently created/updated items and display maps/map groups only.

Create Geo Map

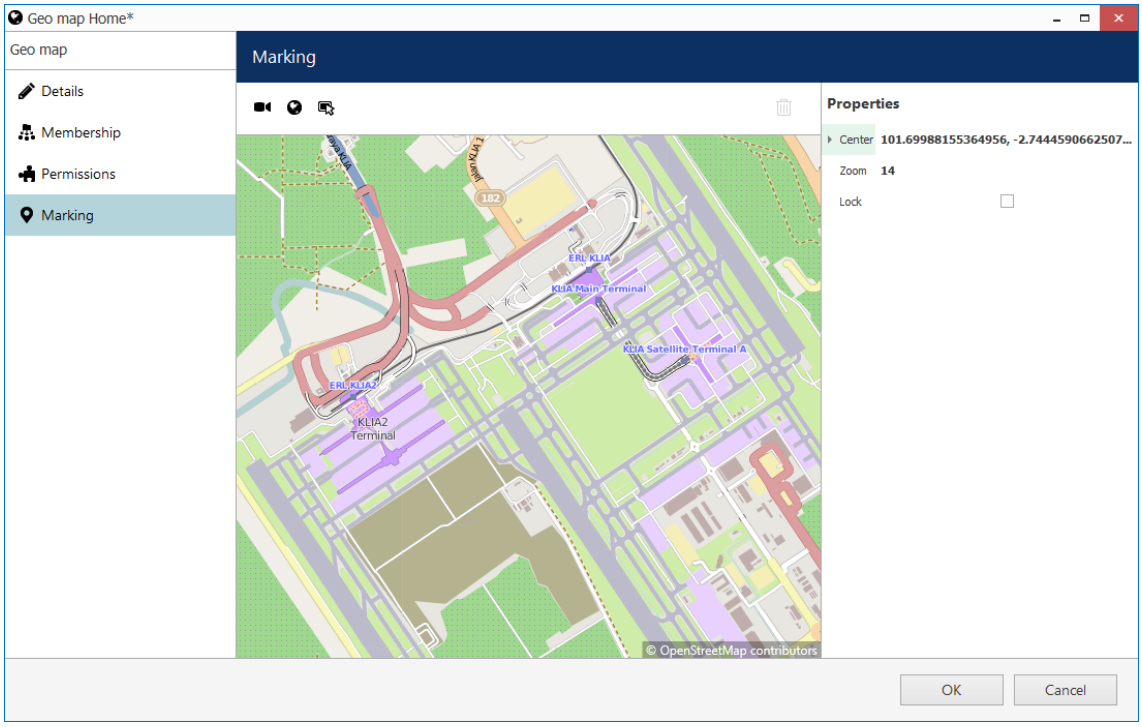
It is also possible to use a **world map** instead of user-defined pictures to put the markings on it. To create a new geo map, click the drop-down arrow near the + *New map* button and select *New geo map* to bring up the geo map creation dialog box.

> ⚠ Geo map functionality requires that constant **Internet connection** is present in order the world map to be loaded from the remote server. Internet connection is required from Macula Monitor as well to load the map and present it to the end user.

Geo map creation is similar to the creation of a regular map, with the difference that you do not need to specify the image to be used: instead, the world map is loaded from the server provided by GSF. You just need to find the right place on the map by zooming IN/OUT and moving the map:

- use your mouse wheel to zoom IN and OUT
- click and drag with your left mouse button to move the map around

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Markers of all available kinds can be placed on the geo map in the same manner as with the regular map, and the rest of the tabs also provide the same functionality.

> Use the Lock option in the right-hand-side panel to prevent users from moving or zooming the map IN/OUT in the Macula Monitor application.

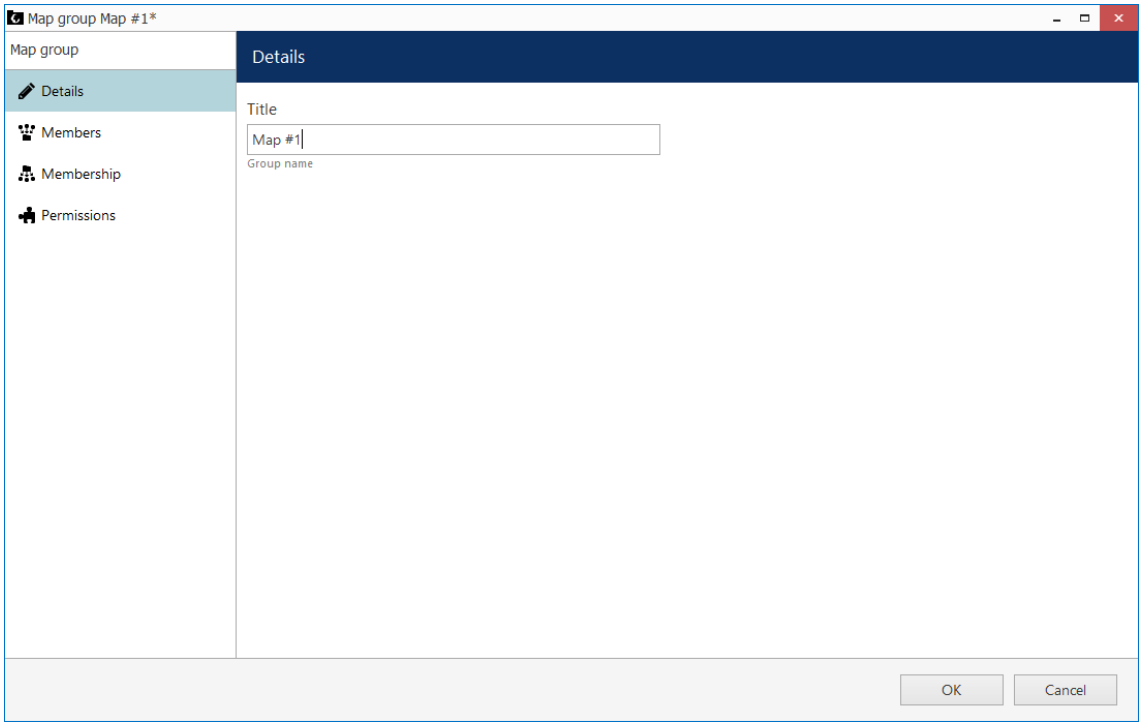
Create Map Group

Map groups can be used for easier management in Macula Console. Note that map groups are not displayed in Macula Monitor; to group maps and geo maps in Macula Console, use Visual Groups.

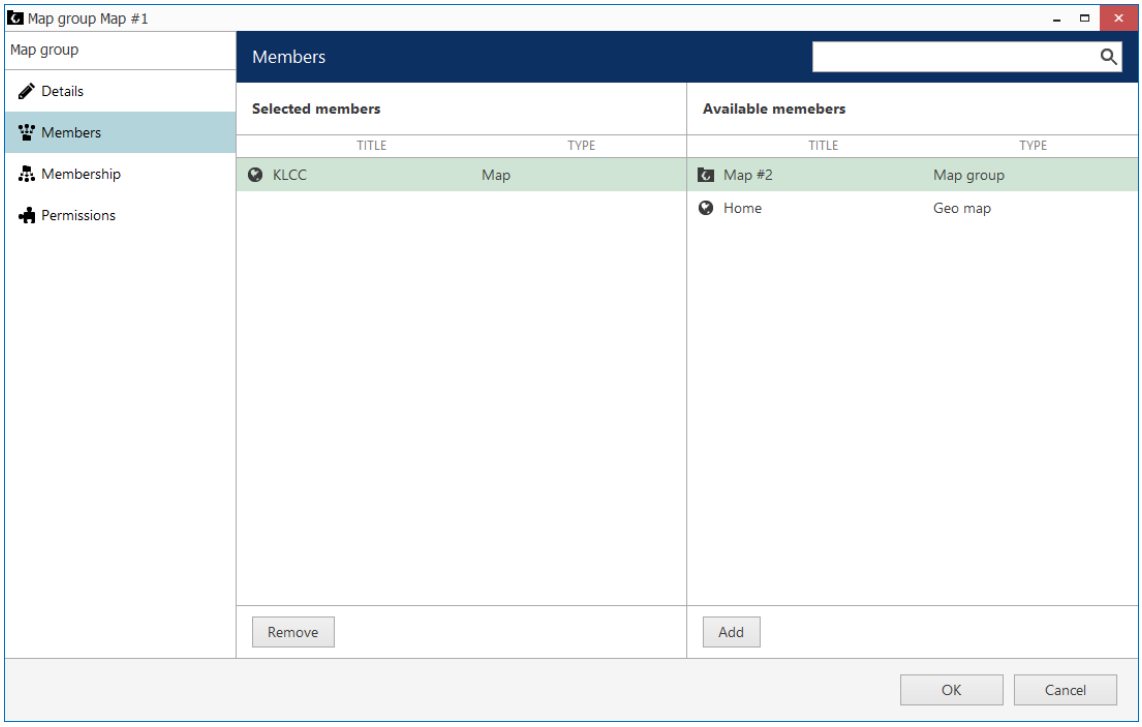
Click the drop-down arrow near the + *New map button* and select *New map group* to bring up the map configuration dialog box.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



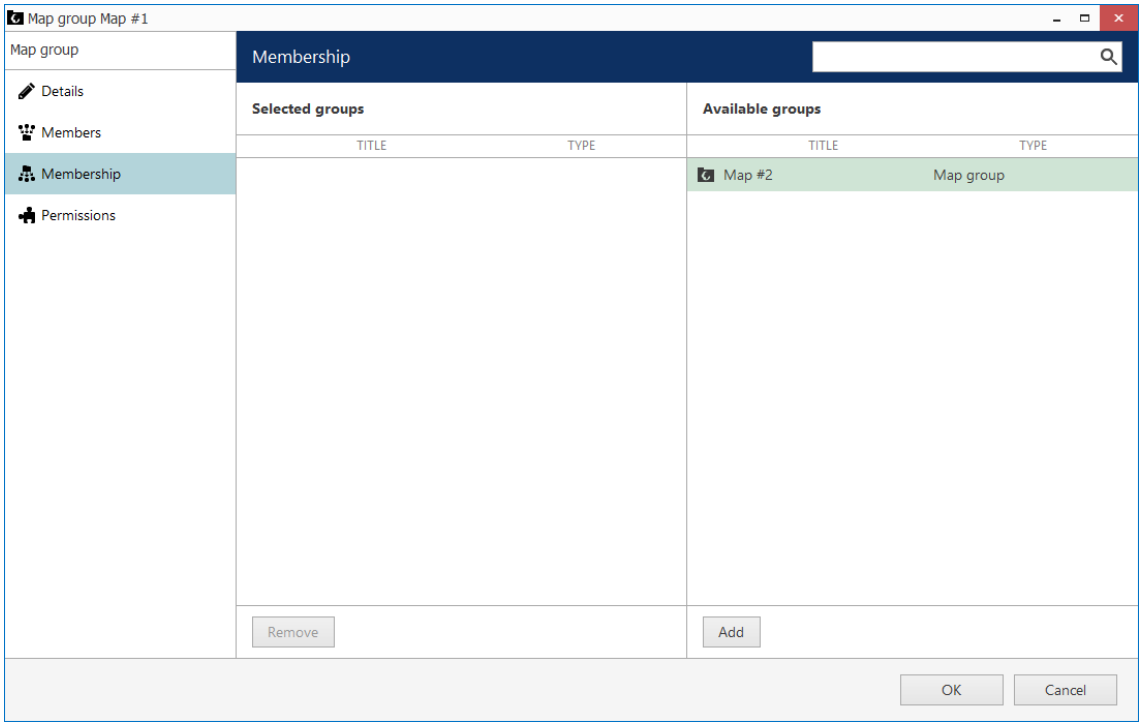
Enter group name on the *Details* tab and proceed with selecting maps for this group on the *Members* tab.



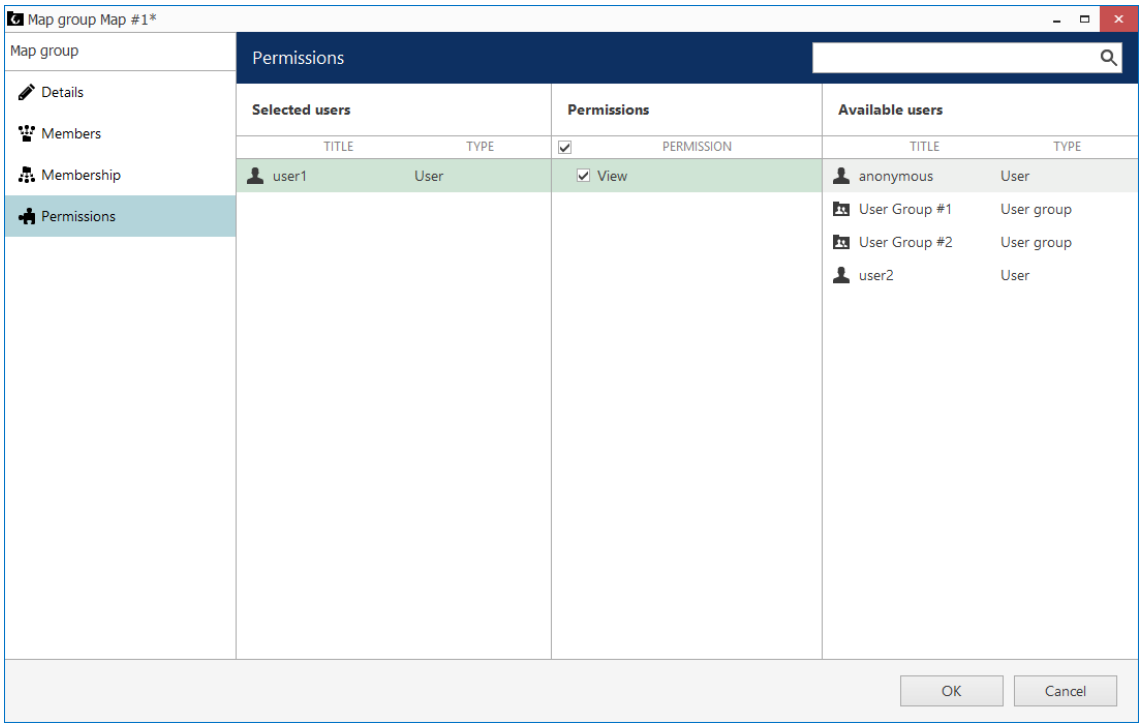
You can select both maps and map groups to be members of any map group.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



On the *Membership* tab, choose groups to contain target map group as a member, thus creating nested groups.



Switch to the *Permissions* tab to assign user privileges for the target map group. Select at least one permission to select user/user group; deselect by unchecking manually or by using the *Clear* button below to remove all. *Administer* permission means user will be able to see, open and edit all maps in this and nested groups via Macula Console, and *View* only allows user to load the maps in Macula Monitor.

When you have finished, click *OK* to save and close the dialog box. The newly created map group will appear in the item list in the *Maps* section. Use the buttons on the upper panels to perform item-specific actions: remove, edit and quickly assign map group; filters on the bottom panel will help you switch between recently created/updated items and load maps/map groups only.

10.5 User Buttons

User buttons are visual controls used in Macula Monitor and Macula Mobile for manual event triggering. Once you have created a user button, it will become available in the Event & Action Configurator and you will be able to **assign actions** to the *User button clicked* event.

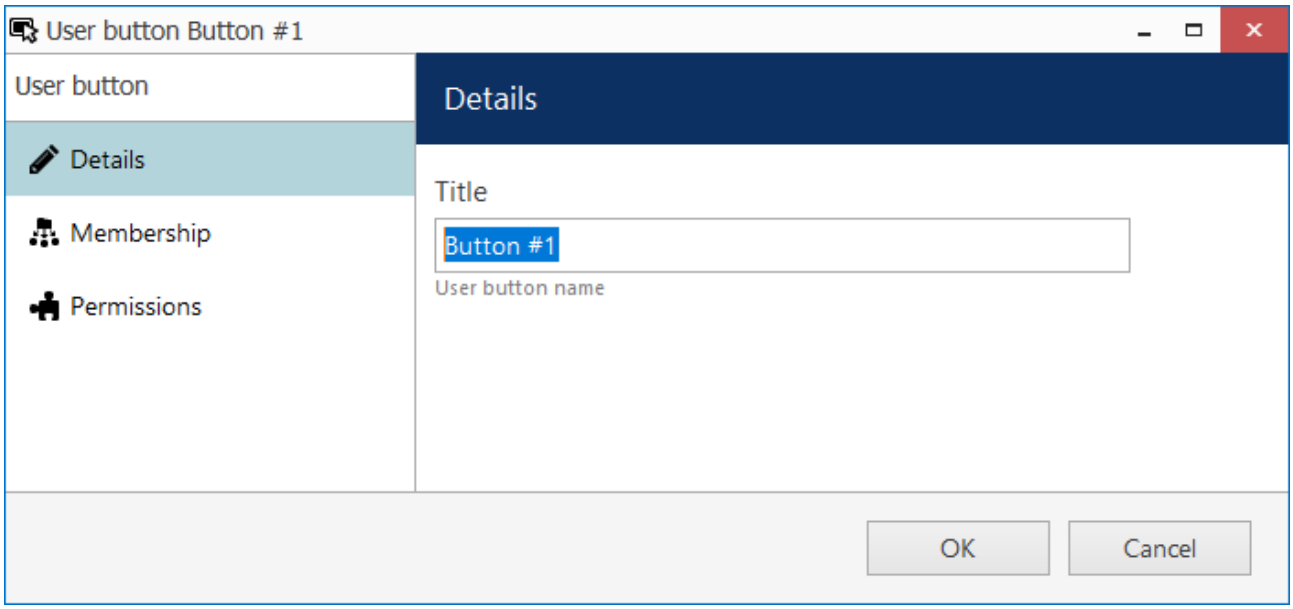
After a user button has been created and associated with at least one action, you will be able to use it in the following ways:

- bind the user button to a channel or channels so that it appears as a live video overlay control in the Macula Monitor application
- place the user button marker onto maps
- trigger it from the Macula Monitor application from the user button list, from any map or from the channel overlay controls
- highlight it on a map or all maps where the corresponding marker is present
- trigger it from the Macula Mobile application

To access user button management via Macula Console, select the *Configuration* section from the bottom left menu and then click *User buttons* in the menu on the left.

New User Button

Click the + *New user button* on the upper panel to bring up the configuration dialog box. On the *Details* tab, enter a name for the resource and choose Organization attachment.



Switch to the *Membership* tab to choose groups for this user button to become a member of: select groups by double-clicking items in both columns or by using the *Add/Remove* buttons below. Apart from grouping, this tab allows you to bind user buttons to particular channels.

> Starting from the software version 1.5.0, user buttons can be **bound to one or more channels** for their presentation in Macula Monitor. This means that once such a channel is put into a viewport, the related user button automatically appears with it. The same user button can be also manually

put into other viewports and also removed from the bound channels in the live view without any limitations. Multiple user buttons per channel are allowed.

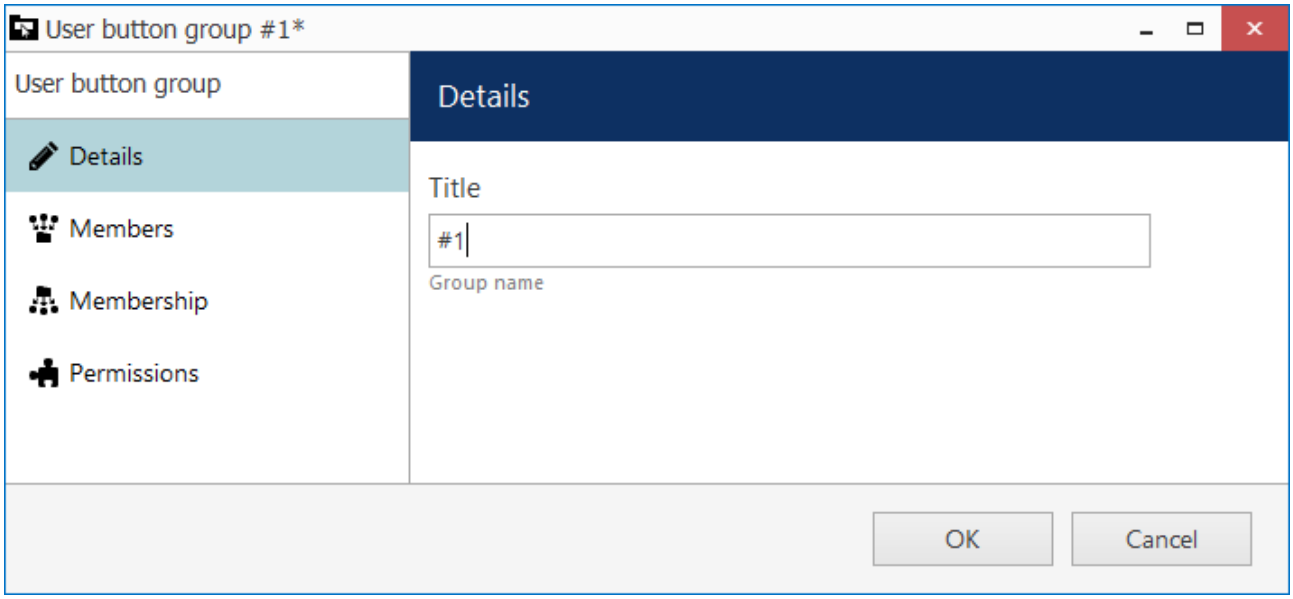
In order to set this up, open the target user button for editing, go to the *Membership* tab and add the desired channel(s) from the right-hand column (the same one that contains user button groups).

The *Permissions* tab allows you to choose which users and user groups will be privileged to have access to this resource. Select at least one permission to select the user/user group; deselect by unmarking manually or using the *Clear* button below.

When you are finished, click *OK* to save and close the dialog box. The newly created user button will appear in the item list. Use the buttons on the upper panels to perform item-specific actions: remove, edit and quickly assign user button group; filters on the bottom panel will help you switch between recently created/updated items and load user buttons/button groups only.

New User Button Group

For easier management, user buttons can be grouped together. Click the drop-down arrow next to the + *New user button* and select *New user button group* to bring up the configuration dialog box.



Switch to the *Members* tab to choose resources for this group. Double-click items or use the *Add/Remove* buttons below to manipulate resources; use the *Search* field in the upper-right-hand corner to quickly find entries in the list.

Using the *Membership* tab, you can choose groups for this user button to become a member of; select groups by double-clicking items in both columns or by using the *Add/Remove* buttons below.

Permissions tab allows you to choose users and user groups privileged to have access to this resource. Select at least one permission to select the user/user group; deselect by unchecking manually or using the *Clear* button below to remove all permissions.

When you have finished, click *OK* to save and close the dialog box. The newly created user button will appear in the item list. Use the buttons on the upper panels to perform item-specific actions: remove, edit

and quickly assign user button group; filters on the bottom panel will help you switch between recently created/updated items and load user buttons/button groups only.

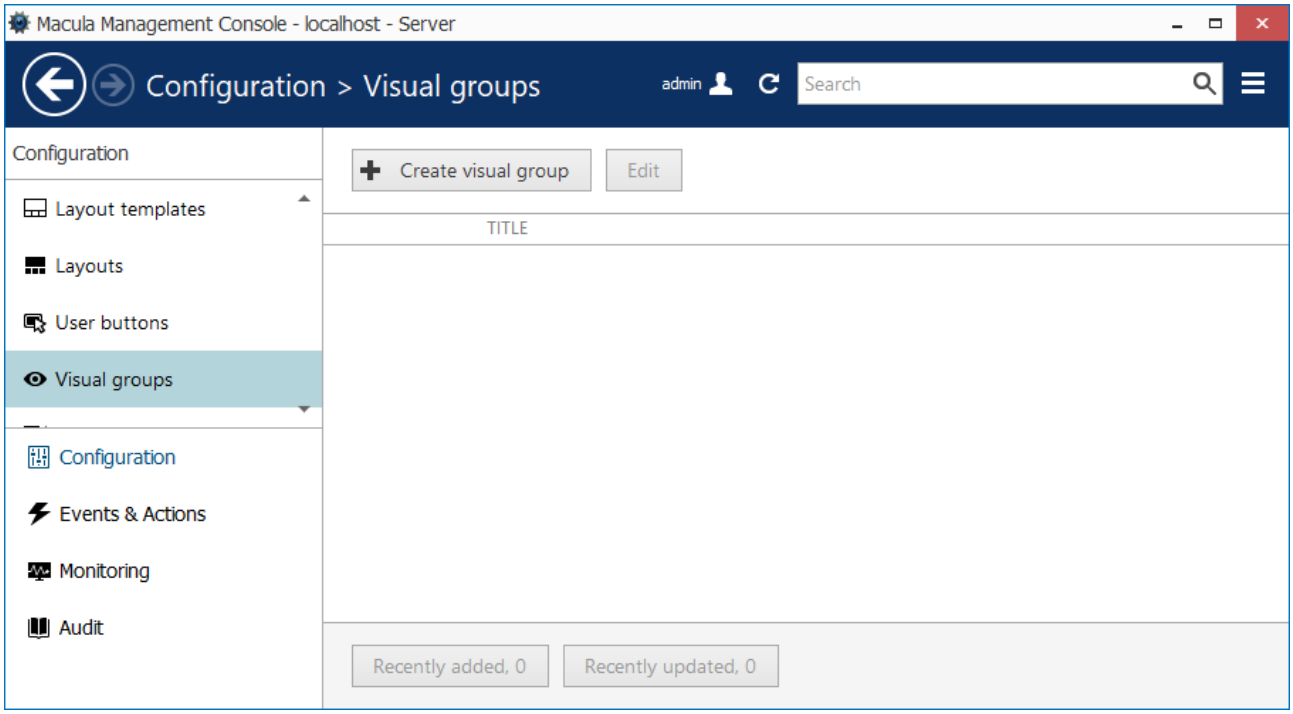
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.6 Visual Groups

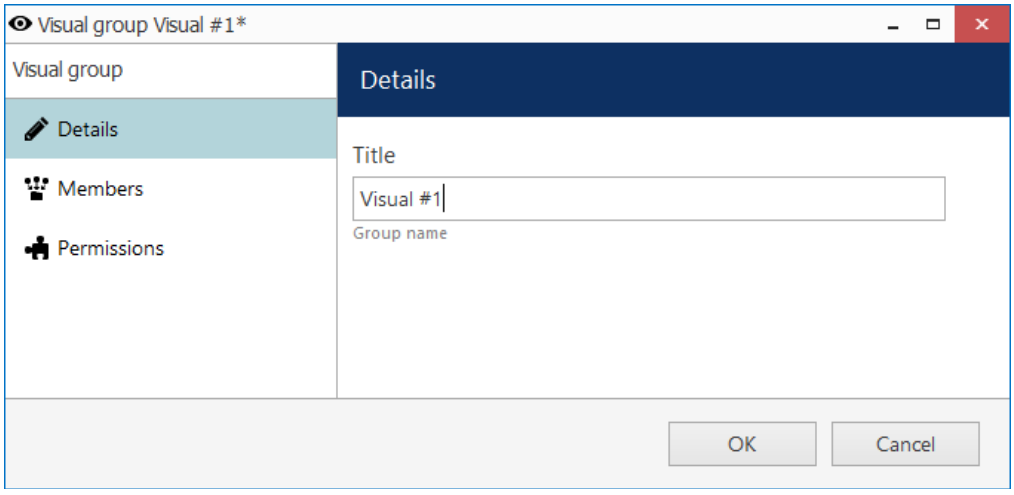
Device, channel and map groups are used solely for management and are only accessible in Macula Console.; in order to set up resource arrangement for Macula Monitor, **visual groups** are used. They allow custom grouping for channels and maps displayed in the connected Macula Monitor applications. You can create single-level or **multi-level** (nested) visual groups by putting them inside one another. Nested visual groups will also appear in the *Resources* section of the Macula Monitor application.

Starting from software version 1.17.0, visual groups are also available in the Archive Backup Wizard.

To access visual group management in Macula Console, go to the *Configuration* section in the bottom left panel and select the *Visual Groups* component in the menu on the left.



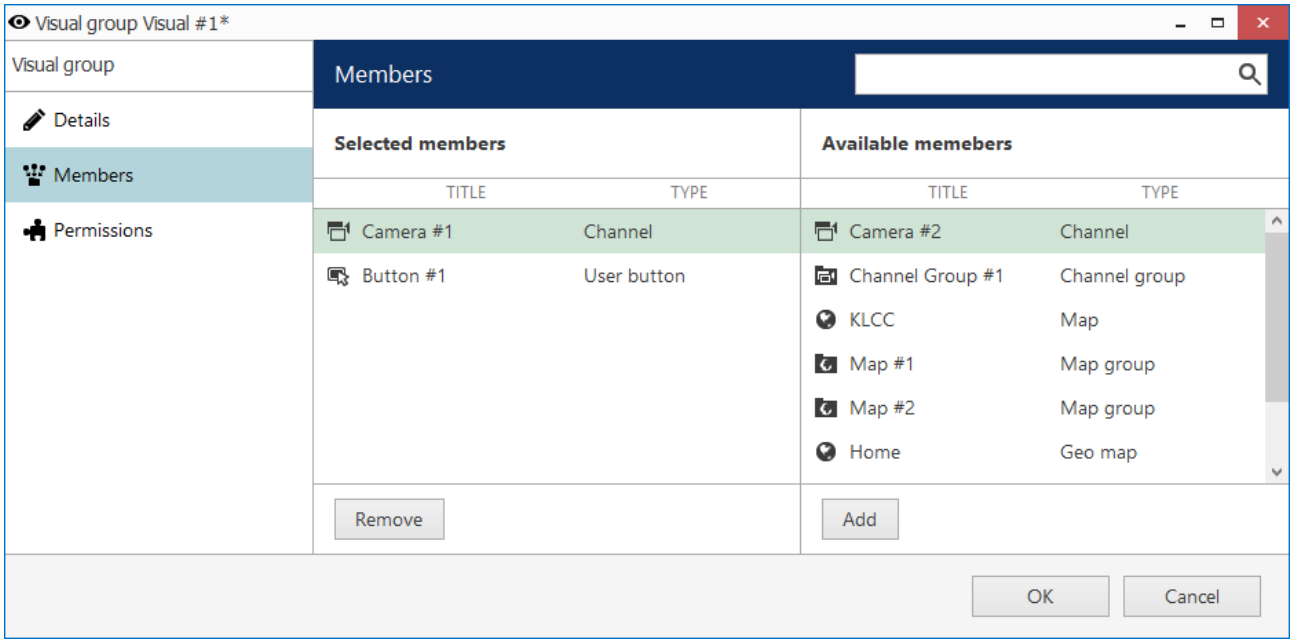
Click the + *Create visual group* button in the upper panel to bring up visual group creation dialog box.



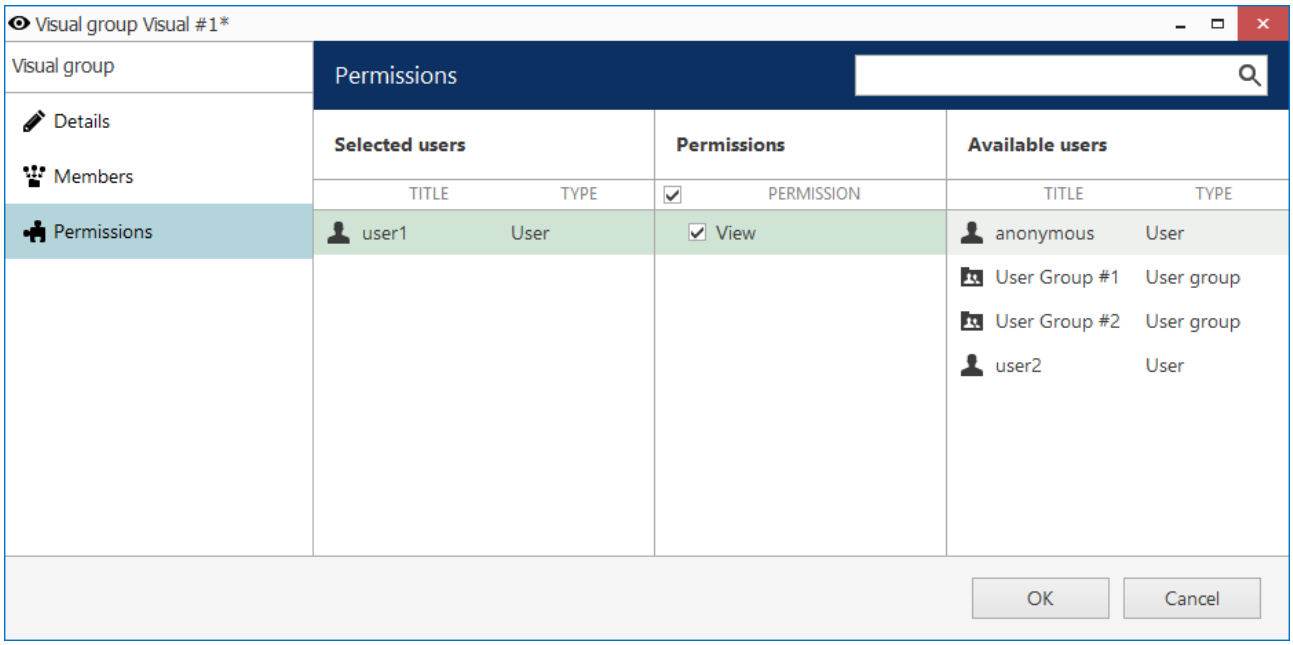
In the *Details* tab, enter a user-defined name for the target visual group. This name will appear in connected Macula Monitor applications.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Switch to the *Members* tab to choose resources for this group. You can create nested visual groups (i.e., group inside group) - they will appear as a tree in the Macula Monitor application.



Double-click items or use the *Add/Remove* buttons below to manipulate resources; use the *Search* field in the upper-right-hand corner to quickly find entries in the list.



Switch to the *Permissions* tab to allow user access to this visual group. There are two available permissions types:

- **View**: users have access to this resource in Macula Monitor
- **Administer**: users are permitted to edit this group via Macula Console

When you have finished, click *OK* to save and exit; the newly created visual group will appear in the item list.

To edit any of the previously created visual groups, double-click it in the item list or select any with single mouse click and then hit the *Edit* button on the upper panel. Use the *Search* field in the upper-right-hand

corner to quickly find the existing items; the filters in the bottom panel allow you to load recently added/modified items. Use the recycle bin button in the upper-right-hand corner to remove one or multiple visual groups: hold *CTRL* or *Shift* to select several items at once, or *CTRL+A* to select all.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

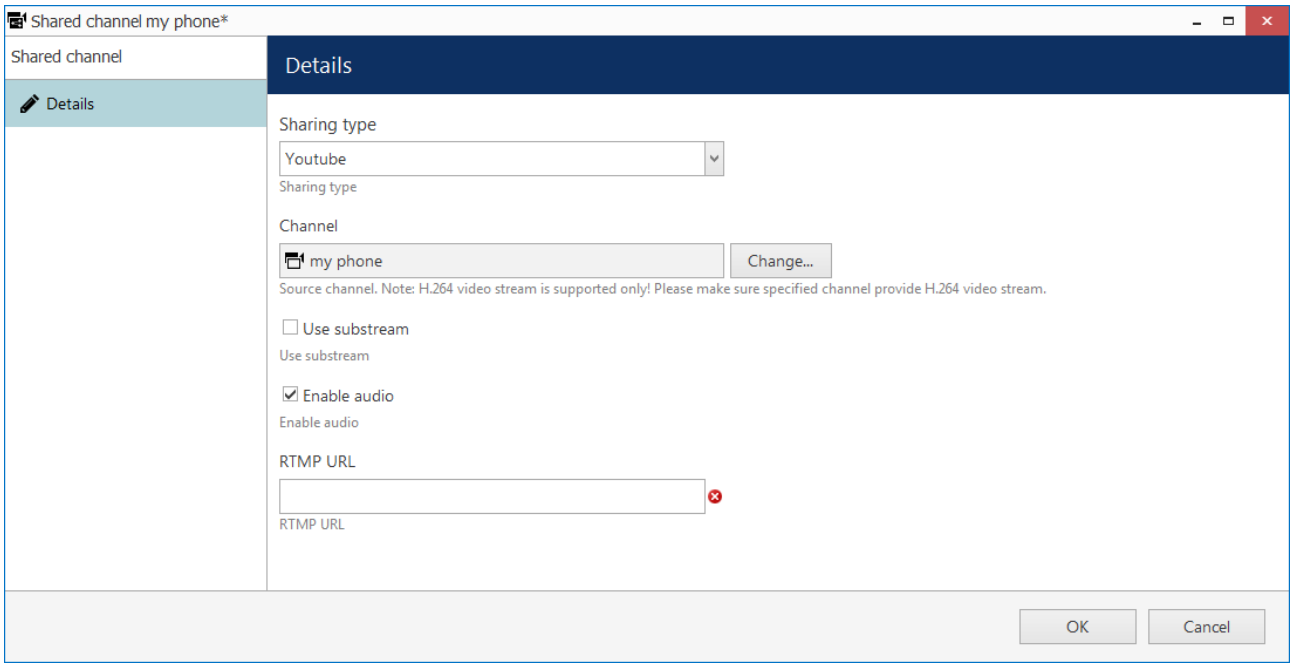
10.7 Live Podcasts

Macula channels can be shared by streaming over RTMP and thus be used for live casting - either with popular streaming services or with your own RTMP server. This manual covers examples of how to set up live streaming for Youtube and Wowza live casts - working with other RTMP servers is similar.

> ⚠ Before sharing a channel, check its settings and make sure that:
> - the channel is enabled in the configuration and video is available,
> - stream codec is **H.264** (other codecs will not work!),
> - if you want to use substream and/or audio, make sure you have enabled them in the channel properties.

To access **shared channel management** in Macula Console, go to the *Configuration* section in the bottom left panel and select the *Live Podcasts* component in the menu on the left.

Click the + *New live podcast* button in the upper panel to bring up the shared channel creation dialog box.



First, choose where you are going to stream the channel: it can be a specific public service or generic RTMP streaming to a service that is not listed, including your own RTMP server; depending on your choice, settings may vary to suit the specific service. Then, enter streaming configuration.

The table below explains the settings in details.

Setting	Description	Default value
Sharing type	Choose between Youtube, Wowza or generic RTMP streaming	Generic RTMP
Channel	Target channel to be streamed	[none]
Use substream	When not enabled, main (higher resolution) stream will be used; enable this option if you want to cast the lower resolution stream	Disabled
Enable audio	Enable this option to include sound for the shared channel, works both for main and secondary streams	Enabled
RTMP URL	Full URL to be used for casting, the link is normally provided by the RTMP streaming engine	[empty]

Youtube Live Streaming

Youtube live casting can use RTMP streams from your Macula server for further streaming.

In order to set up live streaming with Youtube, log in to your account on youtube.com and go to Creator Studio tools -> Live streaming -> Stream now. If you have never created any live casts before, you may have to verify your account - just follow the guidelines on the website.

> ⚠ You need to have a valid Youtube (Google) account in order to be able to use this type of streaming, and comply with Youtube live streaming conditions. GSF is not responsible for the third-party service operability and policies.

Scroll down to the *Encoder Setup* section: you will need the link and the secret stream key in order to build the RTMP link.

In Macula Console, open the *Shared Channels* section and add a new shared channel, fill in the settings as follows:

- **Sharing type**: Youtube
- **Channel**: target channel from the list of existing channels
- **Use substream**: up to you
- **Enable audio**: up to you
- **RTMP URL**: *rtmp://<server_URL>/<stream_key>*, where
  - *rtmp://* indicates that RTMP protocol will be used for streaming
  - *<server_URL>* is Server URL link provided by Youtube, e.g., *a.rtmp.youtube.com/live2/*
  - *<stream_key>* is Stream Name/Key generated by Youtube in the form of xxxx-xxxx-xxxx-xxxx

Wowza Streaming

Alike Youtube, Wowza streaming engine can receive video feeds from Macula server and stream them out to any device. You need to install Wowza Streaming Engine first and then configure live streaming as described below.

> ⚠ Macula does not include any installation files or licenses for Wowza Media Systems software. Wowza engine is used as a third-party agent capable of receiving RTMP streams; all installation, setup and management of this engine is to be handled by you or your Wowza administrator, and GSF is not responsible for the third-party engine operability and policies.

First, go to your Wowza Streaming Engine Manager and create a **new application** of the *Live* type.

> ⚠ Once you have created a new application, go to the *Source Security* settings of that application in your Wowza Streaming Engine Manager and set **RTMP Sources** security to **Open** (no authentication). This is required as Macula currently does not support authentication for RTMP streaming.

Then, go to Macula Console, open the *Shared Channels* section and add a new shared channel, then fill in the settings as follows:

- **Sharing type**: Wowza
- **Channel**: target channel from the list of existing channels
- **Use substream**: up to you
- **Enable audio**: up to you
- **RTMP URL**: *rtmp://<ip>:<port>/<app_name>/<stream_name>*, where
    - *rtmp://* indicates that RTMP protocol will be used for streaming
    - *<ip>* is Wowza Streaming Engine server address - either IP or domain name
    - *<port>* is target (remote) RTMP port, 1935 by default
    - *<app_name>* is the name of the application you have created in Wowza
    - *<stream_name>* is a custom name for the RTMP stream (can be any name, use underscores instead of spaces), will appear in Wowza automatically

When you have finished, click *OK* to save and exit; the newly created channel share will appear in the item list and Macula server will attempt to stream the data to the target URL at once. If you wish to pause the streaming, use the *Disable* button on the top panel. After sharing the channel, you should be able to view the stream on the RTMP server side and start the casting, if it has not started automatically.

If you have trouble receiving the stream on the RTMP server side, check the following:
- make sure all used software is allowed through the firewall(s),
- restart the RTMP server,
- refresh connection list on the RTMP server side or refresh the webpage;
- remove the shared channel in Macula Console and try sharing the channel anew.

To edit any of the previously created channel shares, double-click it in the item list or select any with single mouse click and then hit the *Edit* button on the upper panel. Use the *Search* field in the upper-right-hand corner to quickly find the existing items, and the *Disable* button to **disable and enable** channel sharing. Use the recycle bin button in the upper-right-hand corner to remove one or multiple shares: hold *CTRL* or *Shift* to select several items at once, or *CTRL+A* to select all (actual original channels will not be affected).

When you remove the original channel (with or without its originating device), all shared channels based on it are removed from the configuration automatically as well.

Filters in the bottom panel allow you to load recently added/modified items.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.8 Data Sources and Data Channels

This part of the manual covers the feature of data sources in Macula. Data sources are a means of retrieving textual data from a serial source, such as a Point of Sale (POS)terminal. You can receive information in textual form from various **third-party serial data providers** like intercoms, bank machines, and a multitude of other devices capable of delivering data strings over the following connection types:

- UDP port (remote connection)
- TCP port (remote connection)
- COM port (direct hardware connection to the server)

As a result, you get textual information, which you can store, analyze, react to, run queries to, and visualize in Macula Monitor.

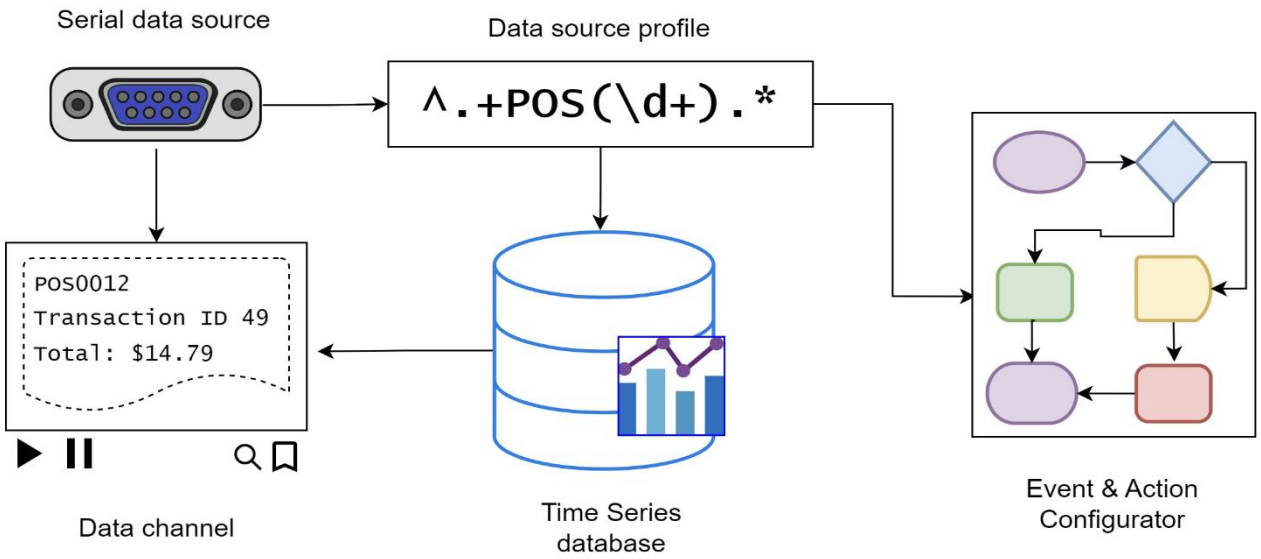
The following entities exist in Macula Console for this feature configuration:

- **Data source**: defines how the data are retrieved from the external source
- **Data source** profile: describes how the data are parsed and extracted on the Macula side
- **Database**: keeps the extracted data
- **Data channel**: displays the data from the database and allows detailed DB search in Macula Monitor

Data channels require an additional license.

General Concept

Macula servers receive serial data from the defined sources, splits it into transactions and individual lines of text, extracts and stores keywords and values, combines the text with the video streams, and allows advanced search across the database.



The diagram shows the data flow between data entities

Simplified configuration steps for the data reception from data sources can be briefly described as follows:

1. Create a **data source**, then

2. Create a data source **profile**, then
3. Link them together, and then
4. Assign the data source to the desired **channel**(s),
5. (optionally) Set up **variables** if you wish to react to certain keywords.

Gathered data are then stored and displayed embedded with the video stream from the channel(s) you choose to associate with it.

Starting from Macula version 1.23, there are additional entities available that allow building more complex scenarios: **databases** and **data channels**. These are not mandatory for receiving the serial data, yet they provide advanced means of storing and searching the data. Hence, you may find databases and data channels most useful when working with an abundance of complicated text like POS transactions, plus when there is a necessity to run complex textual queries on the data from the Macula Monitor side.

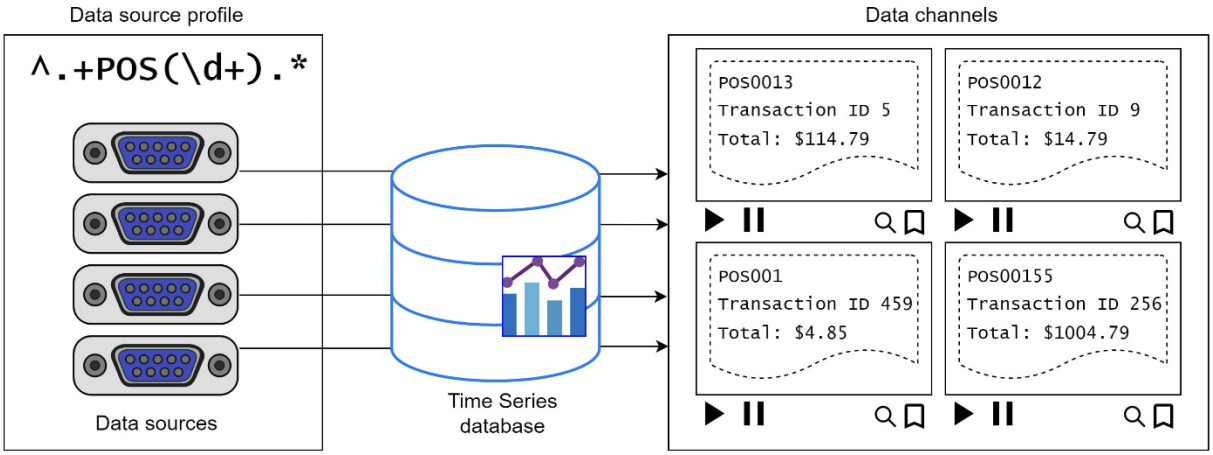
- With **databases**, you can store your selected data (a part of the data stream) in a database with further refined search in the Macula Monitor application.
- **Data channels** display text from data sources as a separate channel without underlying video, creating a convenient representation of the textual feed.

Macula Monitor also has a special playback mode featuring advanced database search.

Take the following steps to set up your **advanced setup** involving databases and data channels:

1. Create a data source (or multiple data sources), and
2. Add a data source profile, and
3. Link them together, and then
4. Create a database,
5. Map variables from the data source profile to the DB, and
6. Add a data channel (or multiple) linked to the data source(s).

In this more complex scenario, you can still use variables to trigger events in the Event & Action scenarios.



Data profiles shape how data from data sources are stored and presented in the form of data channels

Data Visualization

Data sources, data profiles, variables (mappings), and databases are configured in Macula Console. For users to access your data in Macula Monitor, you can:

- Combine data with existing video channel(s) so that the text overlays the video in Macula Monitor. No additional entities are required, the text overlays existing video channel(s) and the combination is displayed in Macula Monitor in the same viewport.
- Add data channel(s) to create a visualization for the transactions. Data channels will be displayed in a separate viewport but you can link them logically to video channels.

The first method is simpler and has usability restrictions. Data channels, on the other hand, provide additional functionality, but require a special license to operate. Both are described below in details.

Below, you will see how these entities are set up in Macula Console. For Macula Monitor part, please see the Macula Monitor user manual chapter on data sources.

Add Data Source

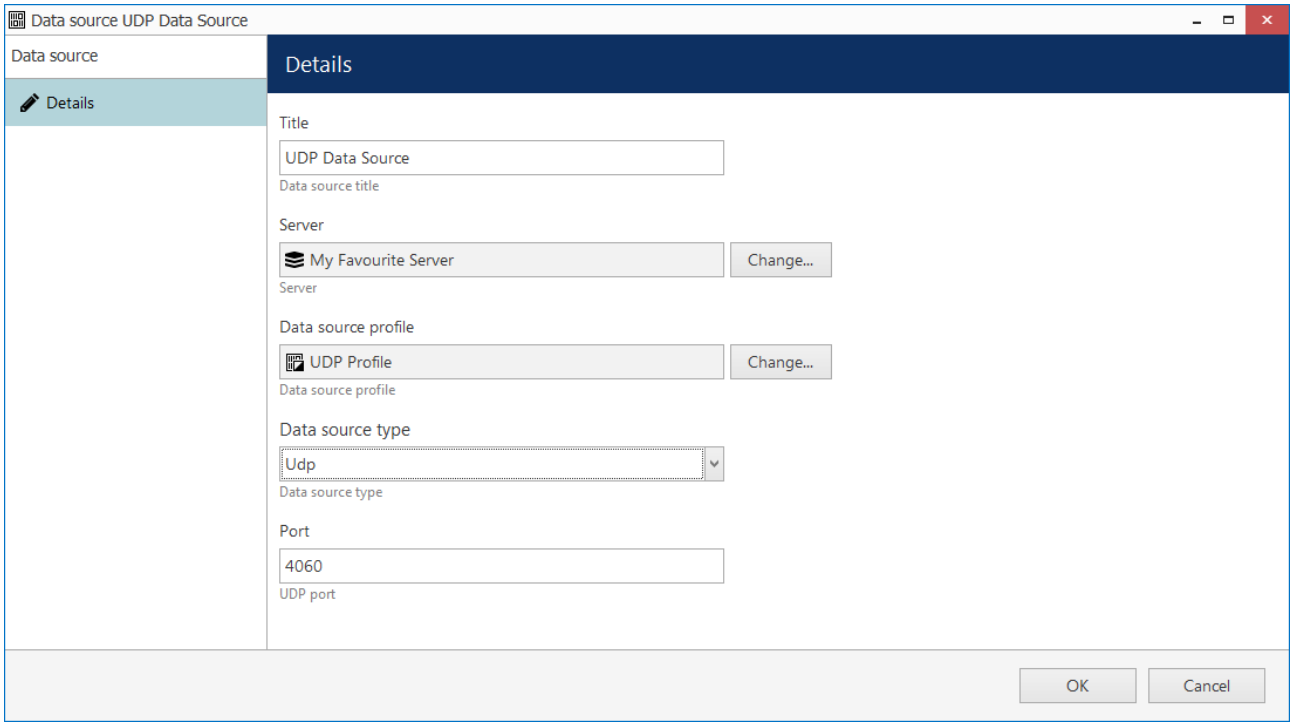
First, go to the *Configuration* section of Macula Console and choose the *Data Sources* component from the menu on the left. Then, click the + *New data source* button on the upper panel to open the data source creation dialog box.

Give your data source a comprehensive name. Then, choose the server that is going to be accepting the serial data. Leave the *Data source profile* field **empty** for now and select the desired transport for the data connection. You will need to return here and choose the profile after you create the profile itself.

There are three possible connection types: UDP port, TCP port and COM port.

TCP/UDP Connection

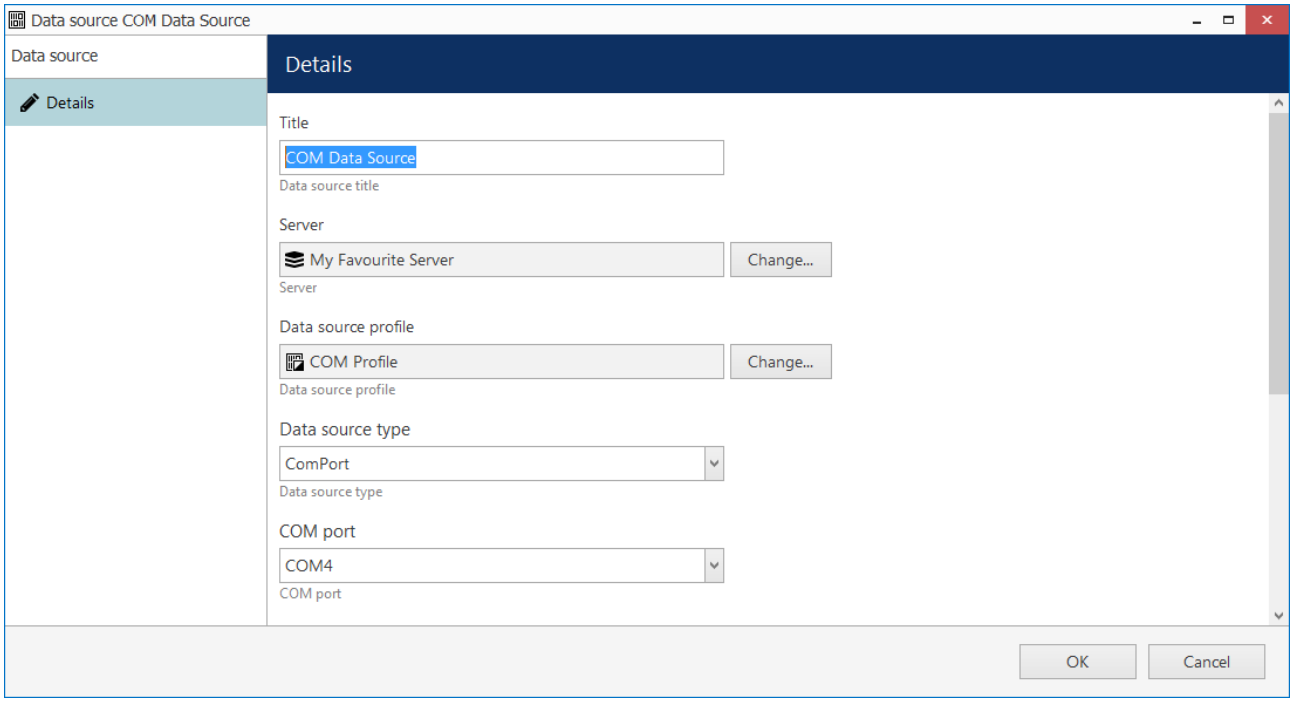
Choose this option if your data provider is configured to feed the textual data into a specific TCP or UDP port.



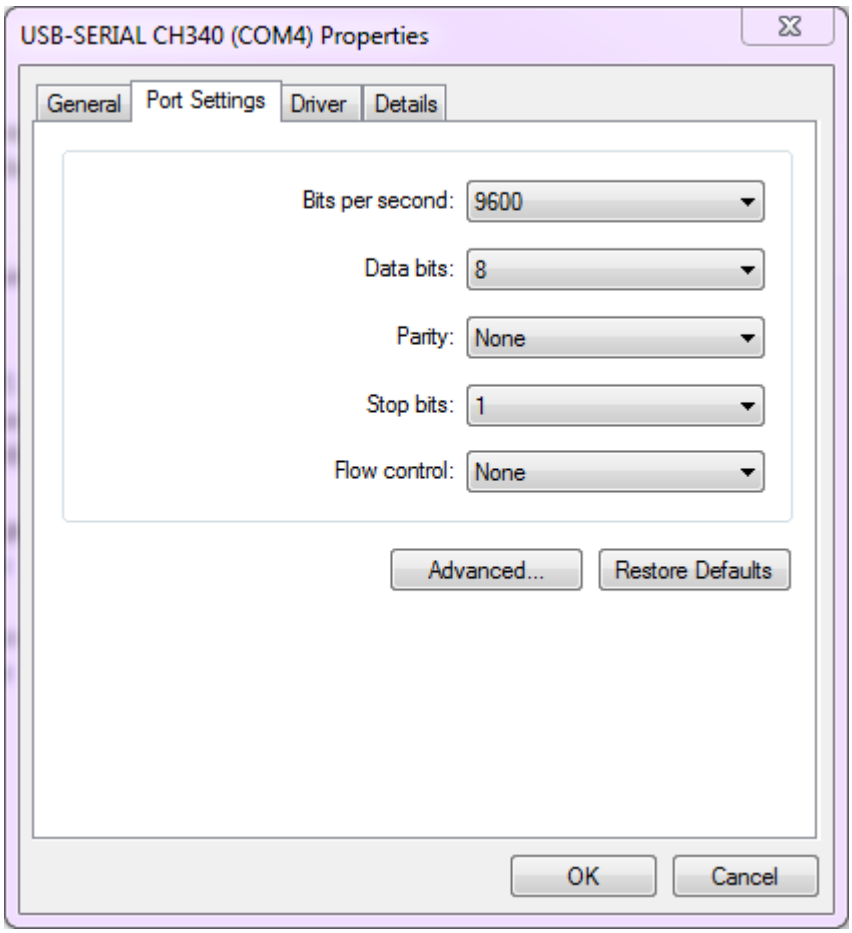
You simply need to specify the incoming port for the server to listen to in the settings here. Make sure the port is opened on all intermediate firewalls and not used by any other software on the server machine.

COM Port Connection

Choose this connection type if your data provider is connected directly into the Macula server's COM port.



For this configuration, you need to match the serial connection settings with those used from the device side. Normally, this can be checked via Windows Device Manager for your target COM port.



The following serial port settings should be specified:

- **COM port**: serial port to read the data from, choose from the list of active ports
- **Baud rate**: information transfer rate (9600 by default)
- **Data bits**: the number of bits transmitted over the serial interface (8 by default)
- **Stop bits**: the number of bits to specify the end of a byte; if you select data bits to be 6, 7, or 8, then the default value is 1 and the other available choice is 2; if you select data bits to be 5, then the only correct choice for the stop bits is 1.5
- **Parity**: how the parity is checked (no parity by default)

Other serial port parameters are not required for the Macula server.

Click *OK* to save and close the data source creation dialog box. The next step is to create a data source profile to help the server determine how the textual data should be parsed.

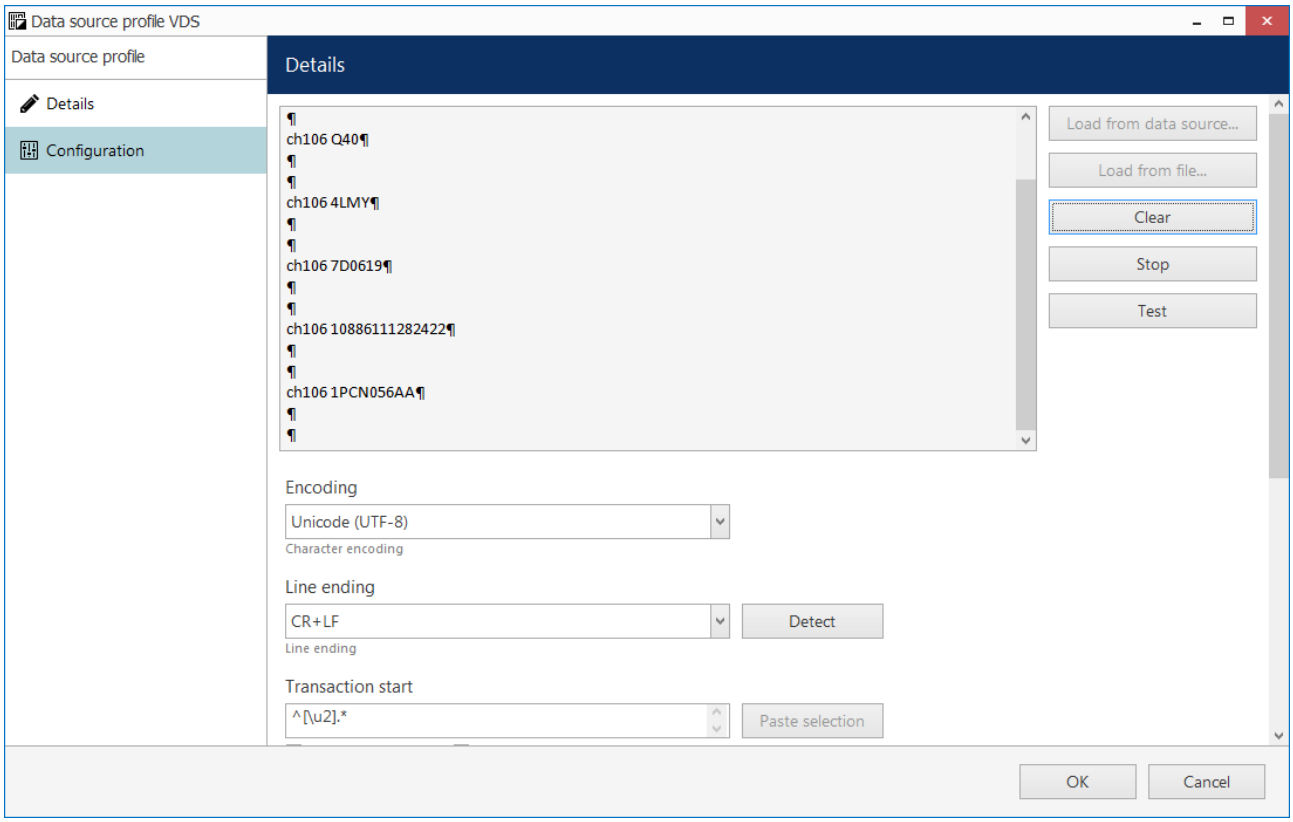
Add Data Source Profile

On this step, you will load a portion of the serial text from the data source configured as shown above, and set up how the text will be parsed. That includes breaking the text into lines and transactions, and adding variable mapping.

In the *Data Sources* section, click the little arrow next to the data source creation button and choose the + *New data source profile* from the list. In the *Details* tab, enter a custom name for your data source profile and switch to the *Configuration* tab.

It is now necessary to use an example of the data strings to set up the profile. This part of the setup is the same regardless of what type of data source you have.

You can either use the **actual data source** you have configured on the previous step, or use a **text file** that contains the lines of data in the expected format (note that the same encoding should be used). Use the buttons on the right side of the text field to load the sample from either source. Use the *Stop* button to finish displaying new text from the data source (do this if you see that the loaded data lines are sufficient to facilitate the configuration process); use the *Clear* button to erase whatever is in the preview window before loading a different file or strings from a data source.



Based on the loaded sample, set the required parameters below:

- **Encoding**: pick the correct encoding to ensure your text is readable
- **Line ending**: choose what non-printable characters represent the end of the line, available options are:
    - CR - carriage return
    - LF - line feed
    - CR+LF - both together
    - Custom - user-defined symbol or group of symbols

If line delimiter in use is one of the standard non-printable ones (LF, CR or CR+LF) but you are not sure, whichever is used, press the *Detect* button for the software to identify automatically, which delimiter is present in the preloaded text. If you know that the provided serial data does not include any standard delimiters, choose the *Custom* option in the drop-down list and define your own delimiting character.

⚠ It is crucial that these settings exactly match the source settings. In case of a slight mismatch, your text may still appear readable but the lines may not be split correctly, causing errors in mappings.

Mappings

Mappings are pre-defined character combinations expected in the data flow. Typically, mappings are defined by regular expressions, which are used to extract required values of all sorts from the incoming text: identifiers, keywords, surnames, codes, etc.

Built-in Mappings

Macula server splits the incoming text into transactions. Each transaction has a certain structure, which can be visualized as follows:

```
-BEGIN TRANSACTION

  //header starts here
 <transaction fields are captured (e.g. POS ID, Cashier Name etc)>
  -HEADER END

  -BEGIN DETAIL
   //item details
 <detail1 fields are captured ( e.g. Item, Price, Quantity etc)>
  -DETAIL END

  -DETAIL BEGIN
    //next item details
 <detail2 fields are captured ( e.g. Item, Price, Quantity etc)>
  -DETAIL END

  -FOOTER BEGIN
    //footer
  <transaction fields are captured (e.g Total )>
    //footer ends here

-END TRANSACTION
```

The CAPS text in the visualization defines the marks for the Macula parser that help it to split the text correctly. For each transaction and for each detail it is necessary to mark both beginnings and ends. For the transaction header, it is enough to mark the header end because the transaction beginning serves as the header start. For the footer, it is enough to mark the place the footer starts, as the footer automatically ends with the transaction. All of these marks are mandatory if you plan to use data channels and databases.

Each incoming serial text stream is split into transactions (each of which has a header and a footer), and each transaction may contain a number of details (transaction items). Further, in databases, you create separate tables for transactions and transaction items.

There are several built-in mappings (existing by default and non-removable) that help you define these BOUNDARIES:

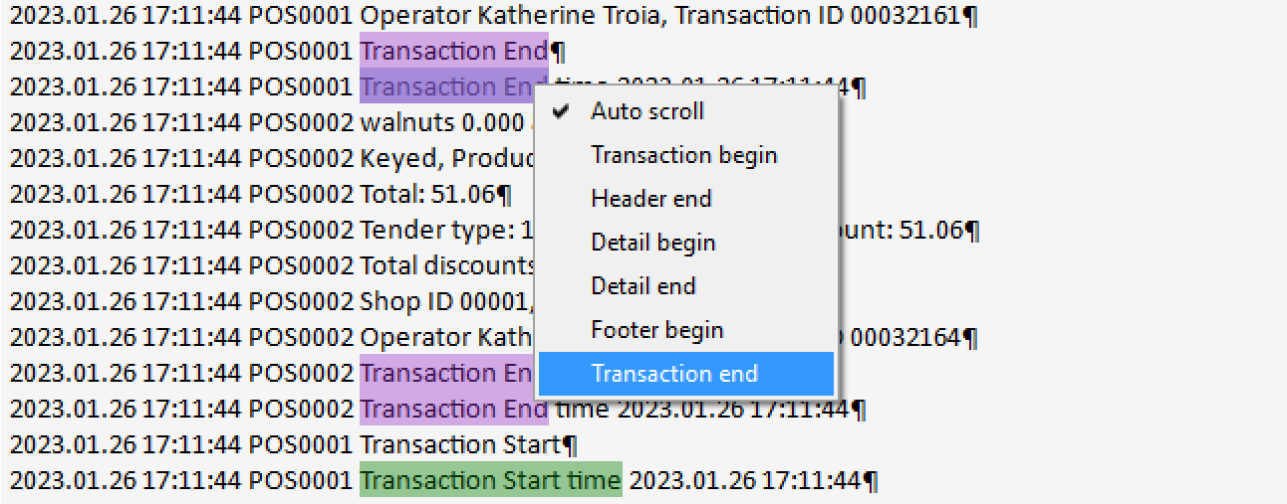
- **BeginTransaction:** specify text that designates the beginning of the data block (transaction)
- **EndTransaction**: the very last data line of the expected data block

- **GetID**: use a regular expression to determine and extract the data ID of each line (skip this if you only have a single data stream)
- **HeaderEnd**: the text that marks the end of the header section, details are expected after it
- **FooterBegin**: the text that designates the beginning of the footer section, and the end of recurring details
- **DetailBegin**: how each detail (item) starts
- **DetailEnd**: how each detail (item) ends

All of these mappings can be plain text or regular expressions, except for GetID, which must be a regular expression because it must capture variable values.

> Determining the Data ID is important if you have multiple data streams coming from a single data source (e.g., multiple POS terminals). In order to split the text between video channels and/or data channels, you need to set the GetID mapping here, and further define the actual Data ID in the video overlay and in the data channel settings.

For the transaction start and end, you can specify **regular expressions** (regex rule) to define the start/end pattern instead of static text. You can also copy and paste the strings for transaction start and end directly from the sample preview field.



Mark the text and right-click to choose the mapping (only for non-regex mappings)

For the non-regex mappings, you can simply highlight the target text in the preview field, right-click it, and choose the mapping to bind the text to.

Custom Mappings

Additionally, you can create any number of mappings of the **user variable** type. These mappings use regular expressions to extract specific pieces of data into a variable, i.e. map variable text into pre-defined value containers. Custom variables have two usage scenarios:

- variables allow you to extract the text and store it in the database. For this, you need to create the database with the desired fields, and then bind mappings to the DB fields.
- E&A event *Variable Condition*. Variables can be used, for instance, to detect exceptions in the cash operation in case the data source is a Point-of-Sale system.

To create a **new variable**, click the + *New* button in the *Mappings* section, fill in the settings on the left and click *Apply changes*. The following settings are available:

- **Type**: variable (cannot be changed)
- **Name**: user-defined variable title
- **Text**: a regular expression that defines what character combination should be extracted into the variable
- **Case sensitive**: enable this if uppercase/lowercase is important (disabled by default)
- **Write to database**: map the variable to a database field for storing and search (if you are not planning to use databases and data channels, ignore this option)

> If you do not have a database yet, you can still create all the required variables at this step. After you add the database at a later point, bind it to the data source that feeds data into this data source profile, and you will have an option to map variables to the database fields.

Load some text and then use the *Test* button to **check if your settings work**: if everything is fine with the setup, lines should be detected correctly, transaction start and end marked as such and variables extracted as specified.

> Use the *Test* button to verify your mappings. The variables extracted from the sample text will display on the right. If your regex rules do not work as expected:
> - make sure your line ending setting is correct
> - verify the regex expressions using a third-party parser (e.g., regex101.com)
> - load a new portion of text and test again

Click *OK* to save and close the profile configuration dialog box.

Now, **go back to your data source settings** and specify the newly created data source profile that was missing in the initial configuration. You can use a single data source profile for different data sources. In this way, you link the two together, ensuring that the data received from the data source is passed to the data source profile for further analysis.

Video Overlay

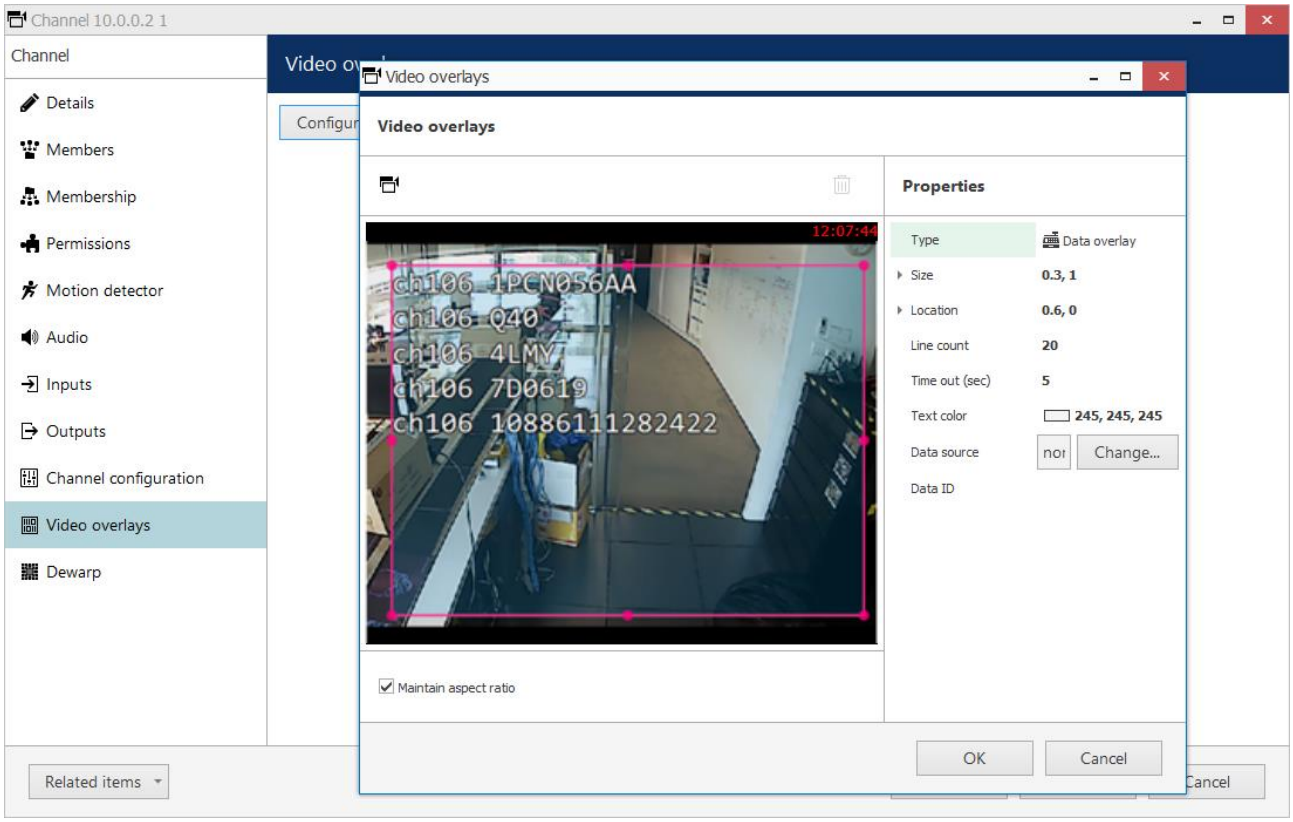
You can put the serial text over the video so that they appear together in the Macula Monitor application. The text will be also available for simple search in the special tab, Data Sources, in Macula Monitor.

Under *Configuration*, go to the *Channels* section and pick a channel that needs to be associated with a data source. Double-click the channel to open it for editing and switch to the *Video overlays* tab. Click the *Configure video overlays* buttons to bring up an additional dialog box.

Macula® Professional Administration Guide

Here, different kinds of video overlays can be configured. The *Data overlay* element is already present by default - it is the pink frame overlaying your video.

On the right side, you will have the available **settings**. Click the *Change* button and select one of your pre-created **data source** for this channel. If the serial data are currently arriving, you will see the text appear in the frame. Then, adjust the settings on the right to define where and how the text should appear on top of the video stream.



Use the visual control - the pink rectangle - to specify the **text output area** within the video stream viewport. There are other types of video overlay elements available in the same window, but the one you need is called *Data overlay* and it exists by default, so you do not have to add it. There are also numerical coordinates on the right side of the preview for your reference: you do not have to edit them manually.

Also, note that the visual control cannot be removed from the configuration; if there are no data to display, this element simply will not exist in the Macula Monitor application. The visual control is only present in this configuration window for your convenience. There is exactly one *Data overlay* element per viewport, meaning that each channel can only have text output from a single data source.

> ⚠ Make sure the video from the target channel is available before setting up the text overlay in order to ensure correct text placement.

Additional settings:

- **Line count**: set the desired number of text lines to be fitted into the overlay area (default value is 20); this will affect the text font size
- **Timeout**: the amount of time in seconds for every line of data to stay on the screen at maximum (older text will disappear and text will be shifted upwards)
- **Text color**: choose a color for the overlay text from the standard palettes (default is white)
- **Data ID**: data source identifier, if present (leave empty if not used)

In the *Data ID* field, you can enter the source identifier in case the serial data are being **split** between two or more channels; leave the field **blank** if this channel is the only destination for all the data received from the selected data source.

> If there are data from multiple devices combined in a single *Data source* feed so that the text comes from the same IP and port via the same protocol, it is possible to use the **Data ID field** in the *Data source profile* configuration to differentiate between the transactions based on their source identifier and split the text between multiple channels for further overlay.
>
> **Example**: if the feed contains serial data from multiple Point-of-Sale terminals and their identifiers look like *POSxxxx* where *xxxx* contains the terminal number so that the identifiers are POS0001, POS0002 and so on, the following **regular expression** can be used to extract these IDs: **^.+?(POS\d+).+**
>
> In this case, the *Data ID* field in every channel configuration is to contain the actual POS ID: POS0001, POS00023, POS6592 etc.

When ready, click *OK* to save and close the data overlay dialog box, then click *OK* to save and close the channel configuration window.

Now your textual data from the data provider will be displayed overlaying the video stream in Macula Monitor and both live view and in the instant/regular archive playback mode in case the corresponding option is enabled in the recording profile for the target channel; also, it will be possible to search through the recorded data.

> If you wish the serial data to be available in the video **playback** mode in Macula Monitor application, make sure to set the *Data stream* to be recorded in the corresponding recording profile.

The overlay text will only be visible in live view and regular/instant playback, and will not be displayed in other views (e.g., smart search). In order to export video from the archive with the text overlay, use MKV file format + VP8 compression + hard or soft subtitles.

If you do not wish to combine the serial data with video, check an alternative method described below. It uses databases to store the serial data instead of the video archive, and provides a dedicated visualization in the form of a data channel.

Time Series Databases

Data received from the data sources can be stored in the databases of a proprietary type, which use the time series database principle. Time series databases are optimized for simple write and search operations, effectively holding a large quantity of the serial data that arrive over time (and are usually written in a series and not injected somewhere in the middle).

Each database (DB):

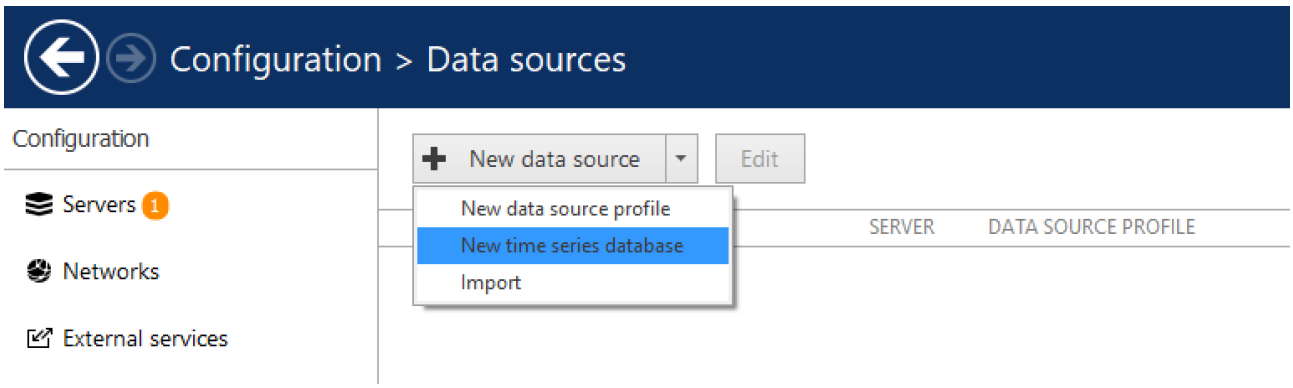
- is bound to one or more data sources,
- receives data from these data sources as defined by mappings in the data source profile,
- writes the data locally (on the same server with the data source), and

- performs search based on user queries from Macula Monitor and returns the requested information.

> You can add any number of databases but they will only operate when you have data channels, which are subject to licensing.

Create New Database

To add a new database via Macula Console, make sure you are in the *Configuration* section > choose *Data Sources* on the left > click the down arrow next to the + *New..* button and choose the *New time series database* option.

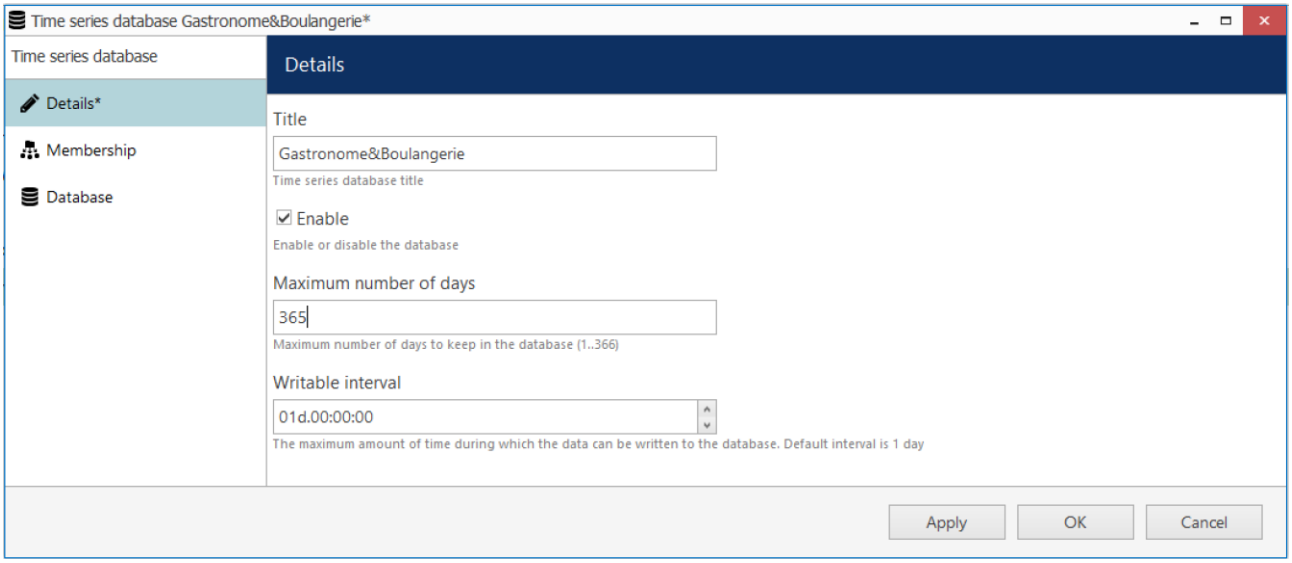


In the new DB dialog box, fill in the database settings.

In the *Details* tab:

- **Title**: user-defined database name that will appear in Macula Monitor
- **Enable**: if marked, the database will be available for write & read
- **Maximum number of days**: entries older than the specified number of days will be removed
- **Writable interval**: the maximum age of a new entry, older entries will be discarded

The data are normally written to the database real-time. However, if there are delays in the synchronization due to network availability issues or other reasons, you may want to write older entries. For this purpose, each database has a limited **writable interval**, during which it will accept new entries with non-real-time timestamps. Keep this interval shorter if you prefer a faster DB, and set a longer interval if you know that some of the data may arrive with a significant delay (e.g., from remote locations). Default value: 1 day, max value: 99 days.



In the *Membership* tab, you can put the database into one of your **visual groups** for a more convenient presentation in Macula Monitor.

After you have set the general settings, switch to the *Database* tab. Here, you need to create the **database structure** using the following guidelines:

- each database can have **2 (two) tables**
  - the first table stores so called transactions (larger chunks of information the serial data are broken into)
  - the second table holds transaction items (repetitive individual elements of the transaction)
- each of the two tables can have up to **32 fields**, for example:
  - transaction fields (main table): POS ID, door ID, transaction ID, operator's name, total, etc.
  - transaction item fields (details table): product ID, product name, amount, subtotal, etc.
- fields that have repetitive values from a fixed list (e.g., operator's name or item name) can have **reference tables**. For such fields, their values are replaced by keys in the main table, while longer textual values are kept in the reference table, speeding up the DB operation.

When you create a new DB, it offers you to create the **main table** first:

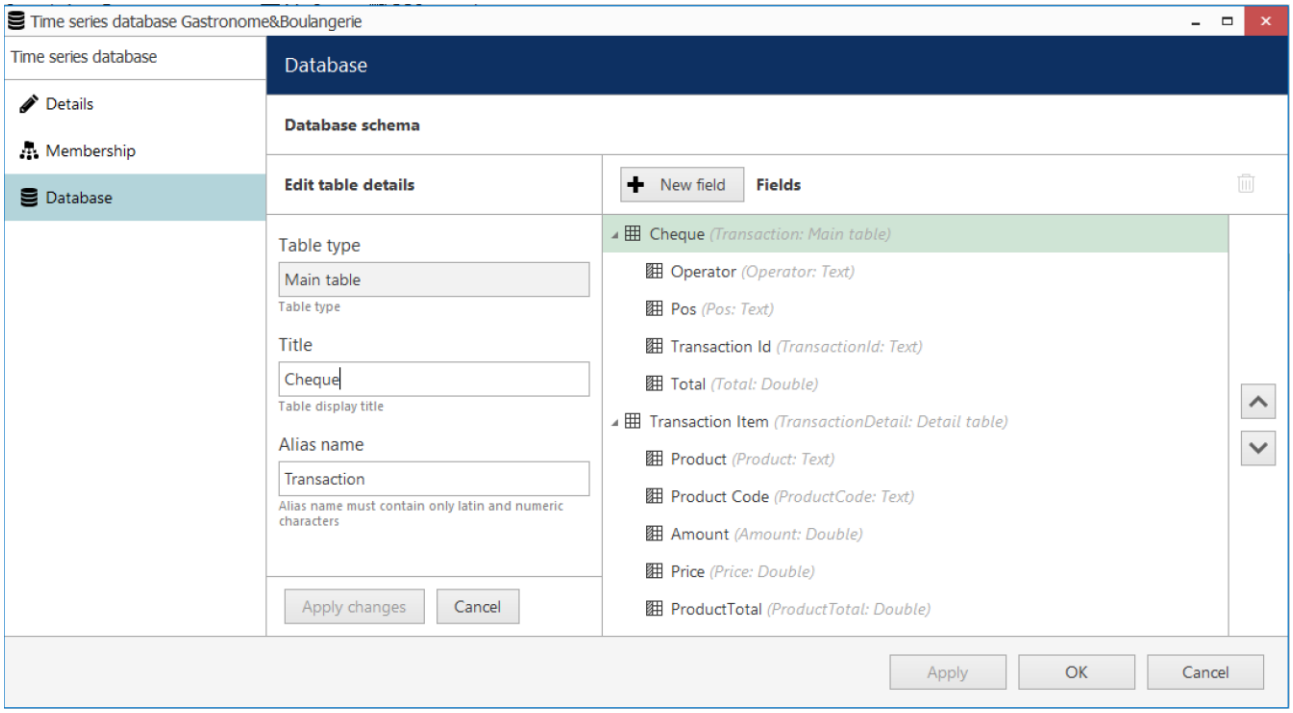
- **Title**: user-defined table name that will appear in Macula Monitor. The title may contain a wide range of characters: non-Latin alphabets (e.g., Cyrillic letters), white spaces, and special characters.
- **Alias name**: internal table name that may only contain Latin letters [A-Za-z] and numbers [0-9].

After changing the settings, click *Apply changes*: your table name will appear in the DB structure on the right.

After that, use the down arrow net to the + *New field* button on the right to add the second table (details table) using the same logic. After you have done that, or if you only plan to have one table, use the + *New field* button to **add fields** to both tables:

- **Title**: user-defined field name that will appear in Macula Monitor. The title may contain a wide range of characters: non-Latin alphabets (e.g., Cyrillic letters), white spaces, and special characters.
- **Alias name**: internal field name that may only contain Latin letters [A-Za-z] and numbers [0-9].

- **Data type**: choose if the value will be stored as text/integer/long/double. Textual fields can have reference tables.
- **Create reference table**: for text fields only; mark this option if you know that the data field value belongs to a finite list of values (e.g., operator's name). Do not use this option if the field value is [mostly] unique.



Note that you do not have to describe everything you expect to receive from the data source, but rather just the values you want to store and search in Macula Monitor.

After having created all the tables and all the fields, click *OK* to save and close the dialog window. The newly created time series database will appear in the list in the *Data Sources* section. Note that the database will only appear in the *Monitoring* section of Macula Console and in Macula Monitor after there are some actual data written to it. For this, you need to create at least one data channel and link it to the same data source.

Data Channels

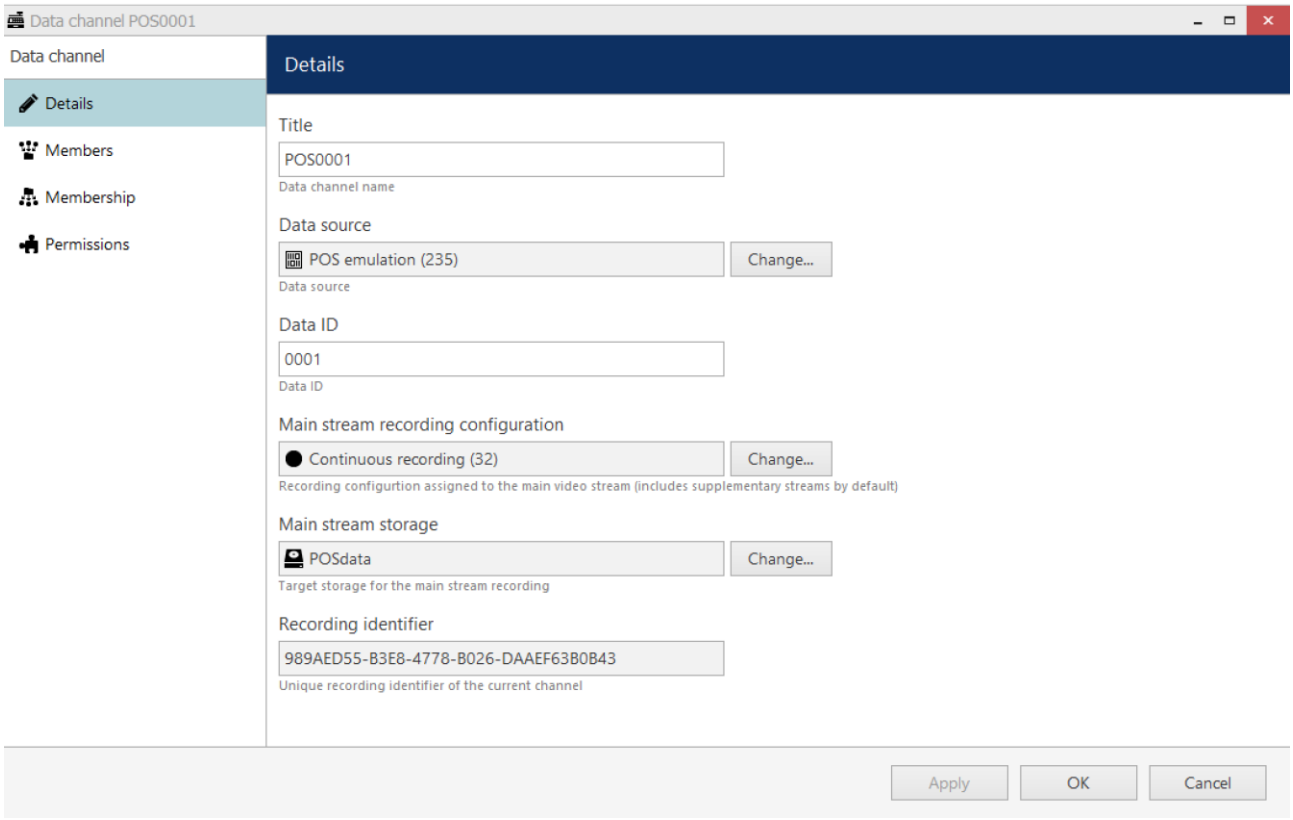
Data channels are a way to visualize the serial data received from data sources without combining it with the video in one viewport. Thus, you get your data displayed neatly in a separate viewport next to the video channels.

⚠ Data channel must be paired with a time series database in order to operate!

Create Data Channels

To create a new data channel in Macula Console, go to the Data Channels section under Configuration. On the top panel, click the + New Data Channel button

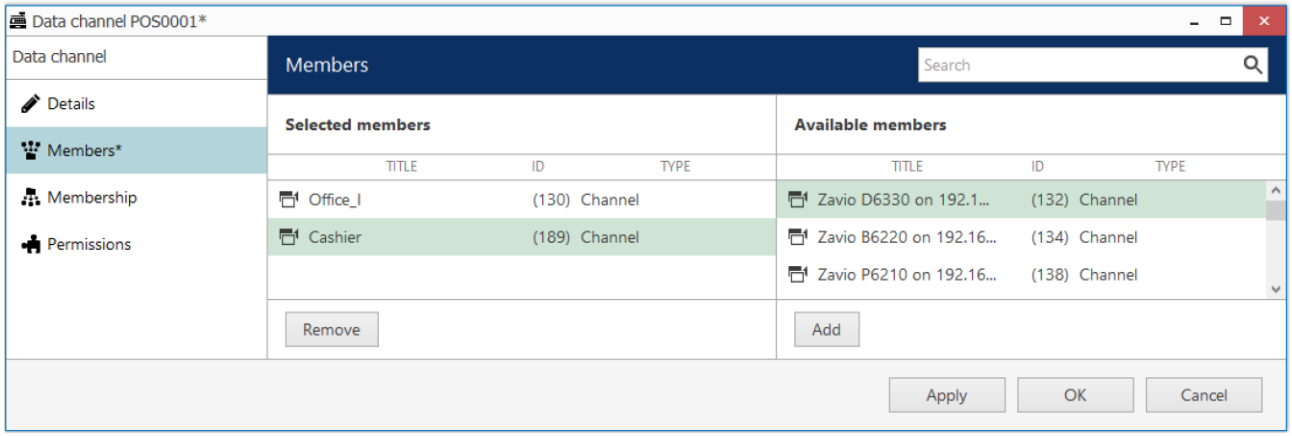
Macula® Professional Administration Guide



In the *Details* tab, fill in the following settings:

- **Title**: user-defined data channel name that will appear in Macula Monitor
- **Data source**: the source of the text to be displayed
- **Data ID**: the actual identifier of the data stream extracted by the mapping **GetID** (defined in the data source profile)
- **Main stream recording configuration**: how the data will be recorded (main stream only)
- **Main stream storage**: destination storage

Not that it is mandatory to fill the Data ID field if your data source has the GetID mapping defined. When the data source parser encounters a GetID variable value, it searches across all data channels for the target data channel and writes the corresponding data to the database. If the GetID mapping is defined but there is a data channel with an empty Data ID field, this data channel will not have any data fed to it.



In the *Members* tab, you can **pair** the data channel with two types of resources:

- **channels**: one or more video channels that will pop up together with the data channel when you search across the database and get results from this data channel

- **user buttons**: paired user buttons will appear in the data channel viewport, next to its name, so that you can click them to trigger the related event

By making video channels members of the data channel, you facilitate the textual search in Macula Monitor. For example, if your data channel is a POS terminal, it would make sense to pair data channels to video channels that face the cashier's desk.

In the *Membership* tab, similarly to the regular channels, you can put your data channels into groups (for permission handling) and visual groups (for grouping on the Macula Monitor side).

Finally, in the *Permissions* tab, just as for any other resource, you can define access permissions for your users and user groups.

For efficient permission management, use groups for both resources and users.

Data channels are similar to video channels; hence the **permission list is very similar:**

- **View live video**: permissions related to the live streaming (Live tab in the server configuration).

In the small window that pops up, choose the desired items, then click *OK* to proceed: the items will appear in the *Data sources* section and you will be able to edit them as usual.

Note that you will need to create data sources and data channels to complete the setup.

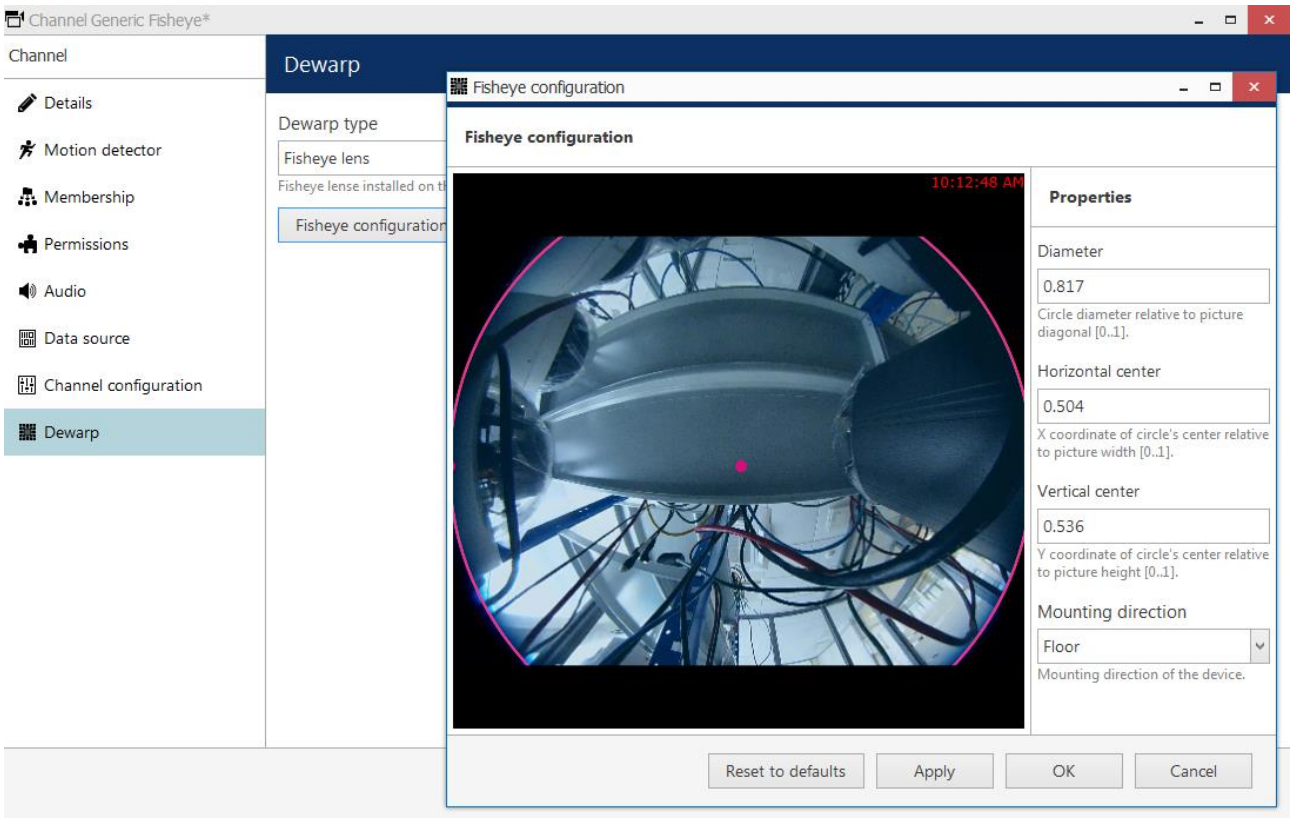
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.9 Dewarp For Fisheye Cameras

Fisheye lens is an ultra-wide-angle lens that produces a wide panoramic image at the cost of strong visual distortion. Usually, devices with such lenses capture a 360-degree geometrically distorted image and projects it as a circle within the image frame. Fisheye lens can be either built-in by design or purchased separately and installed on your desired camera. Macula dewarp feature allows to correct the perspective and obtain several "normal" views from a single distorted fisheye picture.

In order to access dewarp settings via Macula Console, open the *Configuration* section and choose *Channels* from the menu on the left. Find the channel you wish to dewarp in the list (use *Search* or filters, if necessary) and double-click it in order to open it for editing (alternatively, use the *Edit* button on the upper panel to open the dialog box), then switch to the *Dewarp* tab.

> Please note that the location of dewarp settings has changed starting from the product version 1.5.0. For previous software versions, the corresponding settings can be found in the general *Channel Properties* dialog box.



You have the following options here:

- **Regular lens**: choose this option if you wish to disable the dewarp engine (selected by default)
- **Immervision Enables® lens**: choose this option if your camera has a Panomorph lens installed (you can check this in the camera specification)
- **Fisheye lens**: choose this option if your camera has a regular 360-degree view lens
- **Fisheye lens (large resolution)**: dewarp engine optimized for image resolutions of 6MP+

If your fisheye image has a resolution of **6 megapixels or higher**, it is better to use the last option in the drop-down list - fisheye lens **optimized for high resolutions**. This mode will provide smoother DPTZ

experience with the dewarped image. If your graphics card supports **OpenCL version 1.2** or higher, this dewarp driver will use GPU (you can check this in your video driver properties, or request info from the video card manufacturer). Otherwise, more CPU time will be required, compared to the basic fisheye mode. We recommend that you do not use this driver for smaller resolutions, as it may use more CPU yet there will be no difference for the user.

For devices having a Panomoph lens, choose the lens model from the drop-down list - you can find this information in your camera specification or request it from the device manufacturer. You do not need to define any parameters manually in this case; rather, you only need to choose your camera mounting position, and the dewarp engine will automatically produce a correct dewarping result.

> Note that the dewarp engine will fail to operate if you choose a wrong Panomorph lens model. Check with your camera documentation and manufacturer for the precise lens model information.

For a regular fisheye lens, you are requested to define the fisheye sphere size and camera position by using the **overlay controls** and settings on the right side:

- Hemisphere **diameter**: click and drag any of the small pink circles on the overlay sphere to change its size and align it with the actual fisheye sphere in the picture
- **Horizontal** and **vertical** centre: automatically positioned in the picture centre, to change it click and drag the small pink circle inside the sphere
- **Mounting** direction: select camera mounting position from the drop-down list (wall/ceiling/floor)

For your convenience, the defined parameters are also displayed in the numeric form on the right side of the dialog box. Use the button below the preview to **reset** all dewarp settings to the default ones.

> In case you change the stream resolution at some point, its **aspect ratio** may also be changed and this will affect dewarp operation. Therefore, check the dewarp settings after changing the resolution and adjust the parameters, if necessary.

> Note that all dimensions are given not in pixels but in reference to the video stream size, therefore, relative values are used instead of absolute ones.

When finished, click *OK* to save the changes and close this dialog box and return to the general channel configuration. Dewarp results will immediately become available in the Macula Monitor application; you can find the details on usage in the corresponding section of the Macula Monitor documentation.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.10 Audio

Macula is capable of receiving audio streams from cameras, recording and playing them back, as well as sending audio back to the cameras from Macula Monitor stations. It is also possible to bind an external audio source to a video channel.

There are a few conditions stipulating audio feature availability:

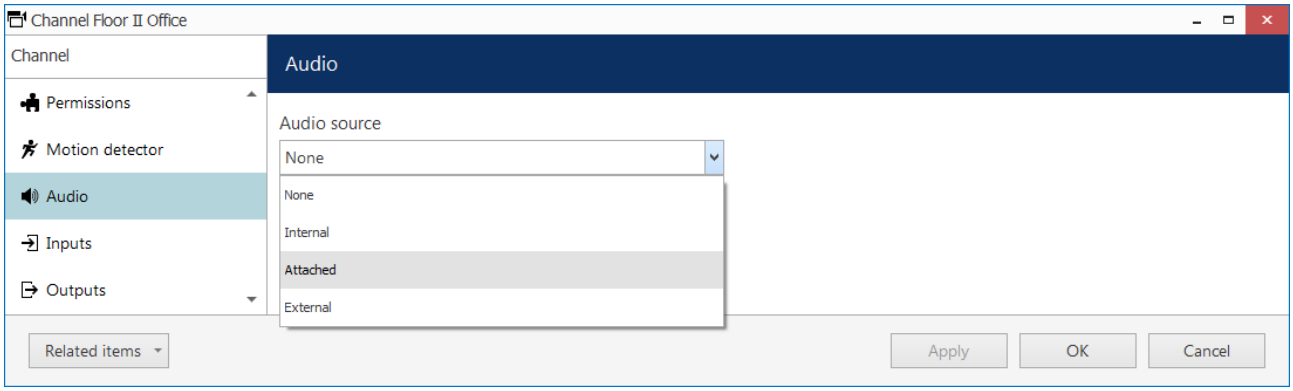
- the target device should be capable of sending/receiving audio
- relevant additional equipment should be plugged into the device (microphone and/or speakers), if necessary (if these are not built in by design)
- one-way or two-way audio should be enabled and set up on the device side so that it is available via device Web interface
- G.711 should be selected as audio codec on the target device side
- audio should be enabled in the channel settings via Macula Console (see the description below)
- feature should be supported by Macula for the target device (see the list of supported devices and features provided by GSF)
- in order to send audio to the device, Macula Monitor workstation must have a microphone connected to it - either a built-in or an external one
- if you plan to use an external audio source, relevant audio capturing equipment should be plugged into the server, to which the target device is connected, and enabled via Windows audio settings

⚠ G.726 and AAC audio codecs, which are often implemented on the camera side, are not supported at this point, so please always select the **G.711** option. Setting other codecs on the device side may result in Macula being unable to decode the incoming video stream.

Enabling Audio

If you plan to use camera-side audio and have not checked audio configuration on the camera side yet, go to the device Web interface and adjust the audio settings, then make sure that audio is operable in the browser preview (you may need to install an ActiveX control in order to get it working; please check with your device's user guide for tips and browser requirements).

In order to **enable audio capabilities** for your desired device, open the *Configuration* section and choose *Channels* from the menu on the left, then open your target channel for editing - either by double-clicking it or by selecting it with a single click and clicking the *Edit* button on the upper panel. In the channel settings' dialog box, switch to the *Audio* tab by selecting it on the left.



Here, you have 4 options. Depending on your selection, additional fields may appear.

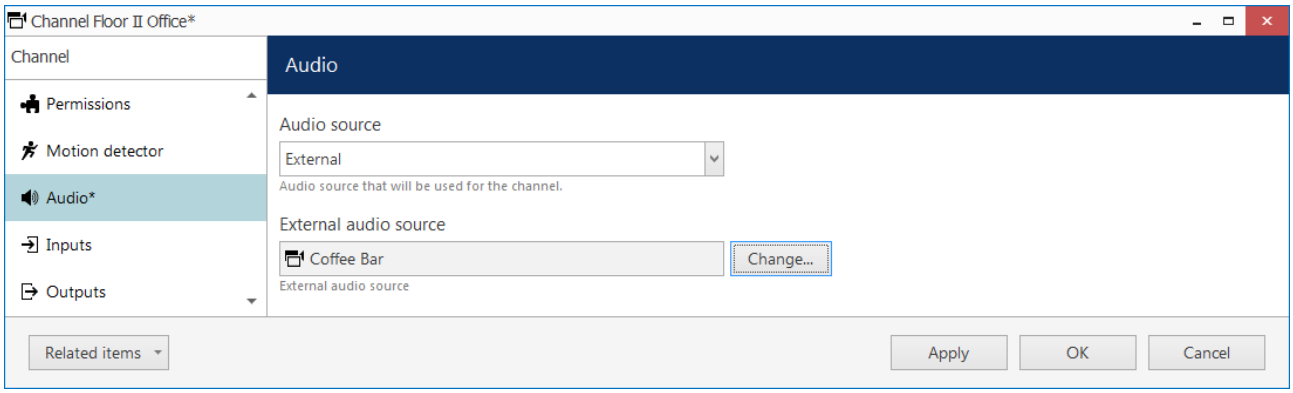
- *None:* **disable** audio functionality for the target channel (default), no additional settings
- *Internal:* enable audio reception **from the device** side and sending the reverse audio to the device
    - choose an audio input from the drop-down list, if the target device has multiple ones
    - if there are none configured or available on the device side, the list will appear empty (this also refers to cases when audio is not supported for the selected device)
- *Attached:* use an external audio source **connected to the** same **server** as the device, from which the
  target channel originates
    - choose an audio input device from the drop-down list, if the target server has multiple ones connected to it
    - all microphones recognized by Windows will appear here
- *External:* use **another channel's audio** as audio for the current channel (see below for more details)
    - choose a channel to serve as audio source

When you have chosen your preferred option, click *OK* to save and close the *Channel settings* dialog box. You should now be able to listen to live audio, record it along with the video stream and talk back to your camera via Macula Monitor and Macula Mobile applications.

Combining Video and Audio Sources

Macula allows channels to use audio coming from a different channel in case the target channel does not have its own incoming audio or in case you wish to combine audio and video data from different channels. Such combinations are used for both live and recording. A common example of this method is to use audio from intercom channels in combination with nearby video cameras.

In order to do this, double-click the target channel (the one without audio) in the channel list to open it for editing, then choose the *Audio* tab on the left.



Choose *External* from the drop-down list, then select a channel to be used as the new audio source: click the Change button to see the list of channels and choose the one that you want audio to be coming from. Hit *Apply* or *OK* to save your changes.

> ⚠ Audio must be configured for the channel used as an external audio source via channel configuration as described earlier. Both cameras and audio-only devices (intercoms) can be used as external audio sources.

10.11 Reports

Macula Console application provides an opportunity to send automatic reports. There are two types of them:

- Reports based on the counter data, which has been recorded with the video stream(s). Depending on the collected information context, these reports can be used, for example, to estimate the average number of customers during specific hours, compare the number of passing cars to the number of trucks etc. Counter information is collected from Macula **Open VCA** video analytics, **camera-side VCA** (for certain manufacturers) and software counters.
- Reports based on the facial recognition (FR) module data. These include the counted detections (by tag) and miscellaneous estimators (age, gender, temperature, sentiment, etc.).

The report configuration process is similar to the manual procedure of reporting in the Macula Monitor application, with the difference that here the settings are defined once and then are used by the Macula servers for automatic report generation.

There are three report types: **bar**, **line** and **pie** diagram. Regardless of the chosen type, all reports are based on the **counters** and have configurable report interval and days and times of interest. Counter values are compared for the given period and with the specified scale, and the results are then reflected in the chart of the selected type. Reports can be configured to be created **automatically** on a **daily**, **weekly** or **monthly** basis and then **emailed** to the specified email address.

> ⚠ Regardless of the report settings, the report will be emailed after the selected report interval has ended.
>
> Example 1: the report interval is previous day with time filter set to 8AM to 6PM. The report will be emailed next day 12:01AM.
>
> Example 2: the report interval is previous week with only working days selected (weekends deselected). The report will be emailed 12:01AM next Monday, i.e., when the week is over.

Prerequisites

Reporting in Macula Console is primarily aimed at automatic report sending via email. In order to achieve this, you need to **configure** a mail server for the emails to be sent through, according to the steps explained in the corresponding section of this document. You can do this prior or after the report setup. If you need a one-time report for a custom time interval, you are welcome to use the reporting function in the Macula Monitor application.

For a counters report to be created successfully, there must be some counter data present in the database. You can use Open VCA, camera-side VCA (for certain manufacturers) or software counters. Open VCA setup in Macula is described in a separate document provided by demand.

For the FR report to be created, you must have at least one channel being analyzed by facial recognition module for the specified period, and the target FR service must be connected.

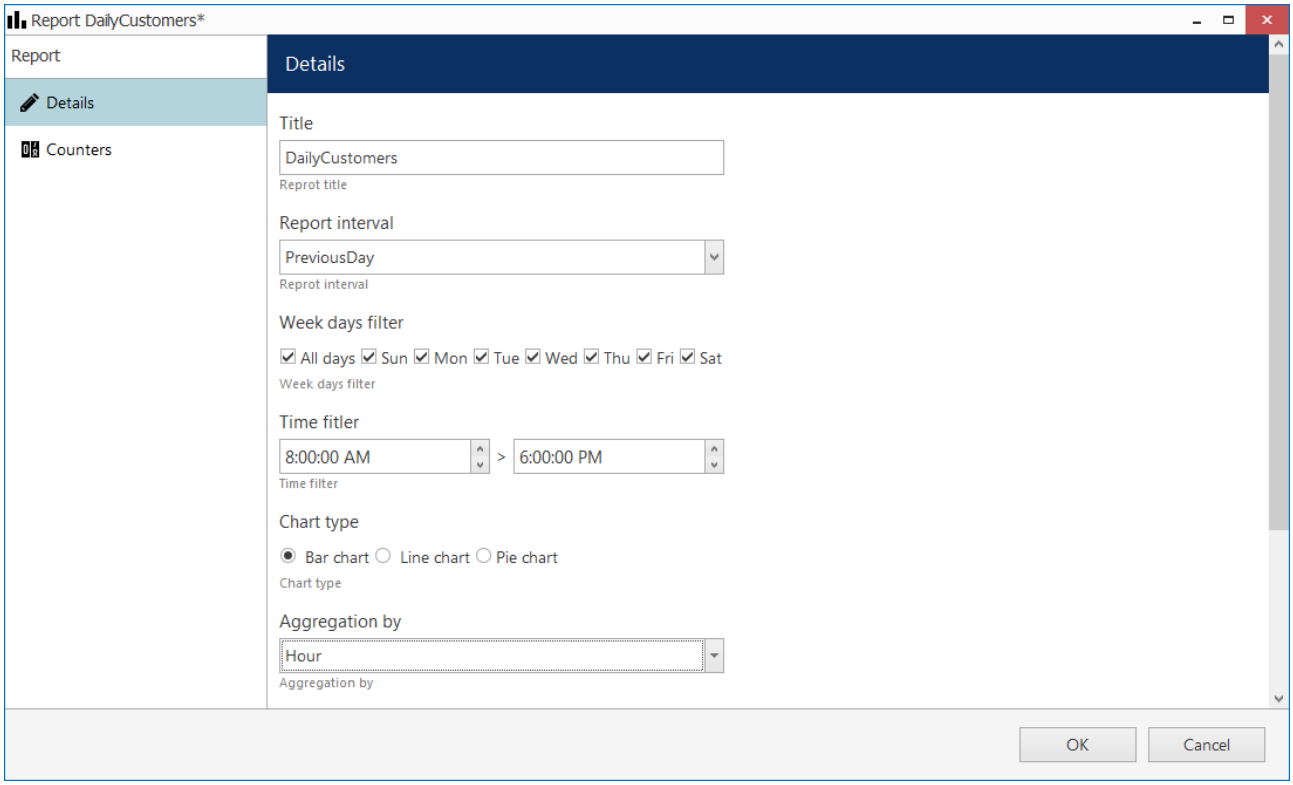
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Report Configuration

In order to start report setup, go to the *Configuration* section of Macula Console and choose *Reports* from the menu on the left. Press the + *New report* button on the top panel to bring up the report configuration dialog box. There are two options: **new counters report** and **new external service report**. These two types differ slightly.

Reports Based On Counters

This type of report is based on camera-side VCA, Open VCA, or software counters. The configuration options are similar to those in Macula Monitor when you create a graph in the *Reports* section.

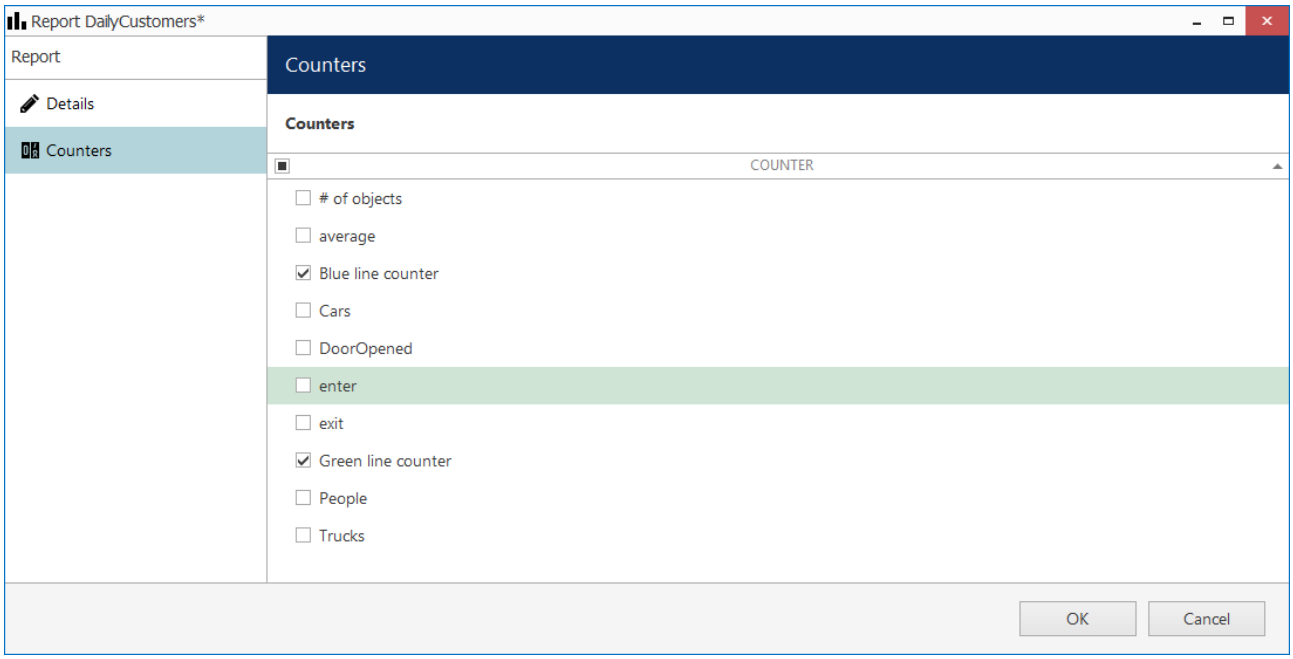


Specify the **reporting criteria** in the *Details* tab; the following settings are available:

Setting	Description	Default Value
Title	User defined title for the report	[empty]
Report interval	Time interval to be represented in the report; can be previous day, week or month	Previous day
Week days filter	Days of the week to be included in the report (e.g., ignore weekends)	All days
Time filter	Target audit interval to be analyzed for each of the selected days	12AM > 12AM (whole day)
Chart type	Diagram type: bar, line or pie	Line chart

Aggregation by	Scale factor for the target diagram - results can be presented for months, weeks, days, hours or minutes (also, the data can be aggregated by counters if the selected chart type is pie diagram)	Day
Value	Counter value to be taken for each report time interval on the X axis (day etc.): • Absolute: actual counter value • Relative: difference compared to the previous interval • Average: arithmetic mean of the given interval • Minimum: minimal value during the given interval • Maximum: maximal value during the given interval	Absolute
Sum counters	Choose whether you want each counter to be represented separately or all counters are to be added up (for bar and line type diagrams only)	Disabled
Automatic	Generate the report and send it automatically to the specified email	Disabled
Mail server	A pre-configured SMTP server to be used for email sending (the setting is revealed when automatic report sending is enabled)	[none]
To	Email recipient the report to be emailed to; enter exactly one valid email address here (the setting is revealed when automatic report sending is enabled)	[empty]

Next, switch to the *Counters* tab: here, you can select the required counters from the list.



All the counters available in the system are listed here - from Open VCA, camera-side VCA (for certain manufacturers) and software counters as well - in case their data are present in the database.

For the exact list of supported camera-side VCA counters, kindly contact our support engineers at support@gsfcorp.com.

When ready, hit the *OK* button in the bottom to save the report configuration based on your selected criteria. To edit and remove reports, use the corresponding buttons on the upper panel.

Reports Based External Service Data

This type of report is based on the data received from external services (specifically, **detections and attributes from the facial recognition** module instances). The configuration options are similar to those in Macula Monitor when you create a graph in the *FR* section. The logic is analogous to that of the counters reports, yet the settings are a bit different.

Specify the **reporting criteria** in the *Details* tab (other settings like target week days are available in the *Filters* tab). The following settings are available:

Setting	Description	Default Value
Title	User defined title for the report	[empty]
Report interval	Time interval to be represented in the report; can be previous day, week or month	Previous day
Chart type	Diagram type: bar, line or pie	Line chart
Group by	Main report values (targets): can be tags, temperature, age, sentiment, or gender estimation	Tag
Aggregation by	Results can be aggregated by months, weeks, days, hours or minutes (for bar and line type diagrams only)	Day
Sum values	Choose whether you want each target group to be represented separately or all values are to be added up (for bar and line type diagrams only)	Disabled
Show labels	Display value labels on the chart	Disabled
File type	Choose between PDF or CSV	PDF
Automatic	Generate the report and send it automatically to the specified email	Disabled
Mail server	A pre-configured SMTP server to be used for email sending (the setting is revealed when automatic report sending is enabled)	[none]
To	Email recipient the report to be emailed to; enter exactly one valid email address here (the setting is revealed when automatic report sending is enabled)	[empty]

The choice between absolute/relative/min/max/avg value is not present here; all values are **relative**, i.e., the chart reflects the value change since the previous aggregation interval.

Next, switch to the *Channels* tab: here, you can select the target channels. The report will include the recognition data from the specified channels.

On the *Filters* tab, you can limit the report sample range by (de)selecting various options. The filters include days, time of the day, and attributes from the external service detections:

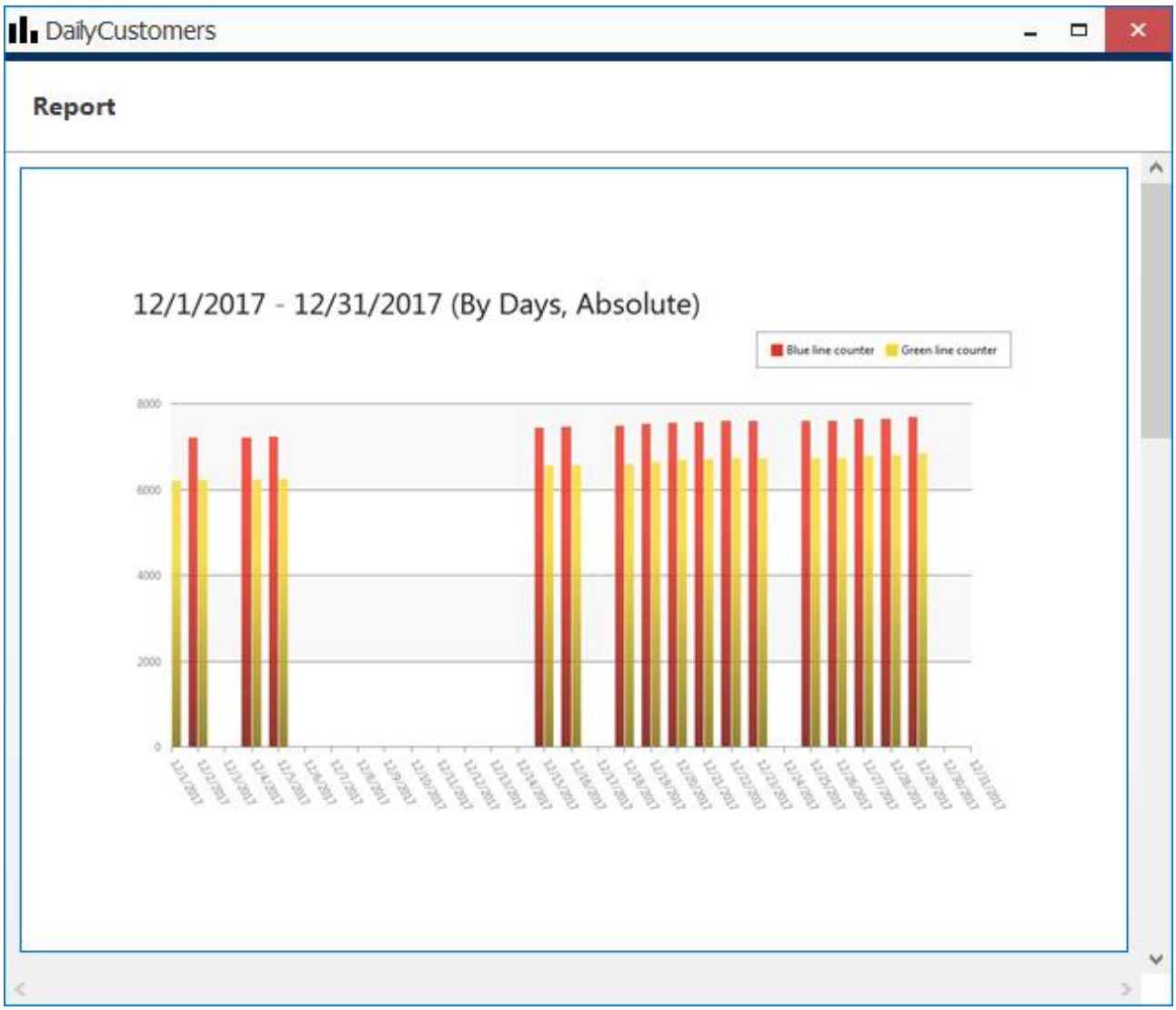
- **Tags** from FR
- Temperature ranges from the readings that were received by FR (works for certain camera integrations; please refer to us for the exact vendor list)
- **Age**, **gender**, and **sentiment** estimators
- **Week days**: select **days of the week** that you want to be included in the report (e.g., ignore weekends) (all days are selected by default)
- **Day time interval**: choose the target **audit interval** to be analyzed for each of the days in the selected report interval

When ready, hit the *OK* button in the bottom to save the report configuration based on your selected criteria. To edit and remove reports, use the corresponding buttons on the upper panel.

Report Preview

After you have created a report, you can check how it will look like by using the *Preview* and *Test* buttons on the upper panel. The **preview** button will generate a report and display it on your screen; the **test** option will create a report and email it to the specified address in PDF format immediately. In either case, the report preview will be based on its configured time interval, so, if you get an empty report, make sure that counter data are present for the previous day, week or month, whichever specified.

> When you have created a new report and wish to test it, please wait about 10-30 seconds before pressing the *Test* button: this time is required to retrieve the counter information from the database.



On each diagram, the **horizontal axis** (X) represents time in the specified scale, and the **vertical axis** (Y) reflects counter values. The counter values for each time interval are calculated based on the selected setting and can reflect absolute, relative, average, minimum or maximum counter value for the given interval. In the **pie diagram** type, each sector can represent either a time interval or a counter, depending on the aggregation setting parameter.

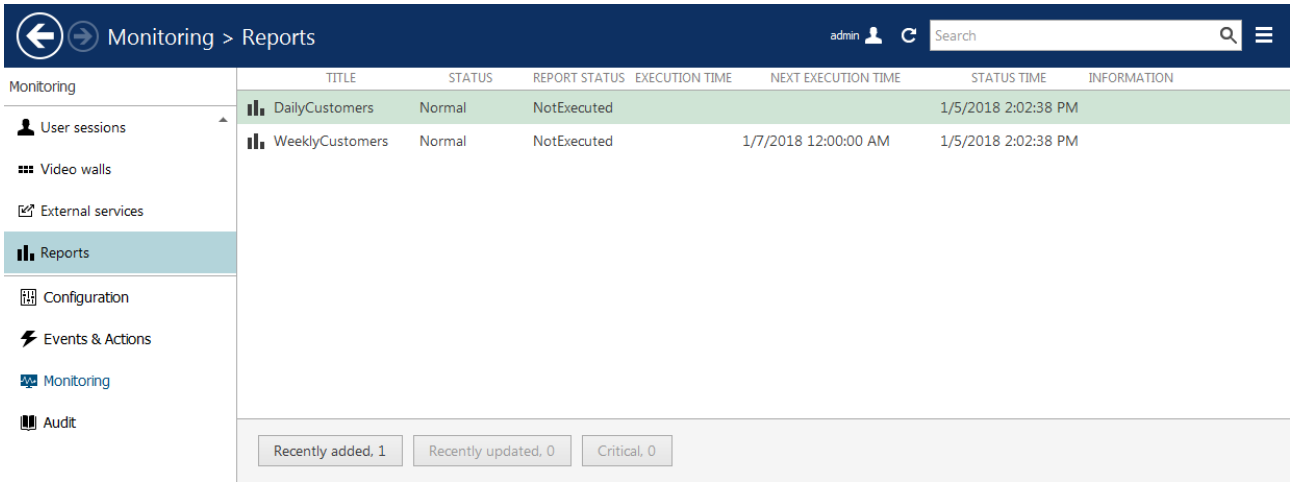
Each chart also contains a **legend** that provides information about colors used in the diagram:

- if you have selected to analyses every counter separately, each counter will be represented with its own color and the legend will reflect counter titles
- if you have chosen to sum the counter values:
  - bar diagram will have just one column for each interval, every column consisting of specified counters and its total height reflecting the total
  - line diagram will contain graphs for each individual counter and the total
- pie chart will reflect the counter sum for each time interval if aggregation by time intervals is chosen, so the legend will contain timestamps; if aggregation by counters is selected, the pie will reflect the proportion of the counter values for the whole selected audit interval

Apart from the diagram itself, each report in PDF format will also contain a table with the reference counter values.

Report Status Monitoring

Report execution status can be tracked from the *Monitoring* section of Macula Console, by choosing *Reports* in the menu on the left.



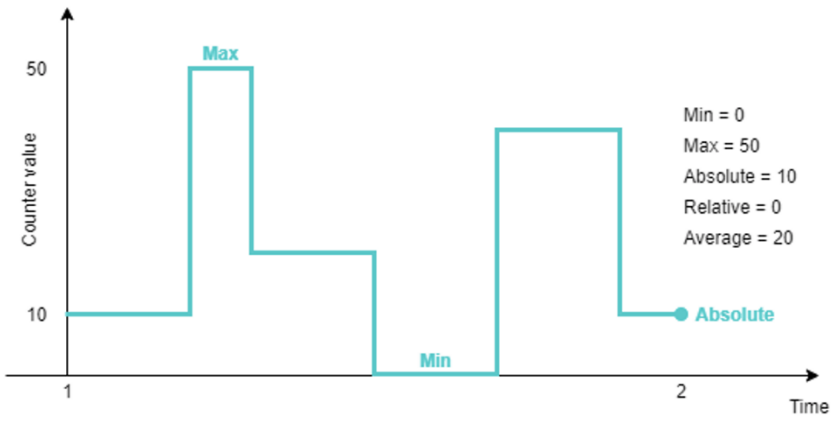
If a report has been sent at least once (by schedule, not as a test), the last execution time is shown here. For the reports that are currently set to be emailed automatically, the next (scheduled) execution time is also displayed.

Math Behind Counters

Different **counter value** settings will produce different results, so you need to understand which value to select in order to get the appropriate result. Below, you will find some details on how **these values are calculated** inside.

For each and every selected interval, five counter values are calculated: **absolute, relative, min/max, and average**. The minimal internal interval is equal to **1 (one) minute**; no matter how the counter value changes during that minute, these five values are recorded into the database. For longer periods (hours, days, etc), these values are calculated using the intermediate results.

In the snapshot below, there is an example of how the counter value might change during one minute, and what values are calculated based on these changes.



Average = (c1*t1 + ... + cN*tN)/(t1+..+tN)
Average = (10*2 + 50*1 + 20*2 + 0*2 + 40*2 + 10*1)/10 = 20

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

An example of counter changes within report interval with corresponding peak values

For correct report results, it is also essential to keep in mind whether the counter in question is increment-only, or if it is both incremented and decremented based on some events.

Counter value options:

1. Absolute

Absolute counter value is its exact value at the **end** of the measurement period. E.g., If the interval is 1h, the absolute counter value is equal to the absolute counter value for the last minute of that hour.

Usage examples:

- increment-only: estimate the total people flow, e.g., incoming customers
- increment/decrement: current number of people in the zone/building

2. Minimum and maximum

Here, simply takes the min and max value from the aggregation interval. For longer intervals, min/max are selected from the list of min/max of smaller periods (regular min/max function).

Note that min/max has nothing to do with absolute value: the counter value may peak inside the aggregation period with the total change (absolute value) being zero. The latter, of course, is only possible for the counters that are both incremented and decremented over time. For increment-only counters, max value will be equal to absolute value.

3/4. Relative

Relative counter value is the sum of all relative changes for the given period, or, even simpler, the difference between the current absolute value and the previous one. Relative value shows how much the counter value has changed for the given period compared to the previous one.

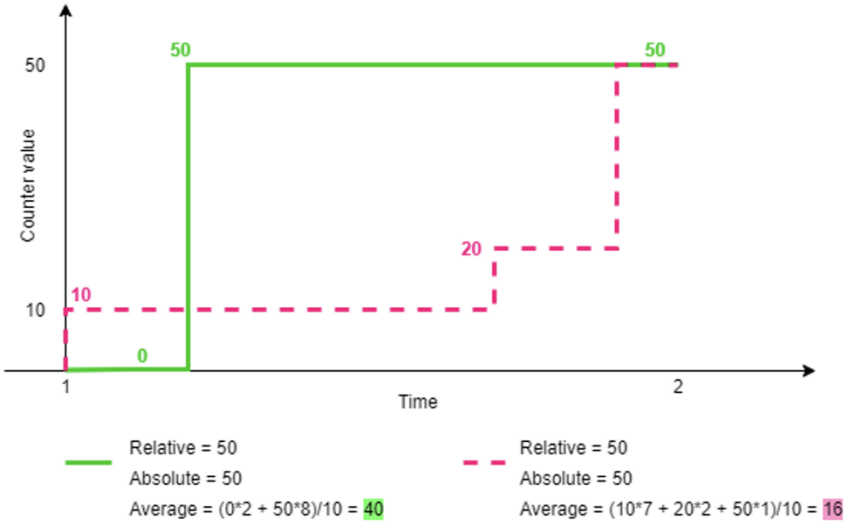
5. Average

Average counter value is counted as weighted arithmetic mean, with the duration serving as weight.

Simple arithmetic mean would not be as useful as it does not take into account the value duration.

Consider the two examples in the snapshot below: two counters have the same absolute and relative values for the given period. Their arithmetic mean would be very similar (25 vs 26.6), while it is obvious that the first (green) counter value stayed higher for a longer period, and this should be taken into account.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Example of two counters with the same absolute values and different average

Usage example: average number of customers in the store per hour, average check total for estimating effectiveness.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.12 Manage Mail Servers

Several Macula components require an SMTP server in order to be able to send emails to a specified address. Specifically, these are:

- email sending actions in E&A and automatic reports
- two-factor authentication on top of the regular login

A **pre-configured mail server is required** for these features to be operational.

You can add one or multiple different outgoing SMTP servers to send notification emails through them. You can use/set up your own SMTP server, if your Organization already has one and/or it is affordable for your Organization; alternatively, free Internet services can be used for this purpose. Note that there are not any default (pre-configured) mail servers.

After adding a mail server configuration, you can verify it by using the *Test* button in the upper panel.

> SMTP servers provided by popular free services and/or ISPs usually have limitations on the number/frequency of emails going through them daily. Make sure you check with SMTP service provider to learn about this.

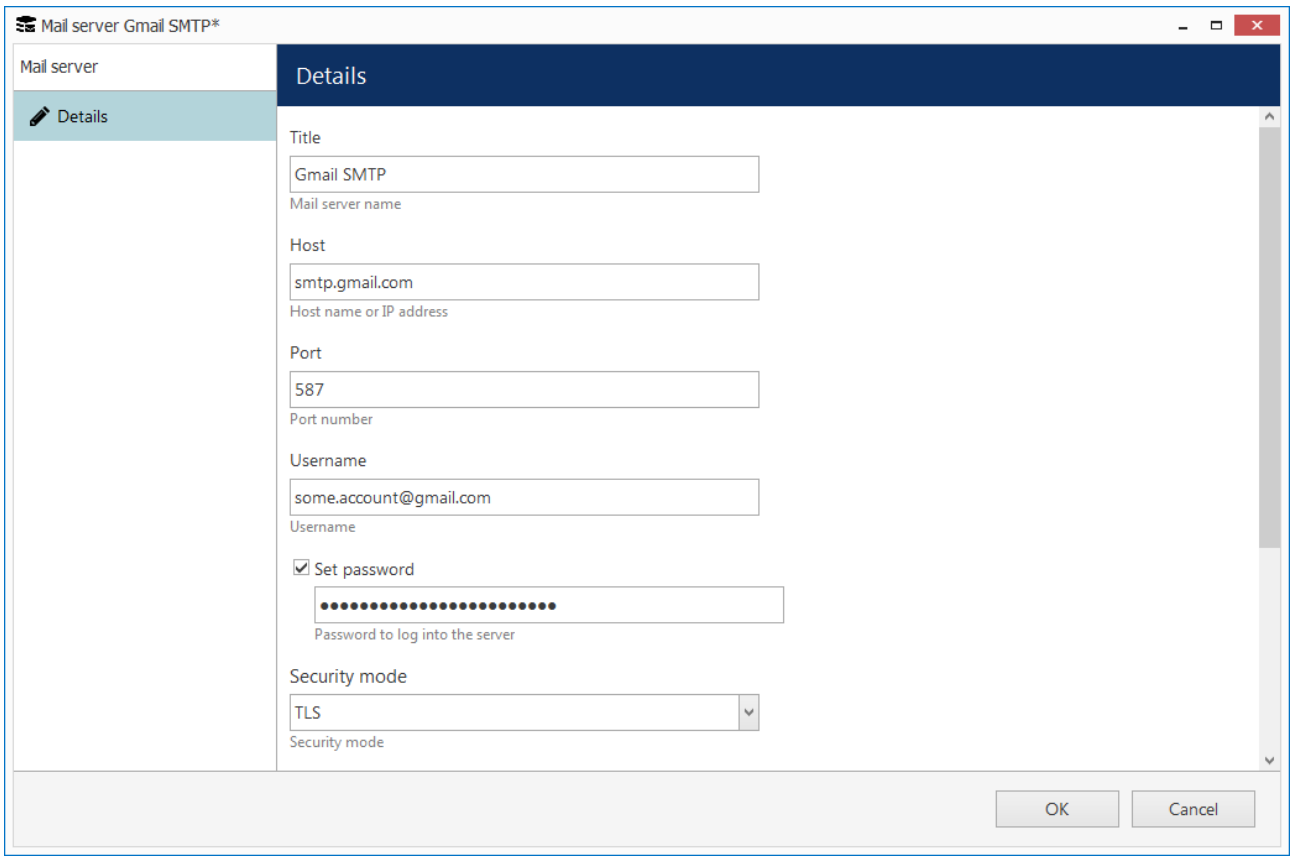
Mail Server Setup

To access mail server setup via Macula Console, open the *Events & Actions* section and select *Mail servers* from the menu on the left. Click the + *New mail* server button on the upper panel or double-click an existing mail server from the item list to open the configuration dialog box.

> Prior to Macula version 1.7.0, mail server configuration was accessible via *Events & Actions* section of Macula Console.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



Setup here is similar to configuring an email client. The table below contains detailed information on the available settings.

Setting	Description	Default Setting
Title	User-defined mail server name	[empty]
Host	Outgoing SMTP server IP address or hostname	[empty]
Port	Outgoing SMTP server port; default is 25, common ports for encrypted connection are 465 and 587	0
Username	Enter valid user account details to log onto the target SMTP server	[empty]
Password	Enter valid user account details to log onto the target SMTP server	[empty]
Security Mode	Logon authentication type according to the SMTP server configuration requirements	none
Sender	Email address on whose behalf emails will be sent	[empty]
Aggregation*Count	Max number of notifications to be aggregated into a single email	10
Aggregation*Time	Max time period in seconds during which notifications are collected together to be sent in a single email	10

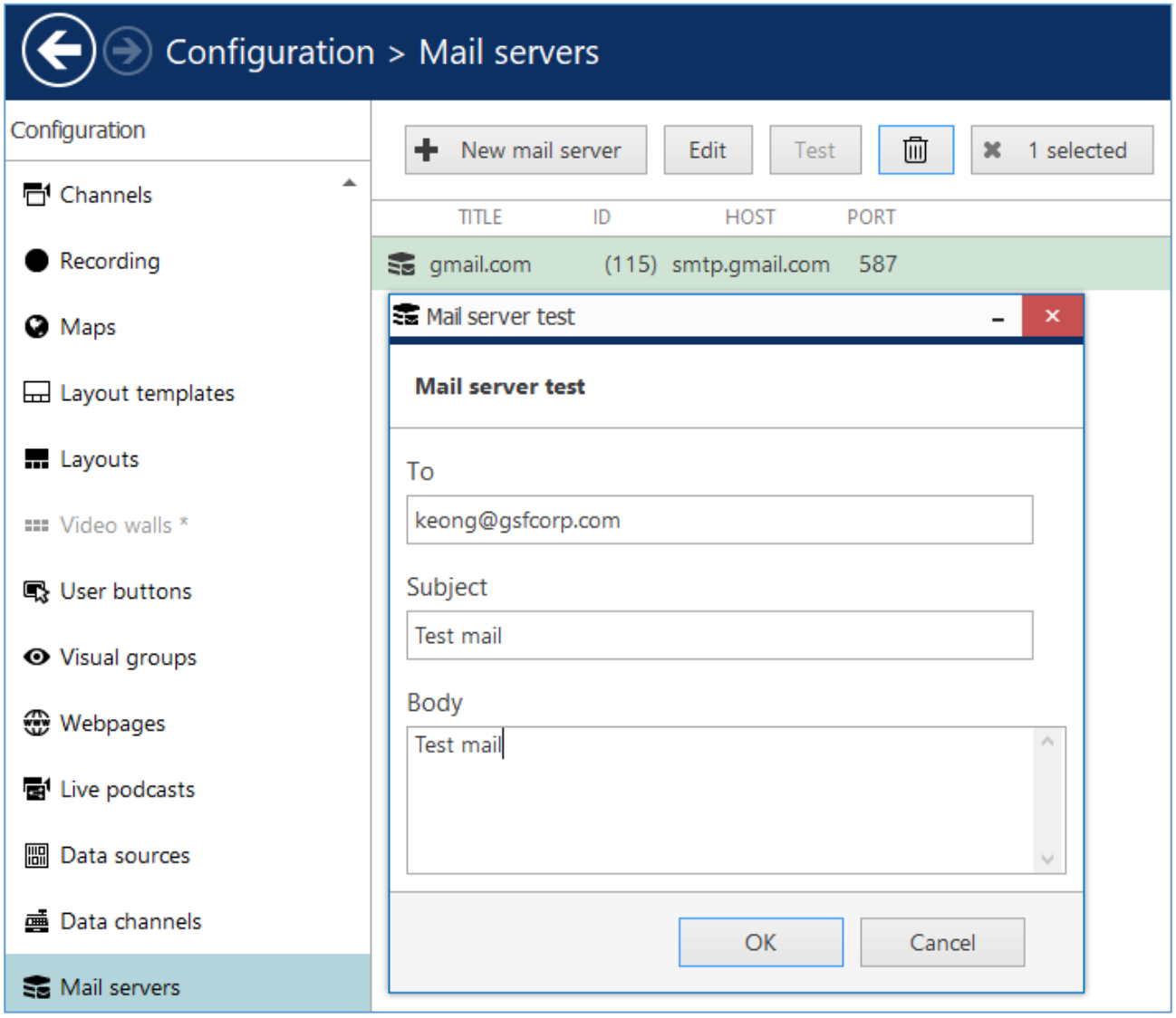
*Email aggregation can be used to accumulate alert notifications and send them in bunches rather than one at a time. This decreases SMTP server load and does not 'spam' your notification inbox, making it easier to search and analyse alerts, and is thus especially useful if the number or frequency of events is high.

> Maximum [time/number of occurrences] in this context means that it will not be exceeded under any circumstances. The actual time or number of occurrences may be either max or less - depending on which aggregation parameter is triggered first.
>
> Example: aggregation time is set to 60 seconds and aggregation count - to 15. If the notifications arrive frequently, and 15 items are collected in under one minute, the email will be sent immediately. If there are just 1 or 2 notifications but 60 seconds have passed, an email will be sent, too.

Click *OK* to save mail server settings; newly created configuration will appear in the item list. Your mail server is now ready to be used for sending notifications.

Verify Mail Server Configuration

Use the *Test* button in the upper panel to verify your mail server configuration.



To perform the test:

1. Choose one of the Macula servers to send the email from
2. Enter the test recipient's email address

3. Enter the email subject and body
4. Click OK

You will see a popup window with the test result and error text, if any.

> ⚠ Some mail servers require additional settings to be changed on the server side to allow third-party applications to send emails through their SMTP service. For example, Google security requires that you log into your account via a browser using the server that will be utilising the SMTP service in order to enable account access from that computer.
>
> If you can successfully use SMTP settings to send emails from the same computer, Macula will also have no trouble sending your notifications.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

10.13 Manage GSM Modems

Apart from email servers, Macula supports GSM modems. These modems with your pre-installed SIM cards can send and receive SMS (short messages), which can be used for the following scenarios:

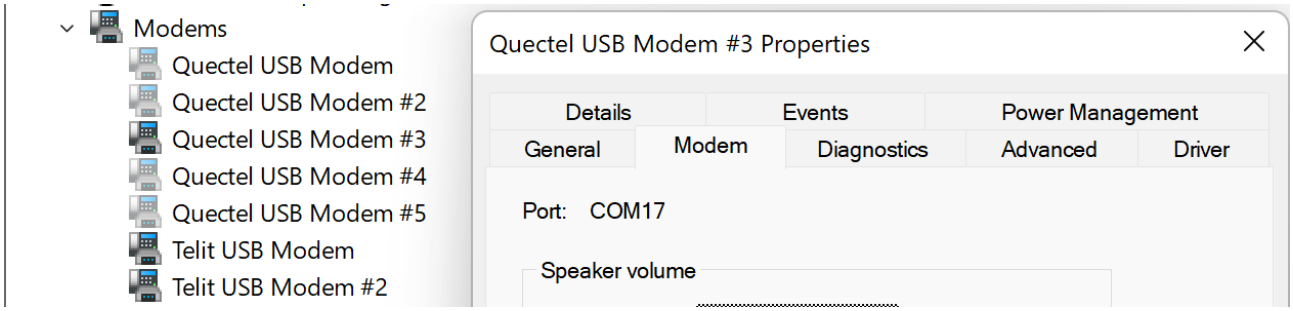
- send custom SMS notifications from Macula servers
- use SMS verification for 2FA
- receive SMS to trigger internal Macula events

If the modem doesn't work in, please try with a third-party app/utility. If the external utility does not work, Macula servers will also be unable to work with that modem. Microsoft offers a free tool called Microsoft Messaging, which you can get in Microsoft Store.

> ⚠ Modem hardware may apply delays (60+ seconds) for SMS receiving. Please make sure that resulting SMS read frequency from the mobile operator is acceptable for your scenario.

Connect and Set Up Modems

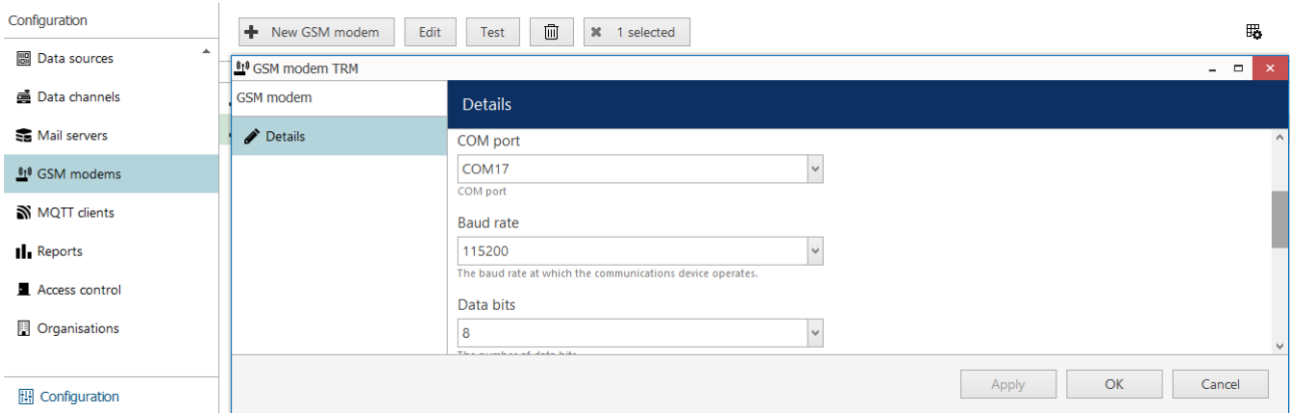
First, plug in your GSM modem as instructed in its manual - usually, modern devices use a USB connector and a virtual COM port. The modem should appear in the Windows Device Manager - if the drivers are installed automatically, you will see it appear under *Ports* > *Modems*, occupying one or several serial ports. Check the **modem properties** to view the occupied port. Some of the ports may be hidden; you can view the hidden entries by clicking the Device Manager main menu > *View* > *Show hidden devices*. Normally, you will not have to do this, as active (non-hidden) modems will be used in Macula.



> ⚠ If you are unplugging the modem, make sure to connect it to the same USB port next time; otherwise, the modem may use a different COM port, and will stop working because the Macula Console settings cannot be updated automatically. If you do insert the modem into a different physical port, make sure to check the new port and re-select it in the modem properties in Macula Console.

Then, in Macula Console, in the *Configuration* section, choose *GSM Modems* on the left. In the upper panel, click the + *New GSM modem* button to open the dialog box, and enter the modem settings. All COM parameters must match those on the modem side.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Available settings:

- **Title**: user-defined modem name that will appear across Macula Console
- **Server**: Macula server that has the modem hardware attached to it
- **COM port**: choose the port used by the target modem
- **Baud rate**: must match the modem setting
- **Data bits**: must match the modem setting
- **Stop bits**: must match the modem setting
- **Parity**: must match the modem setting
- **SMS mode**: choose TEXT mode unless you need (and know how) to use special characters that are only supported in PDU mode (GSM7 encoding only)
- **SMS encoding**: GSM7 (special ASCII for GSM) or USC2 (special version of Unicode for GSM)

For correct COM port, check the modem port under *Modems* in the Device Manager as displayed above; depending on the modem driver, there may be multiple ports, including hidden ones. Some of these are usable by Macula, and some may be auxiliary: after creating the modem, use the *Test* button in the upper panel to test the connection and check if you have picked the right one.

> If you use GSM-7 (ASCII) and your message shows full of ? of other odd characters, try switching to USC2.

After filling in the settings, click *OK* to save: the newly created modem connection will appear in the list. Click the *Test* button to verify the connection: if the status retrieval fails, try selecting a different COM port. If none of the ports work, ensure that the serial port settings (baud rate etc.) match the settings on the modem side exactly.

The *Test* dialog box has two functions:

- modem status: verified automatically
- test SMS: enter phone number and text to send the message

> Macula pings the modem every 30 seconds for the status update, and every 3 seconds for new messages. If you experience delays in message reception, these are most probably introduced by the modem hardware, and are not related to Macula server setup. Use the modem with 3rd party tools and compare the delay to verify.

To test against a specific phone number, enter the phone number - either in the international format (including the country code using either + or 00 prefix), or without the country code if the number is local for the SIM operator. Click OK to attempt sending the short message. If the number is incorrect, you will

get a failure notification. If everything is fine, you will get a success message, and the message will arrive shortly (usually, instantly) to the target phone.

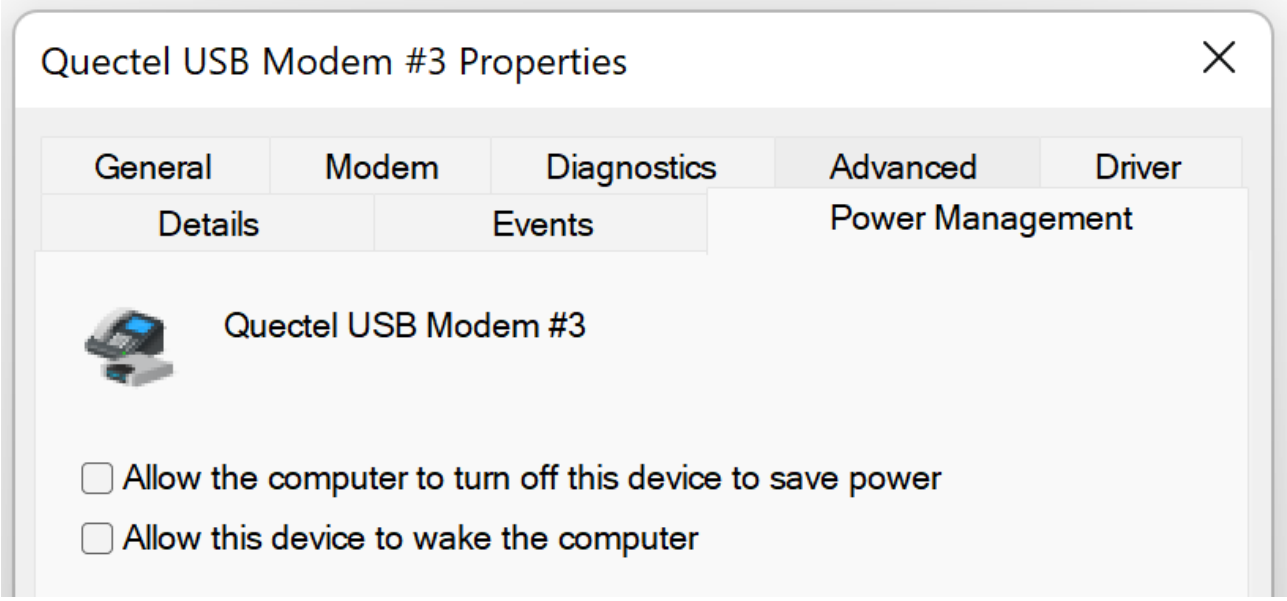
> Wherever you need to enter a phone number in Macula Console, we recommend that you do it in the international format: first + (or 00), then the country code, and then the number itself. The number must not include any spaces, dashes, or parentheses.
> Example:
> - number in the local format: (012) 8090-8080
> - the same number converted into the international format: +601280908080

The billing for the messages will be as per your SIM card plan.

> GSF is not responsible for any losses due to additional mobile operator fees. It is solely your responsibility to keep track of and control the message flow and the event frequency in case the SMS is sent based on an E&A event.

If you respond to that test SMS, the modem will receive it and you will see it appear in the modem status summary under *Last messages*. The exact time of the message reception may vary depending on the modem hardware and settings; Macula does not introduce any additional delays.

Important! Make sure your modem does not go to sleep. To do this, go to the Windows Device Manager, find your modem under Modems, and check the *Power Management* tab for related settings. Do not allow the PC to turn OFF the modem to save power.



Configured modems will appear in the corresponding tab of the *Monitoring* section.

Receive SMS

Once you add a modem, you will be able to receive SMS and use it for event triggering on Macula servers.

Modem Events

To create an SMS event, switch to the *Events & Actions* section of Macula Console, and choose *Events* on the left (you can also create new events right from the E&A Configurator). In the top panel, click the + *New event* button, then select the *SMS message received* event type in the dialog box, and then fill in the rest of the settings:

- **Title**: user-defined event name
- **Source**: existing modem hardware to accept the message
- **Phone**: sender's full phone number*****; leave empty for any number
- **Text**: SMS text to trigger the event, case-sensitive; leave empty for any text to trigger the event
- **Regular expression**: enable if you wish to evaluate the incoming text with **regex**, e.g., use placeholders

*****The phone number must be in the **international format** (with leading + or 00 and a country code) for ALL numbers, even local ones. The event will not work properly without the country code.

Click *OK* to save and close the dialog box. The newly created event will appear in the list.

Once you have created the event, you can use it to build event rules in the Event & Action Configurator, as usual. For example, you can send SMS to trigger start/stop recording, to open doors and gates, or to create alarms and bookmarks.

> ⚠ Please note that modems may introduce **delays** when receiving SMS due to periodic SMS reading approach (messages are received from the mobile operator at certain intervals). Please test your modem hardware and ensure that the resulting SMS reception frequency is acceptable for your event scenario. The Macula software does not add any delays and is not responsible for the delays on the hardware side.

Send SMS

Similarly, modems can send SMS to the pre-configured phone numbers. Macula servers can utilize this in two scenarios:

- send messages based on the triggered events - E&A **actions**
- send codes via SMS for two-factor authentication (**2FA**)

Note that you cannot create actions or 2FA notification providers without actually having a working modem, so make sure to add and test the modem first.

Modem Actions

To create an SMS sending action, switch to the *Events & Actions* section of Macula Console, and choose *Actions* on the left (you can also create new actions right from the E&A Configurator). In the top panel, click the + *New action* button, then select the *Send SMS* action type from the *Notifications* group in the dialog box, and then fill in the rest of the settings:

- **Title**: user-defined action name
- **Source**: existing modem hardware to send the message
- **Phone**: the recipient's phone number*****
- **Text**: SMS text to be sent, right-click to insert text macros

*If the phone number does not have a country code defined, the local country code of the SIM card operator will be appended to the number. If you want to guarantee the number correctness and the message delivery, please enter the number in the international format with a country code and a leading +/00.

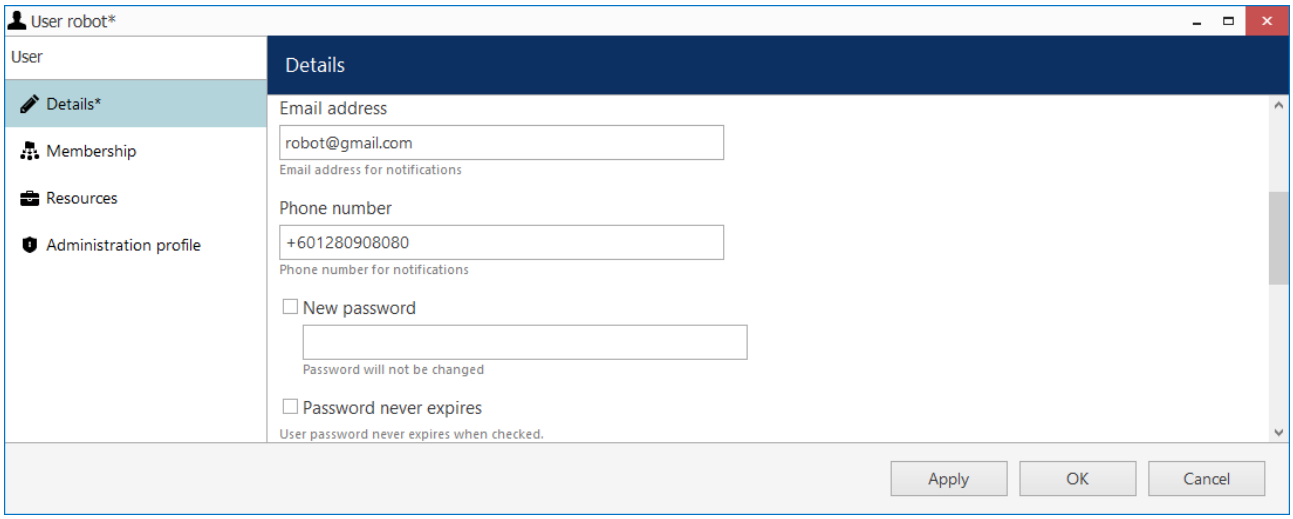
Depending on your modem settings and chosen language, each message may be split into several ones. Before setting up the notifications on production servers, verify the setup and make sure you are getting the desired results.

Two-Factor Authentication (2FA)

Before enabling 2FA:

- add a valid modem and test it
- ensure all users who will use 2FA have a valid and full phone number specified in their account properties in Macula Console

The phone number setting is new (comes with the modem support) so you will need to go each user's properties and enter their phone number to make sure they can receive SMS for the verification.



To set up 2FA, go to your Macula server settings (for Macula Global systems - go to the central management server properties, as this a is system-wide setting) > *Two-Factor Authentication* tab > add a new notification provider and specify the rest of the settings as described in the corresponding chapter about 2FA.

10.14 Quick Access

Quick Access feature simplifies Macula Monitor control via CCTV keyboard or standard keyboard by adding a custom ID to dedicated resources. By creating *Quick Access* IDs, it is possible to assign numerical or any other custom values to frequently used resources or items.

Currently, it is possible to set *Quick access* ID for resources such as:

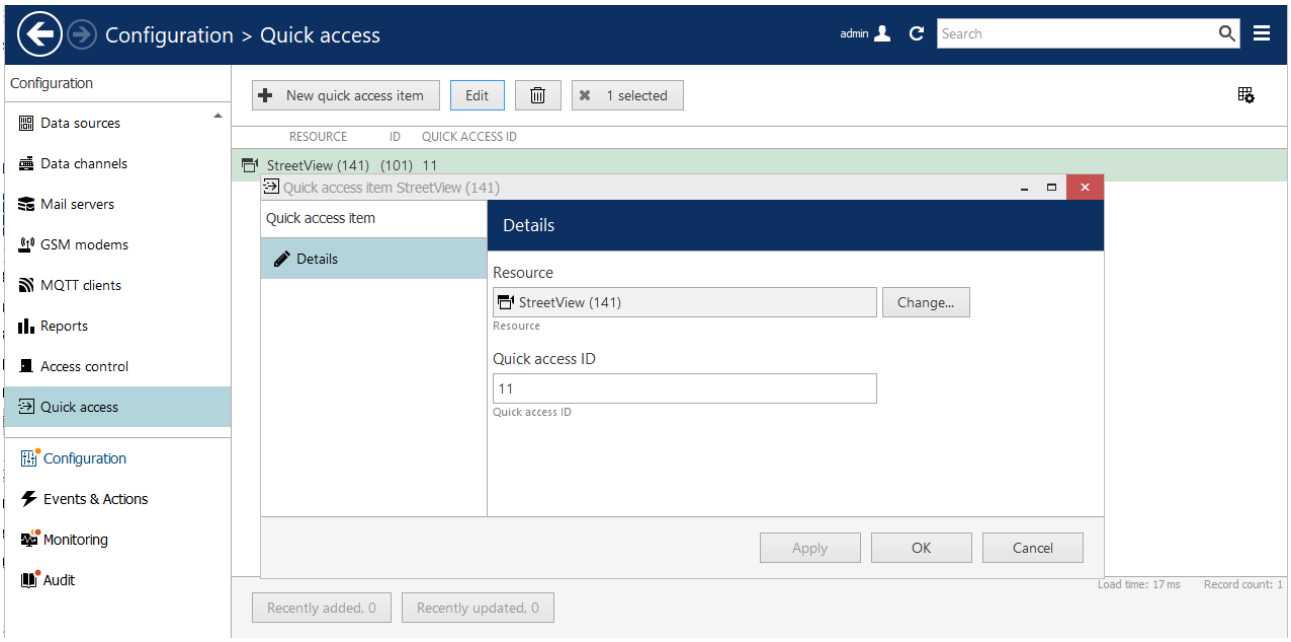
- Video channels
- Data Channels
- Maps
- Buttons
- Web pages
- Shared layouts

Adding Resources:

To add any resource to *Quick Access*, go to:

- *Configuration → Quick access → New quick access item*
- Select the existing resource
- Provide an ID of your own choice
- Press the *OK* button

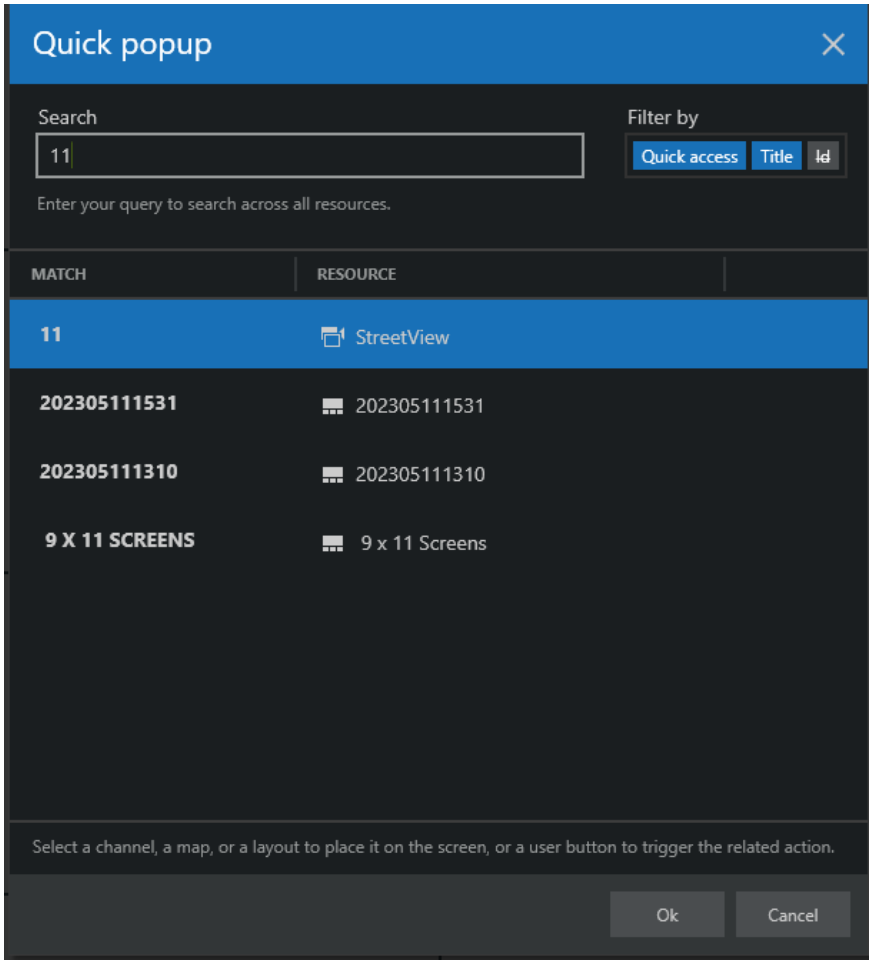
After that, you can reach assigned resources in the Macula Monitor in the *Quick popup* window.



Using Quick Access items in Macula Monitor:

After creating a *Quick Access ID* for the resource or item, you can call for it in the Macula Monitor. To popup resource, change layout, or trigger button – launch the *Quick popup* window ([ctrl+f] using a standard

keyboard or dedicated search button on your CCTV keyboard), write a particular ID in the search field, and confirm your input.



11 External Services

External modules are modules that have been integrated with Macula, including these, which have been designed to work with Macula - license plate and face recognition engines. They operate either independently or based on streams received from Macula server, and Macula server can receive event metadata from these modules and then use these events for Event & Action configuration, as well as provide the opportunity to view these events in both live and investigation mode in the Macula Monitor application.

All the external modules can be connected using the same logic, the main important steps being as follows:

1. Prepare channels to be used for the target external module
2. Install the target external module
3. Connect to the Macula server from the external module and enable HTTP notifications in it, if such an option is explicitly available - this will make the external service automatically appear in Macula Console
4. Create a group for external services in Macula Console and add your external service to the group
5. External service will now be available for E&A configuration and its events will be visible in Macula Monitor

> Important notice for Macula Enterprise systems: prior to Macula version 1.15.0, external services only operate via central management server.
>
> Starting with 1.15.0, you can link external services directly to recording servers (Macula Recording Server instances). Note, however, that this functionality will not be covered for failover servers in case the target Macula Recording Server goes offline. When your external service is linked to Macula Enterprise, streaming will automatically switch from/to failover.
>
> This works for all kinds of external services, except for Camio, which is integrated in a slightly different way

This administrator's manual will cover an example on how to connect an LPR (License Plate Recognition) module. All the other modules are added in a similar way, the only difference being the external module interface.

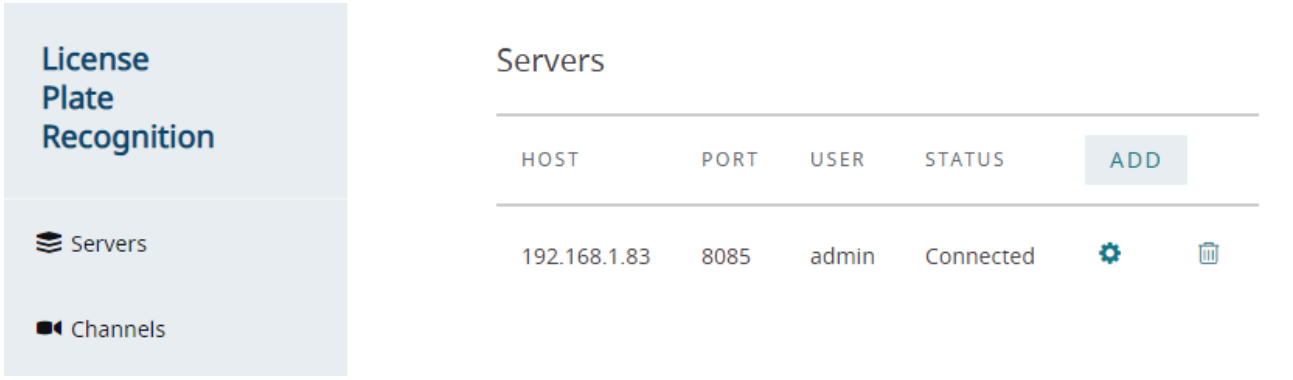
Install External Module

Start LPR installation by double-clicking the installation package, and go through the wizard's steps. Activate LPR using your purchased LPR license and run the software with empty configuration

Set Up External Module

In the LPR module, add a new server connection and enter your Macula server connection details. Make sure that the target HTTP port is reachable and that the user account has the *Login via HTTP* permission granted.

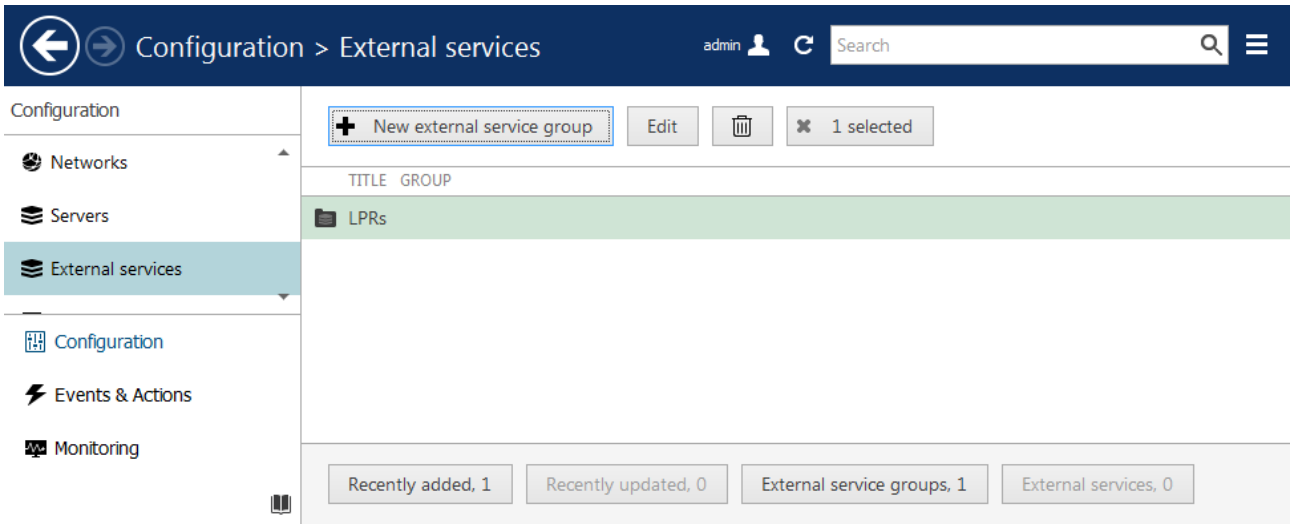
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Then, add your desired channels for LPR analysis and set up license plate recognition as usual. For details on the setup, please refer to the LPR user manual.

Add External Service

In Macula Console, go to the *Configuration* section and choose *External Services* from the left-hand-side menu. On the upper panel, press the + *New external service group* button; in the dialog box, enter a group name and click *OK* to save. The newly created group will appear in the item list.



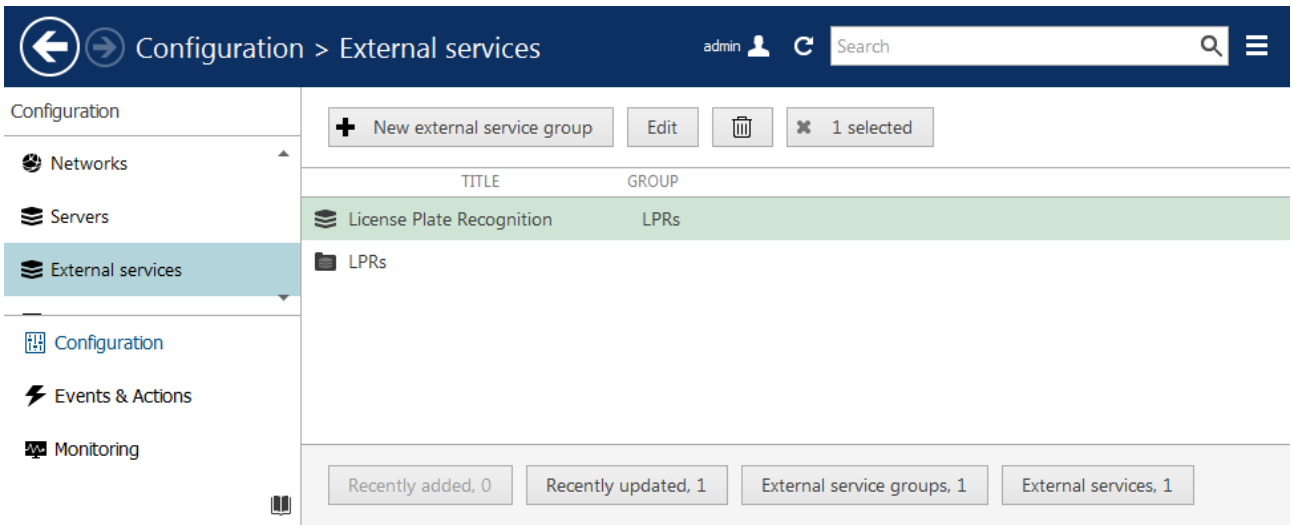
After you have set up LPR to send VMS notifications, as described above, the target service should automatically appear in the *External Services* list. Double-click it to bring up the service settings:

- **Title**: you can either keep the default (auto generated) name, or change it
- **Server**: target server for the external service to connect to (must match server address in the external service configuration)
- **Group**: add it to the group you have just created

Click *OK* to save and close the dialog box.

In the additional tabs - *Events and actions*, *Related resources* - you will see some relevant data, all in one place. *Events and actions* will display actions linked to the target service events, while *Related resources* will reflect the list of channels used by target service (in this case, LPR).

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



From now on, your configured external service will become available in the Event & Action Configurator, and its event streams will also become available for investigation in the Macula Monitor application. Please refer to the Macula Monitor user guide for details on the investigation mode.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

11.1 Access Control

Macula is integrated with a number of access control systems. Macula server can receive events from and send requests/commands to third party access control software.

The current integration includes the following access control software: Keri, Feenics, Gallagher, Roger RACS 5, AEOS by Nedap Securit, Inner Range Integriti, and Visual Access System by GSF Corporation.

Macula obtains the **list of doors**, their **statuses** (opened/closed, locked/unlocked), **cardholder list** and other available/relevant and enables you to lock and unlock the doors based on internal Macula server events (e.g., user button pressed) and also from the Macula Monitor application. Information about doors, their events and cardholders are searchable from Macula Monitor application as well.

Supported functionality overview:

- Receive events, door list and their status, list of cardholders (users)
- Change door status by sending corresponding commands back
- Live door status with linked video channels
- Interactive markers on the maps and geographical maps
- Notifications and other actions based on door events
- Search event history based on doors, cardholders, and time
- Get mobile app notifications
- Lock and unlock doors from the mobile application

Integrations with different access control software are similar. However, there may nuances in configuration. If you encounter any difficulties with the setup, feel free to contact our support engineers at support@gsfcorp.com.

Macula Configuration with 3rd Party Access Control

This topic briefly describes the configuration necessary to make use of the access control software integrations with Macula software.

Prerequisites

Keri uses port 11000 as default and ports 11000 through 110xx for connections so these should be opened and forwarded on the intermediate routers and firewalls.

Macula connection to the Doors.NET system uses a certain license type – **OnSSI**. Make sure that your Keri license includes this type of client license (at least one) and that it is not used by other client connections.

> In earlier Macula versions, a different Doors .NET license connection - RollCallClient - was used. It still works but Kery Systems strongly recommend using the OnSSI license instead.

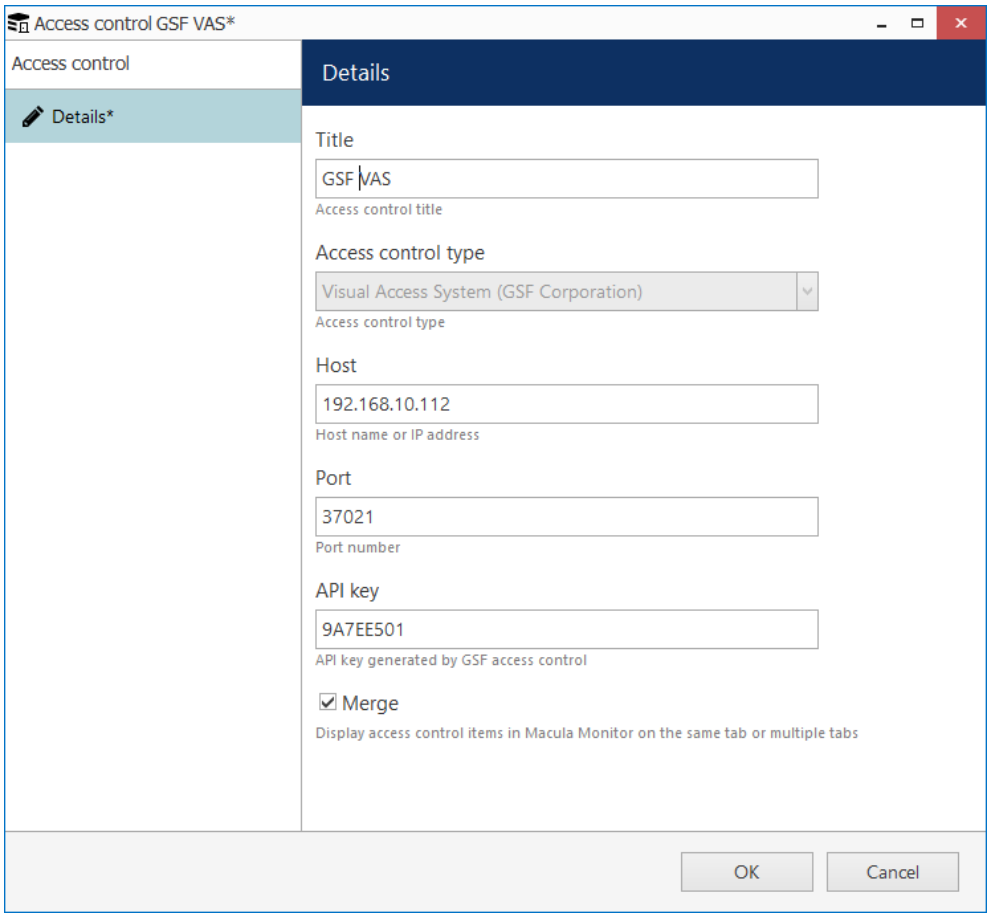
For Keep by Feenics, there are no special requirements. You just set it up as usual, and Macula servers already have a connection to api.feenicshosting.com via HTTP hard-coded. Make sure to allow this connection on your local firewalls.

For Roger RACS 5, there are also no special configuration requirements, set up your VISO as usual. Just make sure you have applied a valid **license** to the access control software. Without it, the integration services on the Roger side will be inactive. You can check the license status by running the RACS Services Manager and then selecting *License service*.

Add Access Control Configuration

In Macula Console, open the *Configuration* section and choose *Access Control* in the menu on the left. Here, you need to create a connection to the Keri server: click the *New access control configuration* button on the upper panel and fill in the settings, then click *OK* to save:

- User-defined **title**
- **Type**: select your access control software name
- **Host**: access control server IP address (required for some types)
- **Instance**: instance name for Feenics (defined on the Keep side)
- **Port**: access control server port
    - Keri: the default port is 11000, ports 11000 through 110xx can be used otherwise, depending on the Keri configuration
    - Roger: leave 0 to use the default port of 8892
- **Username** and **password** to connect to the access control server
- **Merge**: enable this option if you have multiple access control systems and you want to have them all in a single tab in the Macula Monitor application

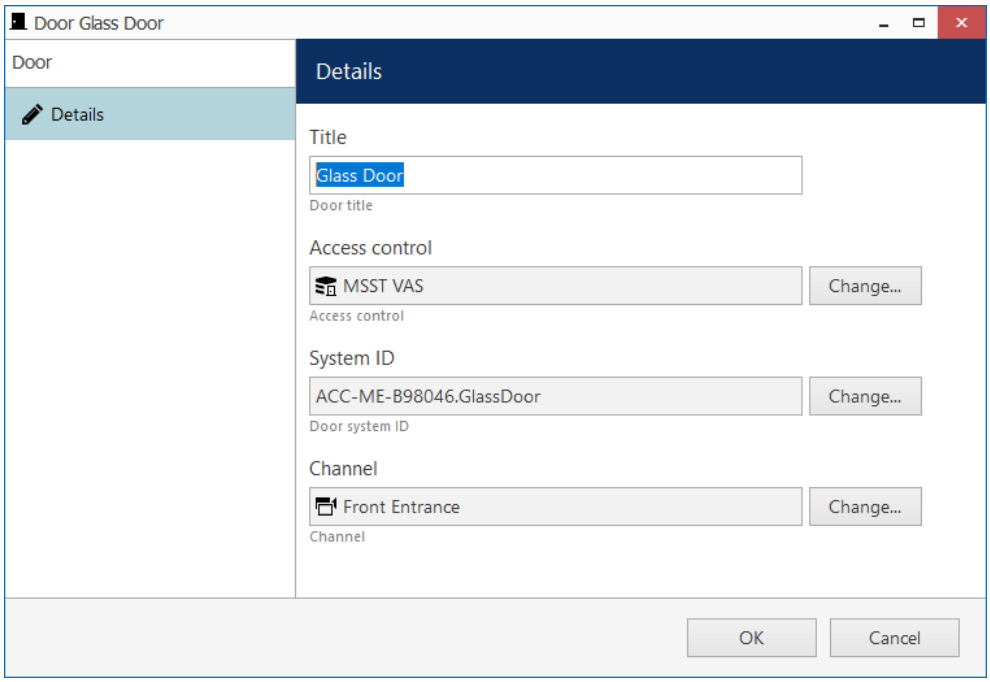


For Roger RACS 5, you check and change the service IP address and port by running the RACS Services Manager and then selecting *Integration service*.

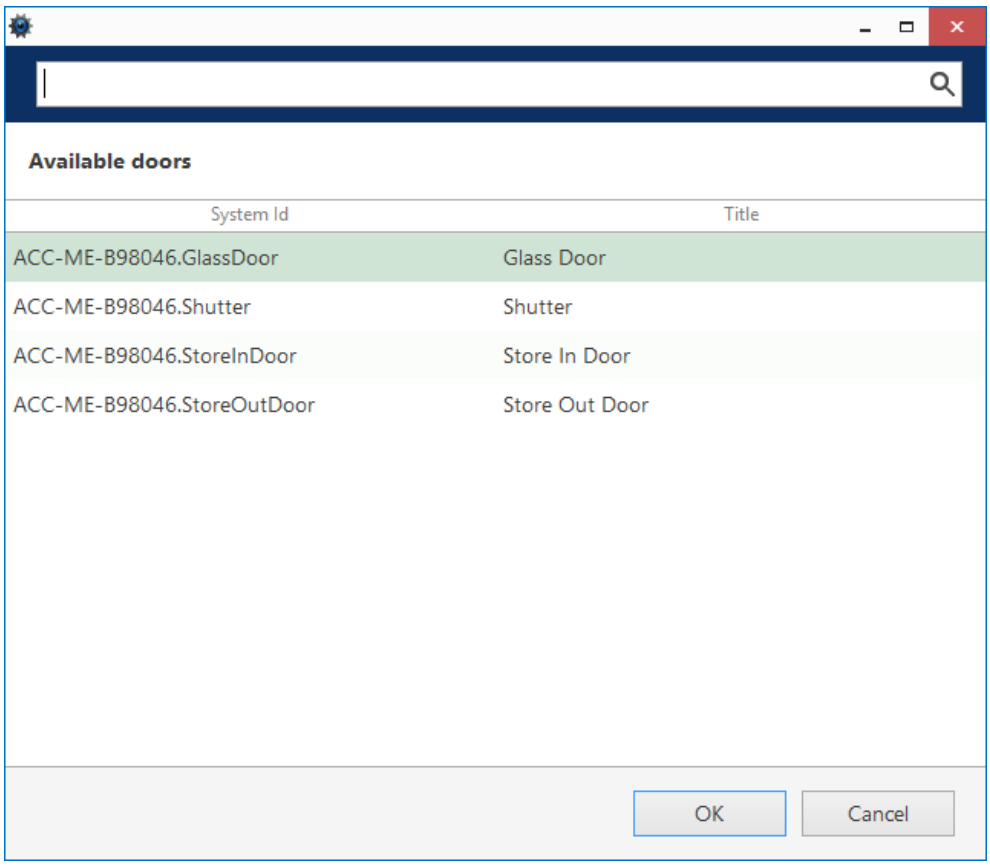
For Gallagher access control, there is a special pairing procedure with additional settings, please see the corresponding topic of this document for more details.

Add Doors

Next, click the arrow next to the *New access control configuration* button and select *New door* in the drop-down list. Choose the access control configuration created on the previous step.



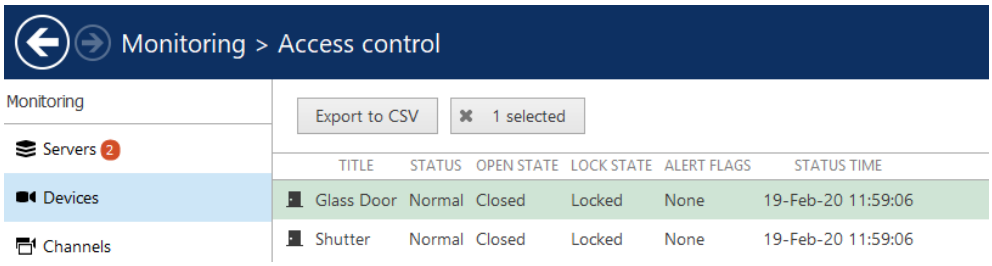
Click the *Change* button next to the *System ID* field to view the list of available doors: if the access control configuration is correct, Macula server will successfully fetch it from the Keri server. Choose the required door and click *OK*.



If you wish to bind a video channel to a door, choose a channel in the corresponding field. This channel will appear when viewing events from that door in the Macula Monitor application, and the event list will be bound to the recorded footage.

Monitoring

For all the doors that have been added it is possible to view their current states in the Macula Console application: to do so, switch to the *Monitoring* section and select Access Control in the list on the left.



The following information is available from Doors.NET:

- **Open state**: opened/closed
- **Lock state**: locked/unlocked
- **Alert flags**: additional information, if any
- **Status time**: last status update time

Use the *Search* field in the top right corner to filter the door list, and the *Refresh* button (or F5) to reload it.

Maps

Apart from the dedicated Access Control sections in Macula Console, it is also possible to place door markers onto maps – either regular ones or geo maps. Markers on the map will reflect door open state and lock state.

To do this, select Maps in the Configuration section of Macula Console and create a map or open an existing one. On the Marking tab, place as many markers as you need – the ones looking as doors – from the top panel. Click any marker to edit its settings on the right side of the dialog box: assign a door to it and adjust colors and icons for different door statuses.

For more details, please see the Maps section of this document.

Events and Actions

After the necessary connection and door(s) have been added, it is possible to use the door status changes as events in the *E&A Configurator* and also send commands to the access control server as door related actions.

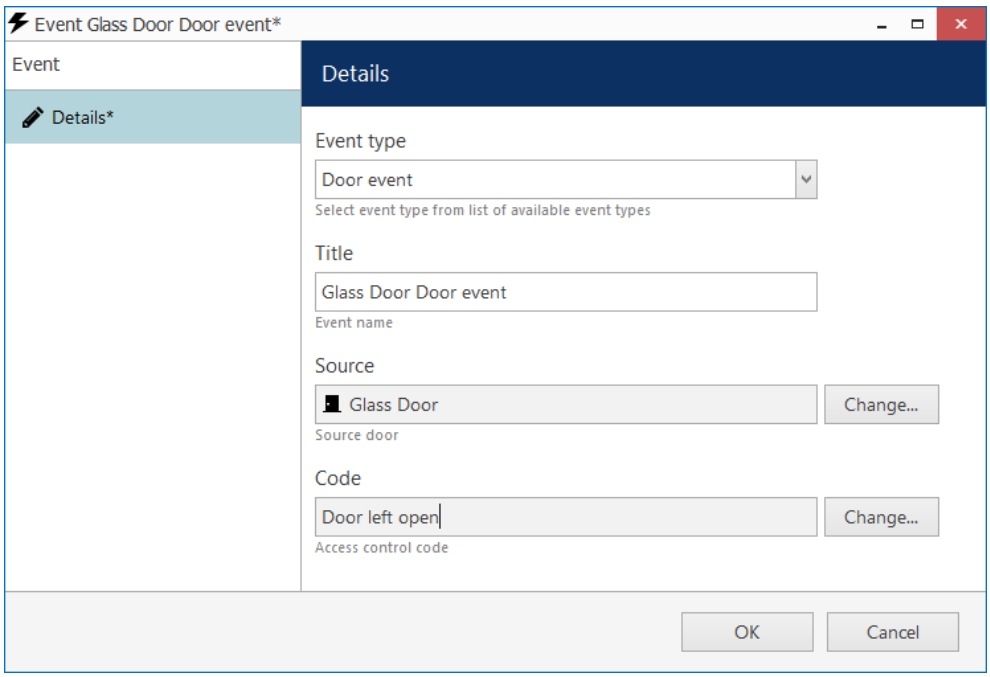
To add events and actions in Macula Console, switch to the *Events & Actions* section and choose *Events* or *Actions* on the left; click the *New <item>* button to add a new entry. Alternatively, you can add new events /actions right from the *E&A Configurator* by clicking the *+ New <item>* button in the bottom of the leftmost and rightmost columns.

There are two events related to the access control integration:

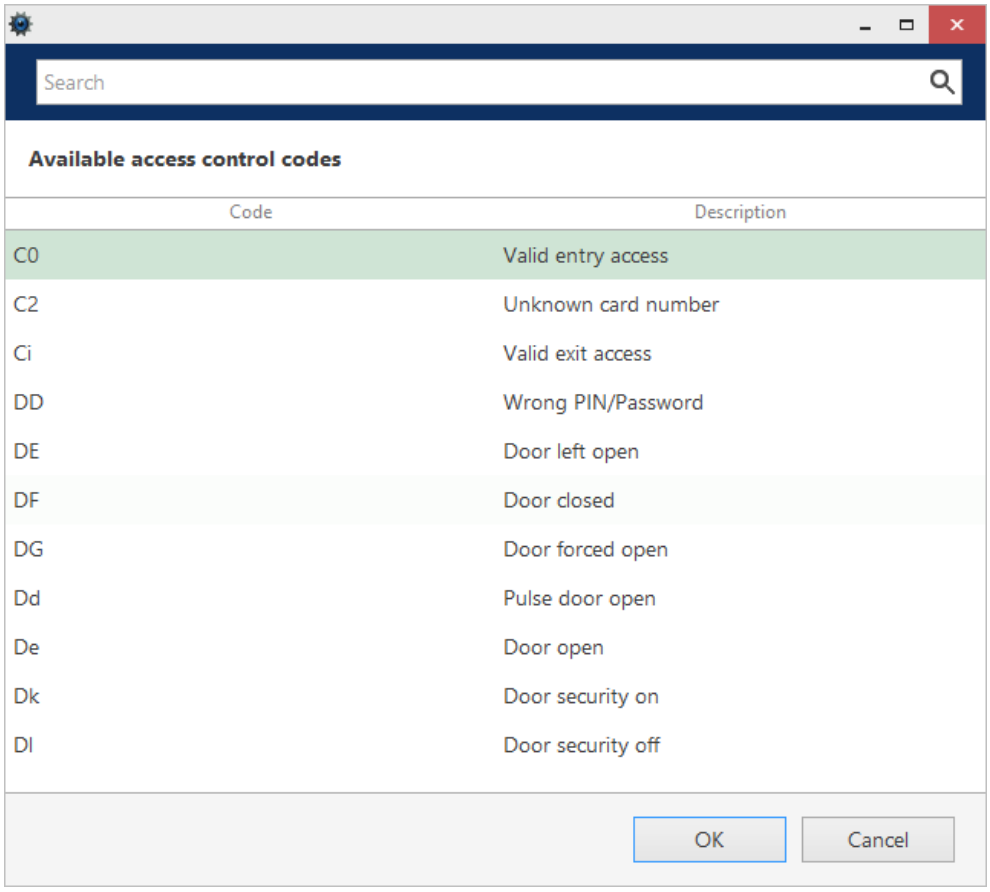
- *Access control event*: items not related to doors but still coming from the access control side (vendor-specific; e.g., other components' status change)
- *Door event*: codes related to door status (i.e., bound to specific nodes)

Door Event

This event category is triggered when the specified code is received from the access control server. Choose the target door as the event source here (the door must be added to the Macula server configuration beforehand), then select the code you wish to set up the reaction for.

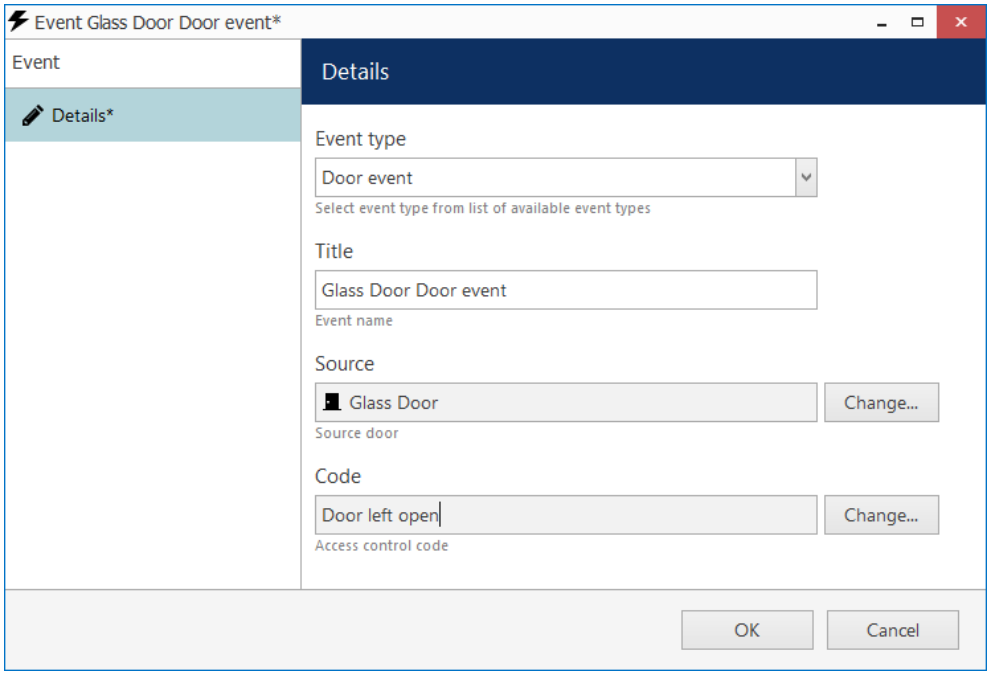


The **code list** is retrieved from the access control software and contains possible event types that can be received and understood by Macula server. Choose the one you want to set up a reaction for.



Access Control Event

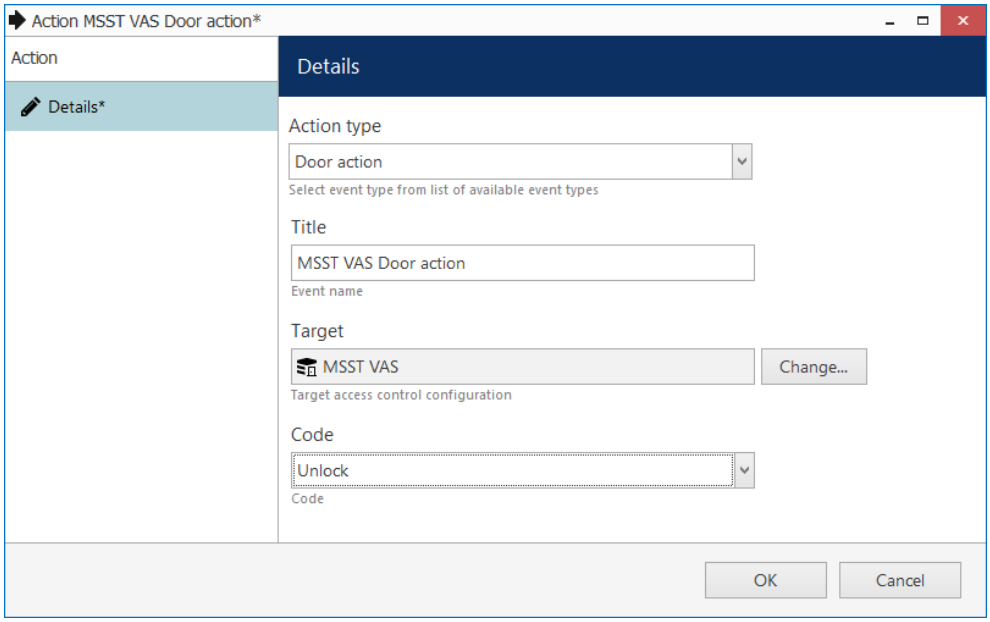
Use this event type if the notifications from the access control are not door-specific.



The exact list of event codes here depends on the vendor; some access control integrations may not support this kind of message.

Actions

Similarly, choose *Actions* on the left and create an action by pressing the *New* action button on the upper panel. You will need the *Door* action type.



As a target, specify the access control configuration added earlier. The specific door for this action will be chosen at the rule creation step, allowing you to use this action for many different doors within the same access control configuration.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Available **action codes** here are: lock, unlock, temporarily unlock, and lock down (standard access control door states). Once the action is triggered, the corresponding command will be sent to the third-party access control module.

E&A Rules

Once you have created necessary events and actions, combine them into rules in the *E&A Configurator*. For door related actions, remember that you need to specify the target door by using the *Target door* **button** in the bottom of the middle column.

Selected door status changes will trigger events in Macula, and actions triggered by internal Macula events will change door state, which will also be reflected in the access control UI.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

11.2 Gallagher

Macula has several integrations with third-party access control software suites. This part of the documentation provides details on how to make Macula work together with your **Gallagher Command Centre**.

The integration ensures two-way information exchange between Macula servers and access control software servers:

- Macula server receives **events**, **door** list and status, and **cardholder** list
- in Macula Console, you can see door status, add them to maps and geo maps, as well as create door related events and actions
    - E&A events help monitor the changes in the door status
    - E&A actions and maps allow you to change the door status (lock/unlock)
- in Macula Monitor, you can search door and cardholder events for the desired period

The details below will help you set up Macula to work with the Gallagher software. It is presumed that you already have the Gallagher Command Centre up and running, and are familiar with its initial configuration process. For details on the Gallagher software setup, please see its own supporting documentation.

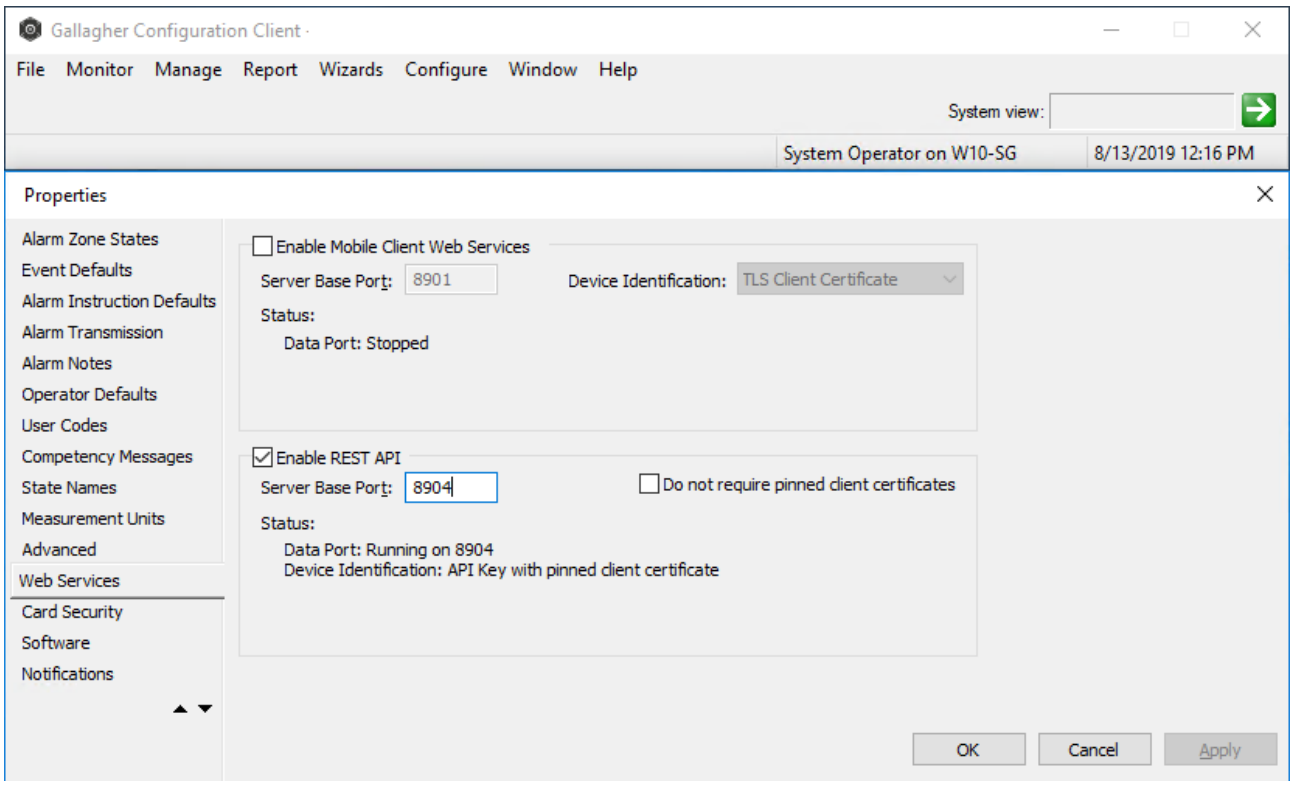
Gallagher Configuration

For the two servers to be able to communicate, a few things should be first set up on the Gallagher side. The integration operates over secure HTTP, therefore, from Gallagher's point of view, Macula will act as a REST API Client. The steps here describe the necessary settings in the Gallagher software.

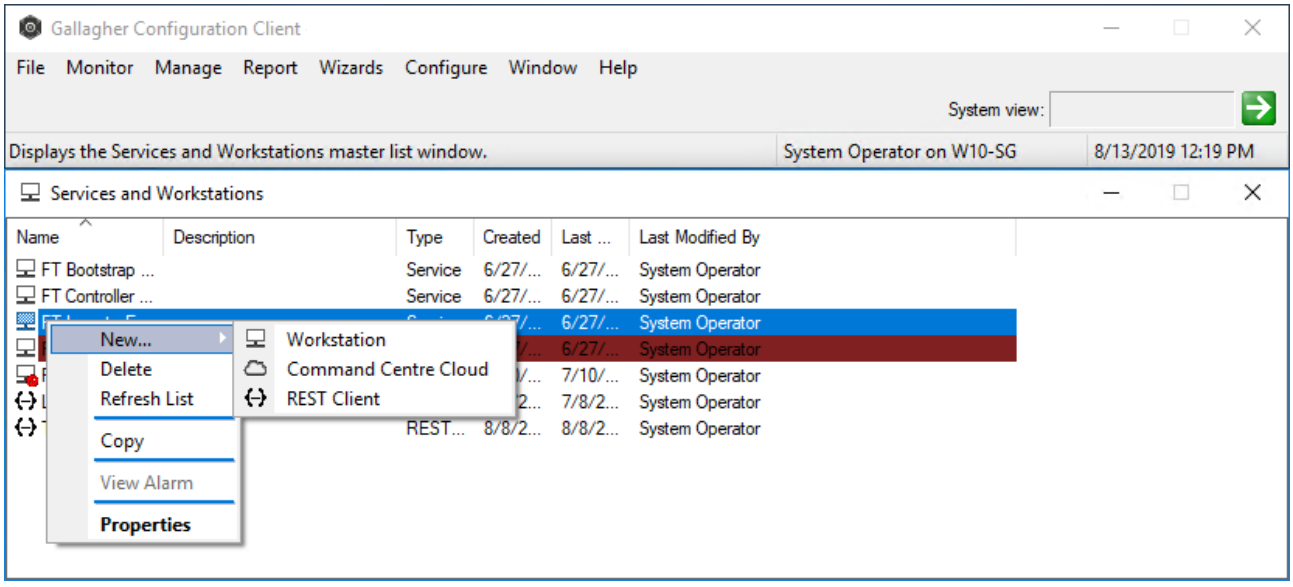
Run Gallagher Configuration Client and log in using your username and password.

In the panel containing the main menu, go to *File* > *Server Properties*, and select *Web Services* on the left. Here, turn ON the *Enable REST API* setting, and specify a HTTPS port for server-to-server communication.

Macula® Professional Administration Guide



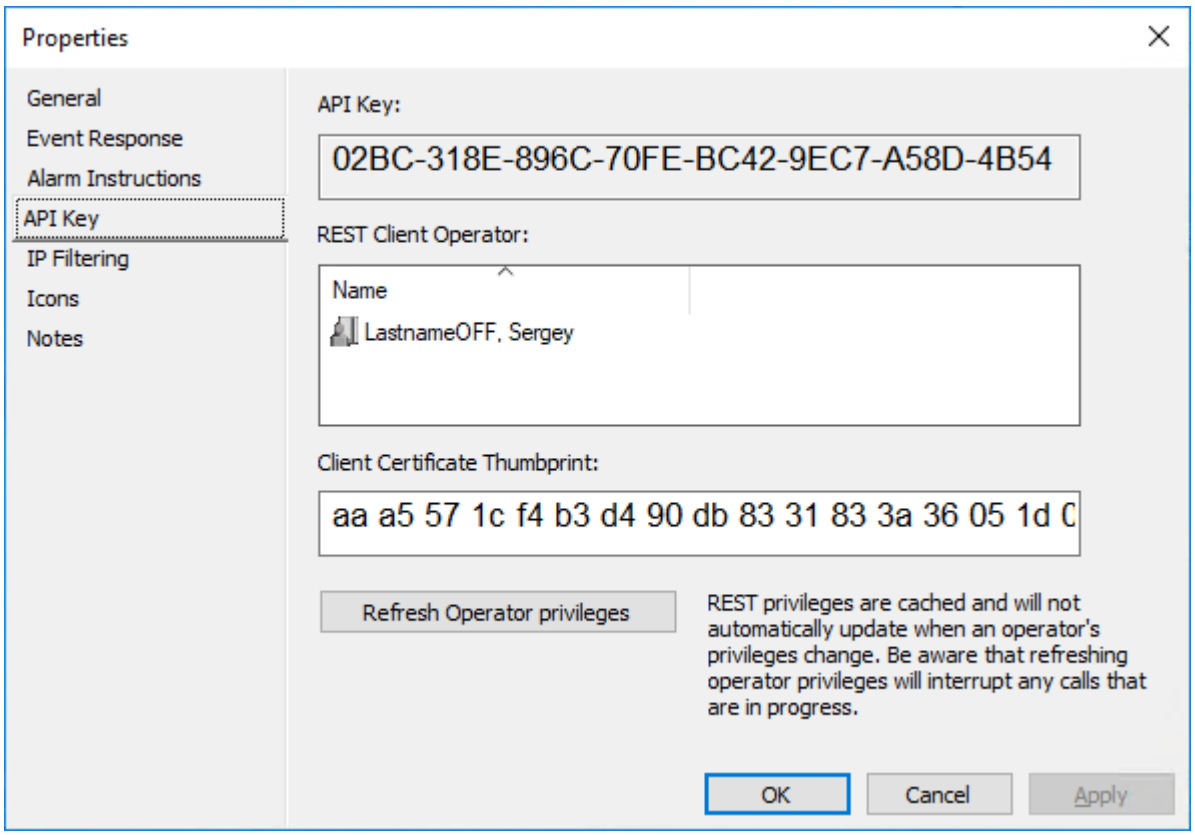
Next, go to the main menu *Configure* > *Services & Workstations*. In the dialog box that appears, right-click anywhere and select *New* > *REST Client*.



All settings here are up to you or default, except for those in the *API Key* tab. Here:

- Copy the **API Key** from the read-only field and paste in into Macula Console later, as described below
- Drag and drop your desired **operator*** into the *REST Client Operator* field from the main menu *Manage* > *Cardholders*
- Copy the *Client Certificate Thumbprint* from Macula Console (see below)

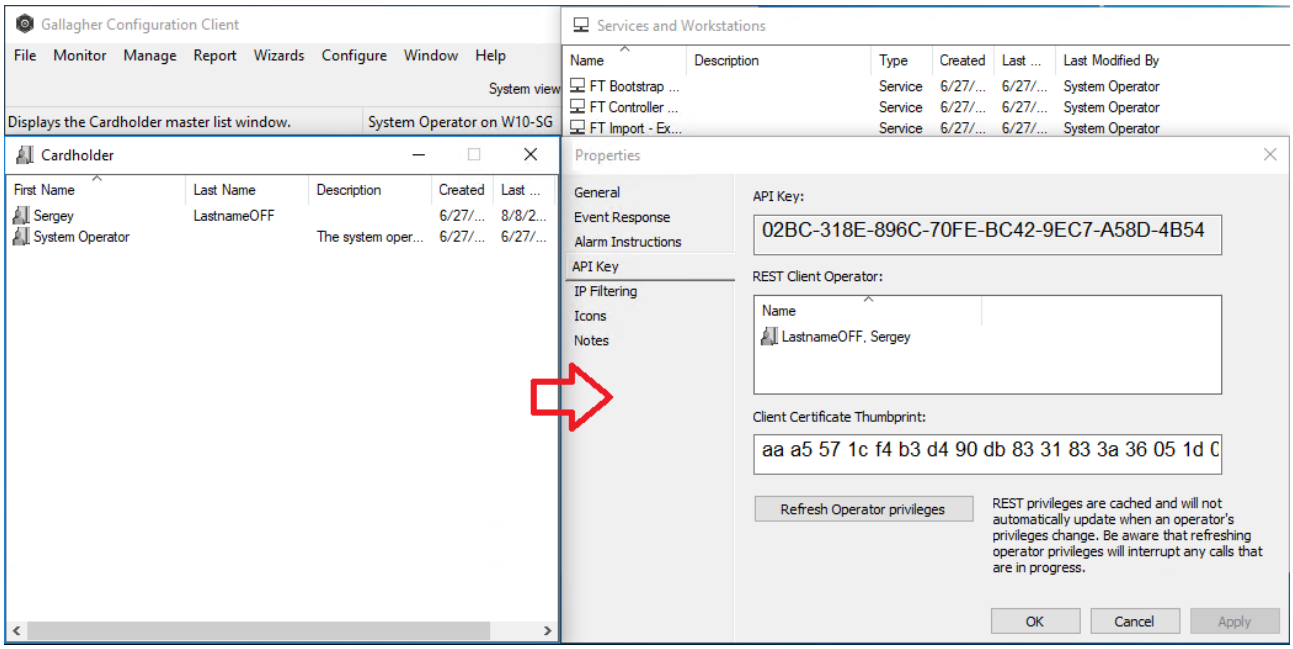
Macula® Professional Administration Guide



The certificate thumbprint is hard-coded into Macula and GSF is responsible for it renewal. You do not have to obtain your own certificate; simply copy the alphanumeric string from the Gallagher configuration dialog box in Macula Console.

> ⚠ *For the REST API integration to work properly, the cardholder acting as operator here **must have** the *Advanced user* **privilege**

The rest of the settings here are default/up to you.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

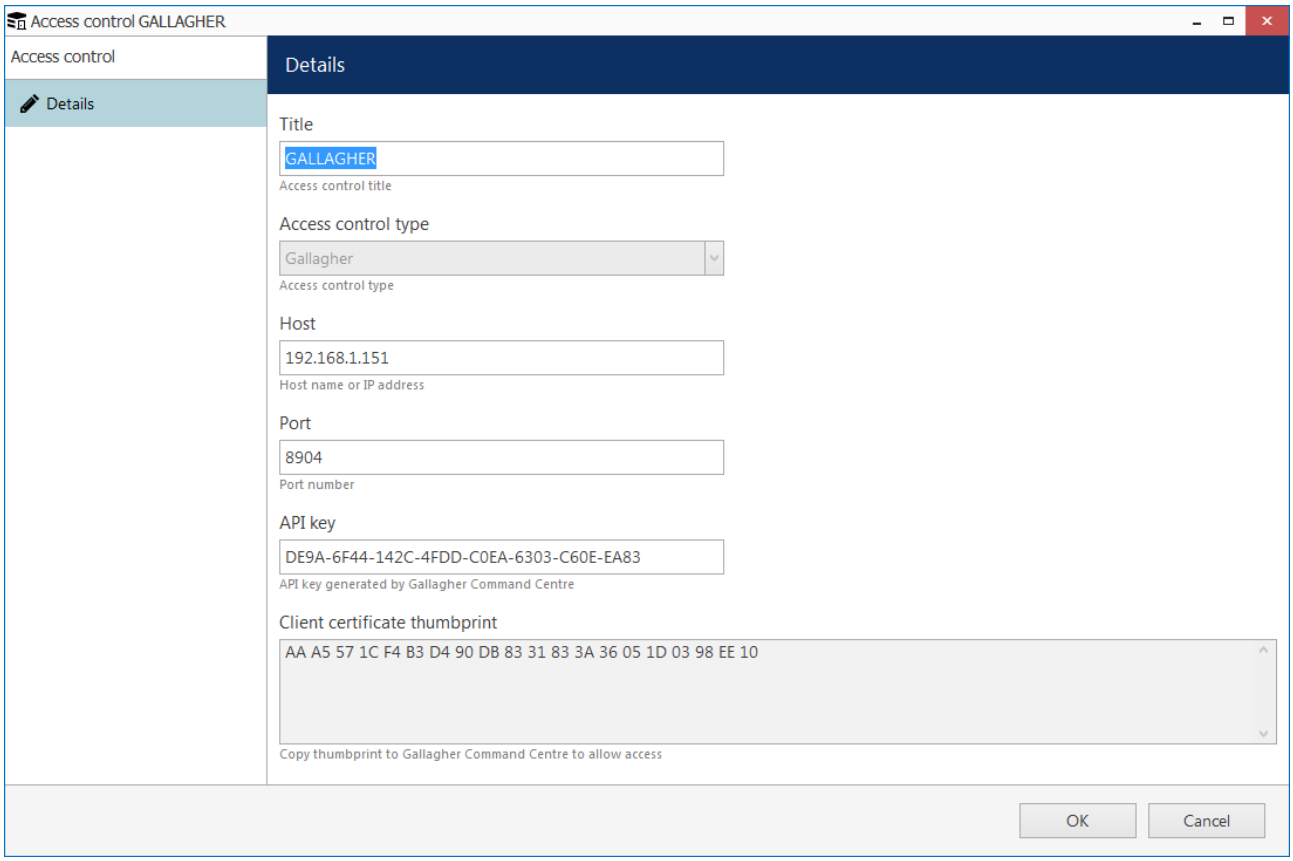
Macula Server Configuration

The rest of the setup will be on the Macula Console side. Macula server must have a Macula Enterprise or a Macula Professional license applied to it for you to have the *Access Control* tab. If you are running Macula Enterprise, make sure to connect to the central server, and use a privileged user account.

Create New Gallagher Connection

In your Macula Console, open the *Configuration* section and choose the *Access control* component on the left. Click the *New access* control configuration button on the upper panel and fill in the settings in the dialog box.

- **Title**: user-defined service name, which will appear in Macula Console
- **Access control type**: Gallagher
- **Host**: IP or hostname of the Gallagher server
- **Port**: server base port from the REST API settings (as specified above)
- **API key**: copy from Gallagher configuration, as shown above
- **Client certificate thumbprint**: copy and paste it into Gallagher REST API Client settings, as described above
- **Merge**: enable this option if you have multiple access control systems and you want to have them all in a single tab in the Macula Monitor application



When done, click OK to save the settings and close the dialog box. The newly created connection will appear in the list. Use the buttons on the upper panel to alter the connection details and to disable it temporarily, if required.

Add Doors

Once the Gallagher connection is created, you can start adding **doors**. To do so, stay in the same section of Macula Console (*Configuration* > *Access control*), click the drop-down list icon (down arrow) next to the *New access control* configuration and select the *New door* option. A dialog box will pop up, allowing you to enter the door configuration.

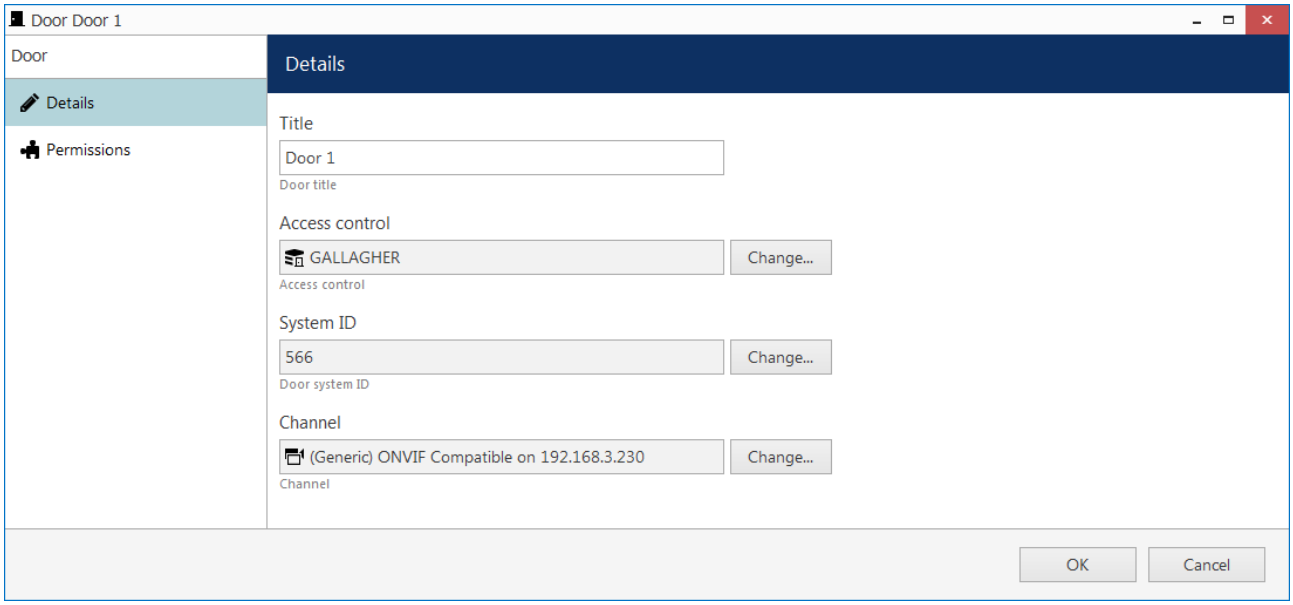
Note that an active connection to the target Gallagher instance must be present for Macula to be able to retrieve the current door list.

The following settings should be specified for each door:

- **Title**: user-defined door name, which will appear in Macula
- **Access control**: select your Gallagher connection from the list
- **System ID**: door identifier in the access control software; select one from the list
- **Channel**: select one of your video channels to associate it with the target door (they will appear linked in Macula Monitor)

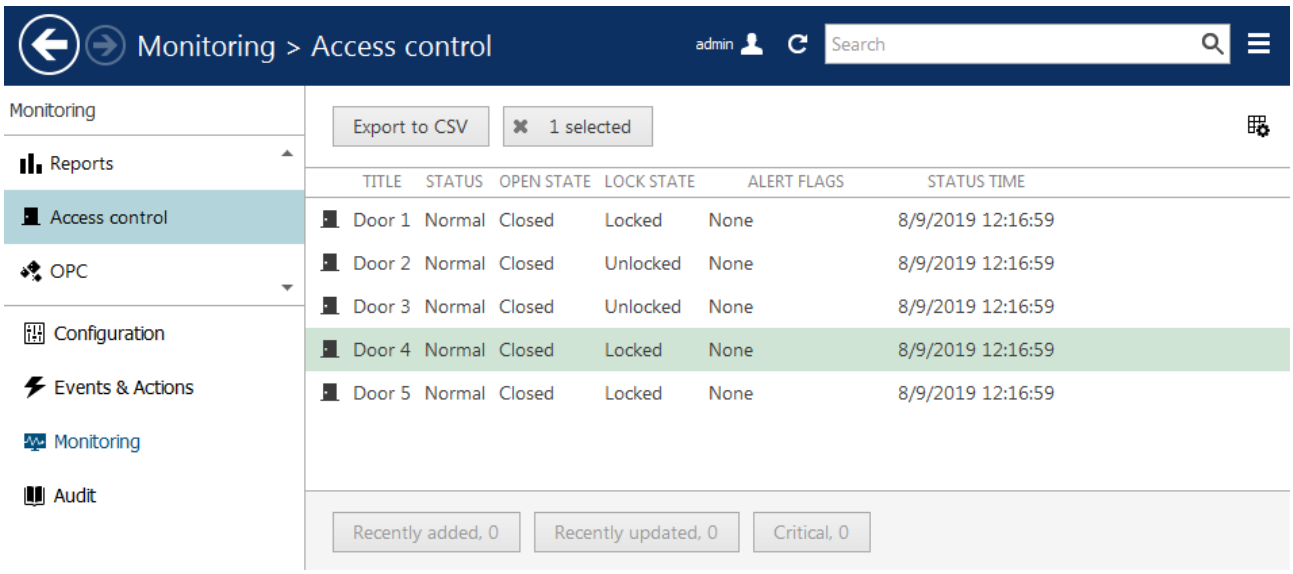
If the door list appears empty, check that:

- the doors are present in the Gallagher configuration
- you have added a REST API Client with a privileged operator, and that it has the certificate thumbprint copied from Macula Console, as described above
- you have copied the correct API key from that REST API Client into the Gallagher configuration in Macula Console



Use the *Disable/Enable* button on the upper panel to temporarily turn OFF the connection and restore it. The recycle bin button will remove doors and/or access control connection entries from the Macula configuration.

To see the **status of the doors** you have added into the Macula server configuration, go to the *Monitoring* section of Macula Console and select the *Access control* component on the left. You will be able to see the **current** door lock **state**, as well as related **alert flags**. Pay attention to the status update time. If a door status shows *Unknown*, it means either the Gallagher service is not connected, or the door may have been removed from the Gallagher configuration.

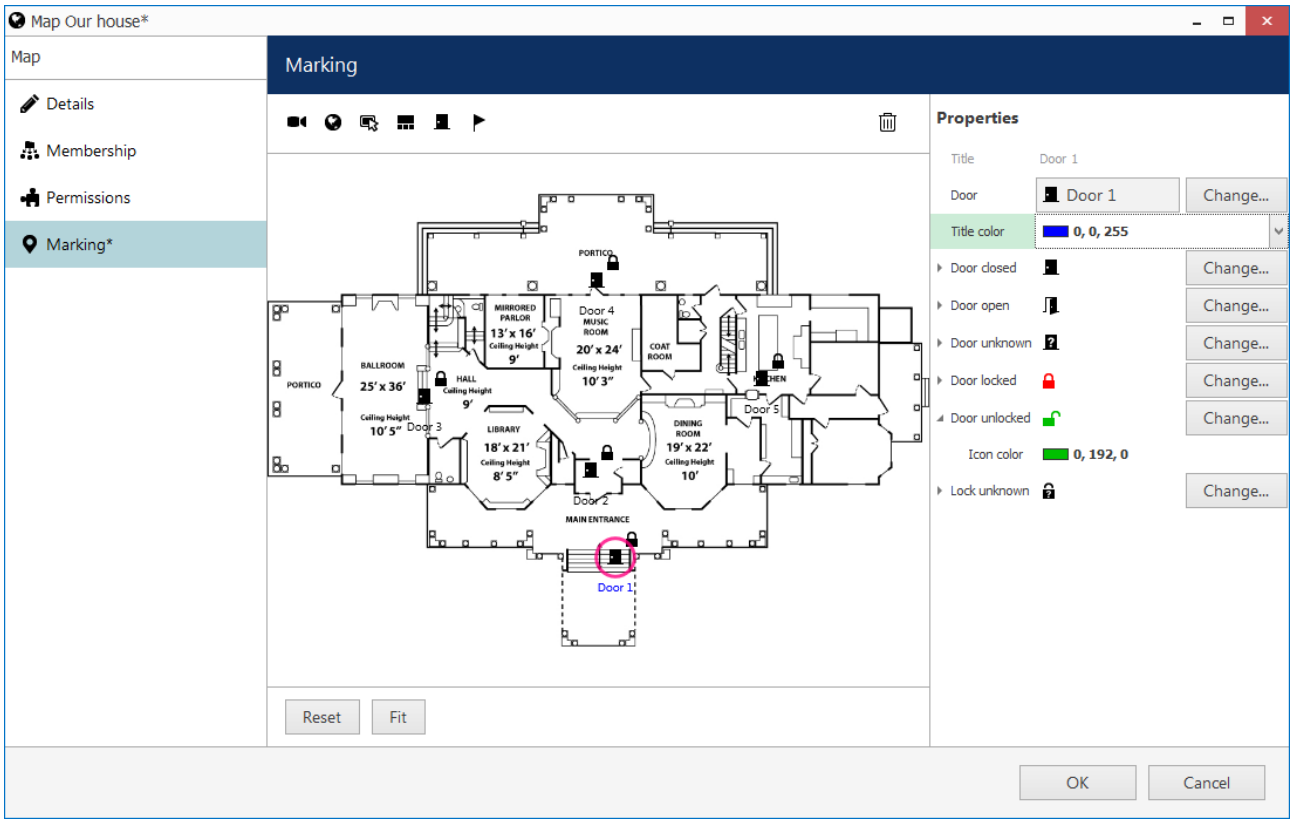


Use Doors in Macula

After you have added Gallagher doors to the Macula server configuration, there are several applications for them.

Add Doors to Maps

You can place **door markers** onto maps and geo maps. These markers will reflect the current **door status** in the Macula Monitor application, and provide interactive **actions** upon single or double click.



To put a marker onto the map, **drag and drop** it from the panel above. In the settings on the right, select the **target door** from the list. You can also adjust the **marker appearance** for each door state by selecting the target icon and its color.

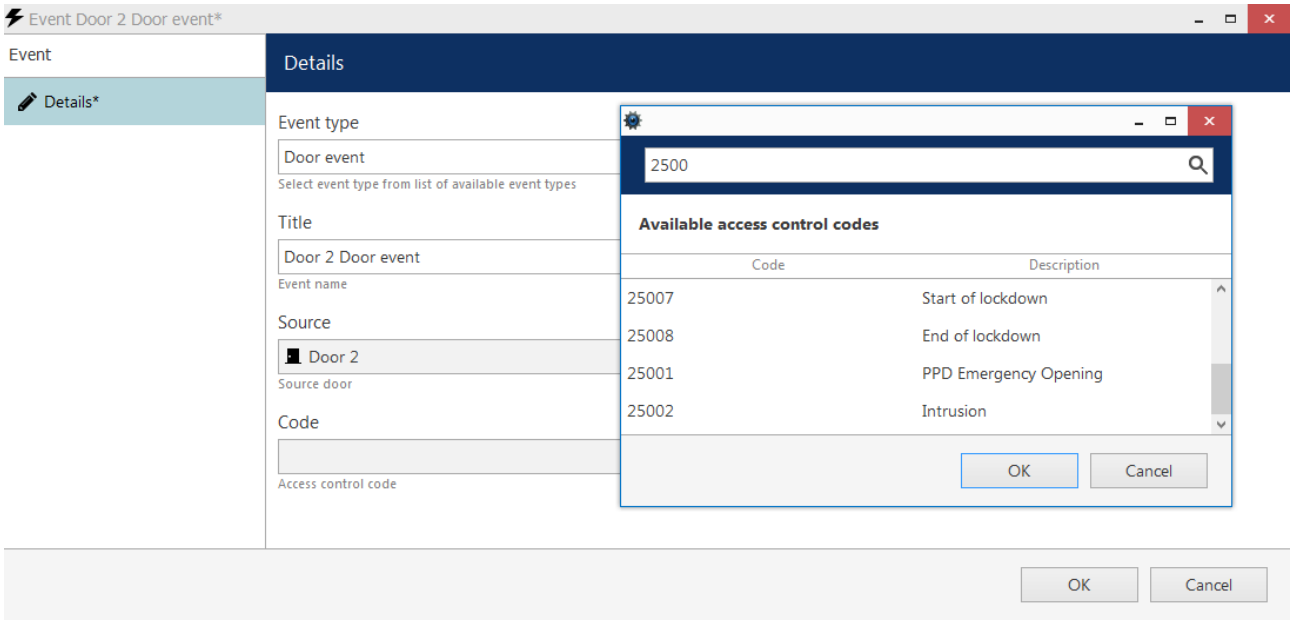
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

Events & Actions

Macula Event & Action Manager (E&A) provides support for both door events (status changes) and actions (change door state).

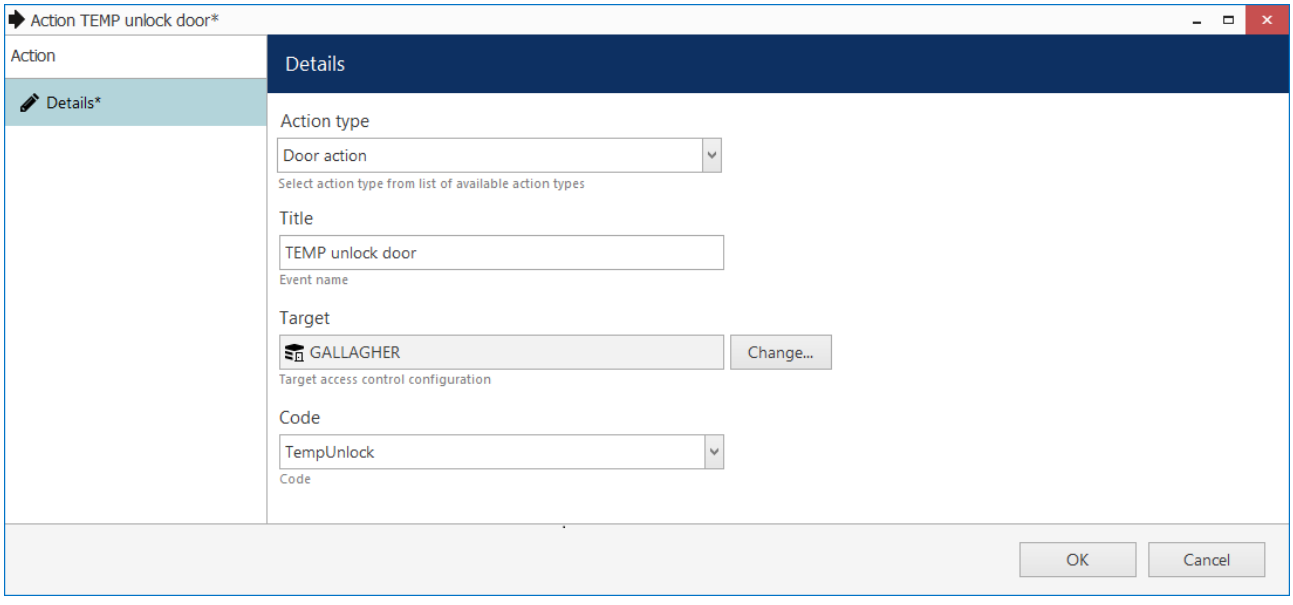
Changes in the door status are sent from Gallagher to Macula. You can set up different reactions for different codes via Macula E&A. Later, these events can be used for building rules, e.g., for logging the events in Macula, bookmarking them, automatically interacting with other system components etc.



To create a new **door event** in Macula Console, go to the *Events & Actions* section > *Events* > click the + *New event* button on the upper panel. In the appeared dialog box, fill in the settings:

- **Event type**: Door event
- **Title**: user-defined event name to be used in E&A Configurator
- **Source**: select a door from the list
- **Code**: desired door status change code received from Gallagher, select one from the list

Thus, such events will be triggered each time the corresponding code is received from Gallagher. One event corresponds to one code from a specific door: create multiple events if required.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

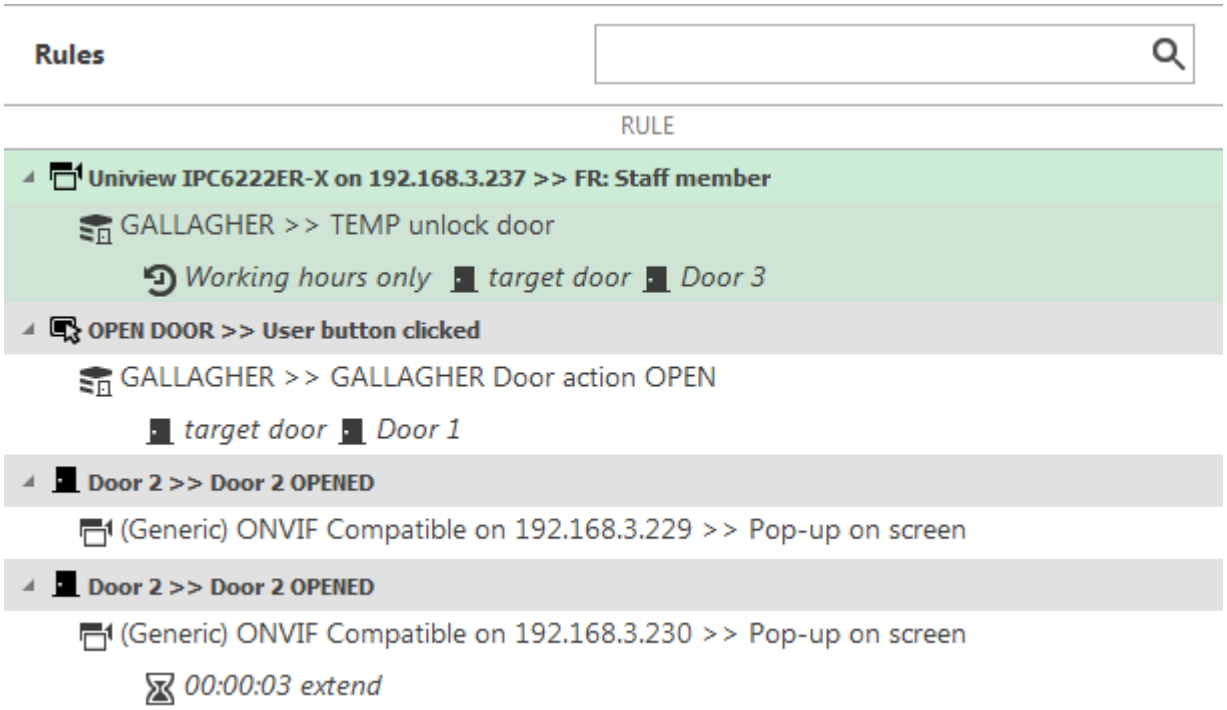
Correspondingly, door action can be created from the *Events & Actions* section > *Actions* by clicking the + *New action* button from the upper panel. Available settings:

- **Action type**: Door action
- **Title**: user-defined action name, which will appear in E&A Configurator
- **Target**: your Gallagher connection
- **Code**: select the desired action from the list
  - *Lock*: change the door state to *Locked*
  - *Unlock*: change the door state to *Unlocked*
  - *TempUnlock*: open (unlock) the door temporarily, then lock it back after ~5s

> The *Lock* and *Unlock* actions will only operate if the target door is the **only** one in the target **access zone** in Gallagher configuration. If there are multiple doors in the same access zone, these actions will still be available in Macula Console but will not actually work. For **multi-door** areas, use the *TempUnlock* action (open the door and close it automatically after a short timeout).

Finally, go to the Events & Actions section > choose Rules on the left > click the Open configurator button on the upper panel to bring up the E&A Configurator dialog box.

Here, you can use all your events and actions, including those related to Gallagher, to build automated scenarios. Every rule can also have modifiers: a delay timer, a condition, and a schedule.



Example: you can temporarily unlock a door by clicking a user button, or make it open automatically when a face from the staff database is recognized.

Gallagher in Macula Monitor

Once your Gallagher service is paired with Macula, you will see a new tab appear in the Macula Monitor application. If you do not, make sure you are connected to the correct Macula server.

Macula® Professional Administration Guide

Switch to the Access control tab to start working with its contents. Similarly to other access control integrations, there are three subsections here:

- **Events**: all events received from Gallagher
- **Doors**: the door list and related actions
- **Cardholders**: the list of cardholders

Note that the door list here will be loaded according to the user permissions. There are two user permissions for each door resource in Macula Console:

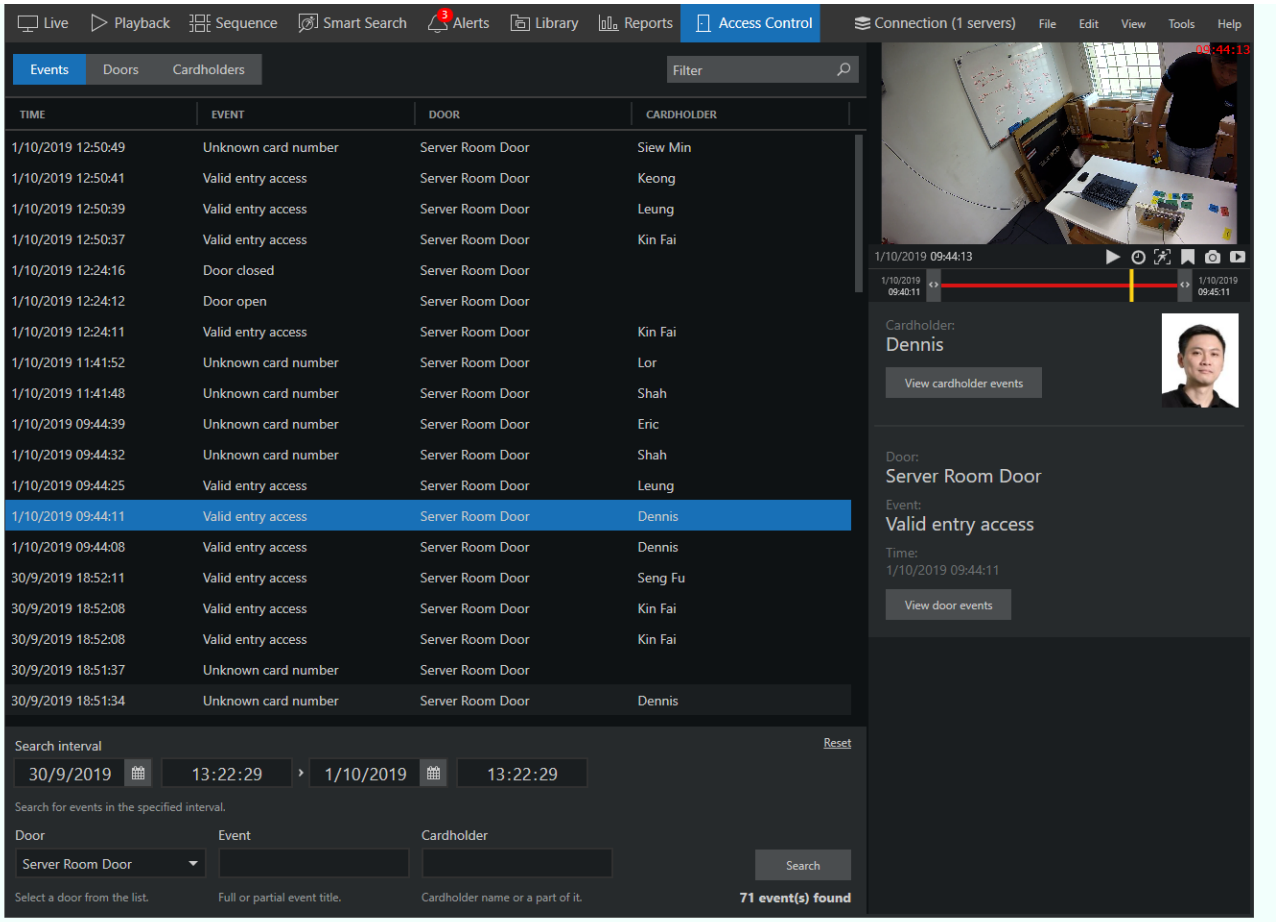
- *View*: see the door and its status in Macula Monitor
- *Door actions*: have the Lock/Unlock/Temporarily Unlock buttons in Macula Monitor

Apart from this permission management via Macula Console, you can hide the Access control tab from all users via Macula Monitor Restrictions (main menu Tools > Administration Tool).

Events

This section is almost identical to the *Event Trail section* in Gallagher Command Centre. Here, you will find door **events** - status changes, lock/unlock operations etc. - as well as other Gallagher events, such as: database maintenance notifications, configuration changes (e.g., new cardholder added), etc.

Enter the search **time range** and **criteria** in the bottom and click *Search*. The results will appear as a list. Use the *Reset* button to **discard** any entered criteria and use the default search settings (any event type, past 24h).



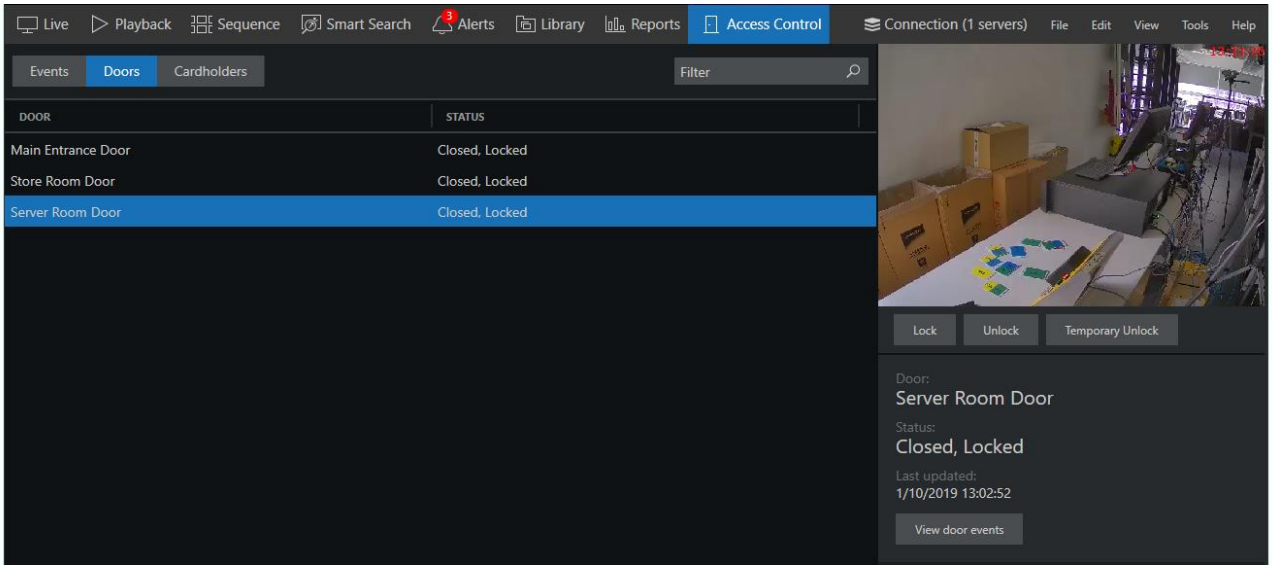
Click any event in the list to see **details** on the right. If the clicked event is related to a door, you will see the linked channel's video appear in the **instant playback** mode. Click the *View* door events button below to view the target door events for the past 24h.

Doors

This tab contains the **list of doors** retrieved from Gallagher. Each door will have its current state reflected in the *Status* tab.

Click any door to see more details on the right:

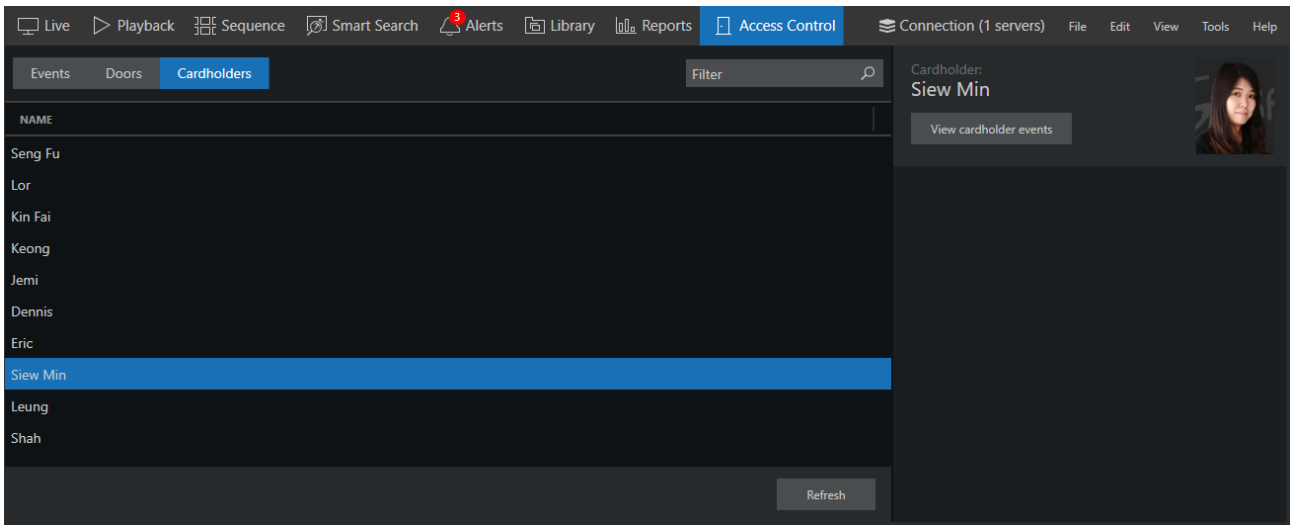
- see the live video from the associated video channel
- click the *Lock, Unlock*, or *Temporarily Unlock* buttons to perform the corresponding action (similarly to E&A actions, *Lock/Unlock* will only work for single door zones)
- click the *View door events* button to switch to the *Events* tab: target door events for the past 24h will be shown automatically



Cardholders

You will see all existing **cardholders** fetched from Gallagher here. As there are no cardholder associated actions, the extra details here will be the name and picture.

Click the *View cardholder events* button to switch to the *Events* tab and see the related events for the past 24h. Use the *Refresh* button in the bottom to **reload** the cardholder list and details - this comes useful if there have been changes on the Gallagher side, which have not been synchronized with Macula yet.



Maps

If you have created **maps** with **door markers** on them, you will be able to use these maps in the *Live* and Playback tabs, as usual. Each door marker, when clicked (or double-clicked, depending on your application setting), will provide an opportunity to lock, unlock, or temporarily unlock the target door. This functionality is identical to door actions in E&A and door buttons in the *Access control* tab.

11.3 Inner Range Integriti

Macula is integrated with a number of **access control systems**. Macula server can receive events from and send requests/commands to third party access control software.

The current integration includes the following **access control software**: Keri, Feenics, Gallagher, Roger RACS 5, AEOS by Nedap Securit, **Inner Range Integriti**, and Visual Access System by GSF Corporation.

Macula obtains the **list of doors**, their **statuses** (opened/closed, locked/unlocked), **cardholder list** and relevant events, and enables you to lock and unlock the doors based on internal Macula server events (e.g., user button pressed) and also from the Macula Monitor application. Information about doors, their events and cardholders are searchable from Macula Monitor application as well.

Supported functionality overview:

- Receive events, door list and their status, list of cardholders (users)
- Change door status by sending corresponding commands back
- Live door status with linked video channels
- Interactive markers on the maps and geographical maps
- Notifications and other actions based on door events
- Search event history based on doors, cardholders, and time
- Set up mobile app notifications
- Lock and unlock doors from the mobile application

Integrations with different access control software are similar. However, there may be nuances in configuration. If you encounter any difficulties with the setup, feel free to contact our support engineers at support@gsfcorp.com.

Macula Configuration with 3rd Party Access Control

This topic briefly describes the configuration necessary to make use of the access control software integrations with Macula software.

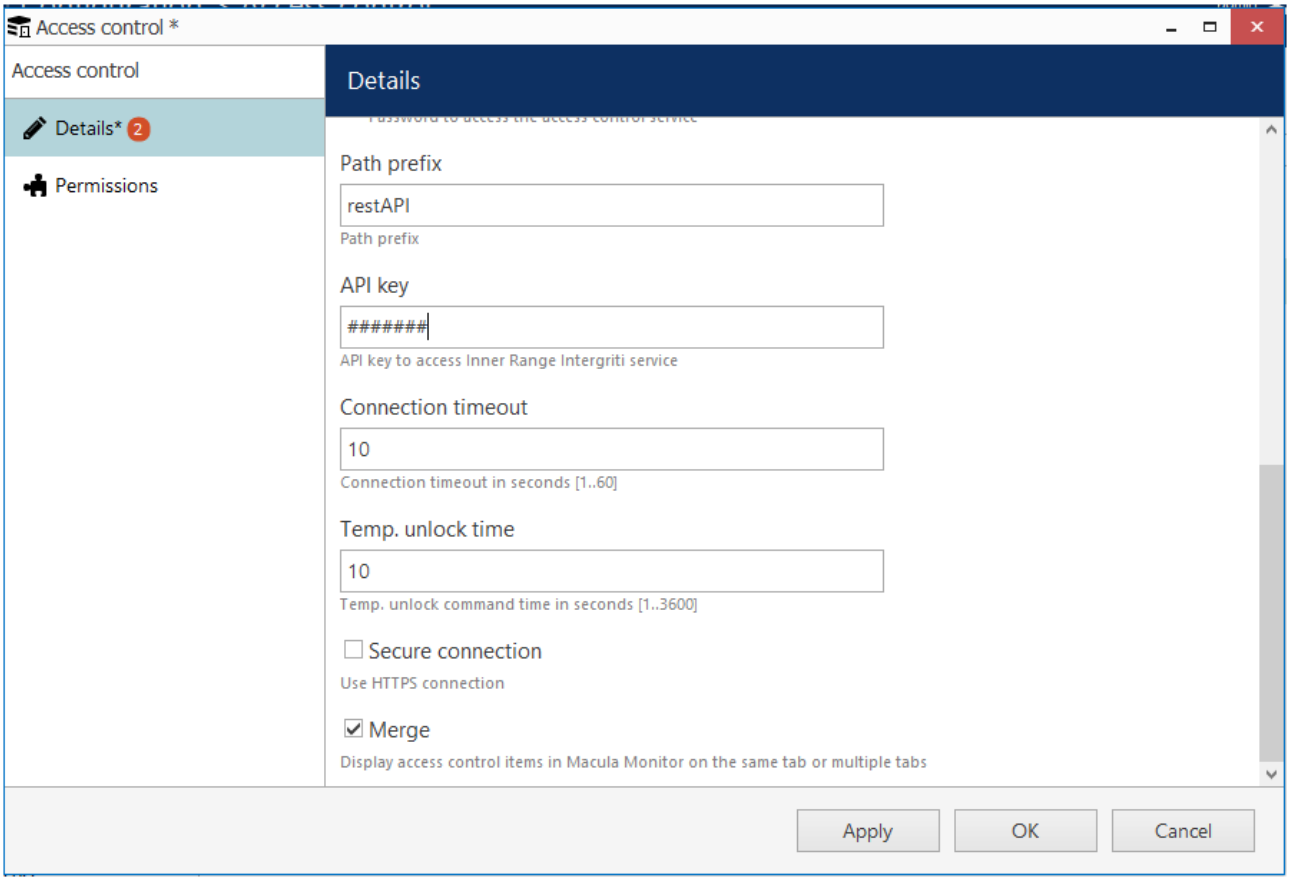
Prerequisites

- Preinstalled **Inner Range Integriti** instance.
- For the configuration, you must enable Inner Range Integriti Communications Handlers. For the additional info - please consult the Inner Range Integriti **REST XML Web API V2 documentation**.
- You also must have Inner Range Integriti **API key** - please contact the Inner Range Integrity sales for the additional details.
- Your firewall settings must be preconfigured to allow communication between Macula and Inner Range Integriti instance.

Add Access Control Configuration

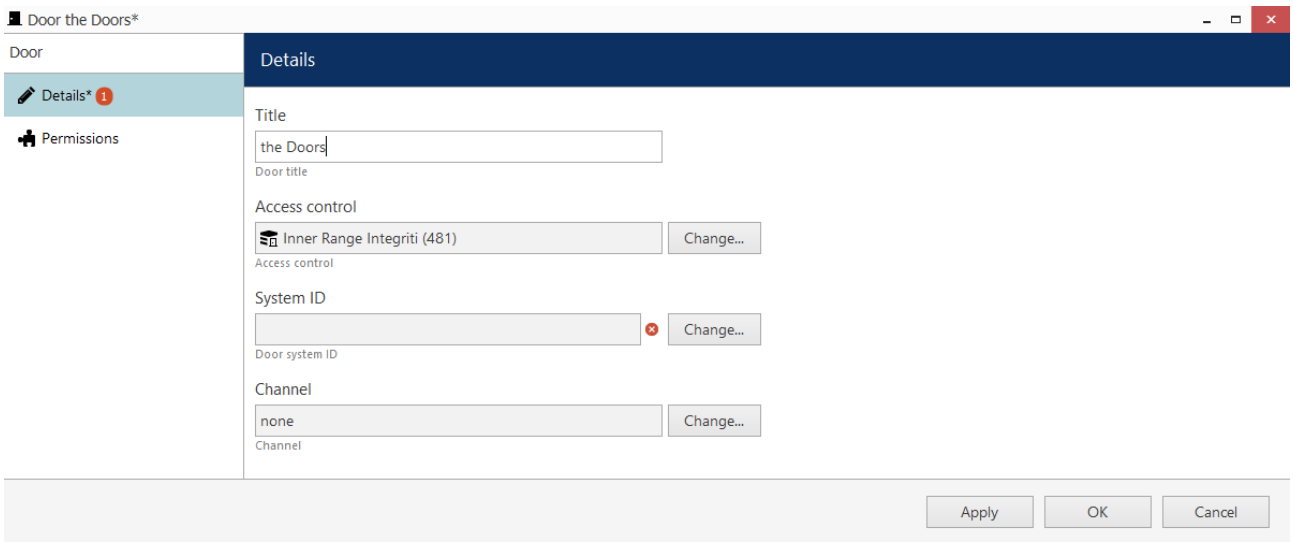
In Macula Console, open the *Configuration* section and choose *Access Control* in the menu on the left. Here, you need to create a connection to the **Inner Range Integriti** server: click the *New access control configuration* button on the upper panel and fill in the settings, then click *OK* to save:

- User-defined **title**
- **Type**: select your access control software name
- **Host**: access control server IP address (required for some types)
- **Port**: access control server port (Default port for the Inner Range Integriti is: 80)
- **Username and password** to connect to the access control server. Use the *Password* and the *Username* you set up inside the Inner Range Integriti instance. Please make sure that you are using the correct *Authentication* (Basic or HTTPS) type and *User* (Default Operator or other specific configuration). If inconvenient - consult with the Inner Range Integriti **REST XML Web API V2 documentation**
- **Path Prefix:** By default the Path Prefix is set to *'restApi*', but check your Inner Range Integriti settings
- **API Key:** reach out to Inner Range Sales and apply for an API Key
- **Connection timeout/Temporary unlock time:** set intervals in seconds
- **Secure Connection**: mark the checkbox for the HTTPS connection type
- **Merge**: enable this option if you have multiple access control systems and you want to have them all in a single tab in the Macula Monitor application

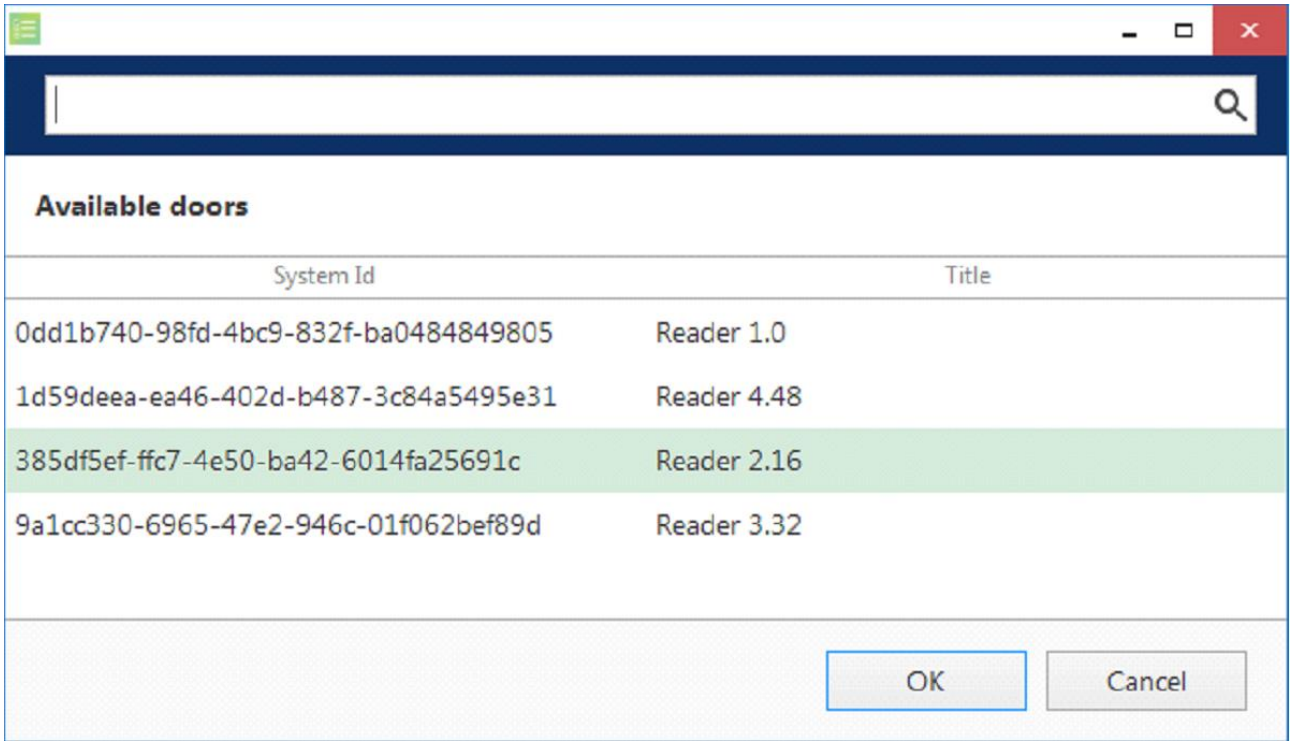


Add Doors

Next, click the arrow next to the *New access control configuration* button and select *New door* in the drop-down list. Choose the access control configuration created on the previous step.



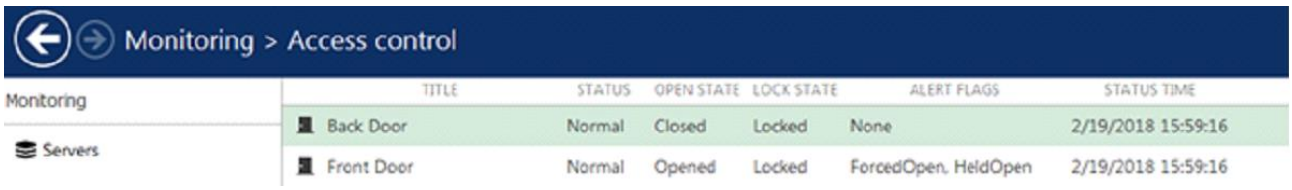
Click the *Change* button next to the *System ID* field to view the list of available doors: if the access control configuration is correct, Macula server will successfully fetch it from the server. Choose the required door and click *OK*.



If you wish to bind a video channel to a door, choose a channel in the corresponding field. This channel will appear when viewing events from that door in the Macula Monitor application, and the event list will be bound to the recorded footage.

Monitoring

For all the doors that have been added it is possible to view their current states in the Macula Console application: to do so, switch to the *Monitoring* section and select *Access Control* in the list on the left.



The following information is available:

- **Open state**: opened/closed
- **Lock state**: locked/unlocked
- **Alert flags**: additional information, if any
- **Status time**: last status update time

Use the *Search* field in the top right corner to filter the door list, and the *Refresh* button (or F5) to reload it.

Maps

Apart from the dedicated *Access Control* sections in Macula Console, it is also possible to place door markers onto maps – either regular ones or geo maps. Markers on the map will reflect door open state and lock state.

To do this, select *Maps* in the *Configuration* section of Macula Console and create a map or open an existing one. On the *Marking* tab, place as many markers as you need – the ones looking as doors – from the top panel. Click any marker to edit its settings on the right side of the dialog box: assign a door to it and adjust colors and icons for different door statuses.

For more details, please see the Maps section of this document.

Events and Actions

After the necessary connection and door(s) have been added, it is possible to use the door status changes as events in the *E&A Configurator* and also send commands to the access control server as door related actions.

To add events and actions in Macula Console, switch to the *Events & Actions* section and choose *Events* or *Actions* on the left; click the *New <item>* button to add a new entry. Alternatively, you can add new events/actions right from the *E&A Configurator* by clicking the *+ New <item>* button in the bottom of the leftmost and rightmost columns.

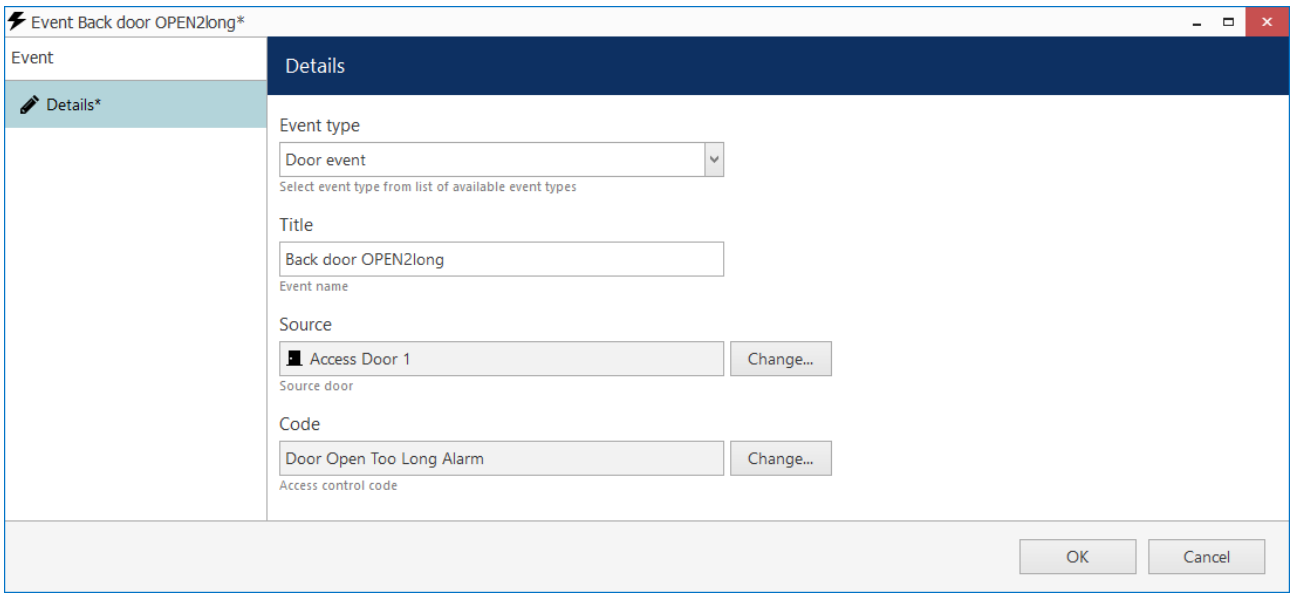
There are two events related to the access control integration:

- *Access control event*: items not related to doors but still coming from the access control side (vendor-specific; e.g., other components' status change)
- *Door event*: codes related to door status (i.e., bound to specific nodes)

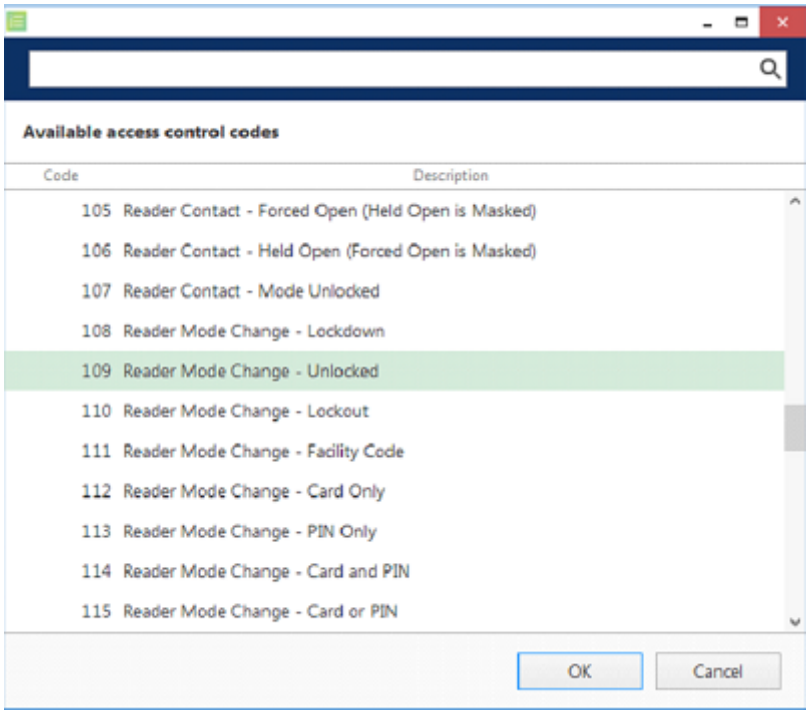
Door Event

This event category is triggered when the specified code is received from the access control server. Choose the target door as the event source here (the door must be added to the Macula server configuration beforehand), then select the code you wish to set up the reaction for.

Macula® Professional Administration Guide

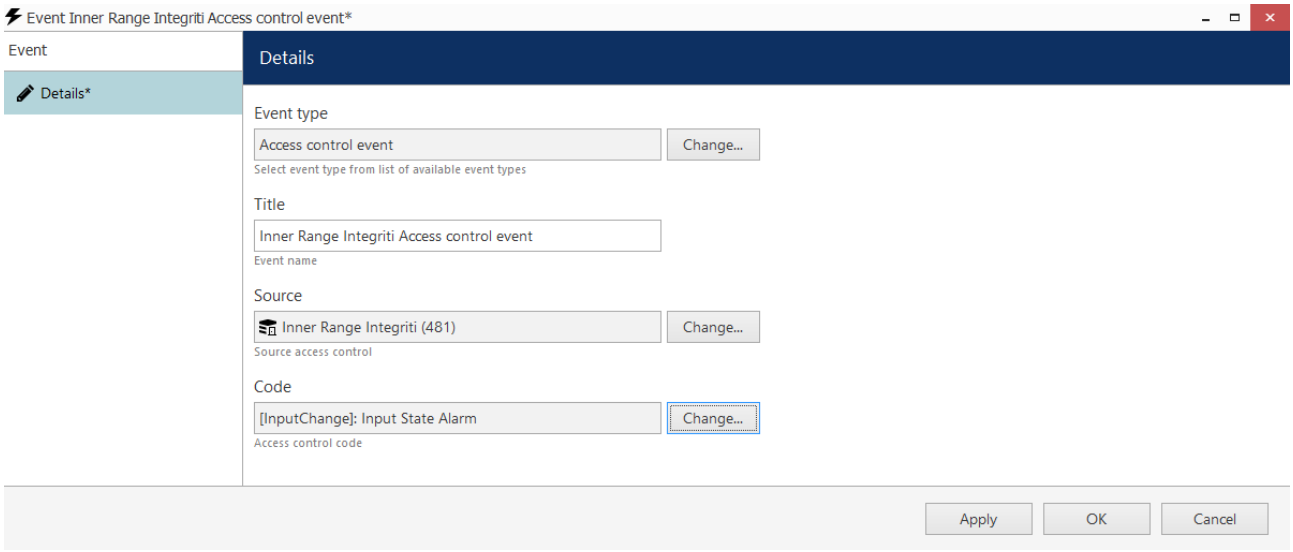


The **code list** is retrieved from the access control software and contains possible event types that can be received and understood by Macula server. Choose the one you want to set up a reaction for.



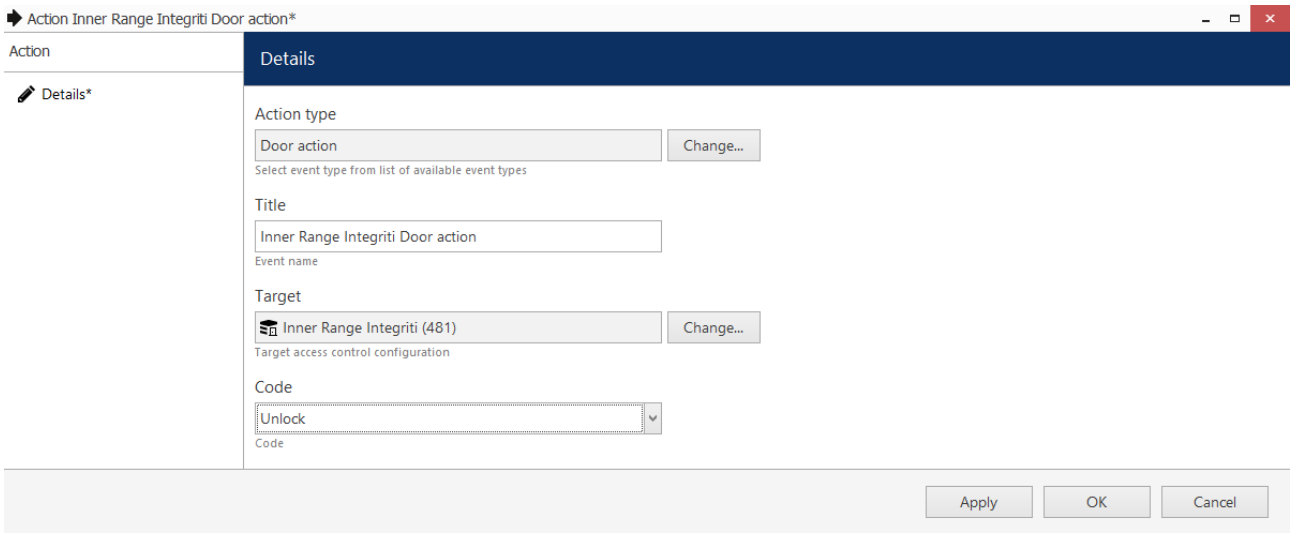
Access Control Event

The exact list of event codes here depends on the vendor; some access control integrations may not support this kind of message.



Actions

Similarly, you can send notifications to the access control servers based on Macula events. To do this: in Macula Console, choose *Actions* in the Events & Actions section and create a new one by pressing the *New action* button on the upper panel. Alternatively, press the + *New action* button on the *E&A Configurator*. You will need the *Door action* type.



As a target, specify the access control configuration added earlier. The specific door for this action will be chosen at the rule creation step, allowing you to use this action for many different doors within the same access control configuration.

Available **action codes** here are: lock, unlock, temporarily unlock, and lock down (standard access control door states). Once the action is triggered, the corresponding command will be sent to the third party access control module.

E&A Rules

Once you have created necessary events and actions, combine them into rules in the *E&A Configurator*. For door related actions, remember that you need to specify the target door by using the *Target door* **button** in the bottom of the middle column.

Selected door status changes will trigger events in Macula, and actions triggered by internal Macula events will change door state, which will also be reflected in the access control UI.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

11.4 Camio

Camio video analytics is a cloud service that can do intelligent video analytics based on the provided video stream. Its integration with Macula is built using REST API. To link Macula server to your existing Camio account, add it as an external service by following the steps below.

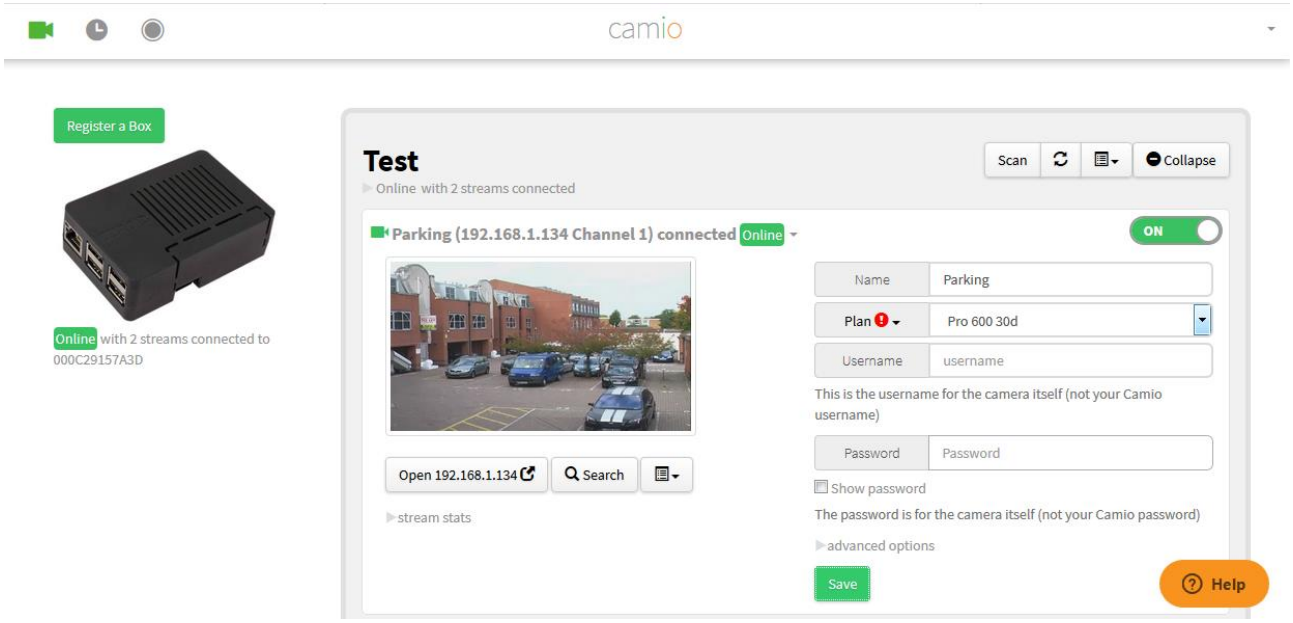
Macula already has the Camio cloud service address. All you need to do is make sure you have added your Camio box to the service Web interface, then add the service connection in Macula Console and configure a channel (or channels) to be processed. Macula will then receive analytical events and will also allow searching the result database. The architecture is such that your Macula server connects to the Camio cloud service. Then, Camio boxes accept H.264 RTSP streams from Macula for video analysis. Whenever there is an event, the box sends it to the Camio cloud service, and then it is forwarded to the Macula server.

The steps described below will help you connect to Camio from your Macula server and take advantage of its video analytics. Note that this document does not provide detailed details on Camio services. For elaborate Camio configuration and usage guidelines, please refer to its own supporting documentation and/or technical support.

Prepare Camio

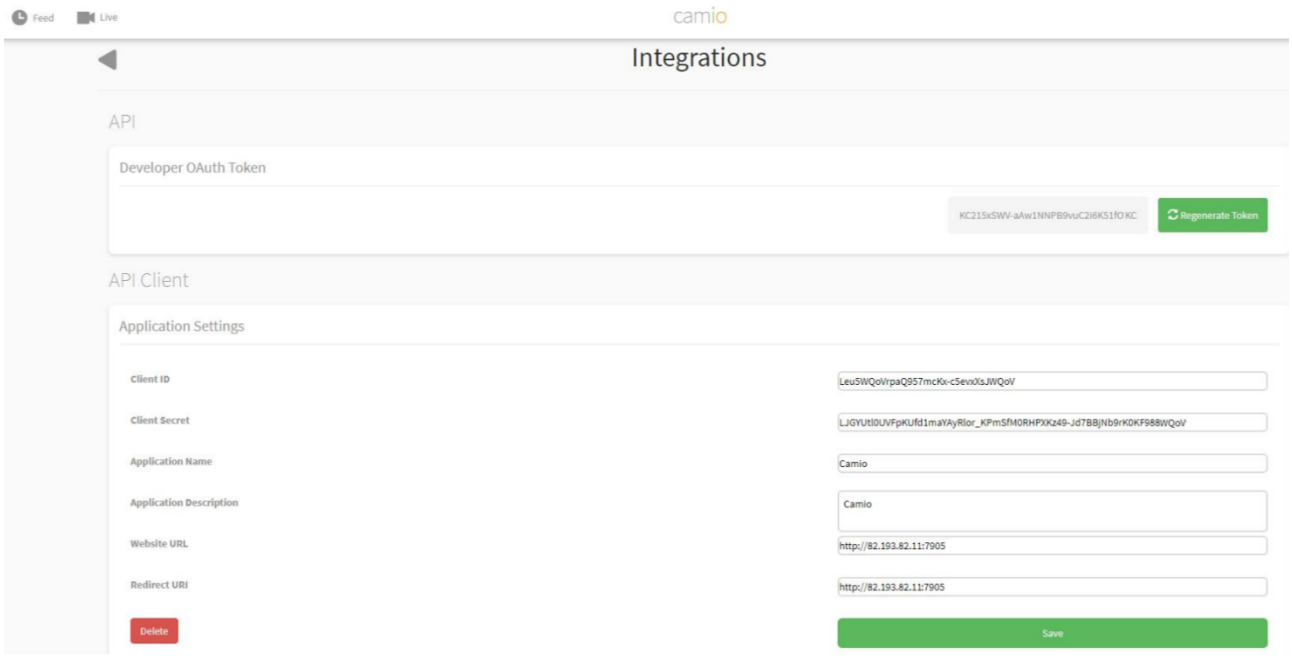
Log into your Camio account via Web browser and add a box. You can do this by clicking your account name in the upper right corner and then by clicking the Register Box button. This will allow you to add Macula channels in Macula Console later.

> ⚠ Your Camio box must be in the same network as your Macula Professional or Macula Enterprise server.



One more preliminary step here is to generate a **token** for the Macula connection. To do this, click your account in the upper right corner and go to *Settings* > *Integrations*, then click the *Generate Token* button in the API section. Save your token somewhere: you will need to enter it when creating a Camio connection

in Macula Console. If you forget/lose the existing token, you will have to generate a new one, and all current connections using the old token will cease to function.



From the Macula server side, make sure you have the external server address (**Internet address**) specified, internet HTTP **port** enabled (different from zero) and opened on the firewall/router. A simple test to check if the configuration is valid is to try entering your Macula server URL into the browser address bar: you should be able to see the streaming server interface. Use this **address and port in the Camio Web** interface to pair it with Macula server.

Example: if your Macula address is 82.193.82.11 and internet HTTP port is set to 7865, enter http://82.193.82.11:7865 into your browser (better test it from another computer, and another network) and verify that you can see the Macula Web client. If successful, use the same address for Camio Web.

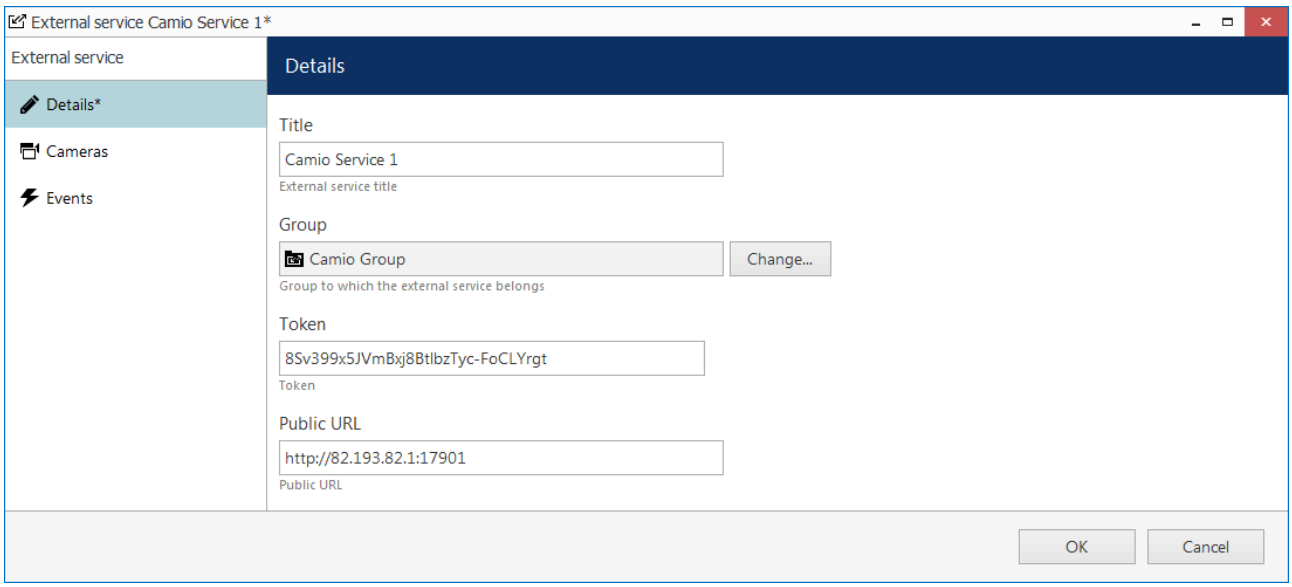
> ⚠ Make sure that your **port forwarding** setup works and that your Macula server is **reachable** from the **Internet** via **HTTP**. (You should be able to open the Macula Web UI from other PC over the Internet, otherwise, Camio will be unable to connect, and it will not work.)

In other words: Camio can connect to Macula servers only using the HTTP API, which is available at the same URL as the Macula Web interface. So, in order for the system to function correctly, specify the Macula Web interface URL and the HTTP port in the Camio settings under API Client, on the same screen where the token is generated.

Add External Service

The next step is to add Camio **connection** into the Macula server configuration. This integration supports Camio as an external service, with a slight difference: external services like LPR and FR appear in Macula Console automatically while Camio service must be added **manually**. For Macula Enterprise systems, Camio works only with the central server, and not with any of the recording servers directly.

Connect to your Macula server via Macula Console. Open the *Configuration* section and select *External services* on the left. Add a new connection by clicking the *New Camio service* button on the top panel.



The following settings are to be specified here in the *Details* tab:

- **Title**: user-defined service name, which will appear in Macula Console and Macula Monitor
- **Group**: external service group, mandatory*
- **Token**: copy and paste the token generated in the Camio Web interface (as described above)
- **Public URL**: external Macula address (IP/hostname and HTTP port) for the Camio cloud connection**
- **Server**: local IP address of the Macula Professional (this field is ONLY for Macula Professional)

*You will need to create an external service group to put the Camio connection into. The group is necessary for the permission management and also ensures that the service appear in the Macula Monitor application. Without the group, your Camio connection will not be visible in Macula Monitor. If there are multiple Camio connections, you can either create a new group for each one, or put all similar external services into one group. Do not mix different external services by putting them into one group.

**Simply forward your Macula server HTTP port to an external port. Camio services are not available without the Internet connection, as the company only provides cloud services.

When done, click *OK* to save and close the dialog box. Your new Camio connection will appear in the list. To check the service status, go to the Monitoring section in Macula Console and select *External services* on the left.

Add Channels for Analysis

Camio can use HTTP connection with or without authorization, and Macula can work with either option.

1) To set up a connection **without authorization**: Macula has a special built-in *Anonymous user* account for such situations. All you need to do is **enable** the **anonymous user** and then allow him to receive **live video** for the required channel(s).

- Enable the **anonymous user account**: *Configuration* > *Users* > select *anonymous* in the list > *Edit* (or double-click the user in the list) > *Enable* > *OK.*
- Add **permission**: *Configuration* > *Channels* > click target channel > *Edit* (or double-click it in the list) > *Permissions* > select the *anonymous* user account on the right > grant the *View live video* permission.

2) A more secure way is to specify the Macula **user** and use **digest authentication** with Camio. For this, specify the internal Macula **user name** and **password** in the camera details (see below).

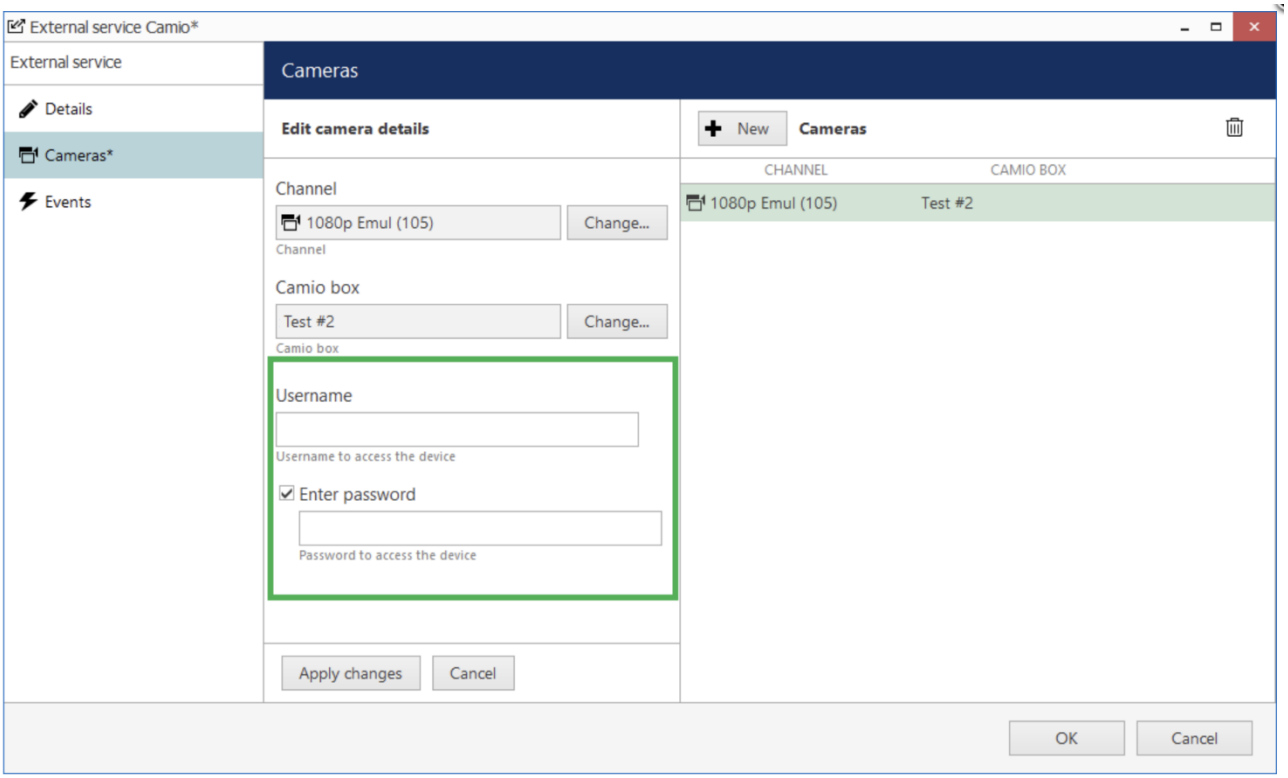
Back in the *Configuration* section > *External services*, double-click your Camio service, or select it and click *Edit* on the upper panel. Select the *Cameras* tab on the left.

Here, click the *+New* button: two fields will appear in the camera details. Basically, you need to bind an existing Macula channel to one of your Camio boxes. To do this, first select the channel, and then specify the Camio box by selecting it from the list. Click OK to save and close the dialog box.

⚠ Camio only supports H.264 RTSP streams. HEVC (H.265) or JPEG streams will have an error in the service Web interface and will not be analyzed.

⚠ Make sure the channel name does **not** have any special characters, especially **backslashes**, otherwise Camio will be unable to parse the channel name.

If the box list appears empty, double-check your Camio connection parameters: the token may be incorrect. If the connection does not work and you know the token is correct, try generating a new token via service Web interface and then pasting the new token into Camio connection in Macula Console.



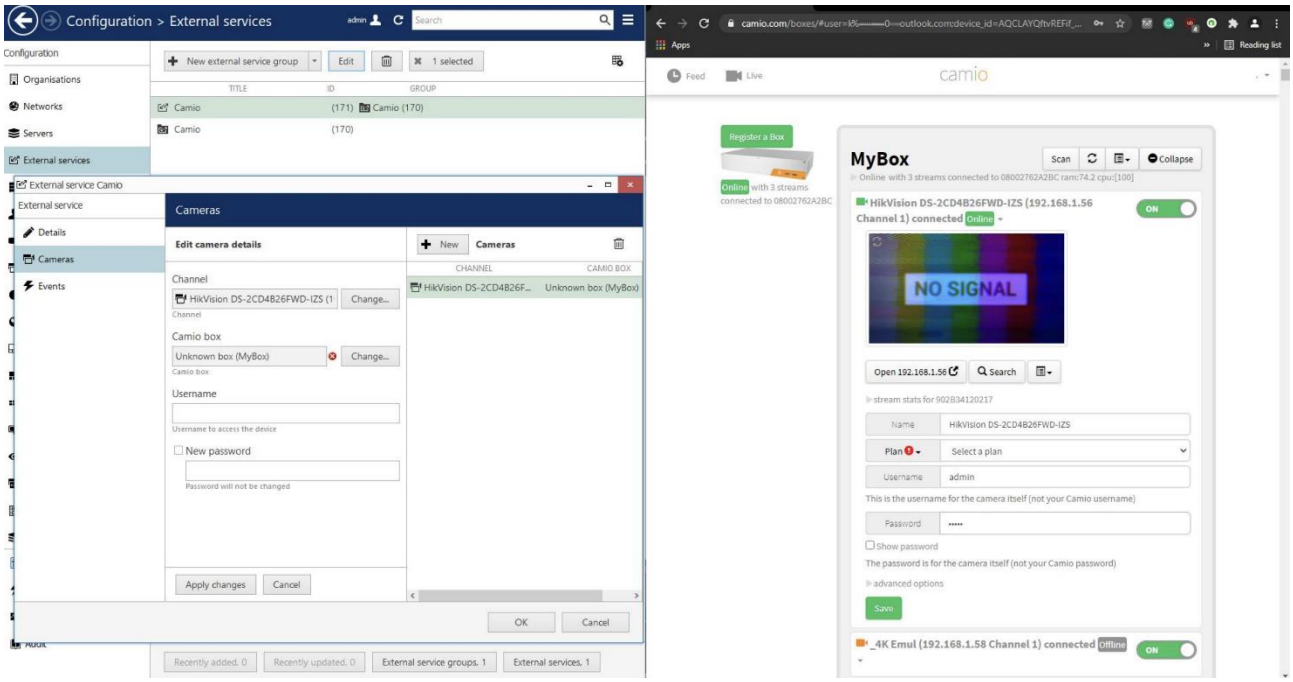
Next, make sure your Camio channel is set to **continuous recording** in Macula Console.

Then, go to the Camio Web interface: your channel will appear **live** in the *Boxes* section. This will happen **automatically**, you do **not** need to add the camera manually in the Web interface.

⚠ If you did everything right, your channel will appear on Camio Web **automatically**. Do not add it in Camio UI!

Macula® Professional Administration Guide

All is left to do is select a **plan** for the target channel (you may have to purchase it from the Camio provider). If the channel is inactive, click the ON/OFF toggle button on the right to activate. The ON position (green) indicates that the channel analysis is activated.



Next to the channel title, you will see its **status**: if the video is coming through, the status should be *Online*. If you disable the channel in Macula Console or there is no actual video, the channel status will appear as *Offline*. Click the *Stream stats* under the live preview to see the video parameters. If something is wrong (e.g., stream codec is not supported), you will see a red exclamation mark: click on it to see more information.

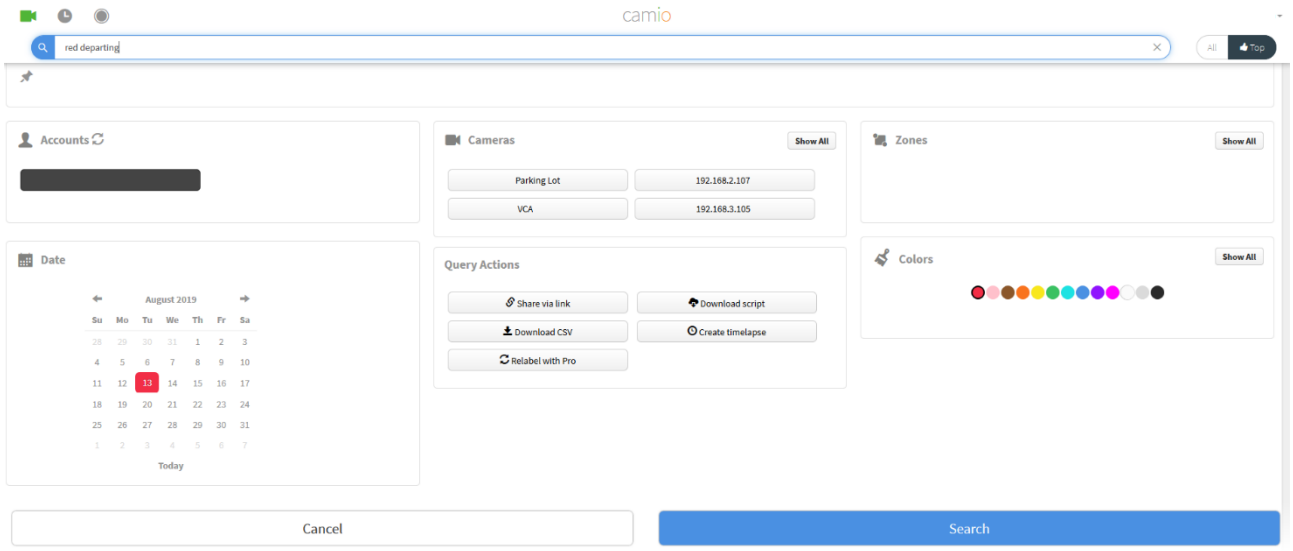
> Some channels may not have the live preview video alongside with the ON/Online status, no errors, and video presence in Macula Console and Macula Monitor. This does not depend on Macula. Usually, this does not affect video analysis and you are able to see the search results. For troubleshooting this and other Web-related issues, kindly contact Camio support.

Camio will now start analyzing your video stream and send the results back to Macula. You can also search the event archive on the service Web.

Web Search

On Camio Web, click the Search button below the channel live preview to enter the search mode. The Web search for your Macula channels works in the same way as for any other channels in Camio.

If Web search does not work, kindly contact Camio technical support.



Macula Monitor Search

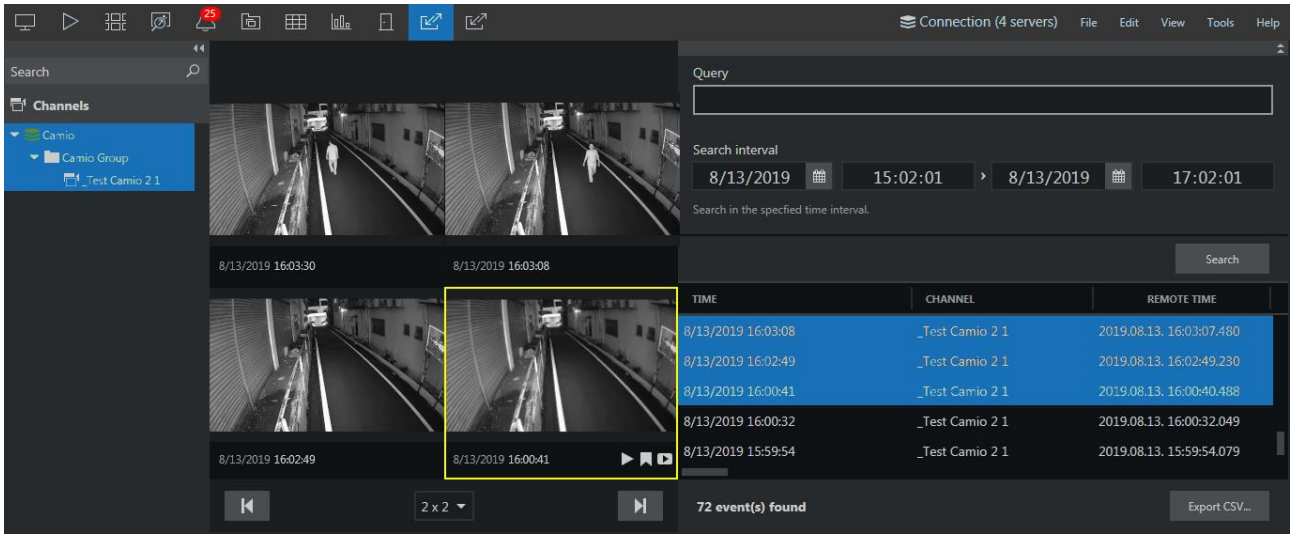
The current integration allows searching the Camio events from the Macula Monitor application.

Open your Macula Monitor application and connect to any Macula server that is linked with Camio. You will see an extra tab on the upper panel named after your Camio external service group.

The search logic is similar to that for other external services:

- in the *Resources* panel on the left, click the + (plus) icon next to the channels you wish to see results from: the **selected** channel(s) will be marked **blue**
- in the right-hand-side panel, enter the **search parameters**:
    - **Query**: text tag to search for, e.g., car, human, truck, also colors
    - Search interval: the time range to be searched for events

When ready, hit *Search*. If there are any **results** for your request, they will appear in the list below and in the grid in the central area. Click any picture to play back the corresponding portion of the video archive. The video clip will be played in a loop.



You can change the grid size by selecting it from the drop-down list below the grid. The available options range from 1x1 and up to 6x6. The single viewport option will provide you will fully functional instant

playback, and the rest of the options (2x2..6x6) are similar to the result preview in *Smart* Search mode., allowing you to add bookmarks, export the result video clips, and switch to the regular playback mode.

Use the arrows |< and >| to load the previous/next portion of the results. You can also do the same by browsing the result list: upon clicking a result from the faraway time range, the target results and its neighbors will be placed onto the preview area.

> ⚠ If the search produces **no results** at all, try the same request on Camio Web: if there are no results on the **Web**, too, kindly contact Camio technical support.

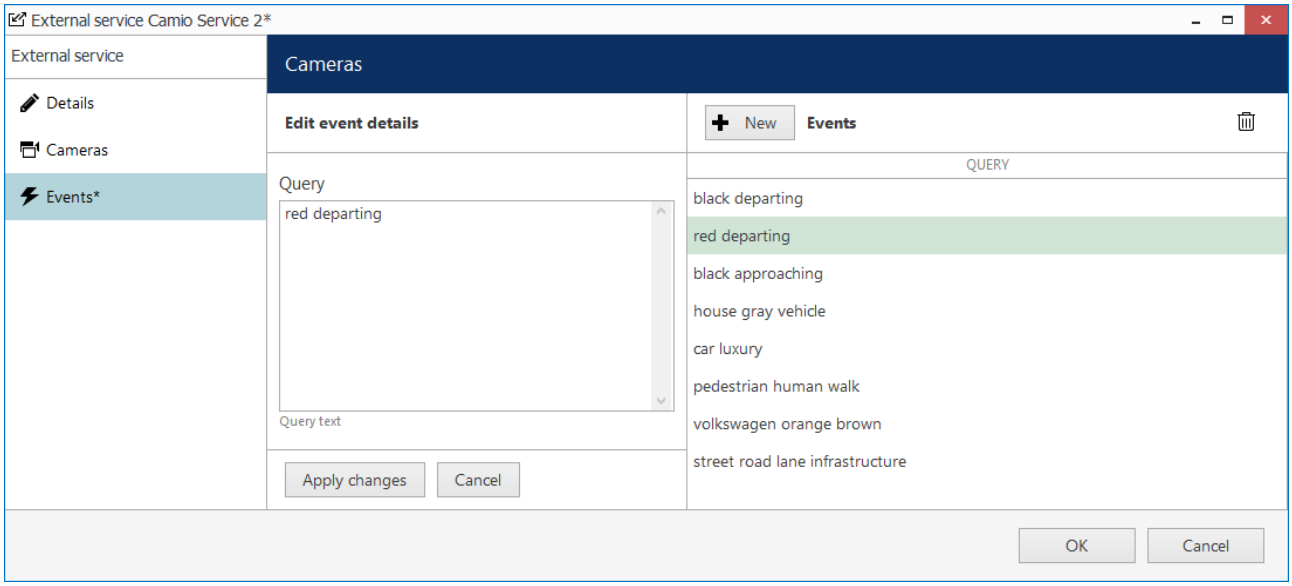
You can also **save** the list of your **search results** by clicking the *Export CSV* button in the bottom right corner.

Events & Actions

Macula E&A Manager provides a powerful mechanism to automate things in your CCTV ecosystem. There are **Camio-specific events** supported by current integration that include reactions to certain keywords. The whole configuration is done via Macula Console. First, you pre-set the **keywords** (tags) of interest in the Camio service settings, and then set up events using these tags in the Event & Action Configurator. These events can be later added to E&A rules, as usual.

Preliminary event setup: in Macula Console, go to the *Configuration* section > *External services* > open your Camio service for editing > switch to the *Events* tab.

Click the + *New* button and enter a keyword or a keyword combination that should trigger the event. Click *Apply changes* to save the current entry, or click cancel to discard the changes. To add another one, click the + *New* button again and repeat. To remove any entry, use the recycle bin button in the upper right corner (also works for several items selected using *CTRL+click*).



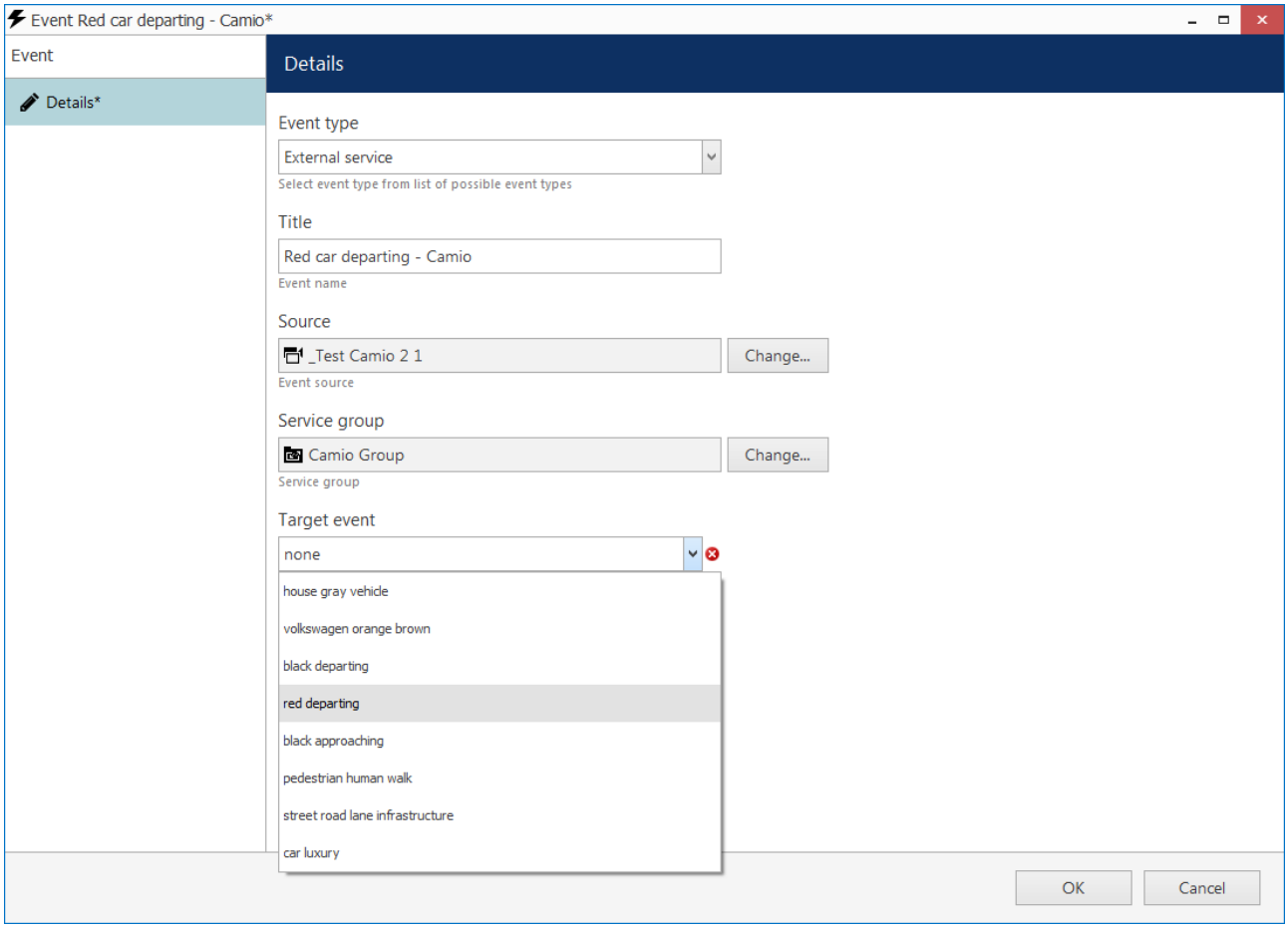
Main setup: switch to the *Events & Actions* section > choose *Events* on the left. Click the + *New* event button on the top panel to bring up the dialog box.

Set event type to *External service* and fill in the parameters:

- **Title**: user-defined event name

- **Source**: video channel that serves as the event source
- **Service group**: select your Camio service group
- **Target event**: choose one of the keyword sets you have specified earlier

If the group list is empty, make sure you have followed the steps above to create both external service and a group for it, and that one field above you have selected a channel that is actually used by that service group. And, if the event list is empty, follow the steps above to add the keywords of interest in the external service settings.



When done, click *OK* to save and close the dialog box. The newly created event will appear in the list, and also in the E&A Configurator (for the server containing the target channel). Now you can use this event for building your automated scenarios.

> Events from Camio service arrive with a **30-60s delay**. This does not depend on the Macula software. Please keep this in mind when configuring rules with Camio events.

11.5 External Metadata

Any external system can send **analytics metadata** to Macula servers. These may be individual cameras with edge analytics, or third-party analytics engines; these can operate independently but it makes sense to send the metadata along with the analyzed video stream to the Macula server. The Macula server can then **overlay** the metadata in both **live and archive** playback, use the data for the Event & Action **rules**, as well as provide the opportunity to **view and search** these events based on the various recognition attributes.

A simple example of such integration is: ANPR camera sending license plate recognition results with the video stream.

At this point, Macula servers support two metadata classes: LPR and FR (license plate and facial recognition).

> This functionality does not require previous integration or API connection of the external service.

Prerequisites

You will need to configure the external analytics source to send the metadata in JSON format over HTTP/HTTPS. The only accepted type is an array of JSON objects named "objects" containing the following properties:

- **x** and **y** - relative coordinates, [0; 1], float
- **width** and **height** - relative object size, [0; 1], float
- **classId** - internal Macula class identifier, string
  - 4 = FR, 17 = LPR
- **id** = object ID, string; used to distinguish between objects and to ensure correct moving object drawing across frames; if not specified and there are multiple objects, they will not be drawn correctly
- **className** - optional user-defined class name, string
- **accuracy** - recognition accuracy, optional, [0; 1], float
- **value** - mandatory parameter, recognition value (plate number or Subject name/surname), string
- **attributes** - optional value attributes delimited by comma, e.g., car color, make, model, year etc., string

If the data are even partially incorrect, the server will return an error. If everything is OK, you should expect the *HTTP/1.1 204 No Content* response.

If **classId** is not equal to 4 or 17, the metadata will be accepted and displayed as overlay but you will be unable to **search** it.

Example

```
{
"objects":[
  {
    "x":0.15,
    "y":0.4,
    "width":0.5,
```

```
    "height":0.6,
    "id":"01",
    "classId":"4",
    "className":"Face",
    "value":"Guy Julius Caesar",
    "accuracy":"0.95"
  },
  {
    "x":0.25,
    "y":0.09,
    "width":0.2,
    "height":0.17,
    "id":"LPR0013",
    "classId":"17",
    "value":"GZ1729",
    "attributes":"silver,Honda,sedan,2007"
  }
]
}
```


Configuration in Macula Console

The Macula servers accept metadata automatically starting from software version 1.21.0.

The metadata are partially stored and displayed in the **archive**, and is represented by a wide semi-transparent line on the archive timeline. Namely, all **bounding boxes** (colorful rectangles) are stored in the video archive. The rest of the data - recognition results, attributes, etc. - are stored in a **separate database**. Without the database, you will only be able to see the data overlay in playback, without event values and properties.

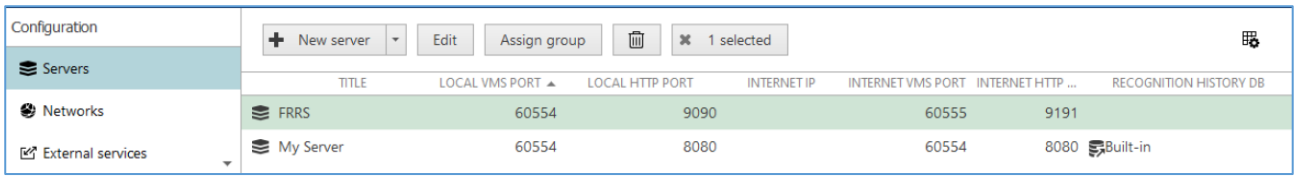
> The external recognition data are stored as follows:
>
> - **bounding boxes**: in the video archive, always
> - events data with **values and attributes**: in a separate database, if the DB is enabled in the server settings

In Macula Console, you can change the **database** that will be used for storing metadata. By default, a built-in database (SQLite) is enabled for all clean installations. To change the database settings (limits etc.), go to the *Configuration* section > choose *Servers* on the left > select *External databases* tab > click *Change* > select a database and click the *Edit* icon.

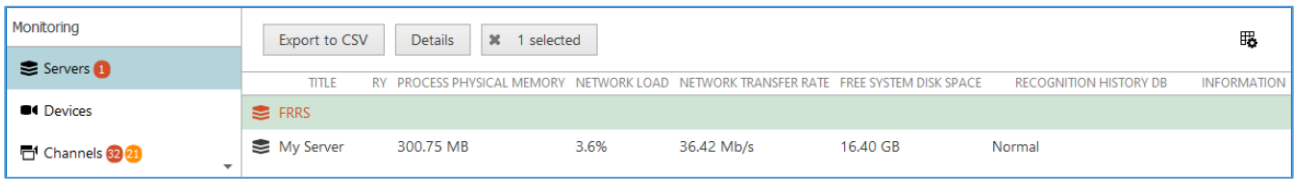
> A built-in VA metadata database is enabled for all **new/clean installations** of any Macula server. For software upgrades, **no database** is selected (*none*) for enhanced compatibility, but you can enable it manually.

To check the DB configuration, in the *Configuration* section > *Servers*, scroll horizontally and check the *Recognition history DB* column. If there is no such column, add it to the displayed columns by editing the item grid using the *Edit columns* button in the upper right corner.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



To verify that the **data are recorded** into the database, switch to the *Monitoring* section > choose *Servers* on the left > check the *Recognition history DB* field. If there is no such column, add it to the displayed column list by configuring the table using the *Edit columns* button in the upper right corner.



External Metadata Display in Macula Monitor

The metadata are displayed as **video overlay** - colorful bounding boxes with parameters - in live and regular/instant playback, as well as in 1x1 view in the dedicated external service tabs. In the middle of the rectangle, object **value** will be displayed. (X) in the corner means that the metadata source is external, and it is accompanied by other parameters (e.g., **className**).

You can perform the **object-based search** in the dedicated tabs (LPR, FR) using the panel on the right-hand-side:

- **Search interval**: start and end of the search period
- **Plate**: enter full or partial value
- **Attributes**: one of more attributes to search for
- **Tag**: Macula tag, if configured

> ⚠ If there is no configured VA database, there will be no dedicated tab and you will be unable to perform value-based search.

Attribute search can be performed in two modes:

- OR: use commas or spaces between attributes to include results that have ANY of the listed attributes
- AND: use + between attributes to display results that have ALL attributes

For example, entering "black sedan" will display all black cars and all sedans, while searching for "black+sedan" will only output black sedans.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

11.6 OPC Client

Macula servers can act as OPC clients and connect to different OPC servers, which communicate with various industrial hardware devices. In this way, Macula servers support thousands of devices from different manufactures without even knowing what those devices and their models are at any particular moment of time: OPC servers take care of that. Once the connection is established, Macula can receive data from OPC servers, compare it to pre-defined values and trigger events based on specific changes in these values; also, Macula can send commands to change the data on the OPC servers, which, in their turn, pass the commands to the hardware devices.

This topic describes how OPC client functionality is configured and used within Macula.

> OPC servers provided by different vendors can be used with Macula. The present document does not cover OPC server installation and configuration, as well as related Windows settings necessary for valid OPC client-server connection setup: these are vendor-specific and can be found in the OPC server documentation.

OPC Functionality

Any Macula server can connect to a third-party OPC server, thus acting as an **OPC client**. These connections are then used within the E&A Configurator to create events and actions based on OPC data (variables): events compare the variable contents to pre-defined values in a specified way; actions change the variable contents to a predefined value.

Communication with OPC servers can be maintained in one of two ways: **synchronous** and **asynchronous**. When in synchronous mode, Macula server polls an OPC server and receives updates with the latest data set as a result; this happens every few seconds. In the asynchronous mode, Macula server "subscribes" to the updates and then waits for a list of updated items from the OPC server.

> Asynchronous reading and writing is a preferred method and is typically more efficient. However, some modifications of Windows security policies and DCOM permissions might be required for this connection mode to work, and these are vendor- and use-case specific. Please follow the guidelines in your OPC server documentation carefully to ensure the operability: there are no settings on the Macula side that could affect your OPC server connection availability.

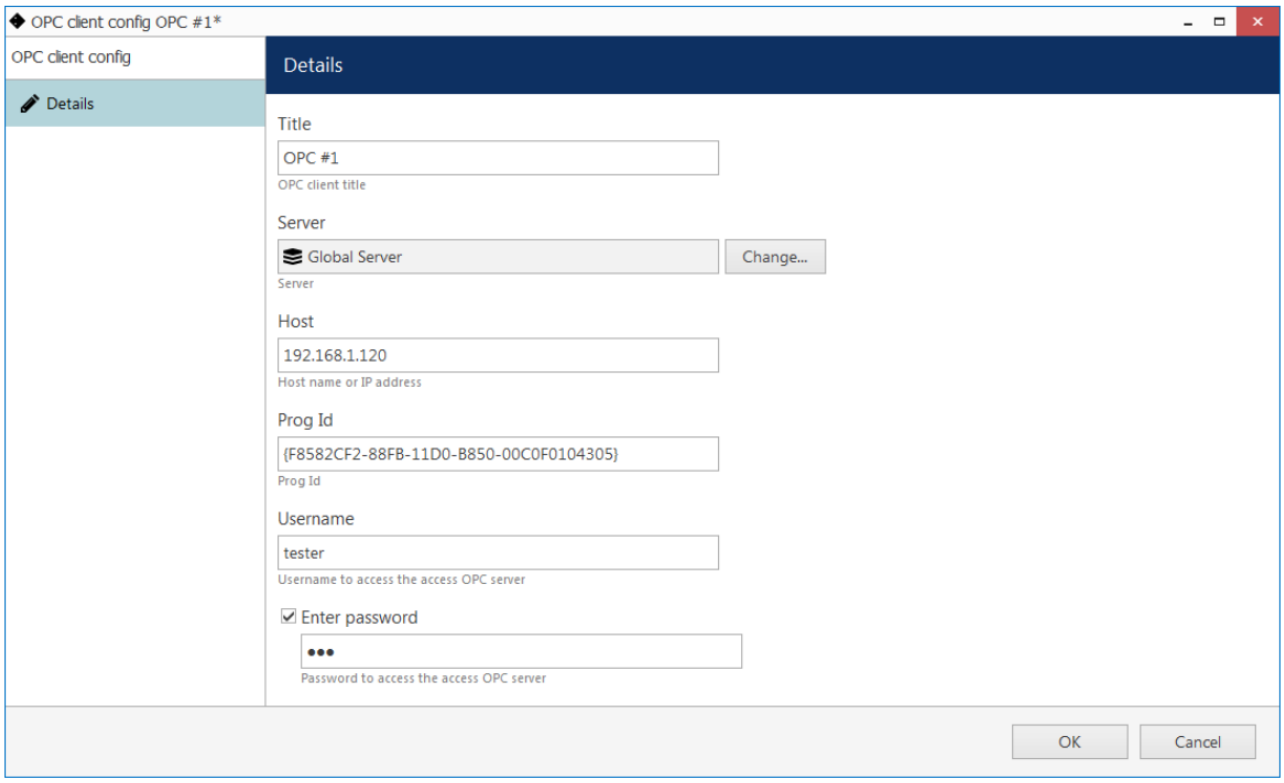
Before getting to OPC setup on the Macula side, install and configure your OPC server with hardware devices, and adjust Windows settings (if required). Configuration instructions below imply that you have done so and a remote OPC server with some data is reachable and operational.

Create and Manage OPC Client

OPC client configurations are located in this section as main OPC integration purpose is event and action scenarios (rules). In your Macula Console, switch to the Events & Actions section and choose OPC in the list on the left.

To add a new configuration, click the + *New OPC client configuration* button in the upper panel.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



The table below details the available settings.

Setting	Description	Default value
Title	User-defined configuration name	[none]
Server*	Macula server that will act as OPC client	[none]
Host	OPC server host name or IP address	[none]
Prog ID**	OPC server program ID, vendor-specific	[none]
Username	User name to connect to the OPC server	[none]
Password	Password to connect to the OPC server	[none]

Fill in the settings and click OK to close the configuration dialog box and save.

⚠ *Once you assign the OPC client configuration to a server, the Server field will become grayed out, meaning that you cannot change this setting anymore. In other words, it is impossible to move an OPC client configuration between servers. To do this, you will need to create a new OPC connection for another server.

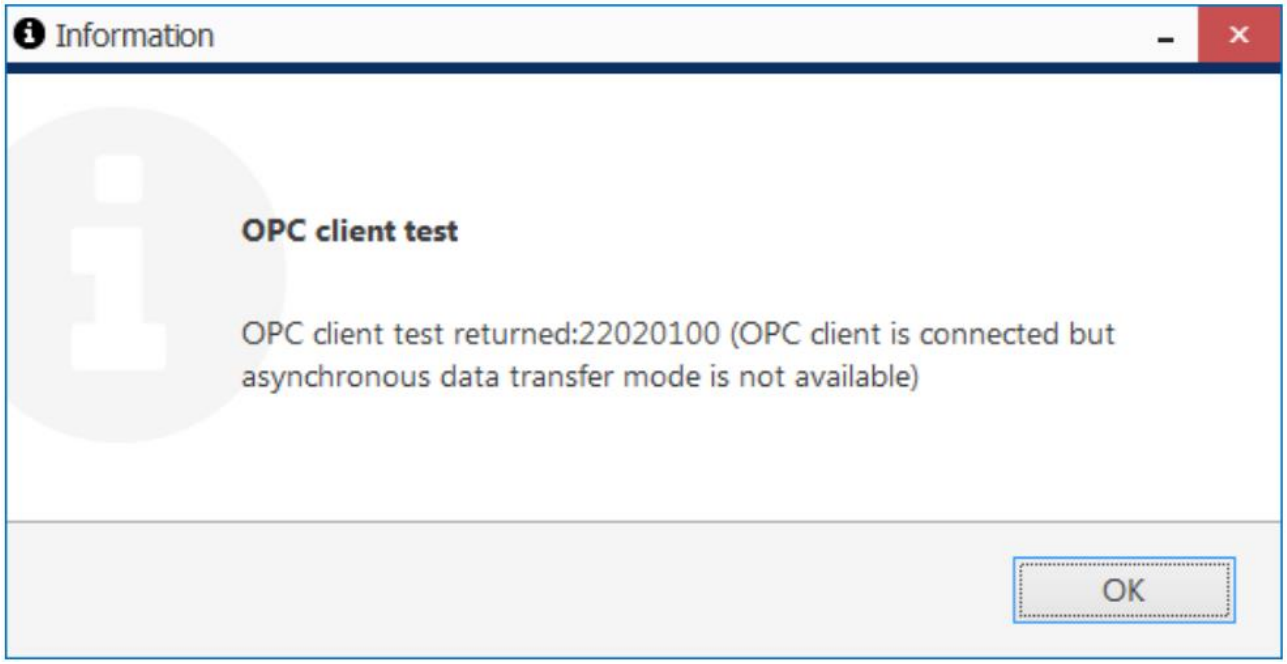
💡 **The **Prog ID** parameter is mandatory and it is supplied by your OPC server. Typically, it is available in the OPC server settings; check your OPC server configuration manual for the exact information.

The newly created profile will appear in the list. Select it and hit the *Test* button on the panel above to **validate** the configuration; the following **responses** may be received:

- *OPC client test passed*: asynchronous connection with the configured OPC server has been successfully established
- *Code 22020100 (asynchronous data mode not available):* connection established successfully but only synchronous mode is available

- *Code -2147023174 (RPC server is unavailable):* connection unavailable due to invalid OPC client settings (e.g., incorrect target host name or IP), Windows settings or connectivity issues
- *Code -2147024809 (parameter is incorrect)*: incorrect OPC client configuration (e.g., no username was entered while expected)
- *Code -2147024891 (access denied)*: OPC server denied connection due to lack of permissions (e.g., invalid user name and/or password was used)
- *Code -2147221164 (class not registered) or code -2147221005 (invalid class string)*: typically, incorrect program ID format or program ID itself

The first two responses indicate successful connection with synchronous or asynchronous read/write mode; other codes mean no connection has been established so it is necessary to review the settings and troubleshoot. Other codes may appear as well in case of miscellaneous Windows configuration and/or connectivity issues.

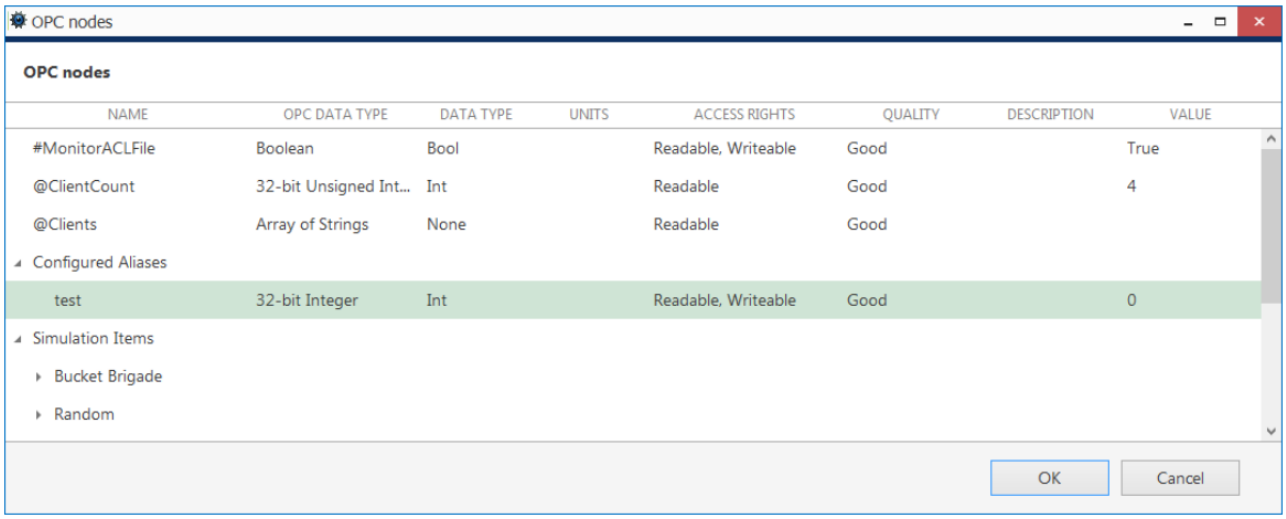


Use the Disable/Enable button on the upper panel to disable the OPC client temporarily and then enable it again: this is useful when OPC server is offline so Macula audit log is not flooded with errors. You can create any number of OPC clients and any number of events and actions based on them.

Events and Actions

Once you have created an OPC server connection, Macula server can retrieve the list of existing data items (nodes) from the OPC server and work with it. All the available nodes, their attributes and their values are listed when you create an event or an action of the *OPC Client type.*

Events allow you to create conditions - react to specific changes in the node values by applying conditional operators: for example, if variable type is boolean, you can check if it is equal to 1 (=true) or 0 (=false). For other variable types, there are other (corresponding) conditional operators.



Actions triggered from Macula servers send write commands to the OPC server, in this way replacing the node value with the pre-defined one. Value of the nodes, which have non-compatible types or do not have the write permission, cannot be changed.

OPC **data types** are converted to standard data types for further use in Macula: for example, both 16-bit and 32-bit integers are converted to the *Int* (integer) type. Some of the data types are not converted (e.g., currency, date&time, miscellaneous arrays) so it is not possible to use them as variables in the events and actions.

Pay attention to the **access rights** of the nodes: for events, it is enough to have the read permission; for actions, the node must be writable, otherwise you will not be able to select it as the target action variable.

For detailed information on the creation of events and actions, please refer to the corresponding topics of this document.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

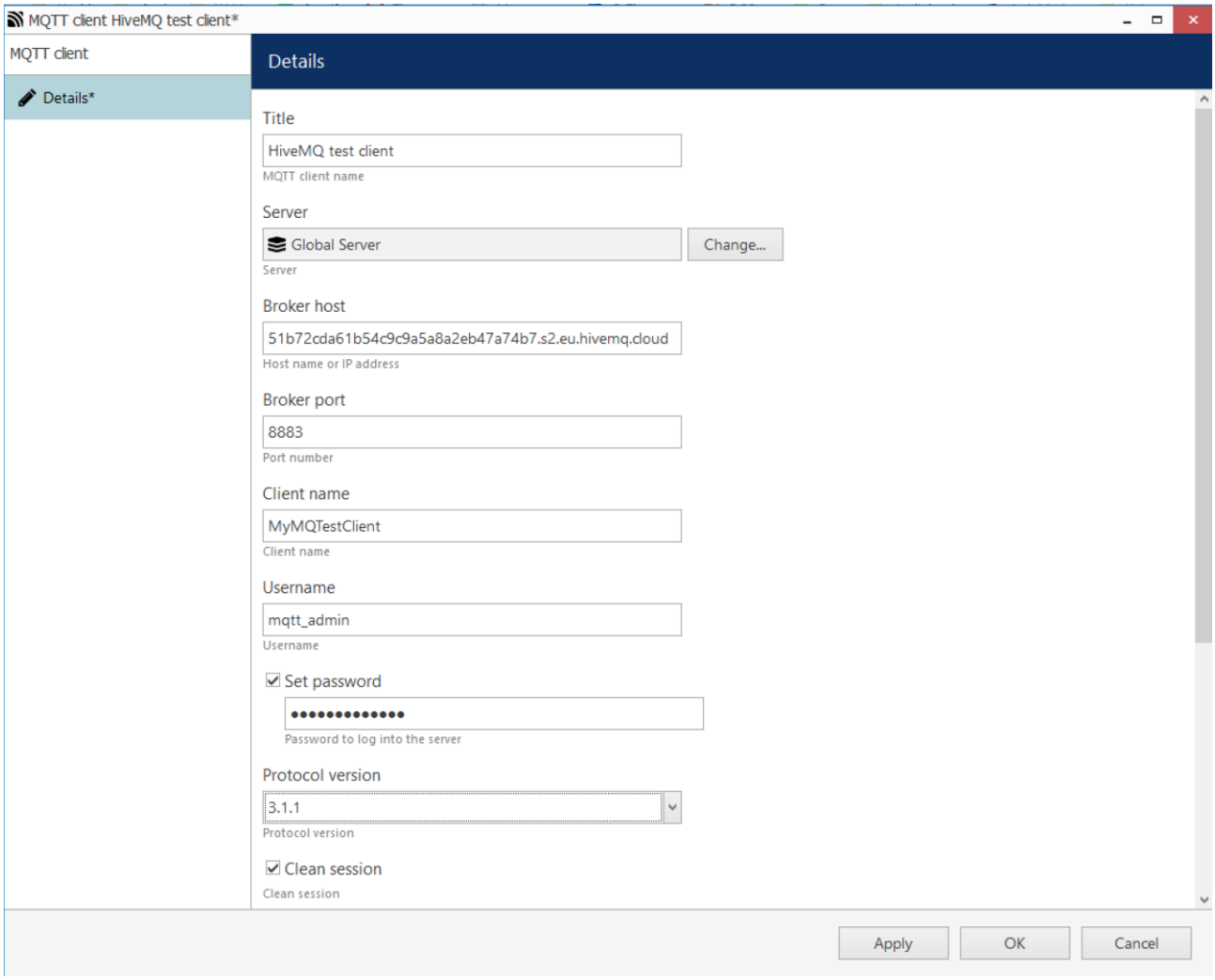
11.7 MQTT Clients

MQTT (MQ Telemetry Transport) is an OASIS standard messaging protocol for the Internet of Things (IoT) that describes how IoT devices (embedded devices, sensors, industrial controllers, etc.) communicate over the Internet. MQTT features clients and brokers; Macula servers have the ability to host MQTT clients, which can connect to existing third-party MQTT brokers, subscribe to topics and publish their own MQTT messages.

On each Macula server, you can create MQTT client(s), and then use it connect to MQTT broker(s) and subscribe to the desired topic or topics, and publish messages. Thus, Macula MQTT clients act as regular MQTT clients, "talking" to the MQTT brokers of your choice. The Macula server installation does not include an MQTT broker, nor does GSF provide such modules as an extra. Before using this functionality in Macula, you need to have a running broker with connected devices.

Create an MQTT Client

To create a new MQTT client in Macula Console, go to the *Configuration* tab and choose *MQTT Clients* on the left. On the upper panel, click the *+ New MQTT Client* button to open up the dialog box.



The available settings are summarized in the table below. Note that the connection settings here must match the allowed connection profile in the MQTT broker configuration. For example, if your broker does not support insecure connections, you must enter relevant secure connection settings matching those on the broker side.

Setting	Description	Default value
Title	User-defined client name that will be used everywhere in Macula Console	[none]
Server	Macula server, to which the MQTT client will be bound. If none are selected, the client will be available on all servers in the Macula Global system	[none]
Broker host	MQTT broker host name or IP address for the client to connect to	[empty]
Broker port	MQTT broker port to be used for client connection	[empty]
Client name	MQTT client name that will be broadcasted. Broker settings may require this field to be set explicitly or allow it to be empty.	[empty]
Username and password	User name and password to authenticate (leave blank if broker allows anonymous connections, allow_anonymous is true)	[empty]
Protocol version	Must be supported by MQTT broker; older version, 3.1.1, is more likely to be supported	3.1.1
Clean session	If enabled, the broker will not queue messages for the Macula server while it is offline	Enabled
Keep alive interval	A ping message will be sent to broker at least at this interval if there is no other traffic occurring	30 seconds
SSL/TLS version	Choose the secure protocol version or leave an insecure connection	none
Certificate	For secure connections, enter the contents of the ca.crt certificate file here (copy from the broker certificate)	[empty]
Enable last will and testament	The message to be sent by broker to other clients in case of a disgraceful disconnect. Specify the message itself, the message topic, QoS*****, and choose whether the message should be retained****** by broker.	Disabled

*****QoS - quality of service - has three levels:

- At most once: no delivery guarantee
- At least once: guarantees that the message is delivered at least once
- Exactly once: highest guarantee, safest and slowest QoS

******The retain flag tells the MQTT broker to always keep the last received message from the client and forward it to every new subscriber. You can retain the LWT message to notify other clients about your MQTT client status.

```
907
908  # listener for mutual authentication
909  listener 8883
910  protocol mqtt
911  require_certificate false
912  allow_anonymous false
913
914  cafile C:\Program Files\mosquitto\certs\ca.crt
915  certfile C:\Program Files\mosquitto\certs\server.crt
916  keyfile C:\Program Files\mosquitto\certs\server.key
917  #tls_version tlsv1.2
918  tls_version tlsv1.3
919
920  password_file C:\Program Files\mosquitto\passwords
921  #per_listener_settings false
922
923
924  #acl_file C:\Program Files\mosquitto\my_acl.acl
925
```

After entering the MQTT client configuration, click *OK* to save and close the dialog box. The newly created client configuration will appear in the list. However, the actual MQTT client will **not** be created not to waste the systems resources: Macula server will create the MQTT client after you use it in an event rule.

> The MQTT Client will only appear in the Monitoring section when there exists a related active (enabled) rule involving an event or an action bound to that client.

Use MQTT Client to Trigger Events

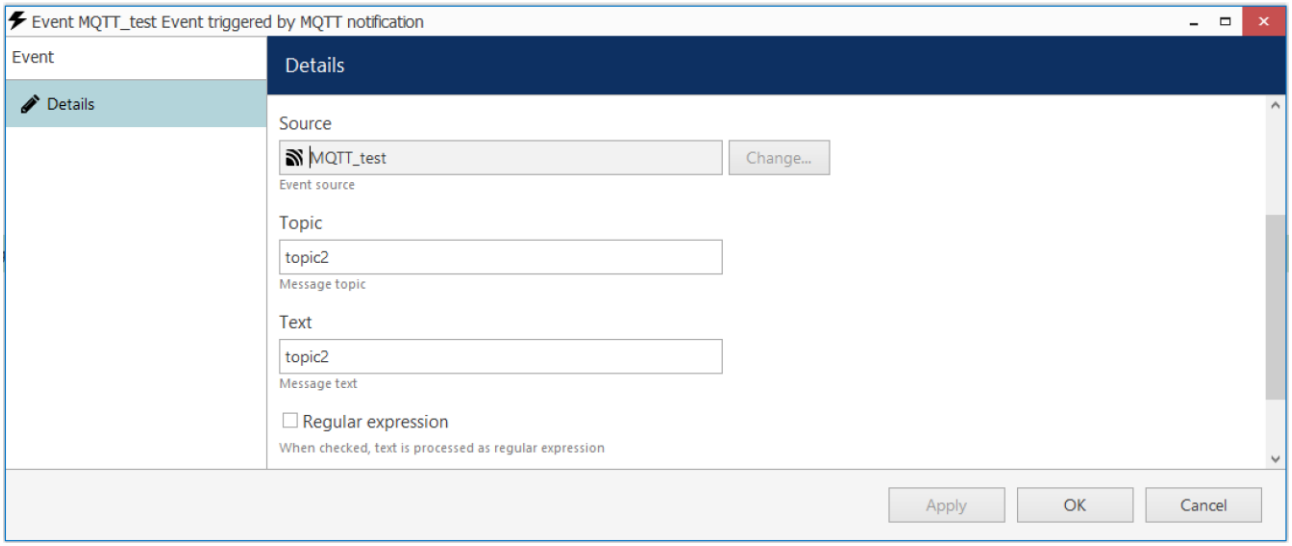
Once you have created one or more MQTT clients, you can use them to subscribe and publish messages to the topics of your choice. For each topic of interest, you need to create one event or action and choose the previously created MQTT client as agent.

To create a new event: in the *Events&Actions* section of Macula Console, under *Events*, add a new event and set its type to *Event triggered by MQTT notification*. Fill in the settings as you would do for your usual MQTT client when subscribing to other clients' messages:

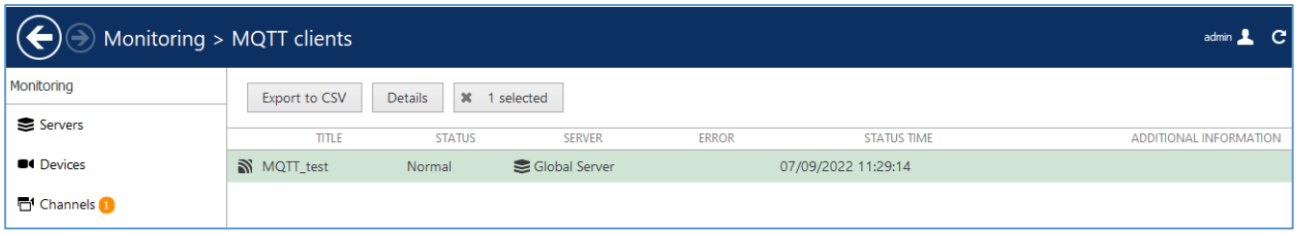
Available settings:

- **Type:** Event triggered by MQTT notification
- **Title**: event name that will appear in the E&A Configurator, corresponds to the macro {EVENT_TITLE}
- **Source**: MQTT client that will subscribe to the current topic and act as event source. Leave empty if you want the event to be visible for all existing MQTT clients
- **Topic**: MQTT topic to subscribe to
- **Text**: incoming message that will trigger the E&A event. If empty, any message will trigger the event. The field cannot be empty if marked as regular expression!
- **Regular expression**: enable this option to enter a regular expression in the Text filed instead of plain text
- **QoS**: required level of quality of service

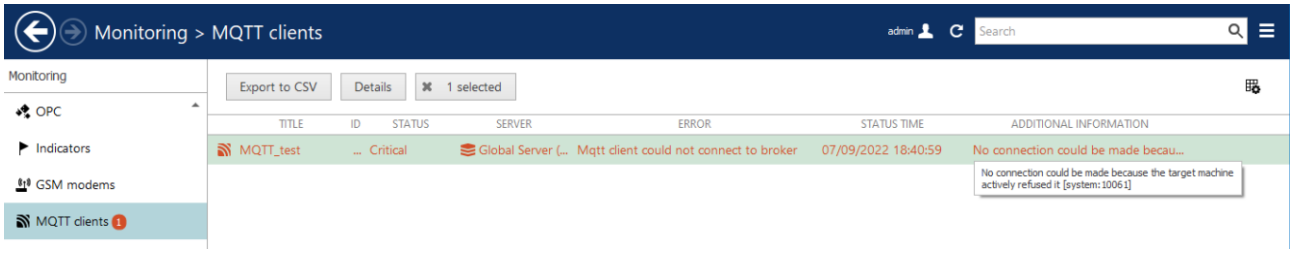
If you don't know what the exact incoming message will be but you know the format, feel free to enter a **regular expression** in the *Text* field.



After you create the event and use it in an active (enabled) rule, the created MQTT client entity will appear in the *Monitoring* section of Macula Console under *MQTT Clients*.



If the MQTT client configuration is invalid, the broker is not running/available, or there are other issues, you will see the corresponding error in the *Monitoring* section of Macula Console. For example, if the broker connection settings are incorrect, the MQTT client status will state that it cannot connect to the broker.



You will also see a relevant message in the *Audit log*, in the *Server* section.

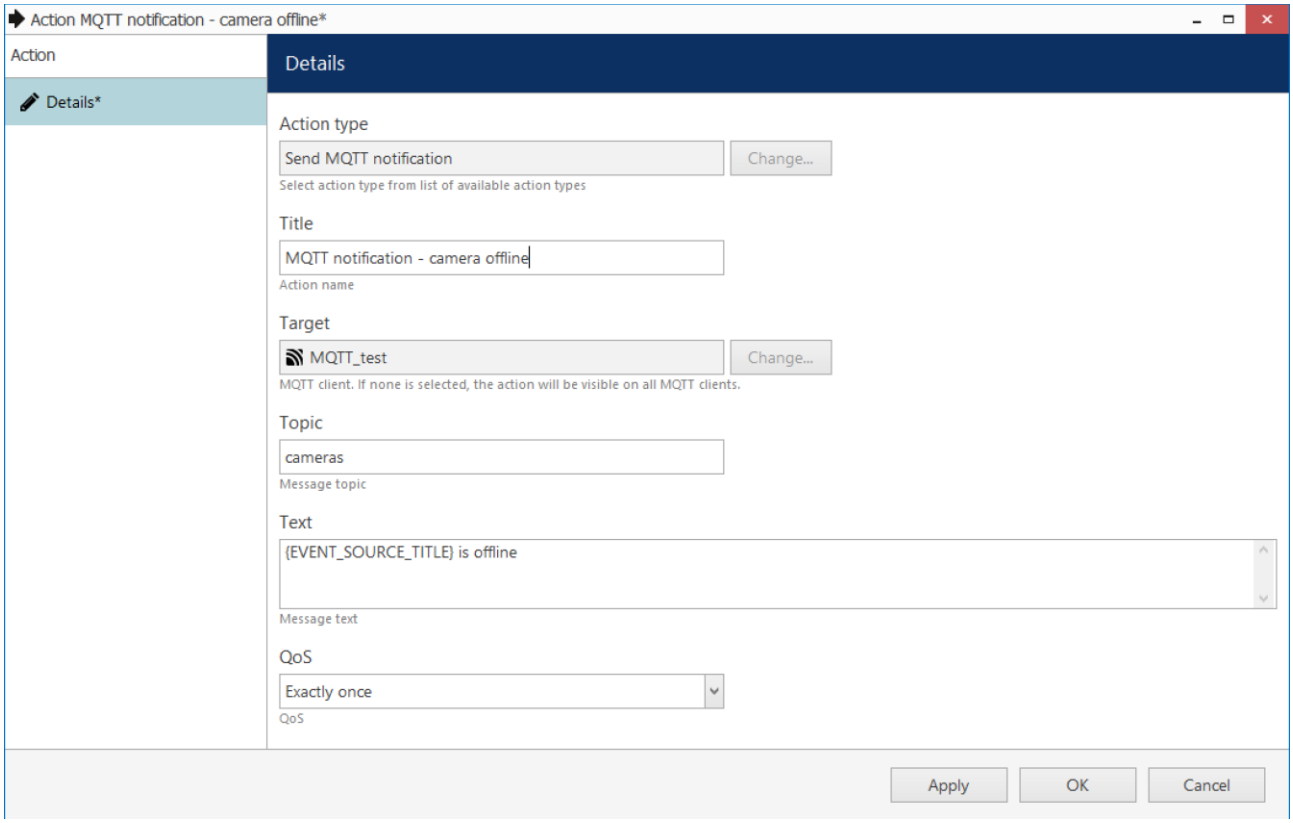
Send MQTT Messages

If you wish to send MQTT messages to for other MQTT clients in your system, all you need to do is create an action of the corresponding type in the Event & Action Configurator, and then use it in a rule.

Macula® Professional Administration Guide

To create a new action in Macula Console, choose *Actions* in the *Events&Actions* section, then click the + *New action* button on the upper panel. Fill in the settings:

- **Action type**: Send MQTT notification
- **Title**: action name that will appear in the E&A Configurator, corresponds to the macro {ACTION_TITLE}
- **Target**: MQTT client pre-configured on the current server; leave empty for the action to be available for all MQTT clients
- **Topic**: MQTT topic
- **Text**: MQTT message text to be published (right-click to insert macros)
- **QoS**: required level of the MQTT quality of service



Click *OK* to save and close the dialog box; the newly created action will appear in the action list. In the E&A Configurator, the action will appear in the right-hand column, under the MQTT client defined as the action target. If you have not specified the client, the action will appear for every existing and new MQTT clients in your Macula Console configuration.

11.8 Modbus

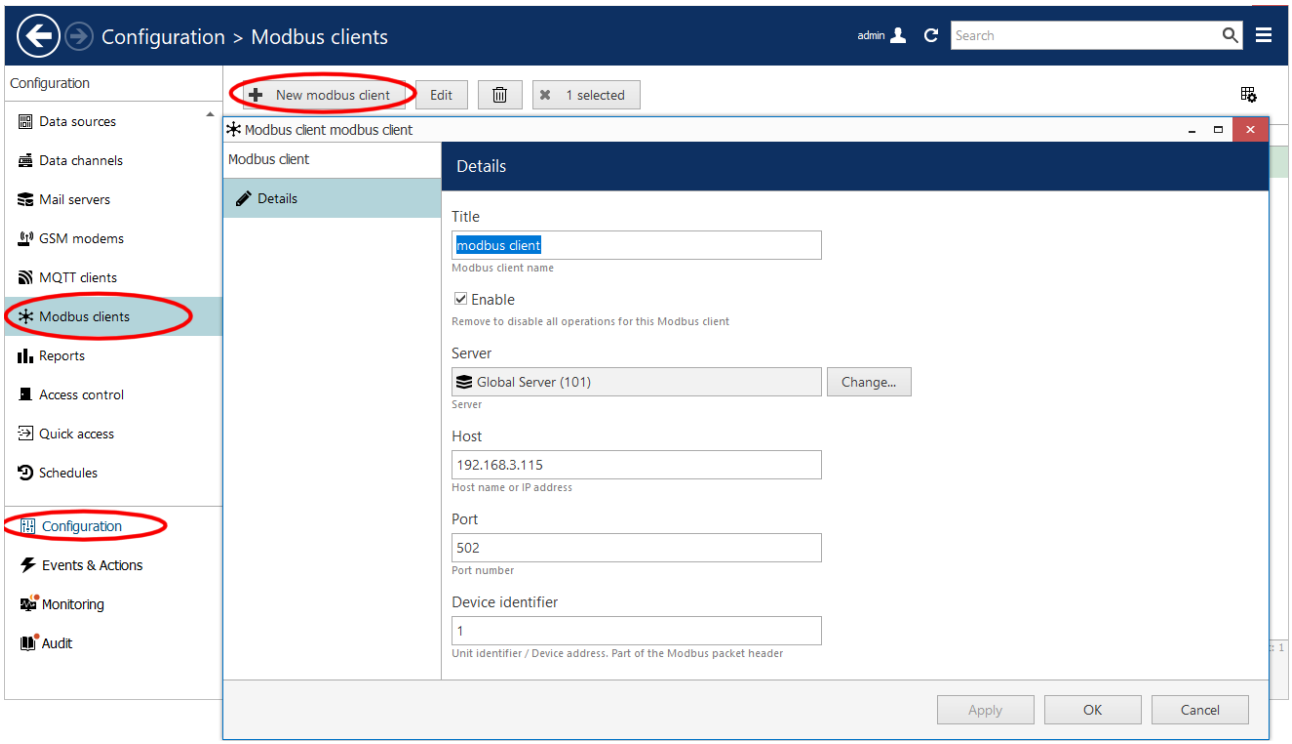
Introduction

Modbus, or MODBUS, is a client/server data communications protocol in the OSI model's application layer. This protocol allows DI/DO devices to connect to the Macula and create *Actions* based on the device Input.

Modbus setup

To set up a device, you need to go to:

1. *Configuration -> Modbus clients*
2. Click the + *New Modbus client* button at the top of the *Modbus clients* subsection. This action will bring a new pop-up window.
3. Fill the *Title* input field with a meaningful name, select the *Server* the device is connected to, and provide the *Device IP address* in the *Host* input field
4. You must also know what port the device uses.
5. If you need to provide a **Unit identifier/slave address**, you can fill out the *Device identifier* field; otherwise, leave it value 0.
6. Confirm your setup with the *Apply* and *OK* buttons.

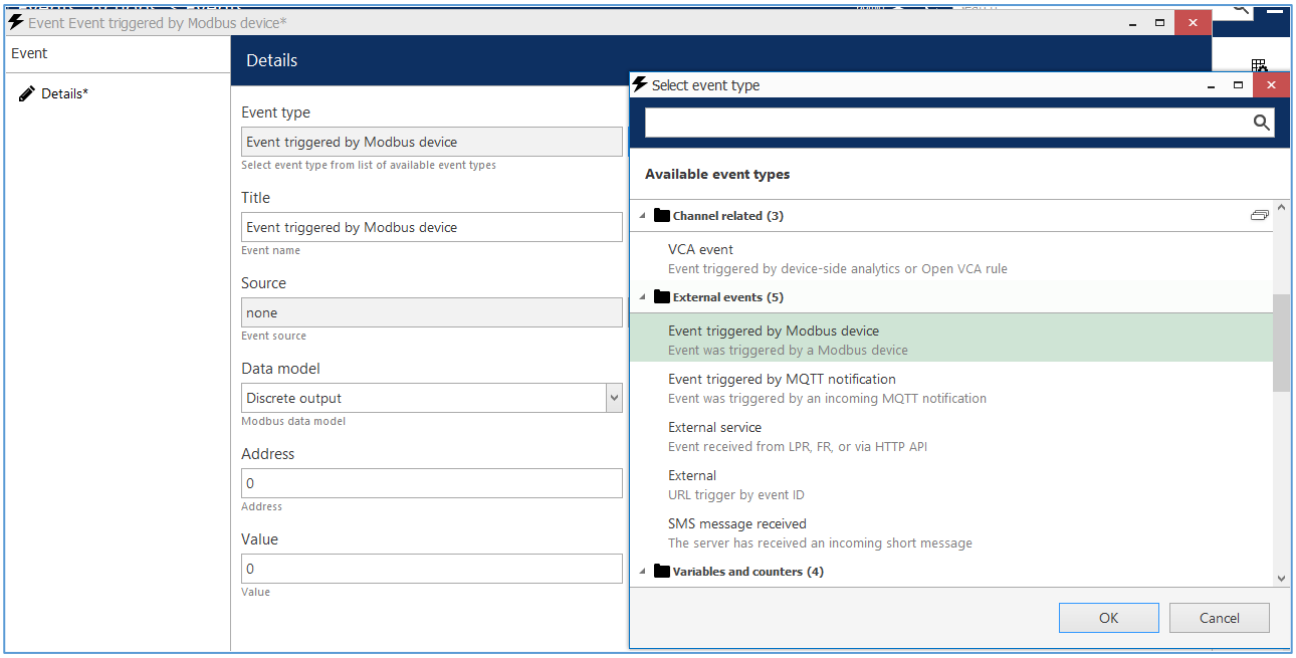


Modbus event setup

After adding the device, you can create events and actions based on the device's DI/DO signals.

1. To create an *Event*, go to the *Events &Actions -> Events*.
2. Click on the + *New event* button at the top of the *Events* subsection.

3. You will find the Modbus device events under *External events -> Event triggered by Modbus device*. Please select it and press the *OK* button.
4. Fill in the *Title* input field with a meaningful name.
5. Click the *Change...* button in front of the *Source* field and select your connected device.
6. Select *Discrete input* from the *Data model* dropdown menu.
7. The *Address* field allows configuring which particular input will trigger the event.
8. The *Value* field allows configuring the state of the contact. Allowed values for the DI/DO is 0 or 1.
9. Confirm your setup with the *Apply* and *OK* buttons.

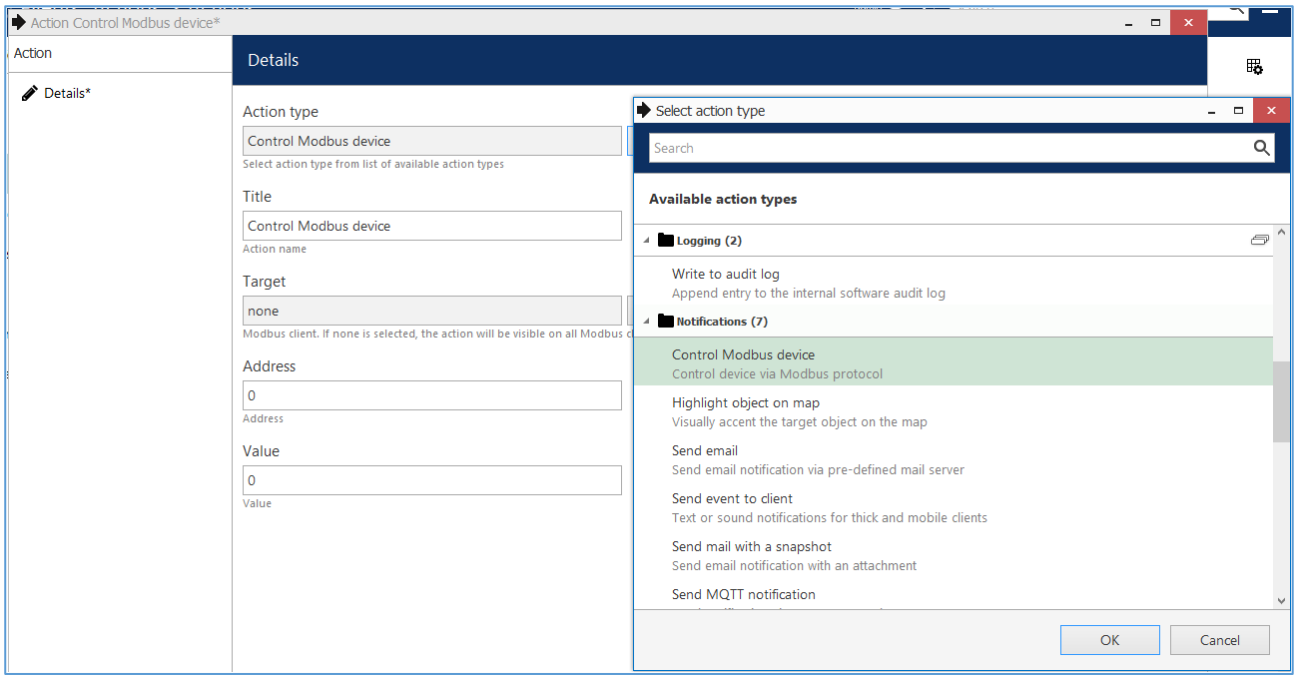


Modbus action setup

To complete the Modbus device setup, you also need to create an *Action*. To do so, go to:

1. *Events & Actions -> Actions*
2. Click the + *New action* button on the top of the *Actions* subsection
3. Inside the new pop-up window, locate *Notifications -> Control Modbus device* and click the *OK* button
4. Fill in the *Title* field with the meaningful name
5. Select your device as the target device inside the *Target* input field.
6. The *Address* field allows you to set a device particular DO contact.
7. The *Value* field allows to set the value that will be sent to the selected address. Available values: 0-1.

Macula® Professional Administration Guide



Now, you are ready to implement rules for the Modbus device.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

12 Health Monitoring

Macula provides **health monitoring data** for servers, devices and channels, stream recording, as well as **live status** of connected user sessions and other resource information, including external services. In the *Archive statistics section*, it is possible to view the stream details and also **un-protect** footage that has been locked via Macula Monitor application.

To access live reports in Macula Console, choose the *Monitoring* section in the bottom-left-hand panel and switch between components using the menu on the left. Use the *Search* field in the upper-right-hand menu to filter the records; press the *Refresh* button or **F5** on your keyboard to **reload** the item list. The statistics are not refreshed automatically, so do not forget to reload the list tin order to obtain the most recent information.

The contents of any subsection in *Monitoring* can be exported in **CSV** (comma-separated value) format using the button on the upper panel.

The *Details* button (available for some of the sections) on the top panel allows you to view **detailed information about important events** related to the target resource. For example, you can view the list of recent connection and VCA license errors for every channel. The details are discarded after each server reboot.

Each section here contains a number of **columns** with miscellaneous information. Not all of them are available by default; to modify the displayed details and their layout, use the grid icon in the upper right corner: an additional configuration window will pop up. You can hide the fields you do not need, and also freeze the leftmost columns for convenient horizontal scrolling. Hidden fields cannot be used for search or sorting.

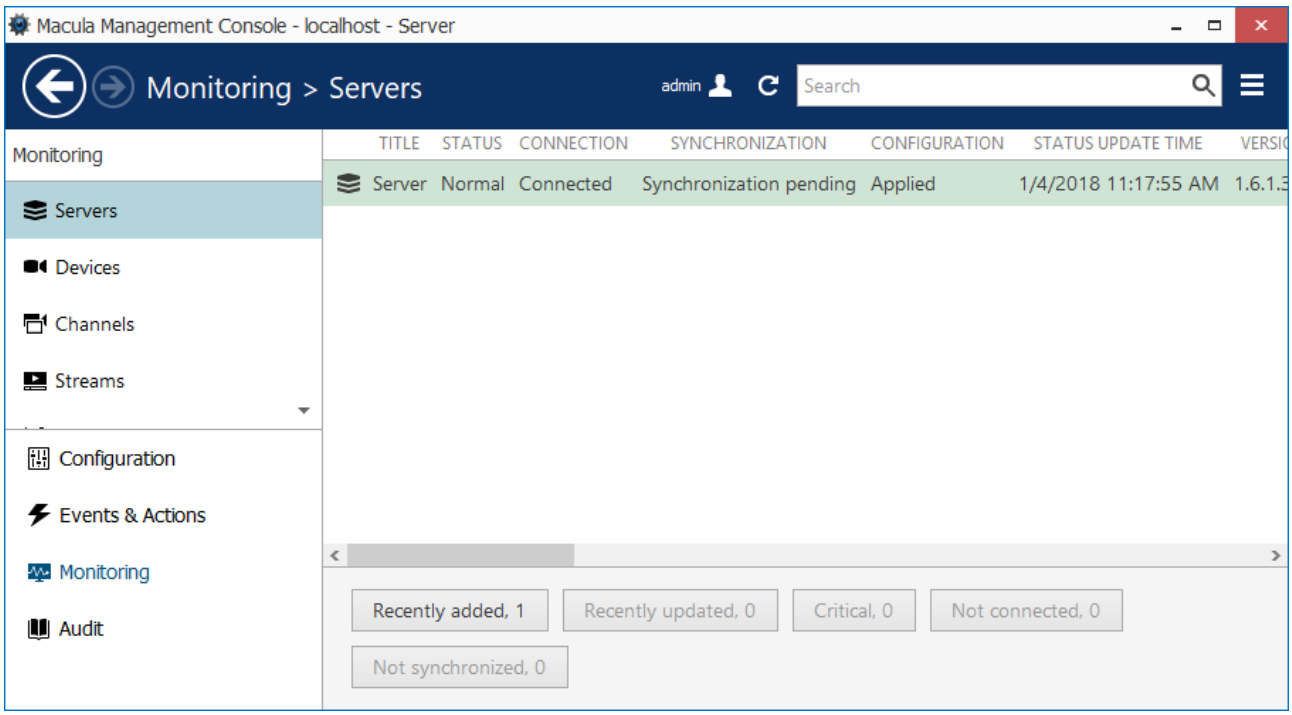
All information written in plain black is informative. When things go wrong, there are two levels of errors here: **critical** and **warning**. Critical errors are marked red; those usually indicate important stuff like missing main stream video, no connection to services etc. Warnings are yellow and are used to highlight minor issues like missing secondary stream, too long GOP period, or not enough space on the disk. You can ignore warnings by right-clicking the selected items and selecting *Ignore > (preference).* This helps if the warning is irrelevant, e.g., if you do not use substreams. Critical errors cannot be ignored as they need to be fixed for correct server operation.

Further in this chapter you will find a brief description of each information field.

Servers

This section includes information about connection and synchronization between the central server and the rest of the servers, as well as each server status and system load.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

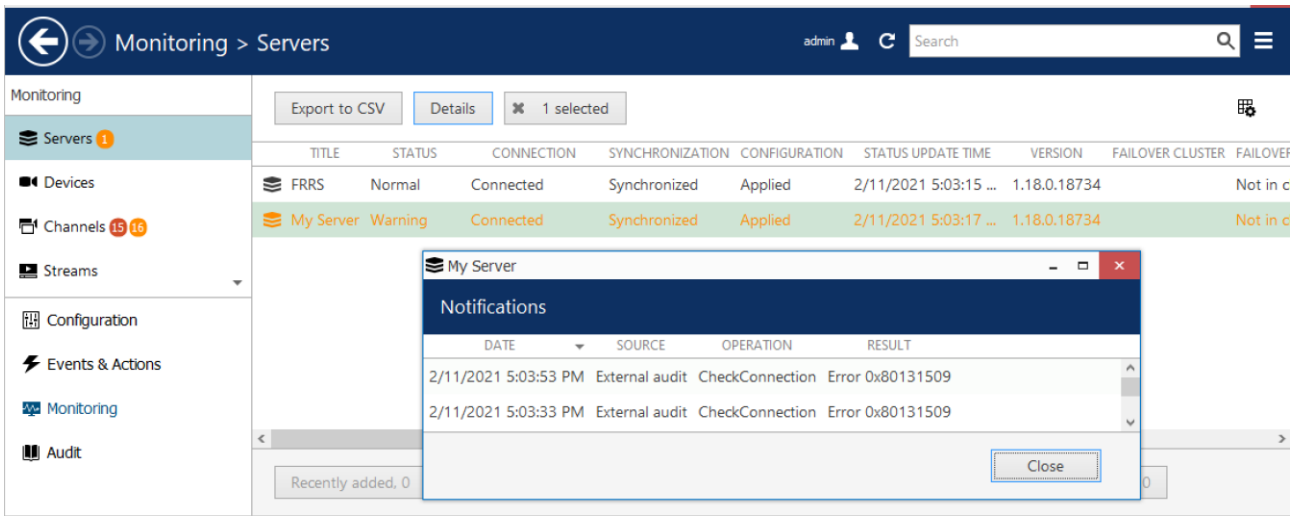


For each server, the following information is displayed:

- **Title**: server name
- **Status**: current server status (*Critical* status, indicating an unreachable or otherwise "bad" server, is also marked with red with the corresponding error description in the *Synchronization* column)
- **Connection**: connectivity status
- **Synchronization**: configuration and audit sync status, including errors (if present)
- **Configuration**: indicates if the central server has successfully applied current configuration to the connected server
- **Status update time**: last sync/connection attempt timestamp
- **Version**: server software version (version differences may cause sync issues!)
- **Failover cluster**: failover cluster name, if applicable
- **Failover status**: if applicable
    - *Not in cluster*: target server is not a part of any failover cluster (may be a mirror server, the central server itself, or a recording server not belonging to any clusters)
    - *Normal*: target server is a part of a failover cluster
    - *Unknown*: undefined; this status may appear in case of incompatible database version or corrupt configuration
- **Failover server**: current failover node that is acting instead of the target server; if none, server is operating on its own (for regular recording servers only)
- **Failover configuration**: original recording server configuration assigned to the target failover node; if none, failover node is idle (only for failover servers)
- **Connected/disconnected** time: status change timestamp
- **Configuration load duration**: how long it took for the server to load the configuration on startup
- **CPU load**: CPU utilization of the target server, %
- **Process uptime**: amount of time elapsed since the last service (re-)start, DD.HH:MM:ss
- **Process CPU load**: CPU load from Macula service on the target server, %
- **Memory load**: current memory utilization of the target server, %
- **Total physical memory**: amount of RAM installed on the target server, GBytes

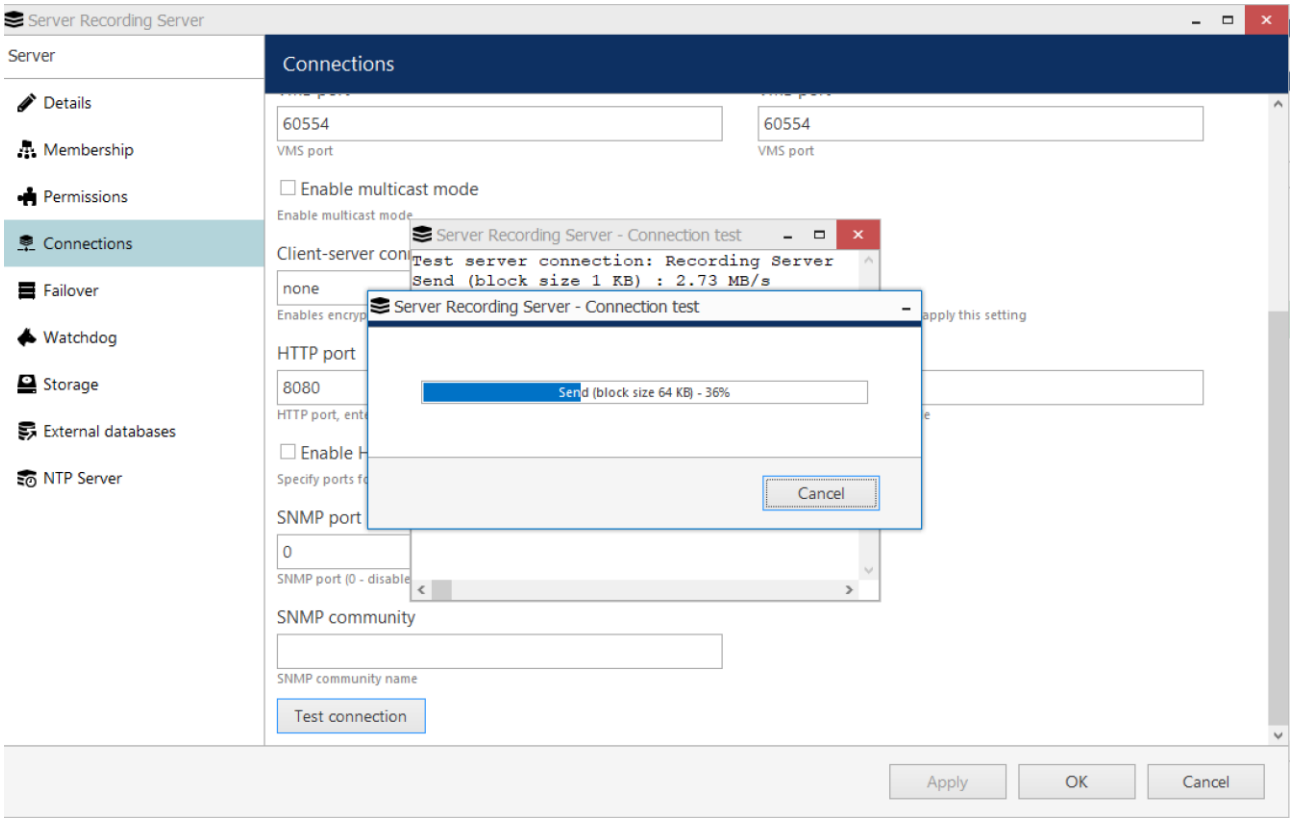
- **Available physical memory**: amount of free physical memory on the target server, GBytes
- **Process virtual memory**: amount of virtual memory used by Macula service, MBytes
- **Process physical memory**: amount of physical memory used by Macula service, MBytes
- **Network load**: maximum network interface load of the target server (i.e., if the server has multiple interfaces, utilization of the most loaded one will be shown), %
- **Network transfer rate**: total bandwidth utilization of the target server (if server has multiple interfaces, aggregated bandwidth from all interfaces is displayed), MBytes per second
- **Free system disk space**: total amount of free space left on the disk, where OS is installed (system disk, usually C:)
- **Information**: any additional information, if any, will be displayed here

Machine load statistics are updated every five seconds but are not refreshed automatically when the *Monitoring* section is open; press *F5* on your keyboard to refresh the section contents.



Note that all the columns will be present for all servers but for some server types some fields may be not applicable and will be therefore always empty: e.g., failover related details are not shown for the central server and its mirror, as well as for the recording servers that are outside failover clusters.

To verify the connection quality between Macula Global and any Macula Recording Server, go to that server settings in the Configuration tab, choose Connections tab in the server settings, and scroll to the very bottom.



For any Macula Recording Server, you can **test the connection** with the target Macula Recording Server by using the *Test* button in the bottom of this tab. This comes useful when:

- you are adding the server without autodiscovery and helps you avoid issues like port mismatch, but mostly when
- you need to verify the connection quality, resolve synchronization issues, connection drops, or low/unstable speed

The test is performed using different size packets (including large) and helps troubleshoot network issues when the connection can be established and maintained with small packets but larger ones are dropped).

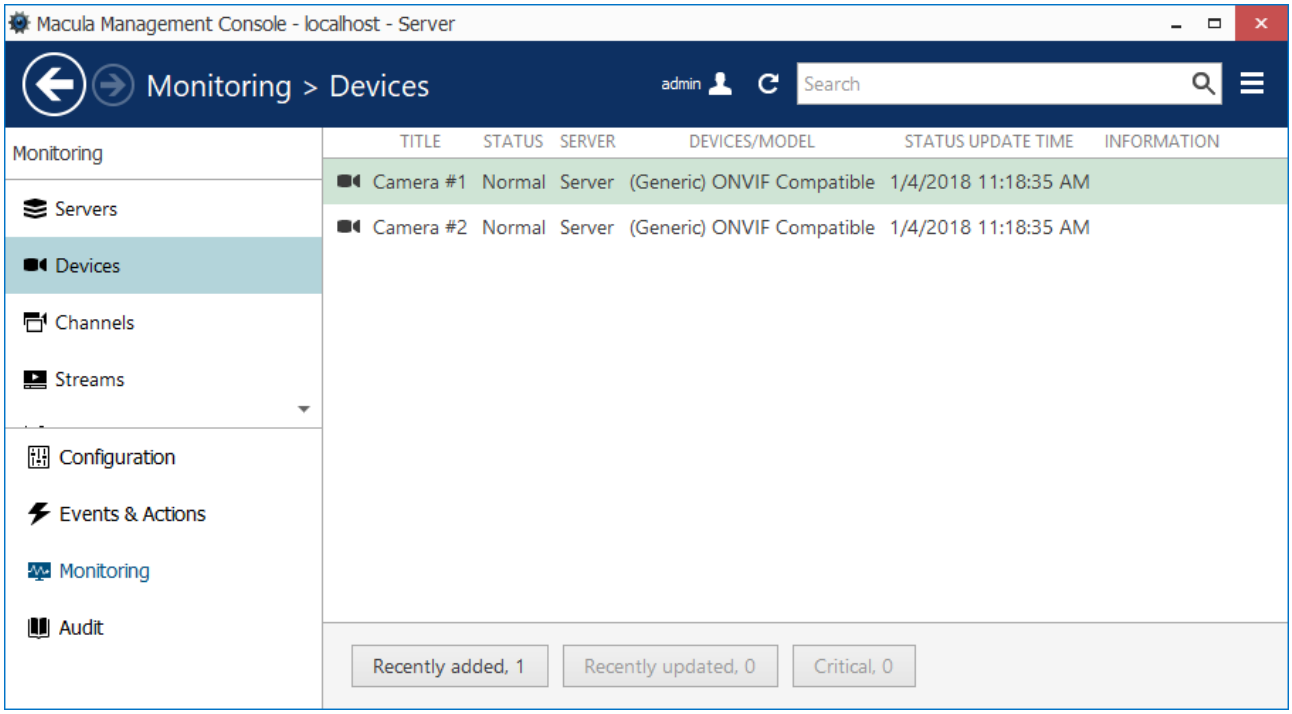
Devices

The device summary provides configuration update status and the time of the last communication between the server and device, as well as shows, to which servers the devices are attached.

The following fields are available:

- **Title**: device name
- **Status**: current device condition
  - *Normal*: the device is functioning properly
  - *Unknown*: the device's channel is disabled, or the device core has not been loaded yet (may appear shortly after server startup)
- **Server**: current server that has this device assigned (may be regular recording server or failover)
- **Devices/model**: device type or model
- **Status update time**: last sync/connection attempt timestamp
- **Information**: additional information, if any, will be displayed here (usually, errors; normally, the field is empty)
- **Host**: device IP address or hostname

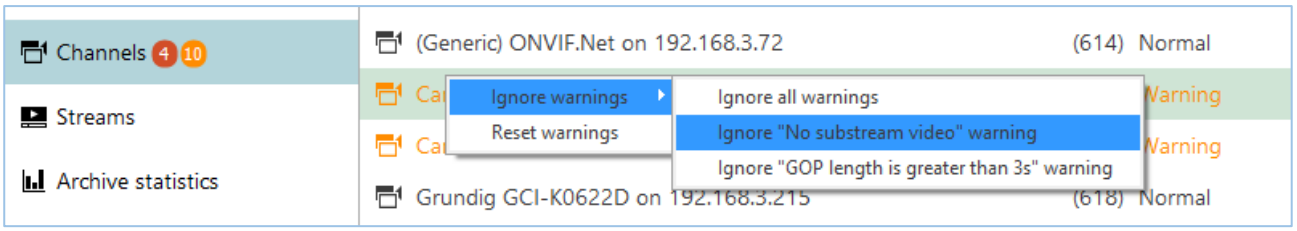
- **Port**: device HTTP/HTTPS port (from device settings, used to exchange service information, not data)



Channels

The channel monitoring section contains details about channel streams. Wherever relevant, there is information about both main and secondary video streams in separate columns.

Channels can have critical errors (red) and/or **warnings** (yellow). Warnings usually appear due to minor issues - e.g., missing substream, too big GOP length etc. You can **ignore** them by right-clicking item(s) and selecting *Ignore warnings > (preference).* If you want the warnings to be shown again, right-click the items and select *Reset warnings*. To **reset** all warnings, go to the Macula Console application settings (main menu > Settings) and select the corresponding option.



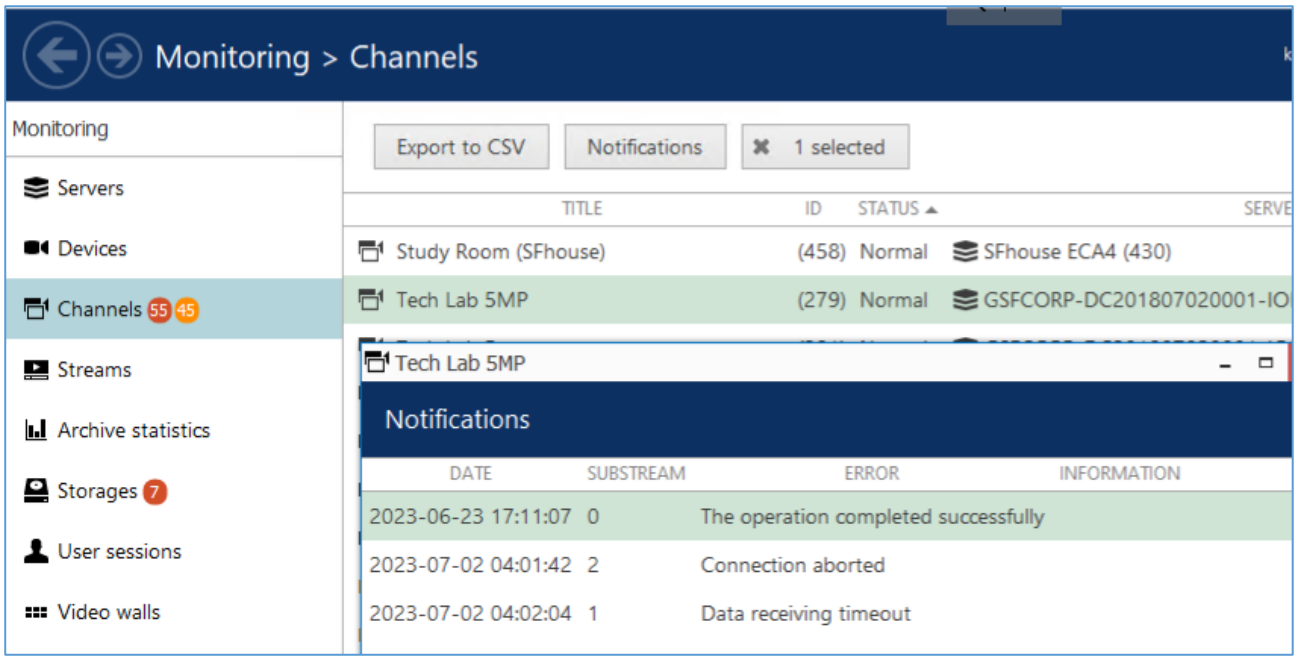
4 critical errors and 10 warnings for channels in the Monitoring section

The Channels section has the following columns in the main area table (some are hidden by default):

- **Title**: channel name
- **Server**: the server currently handling the target channel's device
- **Device**: the name of the underlying hardware piece for the target channel
- **Device model**: underlying device type
- **Organization**: if the channel belongs to an Organization, if will be displayed here
- **Status**: current channel condition (e.g., Disabled means the channel has been turned OFF in the *Channels* section)

- **Status update time**: timestamp of when the channel status was last checked
- **Online**: shows channel uptime in percent compared to the total server run time
- **Video loss duration**: shows if the video stream is not available; if yes, for how long the video stream has been lost
- **Kbit/s**: stream bit rate (Kbits per second), separate columns for the main and secondary streams
- **FPS**: stream frame rate (frames per second), separate columns for the main and secondary streams
- **Resolution**: frame size in pixels, separate columns for the main and secondary streams
- **Codec**: stream compression, for both main and secondary streams, separate columns for the main and secondary streams
- **GOP size**: key frame interval, for both main and secondary streams (only if recording is activated), separate columns for the main and secondary streams
- **Recording**: recording status ON/OFF (activated/not activated)
- **Recording error**: if any
- **Frame cache**: the amount of memory allocated for pre-recording of the target channel (total for all channel streams)
- **Stream storage**: destination storage, for main, secondary, and edge streams
- **Information**: additional information, if any, will be displayed here (usually, errors; normally, the field is empty)
- **Motion detection mode**: currently used motion detection setting (disabled/camera-side/software-side high accuracy mode/software-side high performance mode)
- **IP**: device IP address or hostname
- **Port**: device HTTP/HTTPS port (from device settings, used to exchange service information, not data)
- **Jitter**: frame latency; shows delay (in milliseconds) between expected and actual frame arrival time, separate columns for the main and secondary streams
- **Error**: the latest error related to the channel (same as in *Details*, reset upon server restart)
- **Error date**: the latest error timestamp
- **VA Enabled**: video analytics status
- **VA Detector result**: video analytics response (successful/error)
- **VA Device**: device used for video analytics
- **VA Requested detection rate**: detection frequency interval preset
- **VA Actual detection rate**: actual detection rate
- **VA Average detection time**: average time spent on detection
- **VA Average processing time**: time spent on data processing
- **VA Processed frame count**: how many frames were analyzed
- **VA Skipped frame count**: how many frames were skipped
- **VA Processed frame rate**: how many FPS attached video streams have
- **VA Skipped frame rate**: how many FPS skipped
- **VA Detected frame rate**: actual attached video stream FPS
- **VA Decoder result**: video analytics decoder response
- **VA Decoder device**: video analytics device (if any attached)
- **VA Codec**: what codec is used to decode the attached stream
- **VA Average decoding time**: how much time is spent on video stream decoding

For any channel, you can press the *Notifications* button on the upper panel to see the list of all **channel-related errors**, starting from last the server start. This list is purged upon server restart.

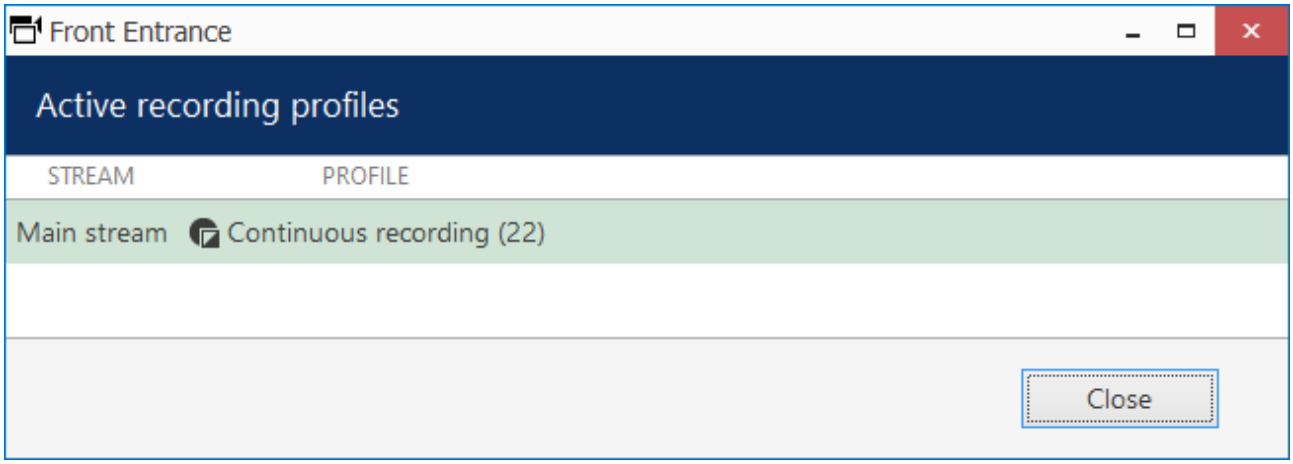


For replication channels, main and secondary stream properties will be shown as zeroes or blank, as there is no actual incoming video stream.

Only channels attached to servers are shown here.

Note that *Not activated* recording status may both mean either that recording is not configured (disabled) or that recording has not been activated according to a schedule. The *Activated* status will appear if at least one of the channel streams is set to be recorded based on any configuration apart from *No recording.*

For any channel, you can also view the currently **active recording profiles** for all its st streams. To do this, press the *Active recording profiles* button in the upper panel. A dialog window will pop up, providing the information about the stream recording configuration. An empty list means no recording configuration is assigned to any of the channel's streams. This feature is useful for verifying if the recording schedule is executed correctly.



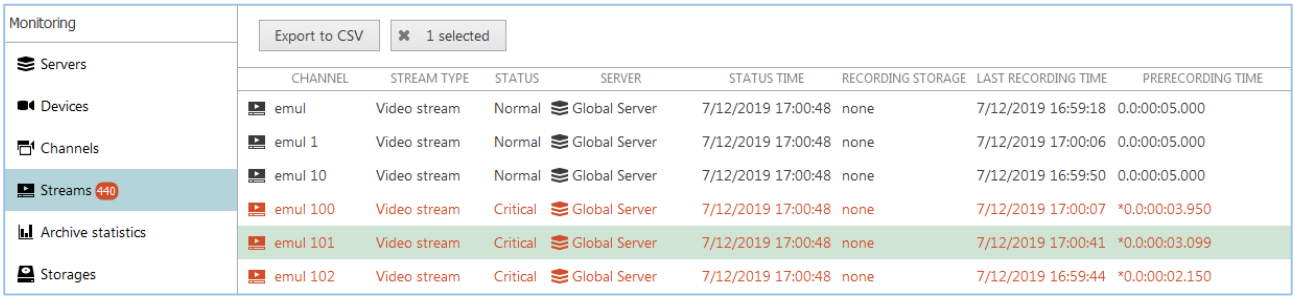
Streams

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

This section displays the properties of **every recorded stream** separately. For example, if a channel has both main and secondary streams with audio activated, there will be three entries. Replication streams are also displayed separately.

- **Channel**: stream source, one of the existing enabled channels
- **Stream type**: video, audio, motion, external data (from data sources), or VCA metadata
- **Status**: current stream condition
- **Server**: originating server
- **Device**: originating device
- **Status time**: last status update timestamp
- **Recording storage**: target storage title
- **Recording directory**: one of the target storages on the corresponding server
- **Last recording time:** timestamp of the last recorded frame (useful for troubleshooting the recording)
- **Prerecording time**: actual number of second held in the pre-recording buffer (may be lower than the setting if not enough memory, or 0 when not required)
- **Information**: additional information, if any, will be displayed here (usually, errors; normally, the field is empty)



Note that the **pre-recording** time here may differ from your pre-recording setting in the recording configuration. Macula server applies smart logic here and traces situations when larger buffer is not necessary, or even preventing the system from normal operation. Thus:

- if the currently used recording profile does not involve any pre-recording (e.g., *Continuous recording*, or event-driven with no defined E&A events), the buffer size will be reduced to 0
- if there is not enough memory for all channels (the server is overloaded), the server will reduce pre-recording buffers; channels with largest frame cache size will have their buffers reduces first pf all
- upon server startup, the buffer size is increased gradually for smoother start

> ⚠ Removed and disabled channels will not be shown under this section: only active recorder tasks are displayed here.

Archive Statistics

Here, you can see **recording statistics** for every channel (all streams and all storages included):

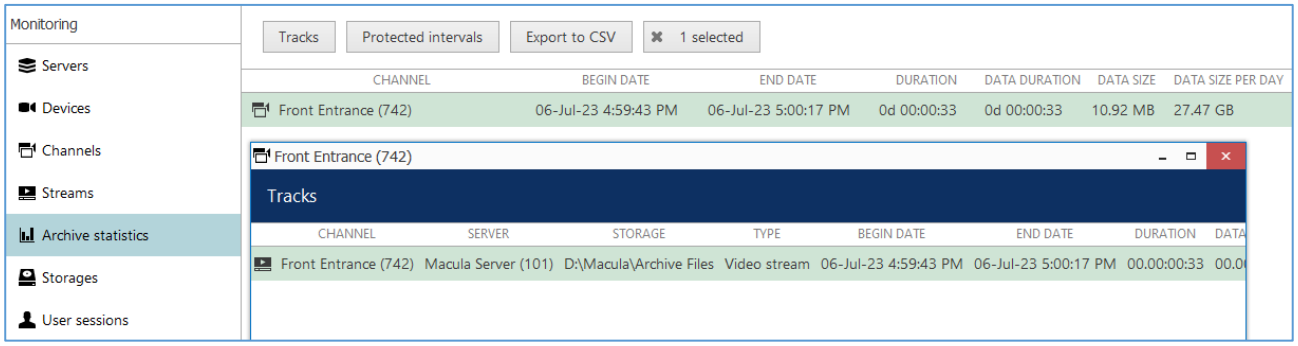
- **Channel**: configured channel title
- **Begin date**: the time of the very **first** recording for the target channel
- **End date**: the time of the very **last** channel's recording
- **Duration**: total archive **duration** for each channel
- **Data size**: total archive **size** per channel, based on the time boundaries mentioned above

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

- **Data size per day**: an estimate of how much space one day's recordings will take (average per day, calculated based on existing archive size)
- **Protected interval**: total duration of the archive, which has been marked as protected, and will not be removed (erased)
- **Protected data size**: total size of the protected archive
- **Server**: the server where the data is recorded (convenient for filtered view based on the server)

Double-click any entry or use the *View* button on the top panel to display **details** for each channel: view the recording statistics per storage and with detailed information on every stream including audio, motion, VCA and external data feeds.

To review and **unlock** the footage that has been **protected** from erasing via Macula Monitor application, select the target channel(s) and click the *Protected intervals* button on the top panel.



From this dialog box, you can **unlock the previously protected** parts of the archive. If these recordings fall under quotas (storage or duration, server wide or individual), they will be erased immediately.

Storages

Statistics, properties and status for each storage unit are displayed here:

- **Title**: storage label, either built-in or user-defined
- **Status**: operation status of the target storage
  - *Normal*: the storage can be used for recording and there are no issues detected
  - *Critical*: the storage cannot be used for recording due to one or more serious errors, check the Information column for description
- **Server**: storage location, i.e., on which server is configured
- **Status update time**: last time the storage status was obtained (use the *F5* button on your keyboard to refresh the list)
- **Path**: storage path on its server of origin
- **Encrypted**: indicates, if the target storage has encryption ON/OFF, or if there are encrypted storages without provided passwords (will be marked red)
- **Free space**: how much free space in gigabytes is left on the disk
- **Free space %**: same but shown as percentage in reference to the total storage size
- **Used space**: the amount of disk taken by all data (including third-party data)
- **Last available time**: the moment of time when the target storage was last available for recording
- **Total space**: entire storage size
- **Information**: additional details, if any (e.g., storage related errors)
- **Disk queue length**: number of read/write requests (local storage only) *

> All storage information is retrieved through the API of the underlying operating system. If you think some of the information may be incorrect, check the same statistics via Windows interface.

*The Disk queue length column is useful for assessing the storage condition. It reflects either the current or the average queue length (whichever is higher) per disk. Generally, 5+ requests per disk indicate a bottleneck in the disk subsystem. 2+ requests per disk for a long period of time may also indicate bottlenecks. For RAID storages, the queue length is summarized, so, for example, for a system with 8 disks the queue length should not exceed 16. A value of 0 means the storage is not overloaded. An absent value (empty) means it cannot be retrieved: the field will be empty for network storages and for unreachable disks (e.g., server offline).

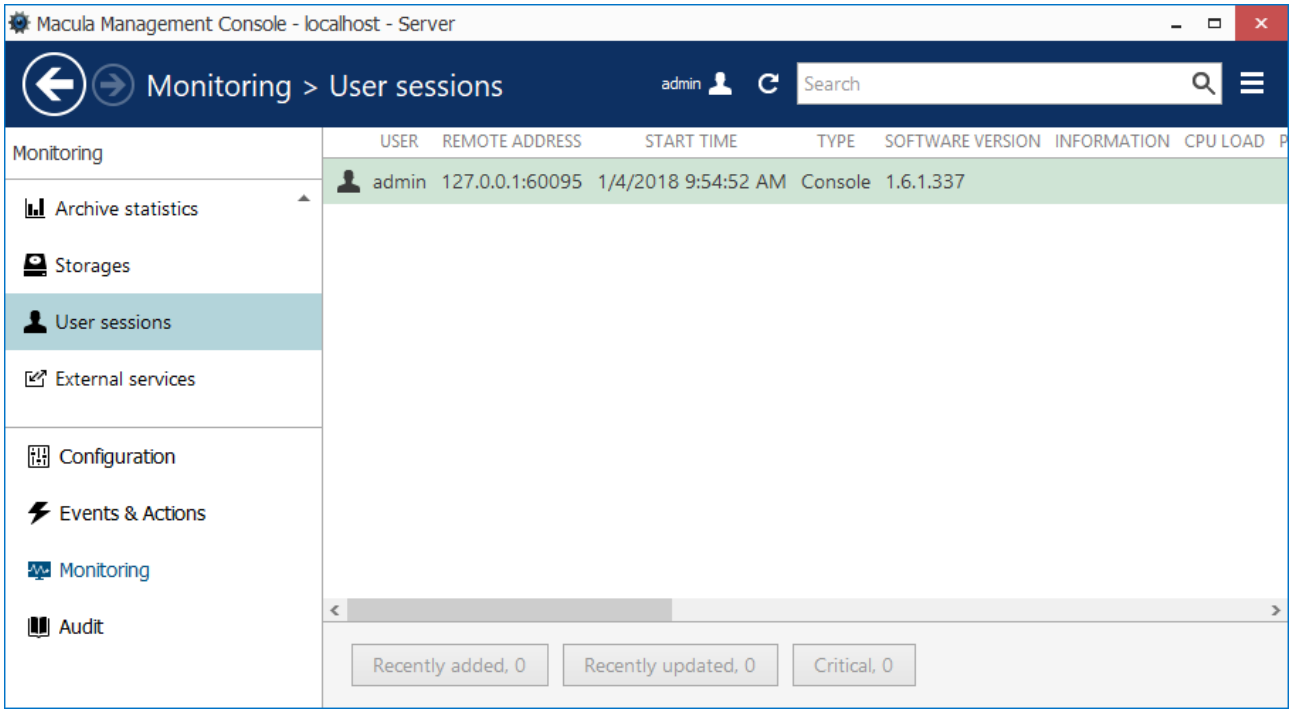
If one or more storages have issues, the corresponding section will have a red circle with the number of detected issues next to the section name. Inaccessible storage units will have no total and free space information.

User Sessions

This monitoring area displays currently active incoming Macula Monitor connections via both TCP and HTTP ports with the following details:

- **User**: user account
- **Remote address**: IP address and port of the client machine, from which the connection is made
- **Start time**: session start time
- **Type**: client application type, may be Macula Console, Macula Monitor, HTTP or Mobile
- **Software version**: remote client version
- a list of **CPU**, **memory and network load** stats from the remotely connected client machine, similarly to the ones in the *Servers* section

Disconnected sessions will automatically disappear from the list.



Video Walls

This section contains information about the currently connected video walls and their displays.

Data Sources

This section contains information about the configured data sources and their status:

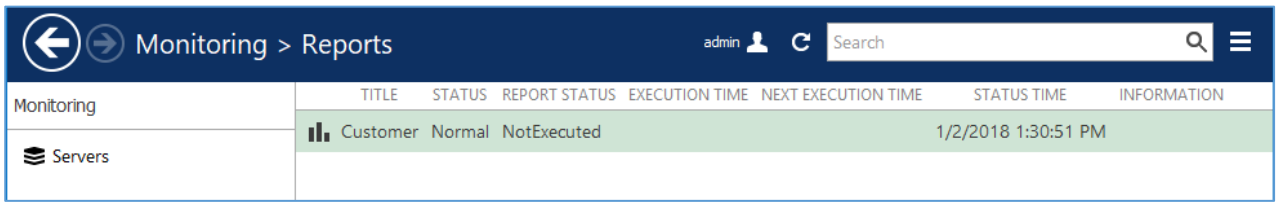
- Title: data source name
- Status: current data source status
- Server: the server that is receiving the data
- Last data receive time: the timestamp of the last received bit of data from the target data source
- Error: if any
- Status time: status timestamp
- Additional information: if any

External Services

If License Plate Recognition, Face Recognition and/or other external services (third-party integrations) are connected, their session properties will be displayed here: service name, remote address and involved user account.

Reports

This section contains health monitoring data for the configured automatic VCA and software counter reports.



If a report has been sent at least once (by schedule, not as a test), the last execution time is shown here. For the reports that are currently set to be emailed automatically, the next (scheduled) execution time is also displayed.

Access control

If any third-party services are connected, their connection properties and status will be displayed here.

OPC

If any third-party OPC servers are connected, their connection properties and status will be displayed here.

Indicators

All indicators configured in your system will be displayed here, so that you can see their status - all in one place.

GSM Modems

All GMS modems configured in the system will appear here:

- **Title**: modem name
- **Status**: current modem status
- **Server**: the server that has the modem physically connected to it
- **Error**: error code or text, if any
- **Status time**: status timestamp
- **Additional information**: error details, if any

MQTT Clients

All currently active MQTT clients will appear here. If the MQTT client is configured but is inactive, it will not be listed.

Databases

This section lists the time series databases associated with data sources and data channels.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

12.1 Audit

To access the global audit log in Macula Console, choose *Audit* section in the bottom-left-hand panel.

The audit log contains detailed information about the most important user activities and server events. Events are organized in a way similar to the Windows Event log, and can be filtered and sorted by any field just by clicking on the relevant field. By default, entries are sorted by time, with latest on top. Use *Search* field in the upper-right-hand menu to filter the records; press *Refresh* button to reload the item list.

> Please note that your actual audited events may vary depending on the software license edition.

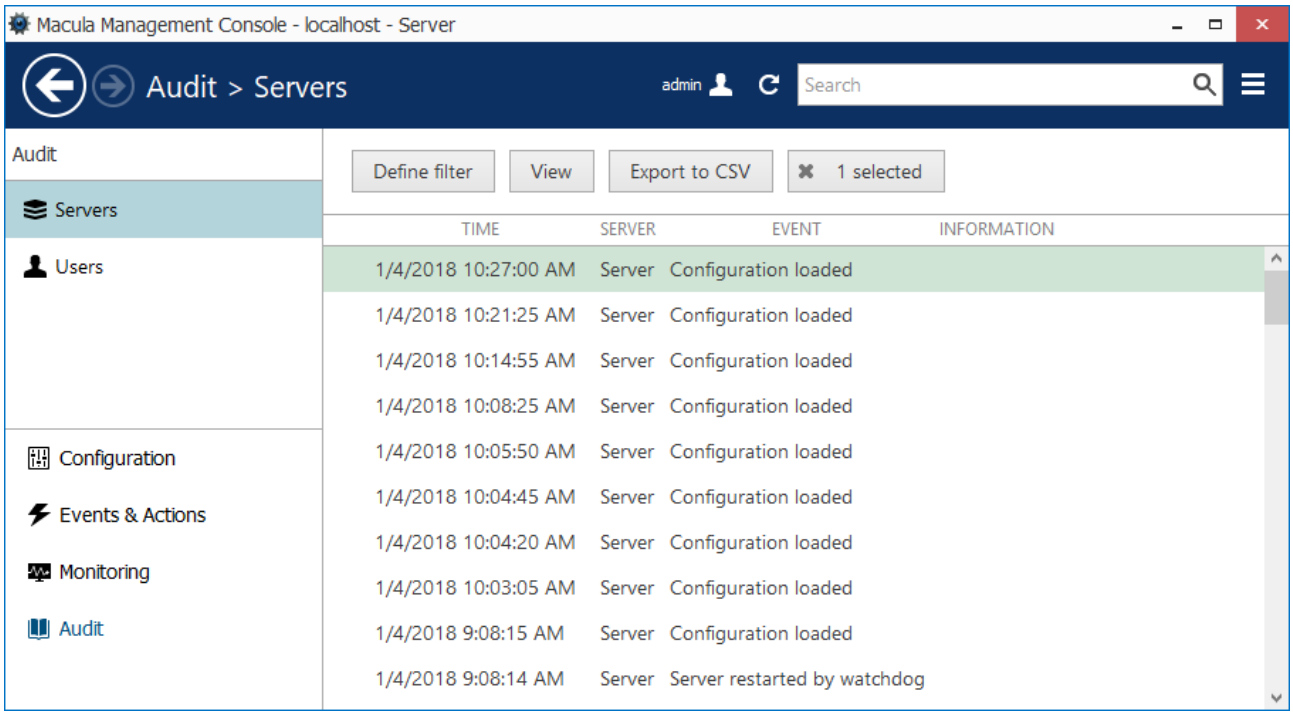
The log has two sections: *Servers* and *Users*; these can be accessed by clicking the corresponding items in the menu on the left, when in the *Audit* section.

Servers

Each event contains the following values:

- **Time**: event timestamp in the system locale-specific format
- **Server**: name of the server from which the event originates
- **Class/subclass**: event category
- **Event**: a brief description of the event; see below for the detailed information about the logged event types
- Other relevant fields - **user**, **resource**, **data**, **info**, misc. **ID**s, : additional information relevant to the event, e.g., error details, target resource type

Double-click any event in the list to view the full information.

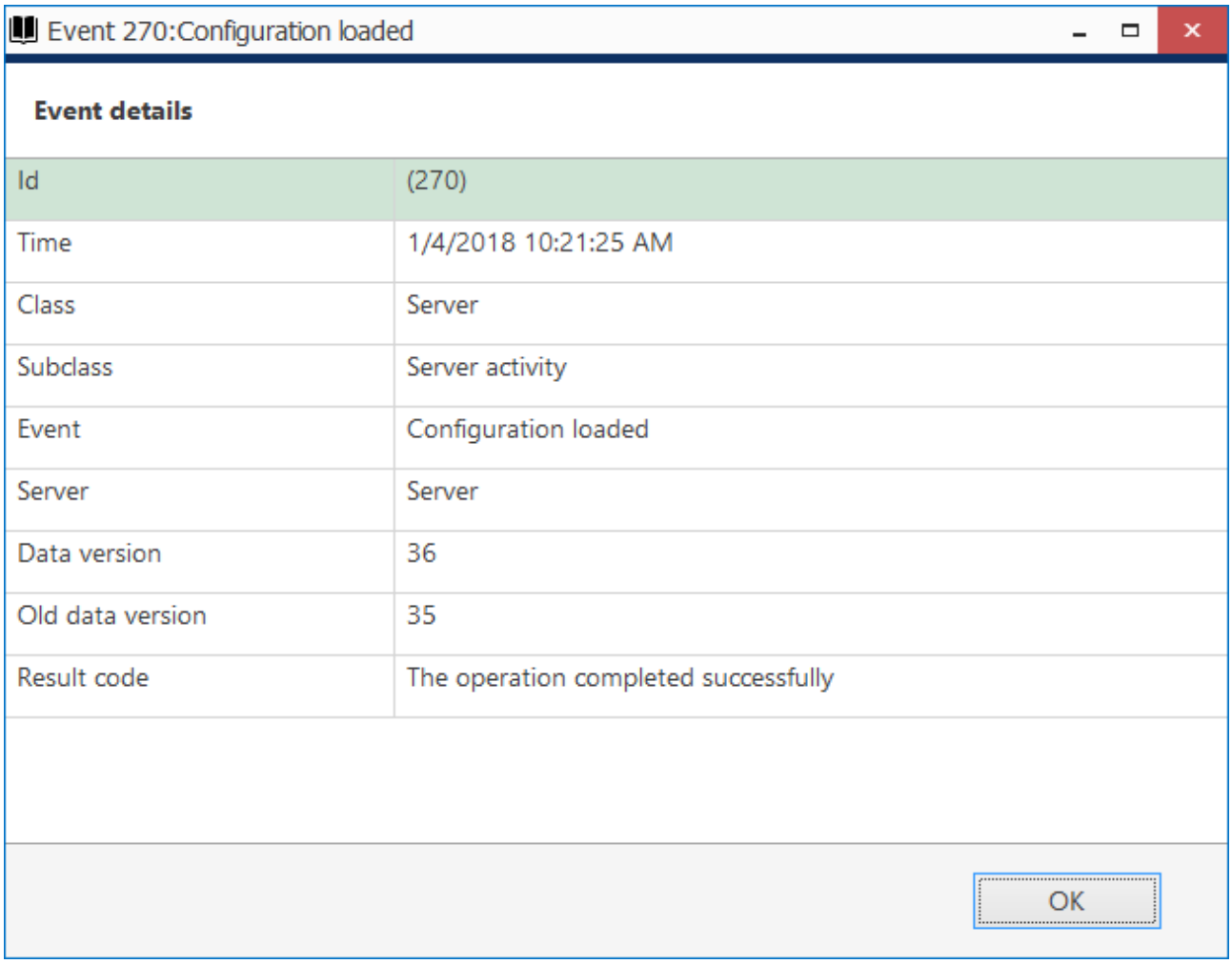


The following **events** are logged in this section:

- **Internal server events**
  - **Audio output action completed**: An E&A action to send audio to device was executed
  - **Automatic backup failed**: an automatic backup was scheduled but failed for some reason
  - **Automatic backup succeeded**: a scheduled backup copy of the databases was successfully created
  - **Central server connected**: central server has successfully connected to the target recording server
  - **Central server disconnected**: central server has disconnected from the target recording server because the target server is offline, unreachable, has been removed from the central server configuration or has invalid configuration
  - **Configuration loaded**: configuration has been successfully loaded from the database and applied to the target server
  - **Configuration Loading failed**: unable to load or apply server configuration
  - **Configuration reset failed**: an attempt to reset the recording server configuration was made but failed for some reason
  - **Configuration reset requested**: recording server configuration reset was requested via Macula Console (this message will be normally followed by another entry reflecting the rest status)
  - **Configuration request succeeded**: recording server configuration was successfully reset
  - **Configuration saved**: server configuration was saved to the database
  - **Connected to mirroring server**: central server successfully connected to its configured mirror
  - **Connected to recording server**: central server successfully connected to a recording server
  - **Disconnected from mirroring server**: central server disconnected from its configured mirror (e.g., because the mirror is no longer available)
  - **Disconnected from recording server**: central server disconnected from a recording server
  - **Event action failed**: An E&A action execution attempt was made but failed, double-click the event entry for details
  - **Event action succeeded**: An E&A action was successfully executed, double-click the event entry for details
  - **External users added**: an attempt to add new external users via AD/LDAP was made, see additional information for status details
  - **External users removed**: external users were removed from the server configuration
  - **External users updated**: AD/LDAP user list was synchronized
  - **Failover node activated**: failover server changed its state from *Idle* and received configuration to act instead of a recording server
  - **Failover status changed**: server was included or excluded from a failover cluster, or its status changed from/to *Unknown* (see server health monitoring for details)
  - **Number of external users exceeded maximum allowed**: the number of imported AD/LDAP users exceeds maximum allowed by the license
  - **Open VCA notification received**: server VCA engine event (e.g., VCA license error)
  - **Remote update initiated**: remote software update was initiated via Macula Console
  - **Server restarted by watchdog for maintenance**: server was restarted by the watchdog service (double-click the event entry for the details about restart reason)
  - **Server started**: Macula server service started
  - **Server stopped**: Macula server service stopped

    - **Synchronization completed**: central server has successfully synchronized configuration data with the target recording server
- **Resource access**
    - **Archive**
        - **Bookmark added**: a bookmark was added to the target channel on behalf of the server (via E&A action, no user interaction)
- **Uncategorized**
    - **Permissions updated**: user permissions were edited, double-click the event entry for details
    - **Recording Error**: Unable to save video stream from particular channel
    - **Recording Recovered**: video stream recording recovered

Double-click any event to open it in a separate dialog box with **additional information** about event source, such as: backup file path for the *Automatic backup* event, error code for the *Open VCA notification* event etc.



Users

The events related to user input (configuration via Macula Console, resource access via client applications) are available here. Some of these (mostly configuration related) are triggered by user actions in Macula Console and some (mostly related to resource access) are based on user actions in Macula Monitor. The following **events** are logged in this section:

- **Events & Actions**

    - **Rule modifiers**: events related to rule schedules and conditions
        - Event **condition** added/removed/updated: a condition was modified
        - Event **schedule** added/removed/updated: a schedule was modified
        - Event **schedule item** added/removed/updated: an individual schedule item was modified
    - **Action** added/removed/updated: An E&A action was modified
    - **Event** added/removed/updated: An E&A event was modified
    - Event-action **rule** added/removed/updated: a rule in the E&A table was modified
    - **Global event** added/removed/updated: a global event was modified
    - **Mail server** added/removed/updated: an SMTP server in E&A configuration was modified
- **External services**: events associated with external services operating via HTTP API, such as FR & LPR
    - **External service** added/removed/updated: external service connection was modified
    - **External service group** added/removed/updated: a group for external services was modified via Macula Console
- **Failover management**
    - Failover cluster added/removed/updated: failover cluster settings were modified via Macula Console
- **Installation**: events related to software installation and upgrade
    - Remote update requested: a user has requested remote server update via Macula Console (usually followed by the *Remote update initiated* event entry in the *Server* audit section)
- **Recording**: changes to recording setup via Macula Console
    - Recording **configuration** added/removed/updated
    - Recording **profile** added/removed/updated
    - Recording **schedule** added/removed/updated
    - Recording **schedule item** added/removed/updated
- **Resource access**: user actions concerning all types of resource access from connected clients
    - **Archive**: playback related events triggered from different Macula Monitor playback modes
        - Archive **replication** accessed: recordings from a channel replica were accessed
        - Archive **search** accessed: recordings from a channel were accessed
        - Archive **snapshot** exported: a single or multichannel snapshot was exported from one of the archive playback modes
        - Archive **timeline** accessed: archived data was accessed in a playback mode that has timeline
        - Archived **data accessed**: available recordings from a channel were played back
        - Archived **data exported**: a video clip was exported (double-click the event entry for details)
        - **Bookmark** added/removed: a new bookmark was appended to the channel timeline or deleted from it
        - **Bookmark popup** confirmed: bookmark popup caused by E&A action was approved by a user via Macula Monitor application
        - **Bookmark search** accessed: bookmark were searched from the Macula Monitor playback mode
    - **Live**
        - **Audio input** received from device: audio IN was activated from live view
        - **Audio output** sent to device: audio OUT was activated from live view
        - **External data** accessed: information from *Data sources* was streamed with live video

        - **Layout** added/removed/updated: a layout was modified in Macula Monitor
        - **Live data** accessed: live video stream was displayed
        - **Motion data** accessed: motion information was streamed with live video
        - **VCA data** accessed: Open VCA metadata was streamed with live video
    - **PTZ**: pan, tilt, zoom, focus, iris related actions, as well as PTZ presets and tours for the target channel
        - **Navigate**: PTZ event from older database versions (backward compatibility)
        - PTZ **auto-focus/auto-iris** activated: device automatic focus/iris feature was activated
        - PTZ **focus/iris** started/stopped: device manual focus/iris capability was used
        - PTZ **pan/tilt started**: device was panned/tilted
        - PTZ **pan/tilt stopped**: this event is generated after five seconds after the last pan/tilt command (after the PTZ control was released)
        - PTZ **preset** saved/activated/deleted: PTZ preset was accessed
        - PTZ **tour** saved/activated/deactivated/deleted: PTZ tour was accessed
        - PTZ **zoom started**: device zoom IN/OUT capability was used
        - PTZ **zoom stopped**: this event is generated after five seconds after the last zoom IN/OUT command (after the PTZ control was released)
    - **User defined**: this event is generated when an audit entry is created based on a user-defined E&A action *Write to audit log*
    - **Video walls**: events based on video wall related user actions in Macula Monitor via *Resources* panel and/or *Video Walls* section
        - Video wall **current layout saved as startup**: the currently displayed layout was set as startup for the target video wall display via video wall management
        - Video wall **layout saved as startup**: a layout was set as startup for the target video wall display
        - Video wall **layout sequence paused**: the layout sequence currently assigned to a video wall display was stopped
        - Video wall **layout sequence set**: a pre-saved layout sequence was assigned to a video wall display
        - Video wall **layout set**: a pre-saved layout was assigned to a video wall display
        - Video wall **object popped up**: An E&A action that displays an object (channel/ map/ layout) an a video wall screen has been executed
        - Video wall **viewport** updated: an individual viewport contents was changed within a layout of a video wall display
    - **Copied exported items**: exported files were copied from the Macula Monitor library to an external destination
    - **External data search** accessed: archived information from *Data sources* was searched from Macula Monitor
    - **External service search** accessed: archived external service data was searched from Macula Monitor
    - **Live snapshot** exported: a snapshot was saved from the Macula Monitor live view mode
    - **VCA search** accessed: archived VCA data was searched from the Macula Monitor playback mode
- **Resource administration**: resource related events caused by user actions in Macula Console management application
    - **Channels**

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

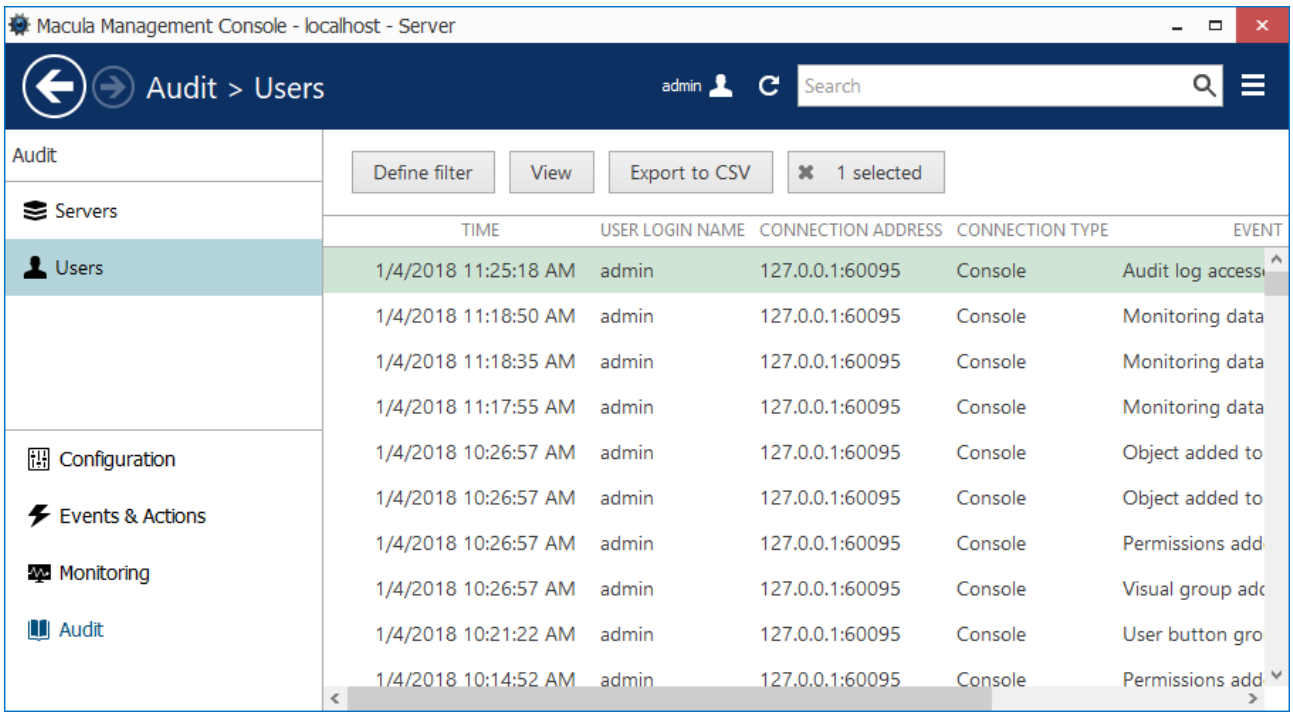
    - Channel **added/removed/updated**: target channel was modified in the described manner
    - Channel **attached/detached**: target channel was attached to/detached from its device
    - Channel **enabled/disabled**: target channel was activated/deactivated
    - Device **channel group** added/removed/updated: a channel group was modified in the described manner
- **Data sources**
    - **Data source** added/removed/updated: a serial data source was modified in the described manner
    - **Data source profile** added/removed/updated: a profile for the data source was modified
- **Devices**
    - **Administer**: device management event from older database versions (backward compatibility)
    - **Device** added/removed/updated: a device was modified in the described manner
    - **Device group** added/removed/updated: a device group was modified in the described manner
- **Layouts** and layout templates
    - **Layout template** added/removed/updated: a layout grid was modified
    - **Layout group** added/removed/updated: a group for shared layouts was modified
- **Live podcasts**
    - Live podcast **added/removed/updated**: a live broadcast was modified
    - Live podcast **enabled/disabled**: a live broadcast was activated/deactivated
- **Maps**
    - **Geo map** added/removed/updated: a map based on the world map was modified
    - **Map** added/removed/updated: a picture-based map was modified
    - **Map group** added/removed/updated: a map/geo map group was modified
    - **Map item** added/removed/updated: an individual map item (e.g., channel marker) was modified on a map/geo map
- **Networks**
    - Network **added/removed/updated**: a network connection was modified
- **Organizations**
    - Organization **added/removed/updated**: an organization was modified
- **Servers**
    - **Connection** updated: server connection (IP, port, SNMP settings) was modified (it is added/removed together with the server)
    - **Server** added/removed/updated: a server was modified in the Macula Global configuration
    - Server **configuration backed up**: server configuration was backed up manually via wizard (this event is only logged if the backup was run while Macula server was stopped)
    - Server **configuration restored**: server configuration was restored manually via wizard (this event is only logged if the wizard was run while Macula server was stopped)
    - **Server group** added/removed/updated: a server group was modified
- **Software counters**
    - Software counter added/removed/updated

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

    - **User buttons**
        - **User button** added/removed/updated: a user button was modified
        - **User button group** added/removed/updated: a user button was modified
    - **Video walls**
        - **Video wall** added/removed/modified: a video wall was modified
        - **Video wall group** added/removed/updated: a video wall was modified
    - **Visual groups**
        - **Visual group** added/removed/modified: a visual group was modified
    - **Access control** added/removed/updated, enabled/disabled
    - **OPC client** added/removed/updated, enabled/disabled
- **Server security**: events related to server security, access and permission/policy/user management
    - **Administration permissions** updated: administrative permissions for Macula Console access were modified for a user or a user group
    - **Audit log** accessed: the *Audit* section of Macula Console was accessed
    - **Confirmed server warning** notification: a popup warning from the server E&A action was confirmed in Macula Monitor
    - **External user group** added/removed/updated: AD/LDAP user group was modified
    - **Client connection** permissions updated: administrative permissions related to remote client access were modified
    - **Log in**: a user has successfully logged into the target server
    - **Log out**: a user has logged out of the server or his session timed out
    - **Monitoring data** accessed: the *Monitoring* section of Macula Console was accessed
    - **Object added** to group: some object in the server configuration was added into a group of the corresponding type
    - **Object removed** from group: some object in the server configuration was deleted from a group of the corresponding type
    - **Permissions** added/removed: user permissions were modified
    - **Security policy** added/removed/updated: server security policy was modified
    - **Unsuccessful log in**: a user has attempted to log into the server without success
    - **User** added/removed/updated: a user account was modified
    - **User group** added/removed/updated: user group settings were modified

Double-click an event entry to see **details** about the related resource, such as: resource name, the user who did the changes or executed the action, destination path for the copied exported files etc.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Problems

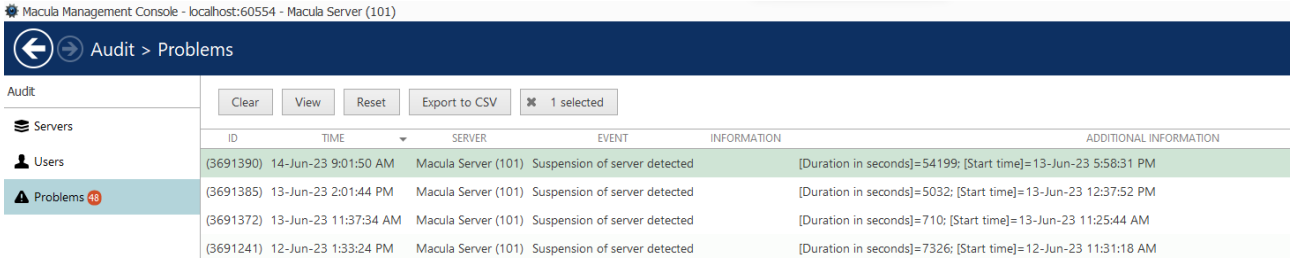
This section is a filter: it contains important messages from Servers and Users sections, which indicates that **the system has a potential problem**. For example, messages about system suspension indicate that some system setting cause system suspension, and this behavior may cause server freezes and gaps in the video archive.

List of potentially problematic errors:

- **Recording Error**: Unable to save video stream from particular channel
- **Configuration Loading failed**: unable to load or apply server configuration
- **Server restarted by Watchdog**: Critical server restart

Use the buttons in the upper panel:

- *Clear*: discard all entries and remove them from the problem list
- *View*: open the item details
- *Reset*: restore all log messages that are considered problems
- *Export to CSV*: save the list of problems and their details into a comma-separated-value format file



The number in the red circle next to the section name indicates the number of logged problems.

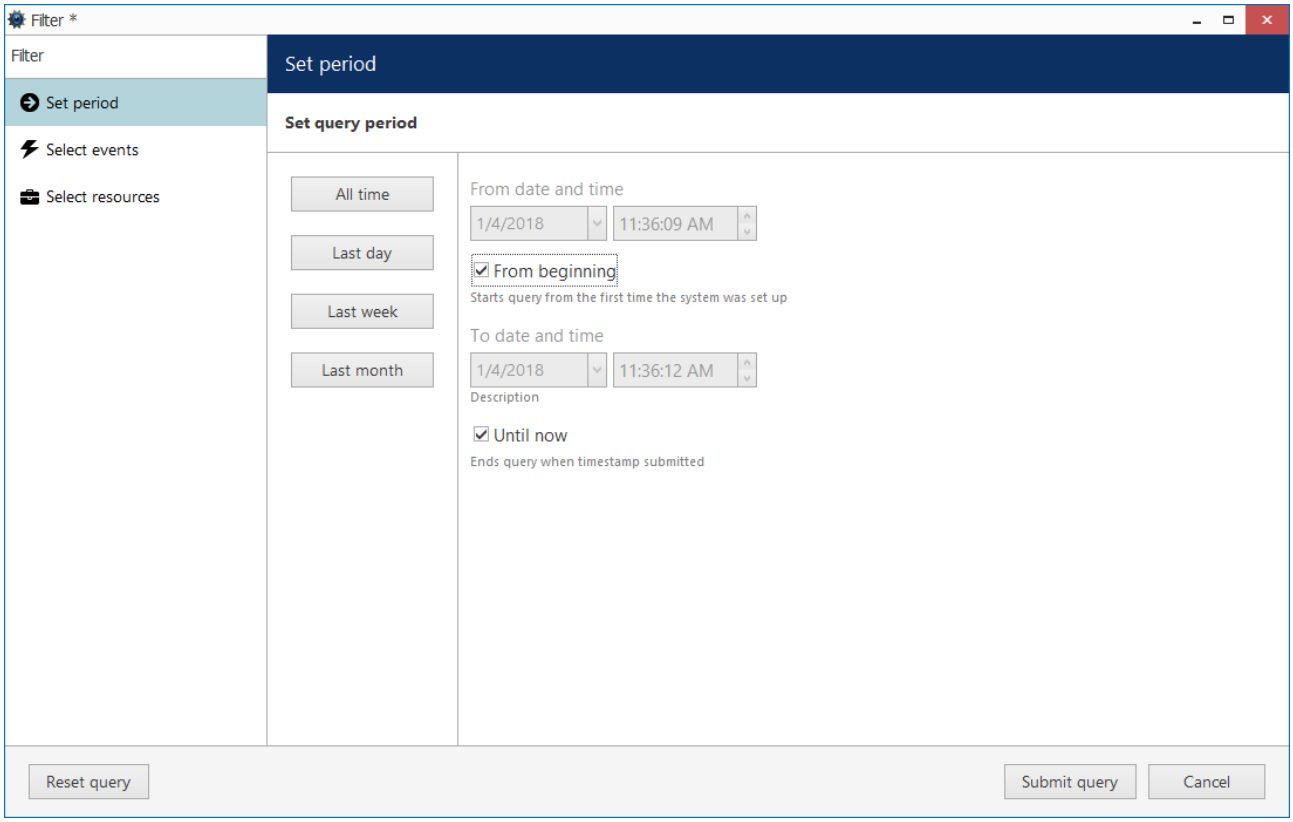
Define Filters

Server and user audit logs can be filtered for easier analysis. Click the *Define filter* button on the upper panel to bring up the dialog box.

Available filters:

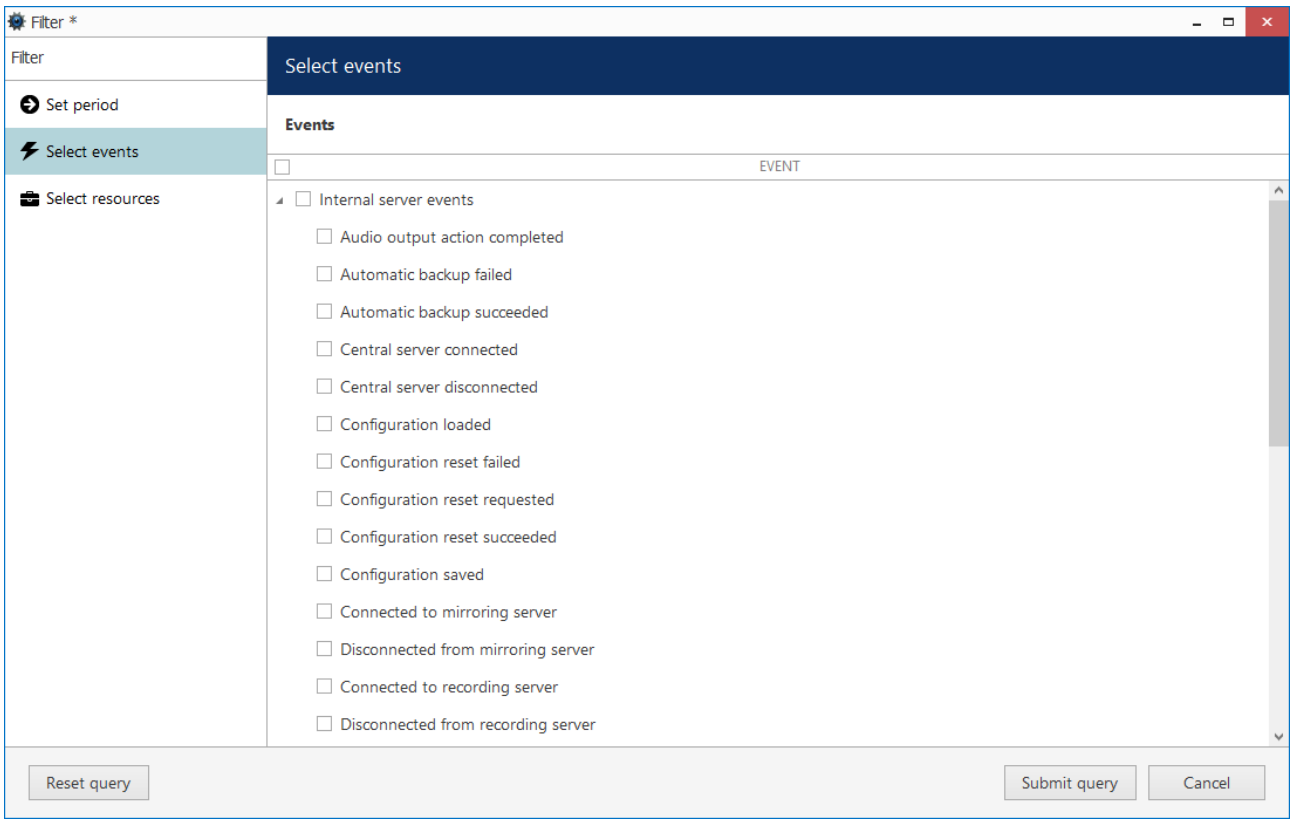
- by period
- by event
- by server
- by resource
- by user (only for the user-initiated events, *Users* tab)

In the *Set period* tab, specify the time limits for log output. You can set the date and time manually or use automated controls for preset time boundaries: last day/week/month, the whole time, and also set start/end boundaries equal to the log beginning/end.



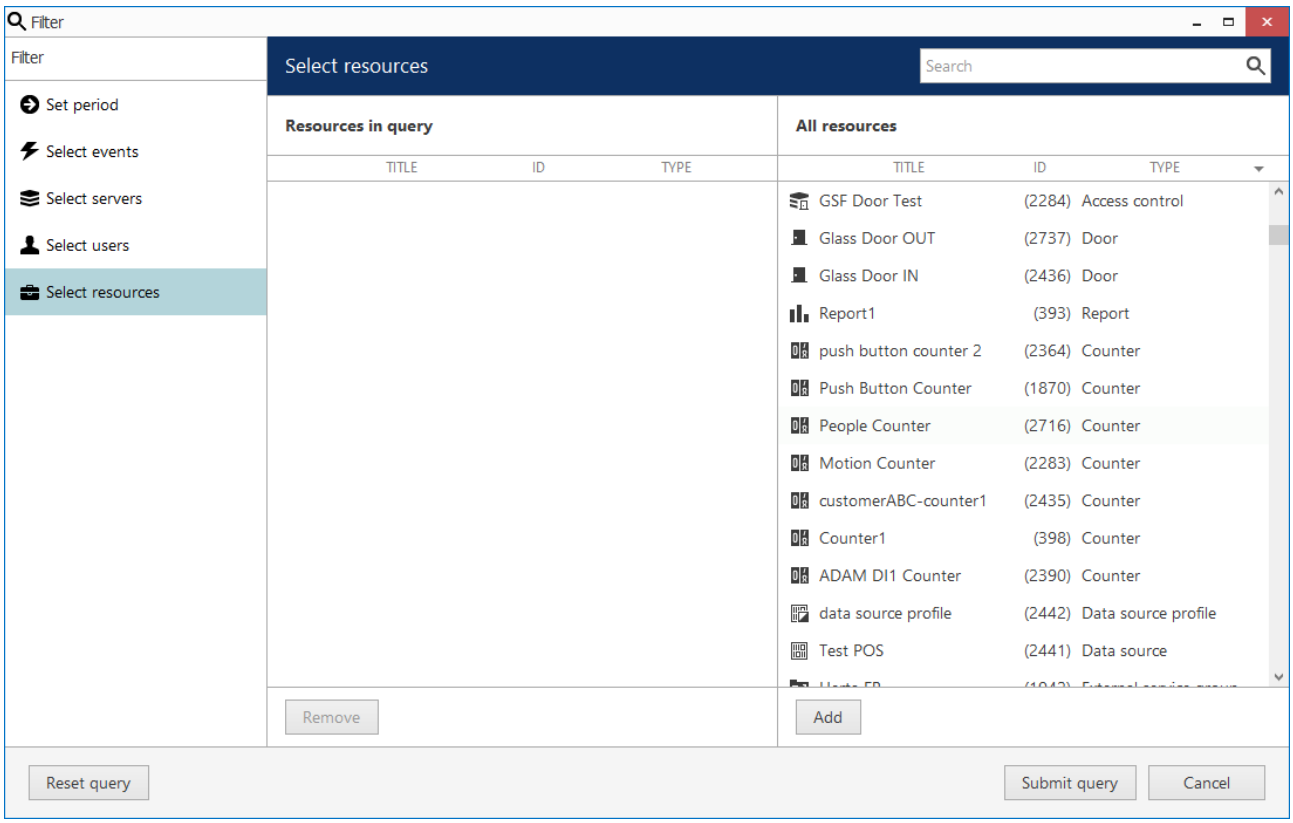
In the *Select events* tab, choose specific event types to narrow down the search. Note how the choice differs for the *Servers* and *Users* log filters.

Macula® Professional Administration Guide

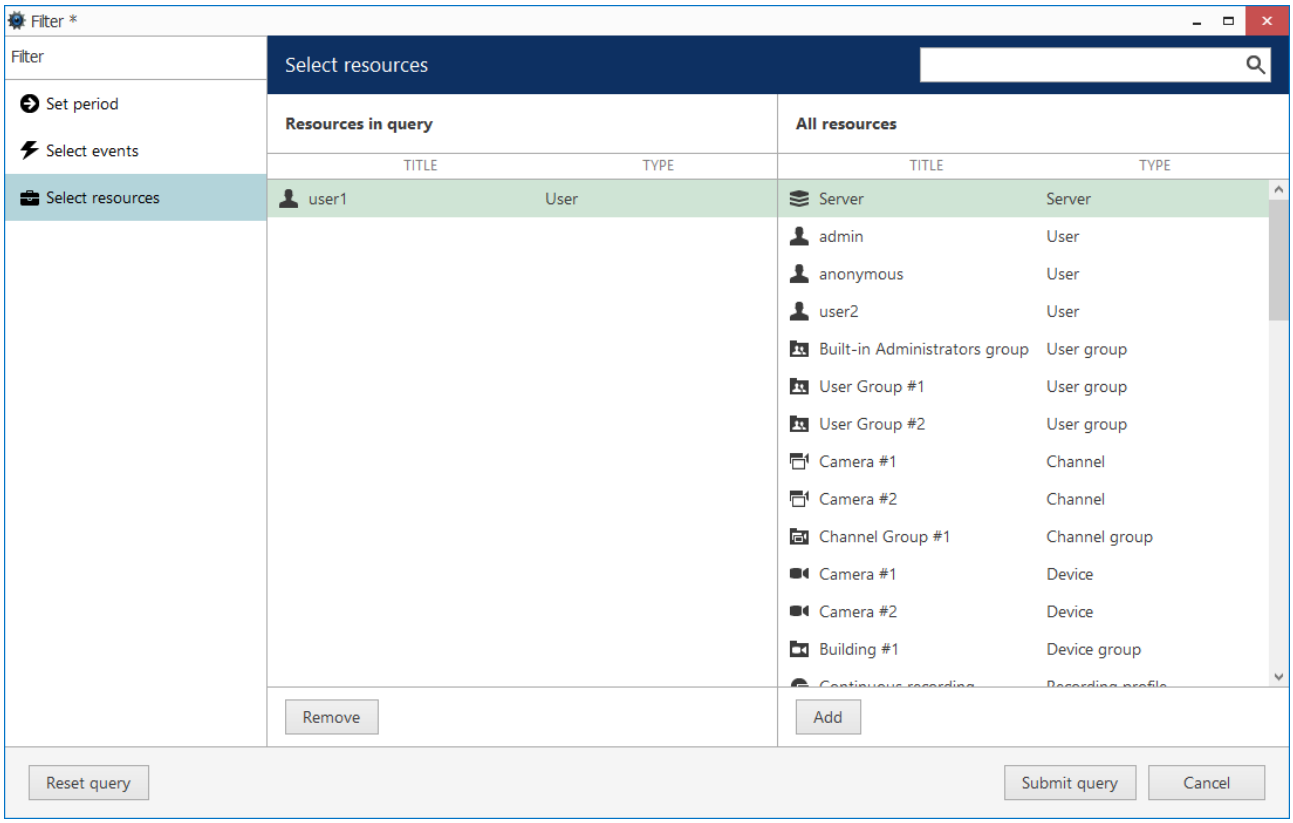


In the *Select users* and *Select servers* tabs, you can choose target servers and users, who initiated the event. Note that if you want to search for events where a user was a target (e.g., user permissions changed), you need to select that user in the *Select resources* tab.

Selecting **resources** will search for them in the additional event fields (i.e., events where these resources were a target). If you want to see events that were initiated by a specific **user** and/or on a specific **server**, choose them in the corresponding tabs - *Select servers* and *Select users*.



In the *Select resources* tab, you can choose which resources will be mentioned in the log entries. Note that if multiple resources are chosen, the filter will apply *OR* logic, meaning that output log will only be displayed if it contains log entries for **at least one** specified resource, and not for the combination of all specified resources.



Use the *Search* field to filter the resource list; both the list of *Resources in query* and general *All resources* will be affected by the *Search* filter. Press the *Reset query* button in the bottom left corner at any time to

restart filter configuration; when you have finished, click *Submit query* to view the results. To discard filtering, simply switch to a different section in the menu on the left and then switch back to your desired section.

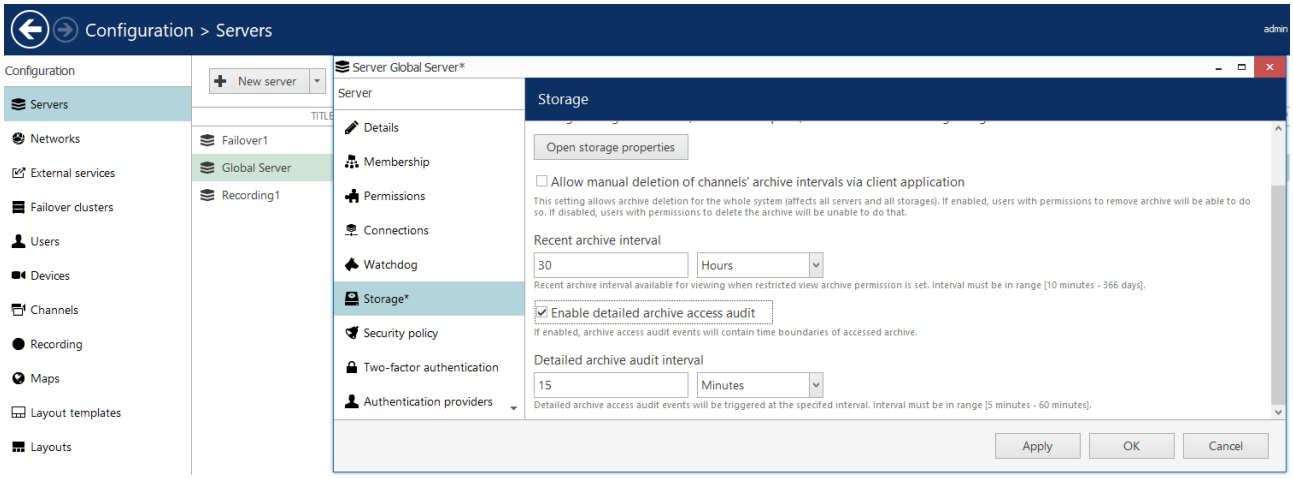
Detailed Audit

To track user activity in the archive playback mode of Macula Monitor, you can enable a *Detailed Archive Access Audit* and its intervals. By default, the feature is disabled. The default value for *Archive Access Audit Interval* is 15 minutes.

Setting up archive access audit and its intervals

To start logging user activity in *Archive Playback* mode, you need to turn the feature on:

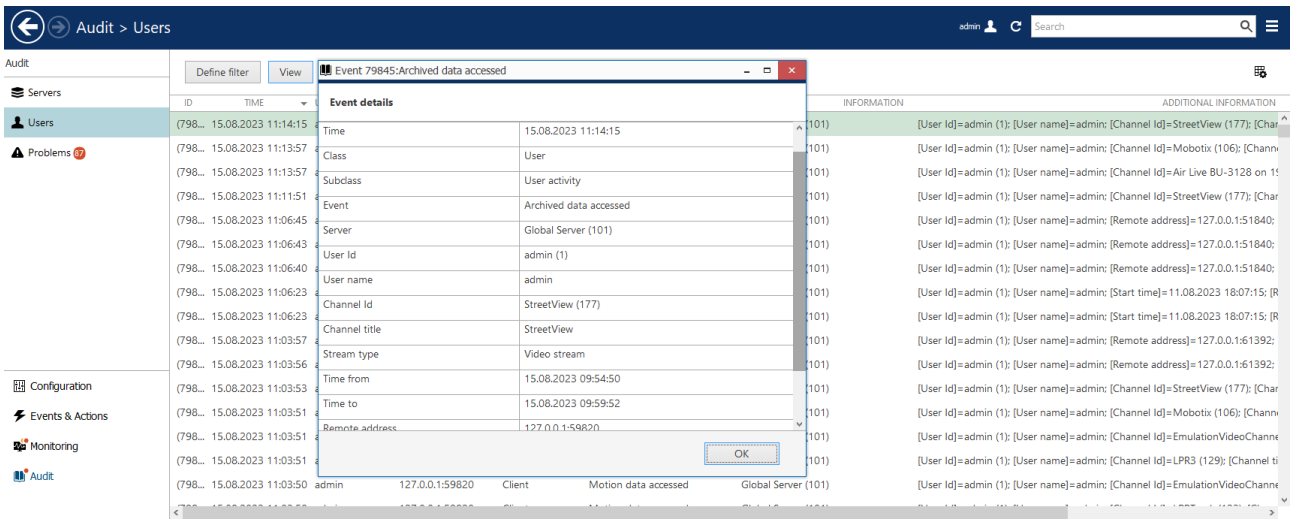
1. In the left bottom panel - click on the *Configuration* tab
2. Select *Servers* on the left and double-click on your chosen server
3. Pick up storage in the popup window
4. Mark checkbox *Enable Detailed Archive Access Audit*
5. Set up your logging interval



Accessing logs

After you turn on playback audit logging, you can access log information in Macula Console:

1. In the left-bottom panel, select the *Audit* tab
2. In the left-top panel, click on *Users* and check for user activity
3. Double-click on the event you are interested in or select the event and use the *View* button on top



Reviewing log details

In the event detail window, you can find many details, including:

- Time - when the record was accessed
- User ID and User name - who accessed the record
- Channel ID/Channel Title - What channel was accessed
- Time from/Time to - what recording interval was accessed
- Remote address - IP and port of the particular machine that was used to access the recording

Logged Events

Events logged with enabled *Detailed Archive Access Audit*:

- **User Archive Data Display Accessed** - reviewing archive record time range
- **User Archive Data Export Accessed** - archived record video export attempts
- **User Archive Data Export Snapshot Accessed** - snapshot export attempts

13 Tools and Wizards

This chapter describes additional tools and wizards that are installed with the Macula server software.

See also earlier in this document: license manager, server setup wizard, quick configuration wizard.

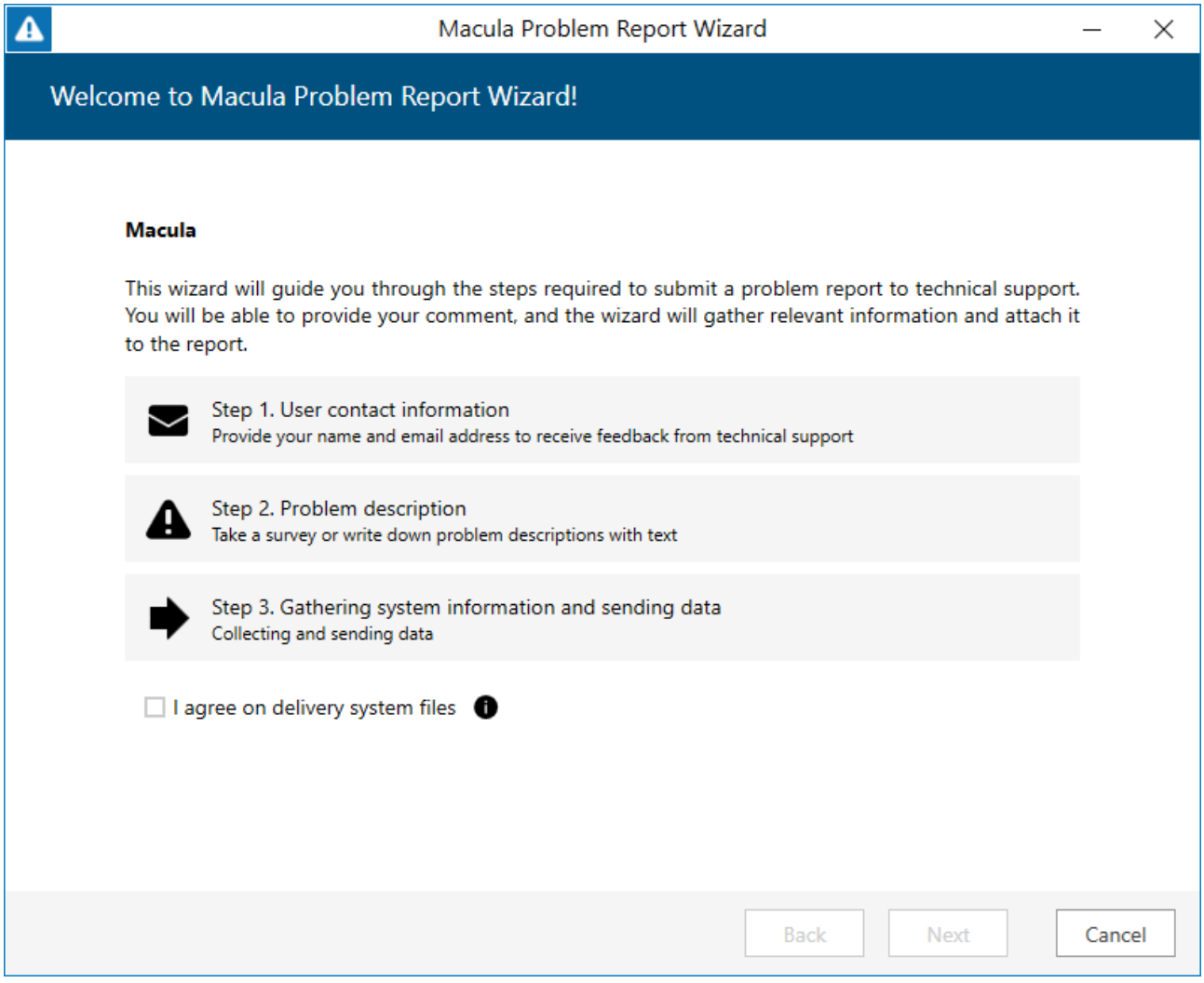
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

13.1 Problem Report Wizard

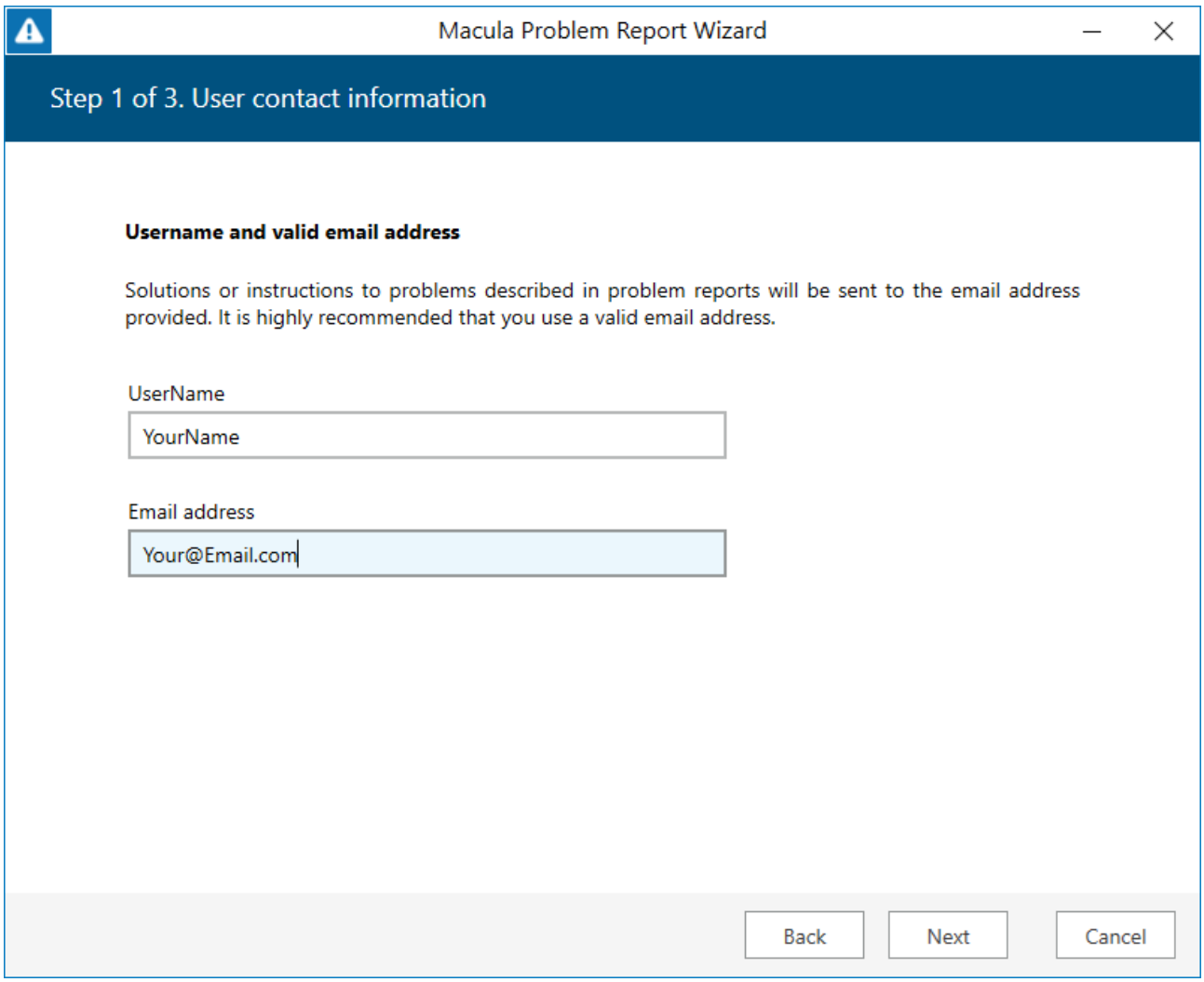
Macula software offers a comprehensive wizard-like tool for structured and detailed problem reporting. The tool is automatically installed at the same time as the product and is thus available on any machine on which Macula software is installed.

Access Problem Report Wizard via *Start -> All Apps -> Macula ->* Macula *Problem Report Wizard* (in Windows 7 and older versions, use *Start -> All Programs -> software installation folder -> Tools ->* Macula *Problem Report Wizard*); alternatively, use Windows Start Menu *Search* to locate the Problem Report Wizard in the programs menu.

> ⚠ Make sure you run the Problem Report Wizard on the right computer: it gathers information from the machine it has been launched on, and **not** from any of the servers connected via Macula Console or Macula Monitor.

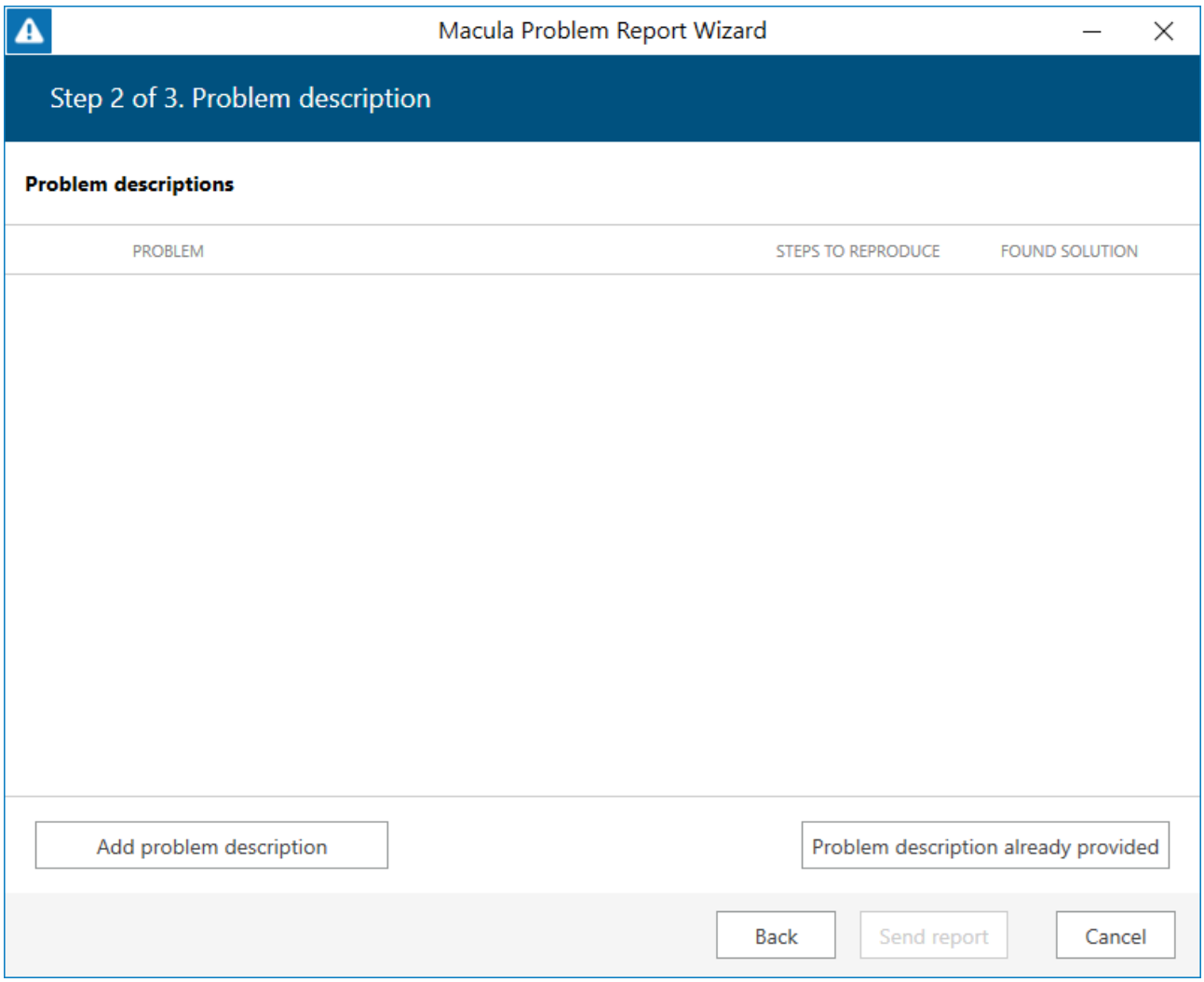


Agree to deliver system files to GSF support and hit *Next*. You can check which files are being taken from your system by clicking on the information button next to the agreement checkbox. Note that GSF will not transfer your data to any third-party companies; all the information gathered is required to help GSF efficiently resolve the reported problems.

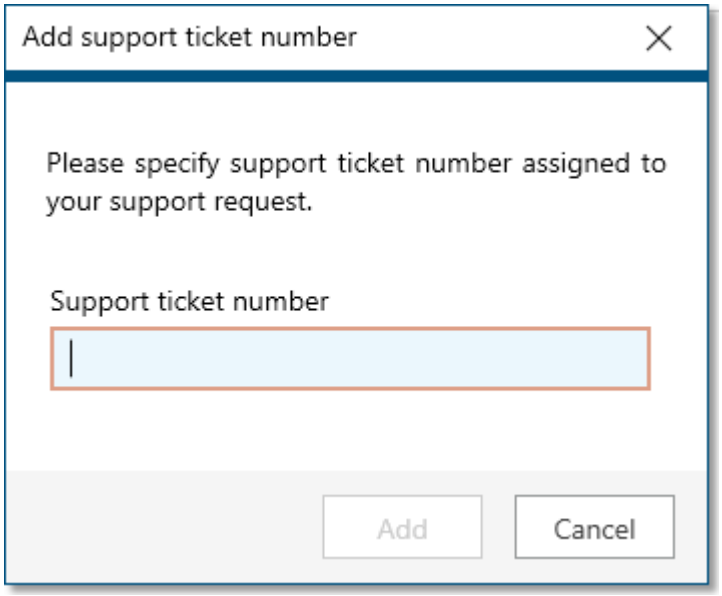


Enter your name and your email address so that the GSF support team can contact you. Click *Next* to proceed.

Macula® Professional Administration Guide



If you were asked by support team to generate a problem report, copy the **ticket ID** from the email communication and add it to the report by clicking the *Problem description already provided* button. This will help the support team to classify your report faster, and it will also guarantee that your report will go directly to the team member responsible for the thread.

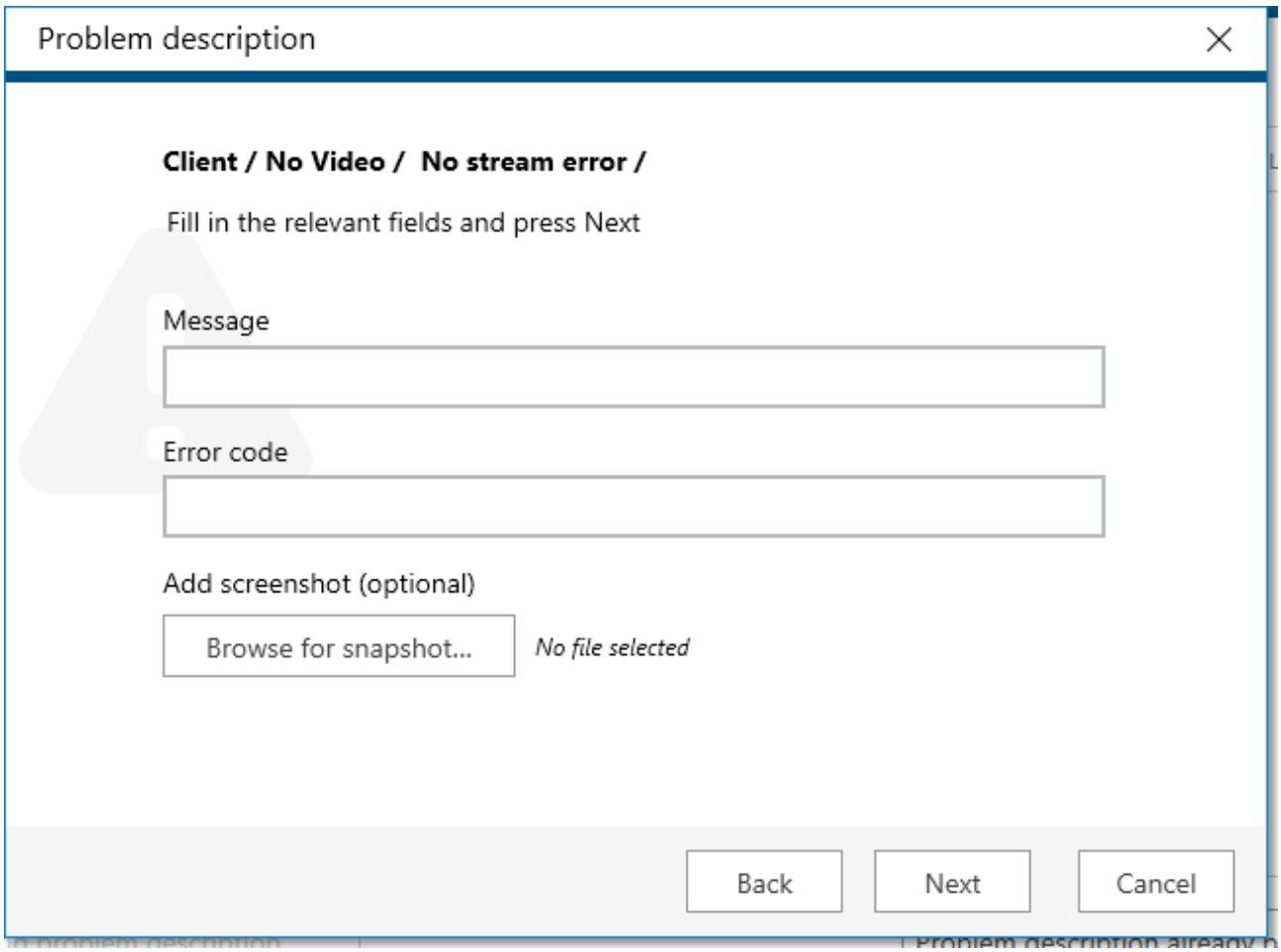


If you are applying a new, unreferenced problem report, click the *Add problem description* button.

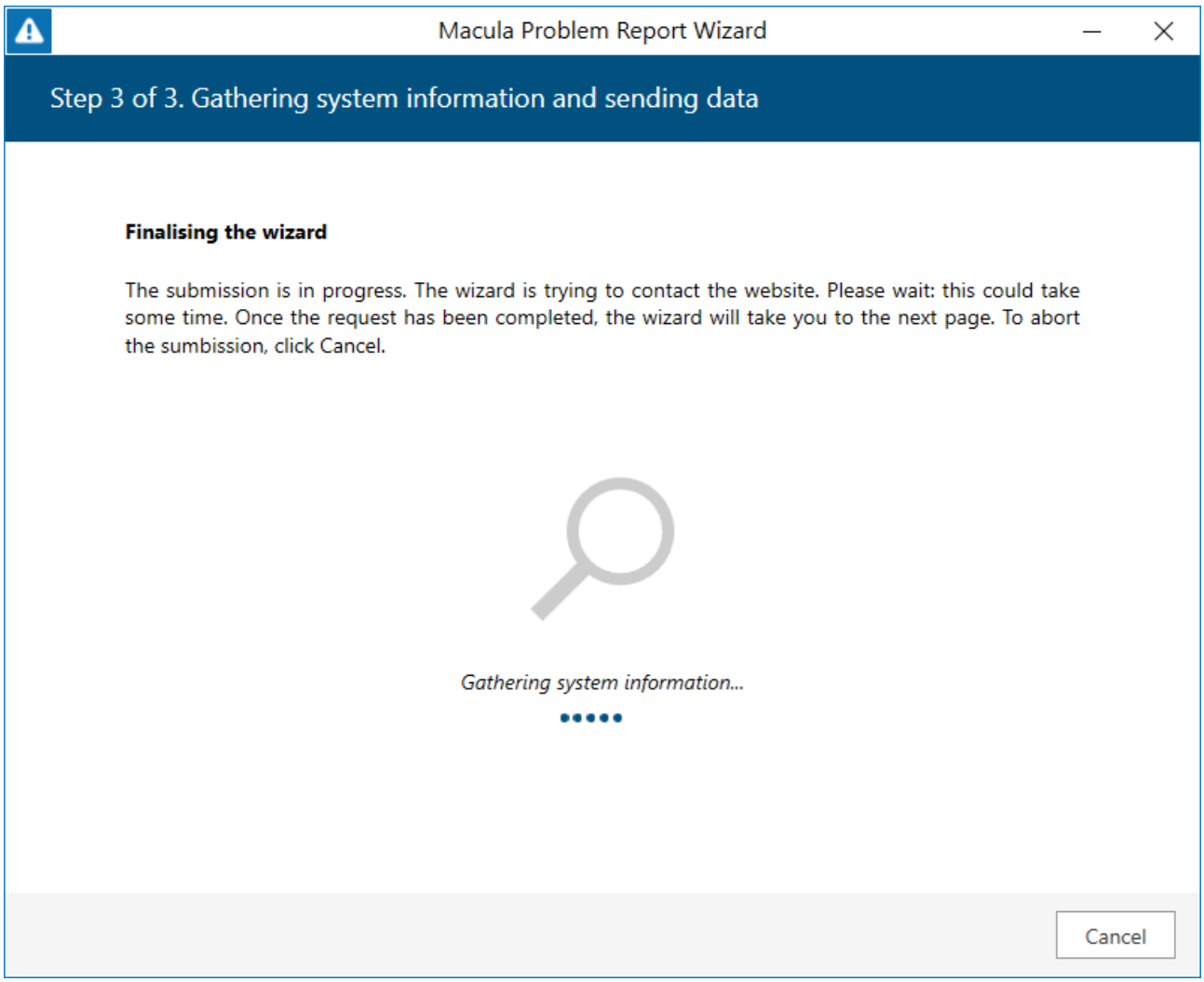
© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide

A short comprehensive wizard will guide you through the main issue categories, allowing you to choose the ones that are most applicable to your situation. You will be given the chance to enter error messages/codes, if there are any, and to attach snapshot(s). Make sure you provide the maximum amount of relevant information about the issue you are experiencing; always include **snapshots** if they are available.



You can add **multiple** descriptions to a single report. When you are ready, press the *Send report* button; the wizard will then try to send the report automatically.



If the server is offline, wizard will not be able to submit the report to GSF; instead, you will be invited to save the generated report locally. Press the *Finalize wizard without upload* button to finish.

Click *Save report as file* to save the compressed report on your computer; you are welcome to send it manually from any other computer to support@gsfcorp.com. Click *Exit* to close the wizard.

13.2 Archive Backup Wizard

Macula offers an option to **back up** any recordings from any server manually, in the proprietary Macula archive format. **Video, motion information, audio, VCA data streams,** as well as **external serial data** can be extracted from the original archive and saved elsewhere, with an option to include the **portable player** tool so that the downloaded recordings can be played on any Windows-based computer, even if it has no Macula installed.

The wizard is included with any Macula installation, including Macula Console management application and Macula Monitor application, and allows connection to **local and remote servers**.

> The archive will be copied to the computer that has *Archive backup wizard* running on it. Thus, if you are connecting to a server remotely via *Archive backup wizard*, the archive copy will be **downloaded** to your computer from the server. As footage may be of significant size, make sure you have the required bandwidth available.

Start the Archive Backup Wizard from the Windows Start menu: *Start -> All Apps ->Macula - > Archive Backup Wizard* (in Windows 7 and older versions, use *Start -> All Programs ->* software installation folder *-> Tools -> Archive Backup Wizard*); alternatively, use *Search* to locate *Archive Backup Wizard* in the programs menu.

From the Macula Monitor application, the wizard can be launched via main application menu by opening *View -> Archive Backup Wizard* and choosing the server (one of the connected ones). The address of the server, and also the username and password, will be taken from the currently configured server connection.

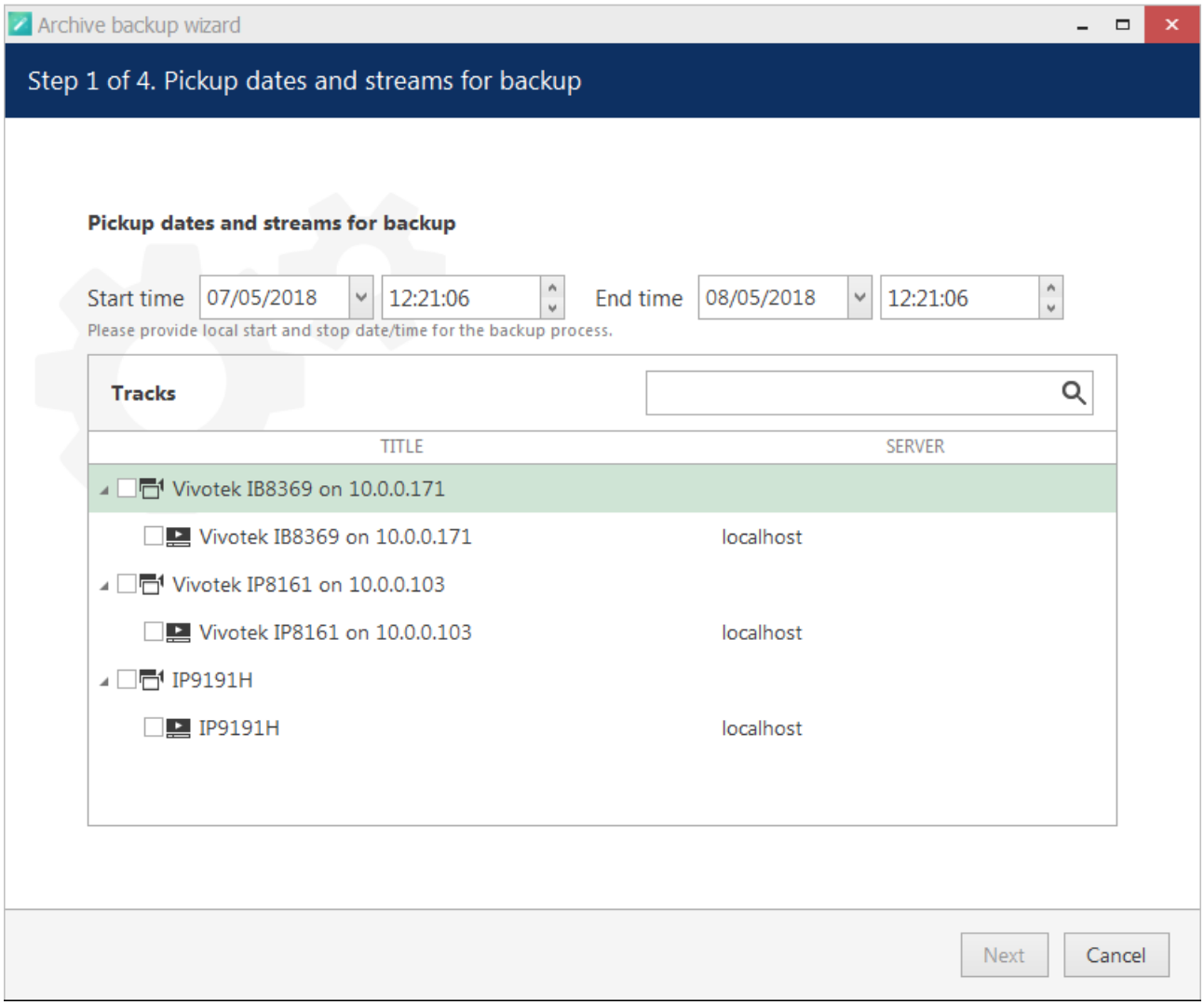
Using Archive Backup Wizard

First, you will be asked to log into the target server: your user account must have an administrative permission to make archive backups plus permissions to back up footage from individual channels/channel groups. You can create archive backups from the local server or from any remote server (login procedure is analogous to Macula Console login), including individual recording servers. If you run the wizard from the Macula Monitor application, you will not be asked to log in; instead, your configured server connection will be used.

After you log in, you will be presented with the list of available recordings, grouped by channel. Select the channel(s) you need by putting a checkmark next to each one; specify the required time range above the channel list and click *Next*.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

Macula® Professional Administration Guide



Depending on the number of selected channels, their footage size, storage speed and connection latency, it may take a few moments to retrieve the stream information. Once it is done, you will be presented with a list of streams for each of the selected channels.

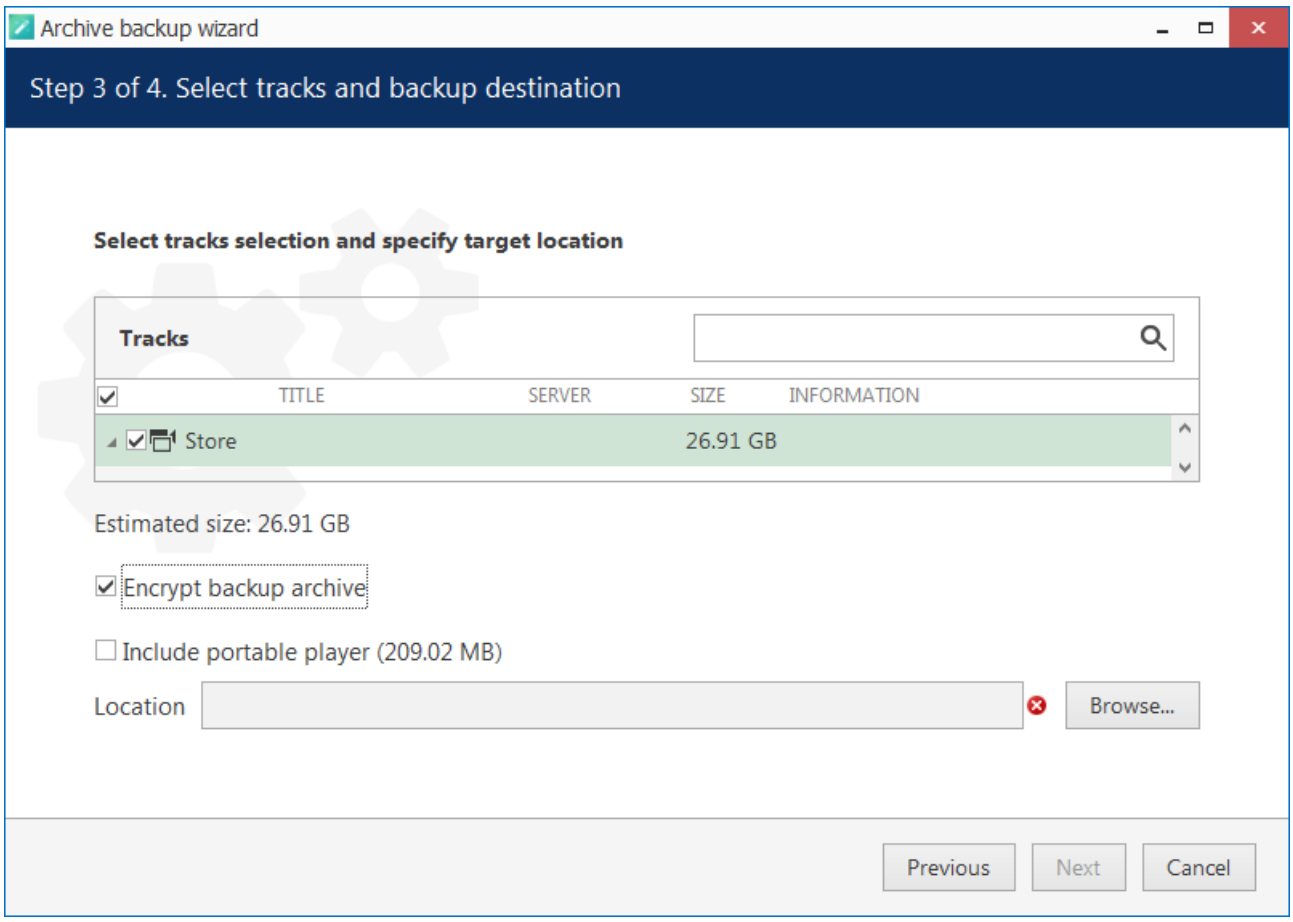
The **following tracks can be backed up**, depending on the channel recording settings and, therefore, stream availability:

- main video stream, substream and edge recordings
- video motion information
- audio stream
- VCA metadata
- external serial data from *Data sources*

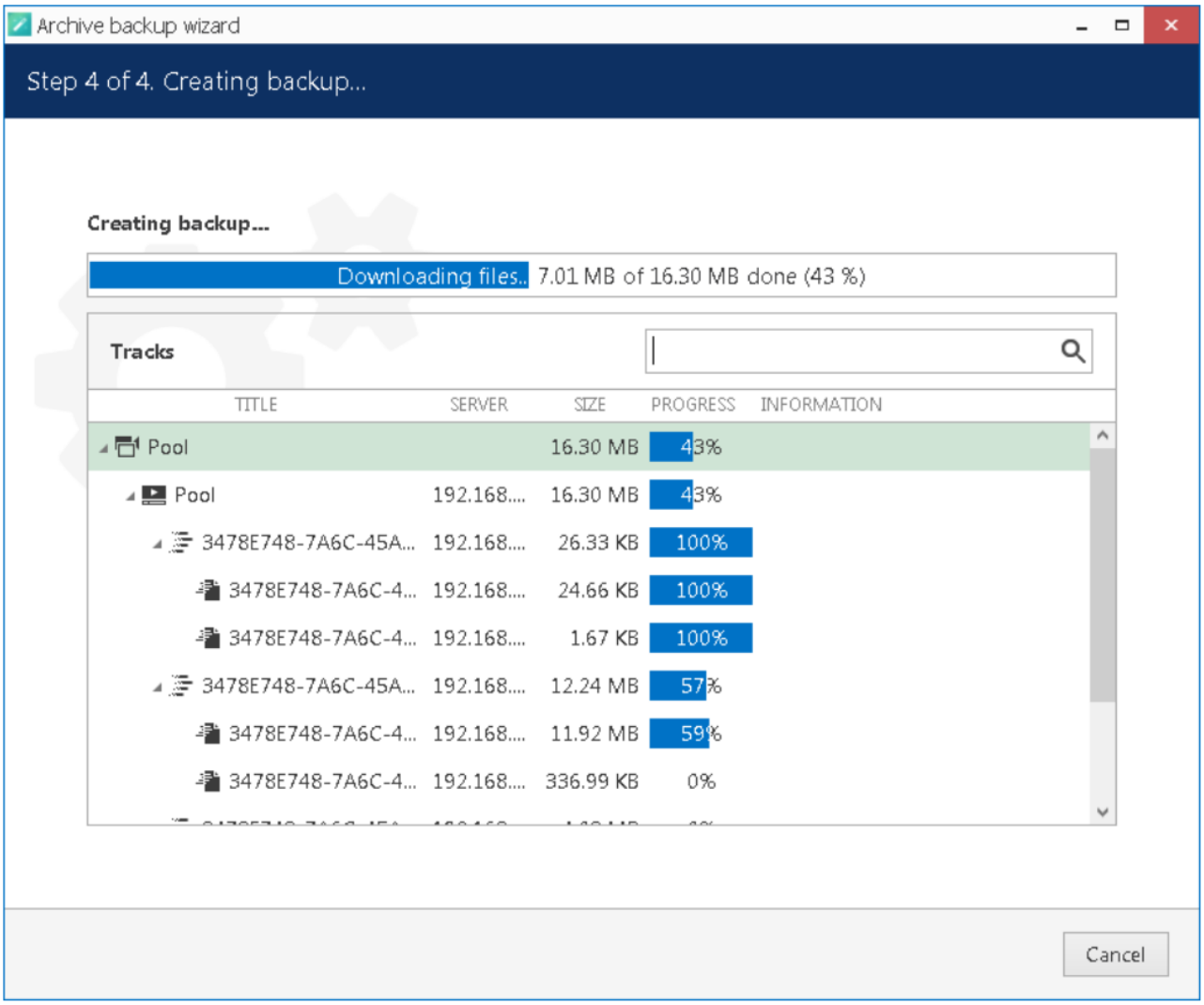
Archive bookmarks and external service data (e.g., LPR/FR recognition results) are not available for backup.

Additionally, you can append the **portable player** tool with the copied part of the archive so that you can play the archive without having to install Macula server on another machine. Guidelines on the portable player usage are available in your Macula Monitor user guide.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



Here, you also need to specify a directory for the archive to be copied to: it may be a local hard disk, a shared network storage, or an attached USB drive. You are asked to choose an **empty folder** as a backup destination, so you may need to create a new folder from the standard *Select folder* dialog.



When ready, hit *Next* for the wizard to proceed with backing up the selected information. Depending on the size of the selected archive, the backup procedure may take some time and its progress will be displayed in the wizard window. When it is finished, you will get a confirmation with a short description of what has been done.

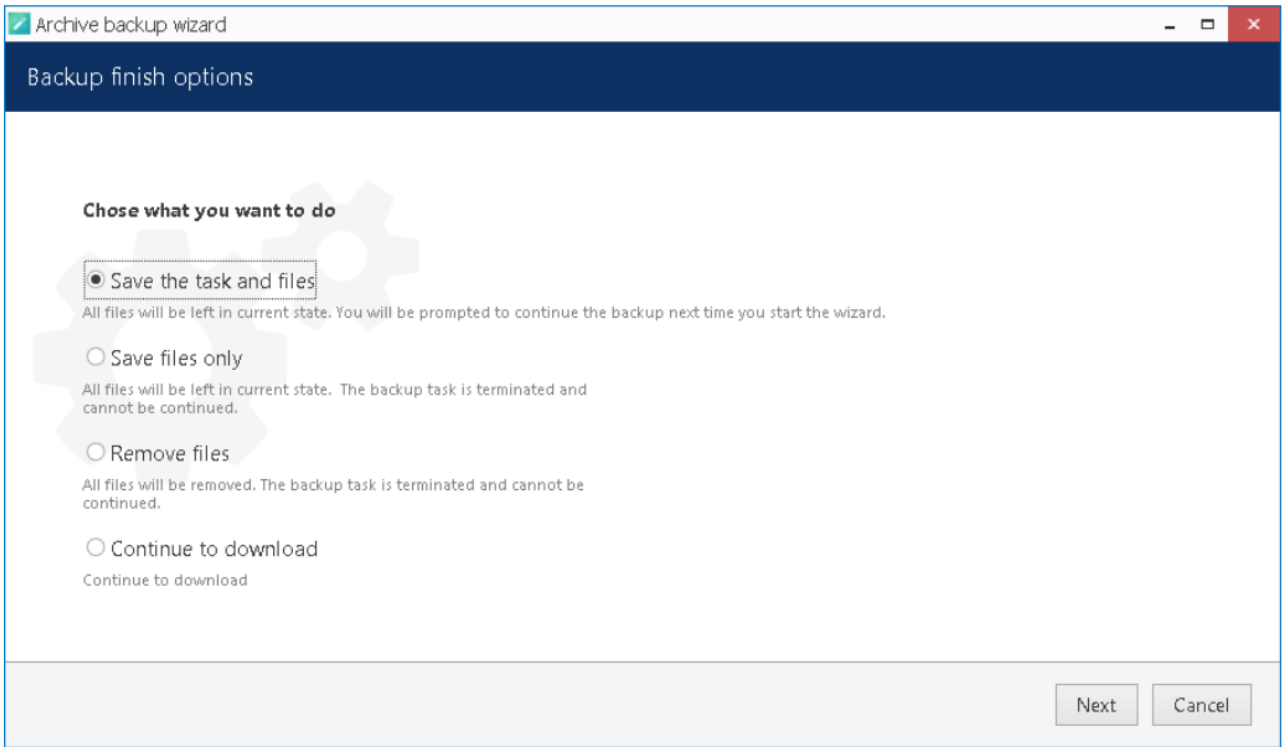
If you wish to back up more recordings, start the wizard again and follow the described procedure once again.

Postpone Your Archive Backup

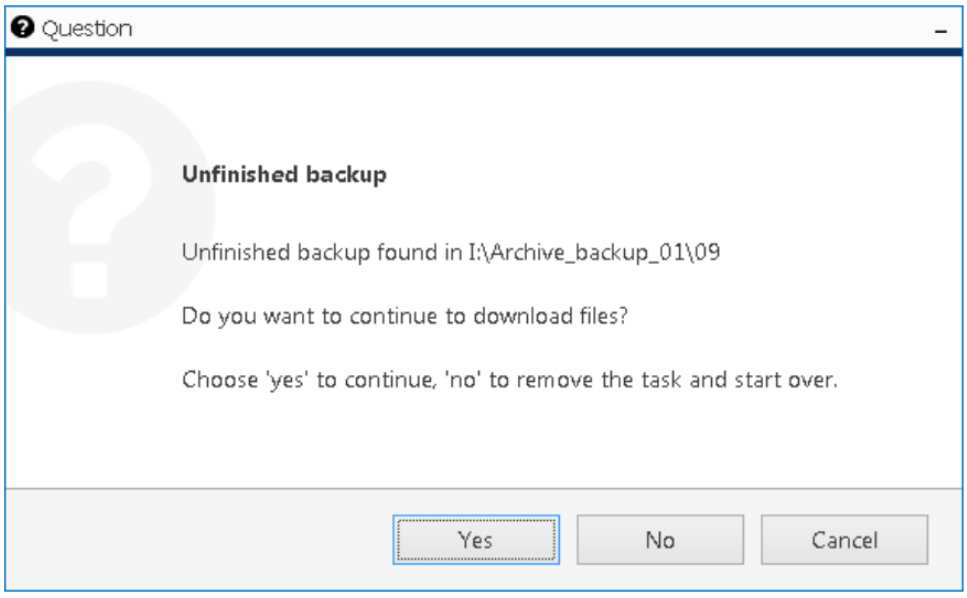
If, during the backup progress, you decide to **stop** it for some reason, simply hit the *Cancel* button in the bottom right corner. You will then be presented with several options of how the wizard can proceed:

- save the task and files: save your current backup progress and preserve the wizard state until the next time you run it; you will be able to continue with the current backup item(s) then
- save files only: leave the files that have been downloaded so far but discard the wizard settings so that the next time you run it you will be presented with default choice
- remove files: discard current backup task completely and remove the downloaded files
- continue to download: go back and continue with the selected backup

Macula® Professional Administration Guide



If you have chosen to save both the task and the files, next time you start the wizard you will be reminded of the unfinished backup job and offered to continue with it. If you click *Yes* to proceed with the unfinished task, it will be started automatically right after you provide your user credentials for the server login.



© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com

13.3 Renderer Test Utility

Macula can utilize GPU for some operations in order to decrease the CPU load. To enable GPU acceleration, run the *Renderer Test Utility* from the Macula suite on the Macula Monitor workstation.

There are two supported GPU operations are:

- frame **decoding** on Macula Monitor side
- **rendering** on Macula Monitor side

> ⚠ GPU acceleration limitations:
> - Only Windows 10 and corresponding Windows server OS editions (2016, 2019) , or Windows 11.
> - Only H.264 streams for live view and digital PTZ in live view
> - For fisheye image dewarp, only Fisheye-II is supported (choose the *Fisheye lens (6MP and larger resolution)* option in Macula Console)
>
> All other cases will use CPU for decoding/rendering operations.

Before configuring GPU acceleration, make sure you have installed the latest official **drivers** for all your graphics cards. We also recommend having more **memory** for GPU (the more, the better). For integrated video cards, you can change this setting in BIOS. For discrete graphics, choose ones with more onboard memory (1GB per display or more).

GPU Test and Configuration

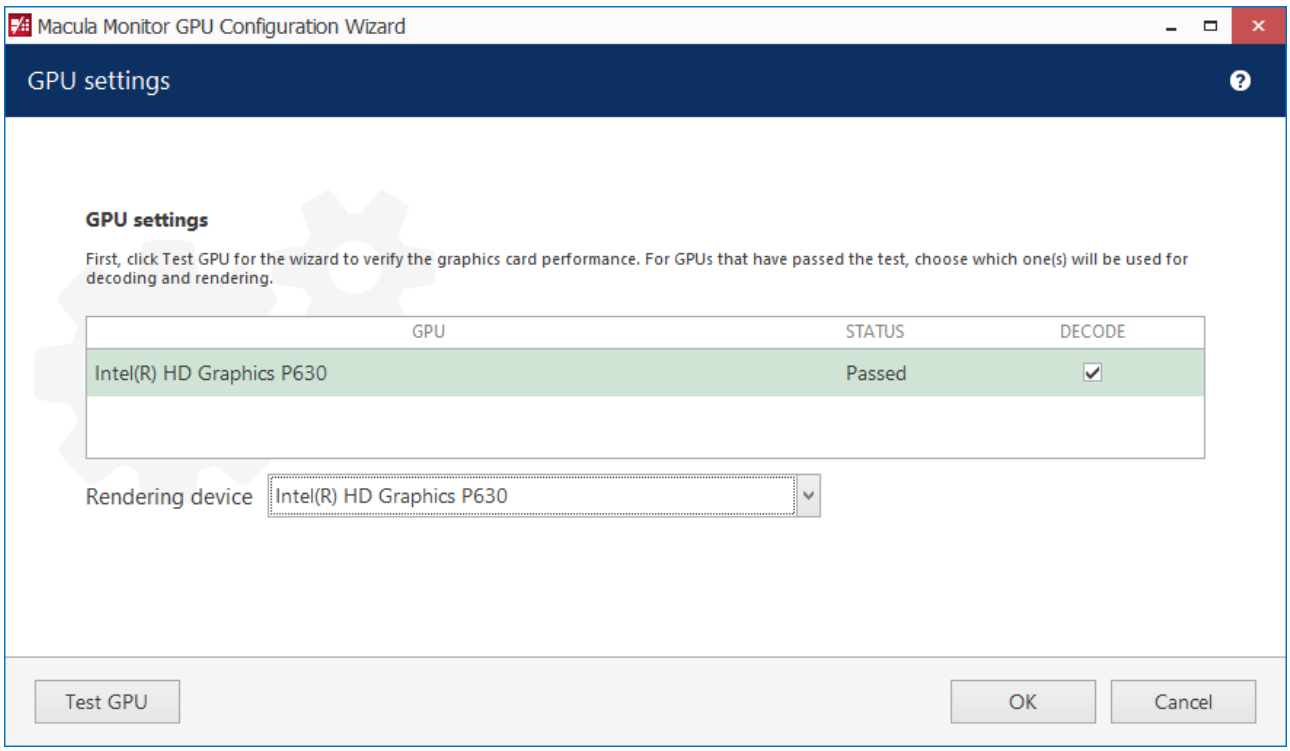
On every client workstation where you want to enable GPU usage, launch the *Renderer Test Utility* by locating it in the *Start* menu, or simply by typing a part of the name in the Windows search.

The first wizard screen is a **summary**. Here, you can select, which graphics cards will be used for decoding and for 3D rendering. To be able to do so, first run the GPU test so that Macula can learn about your GPU capabilities and possible maximum load. During the test, each GPU is consequently loaded with test videos of different resolutions, starting from bigger ones. As a result, a value list is created for each GPU, which is then used by the Macula Monitor application for load balancing.

> 💡 We recommend that you re-run the GPU test after each system change that may be related to graphics, as well as major OS updates (like feature updates) and Macula software upgrade.

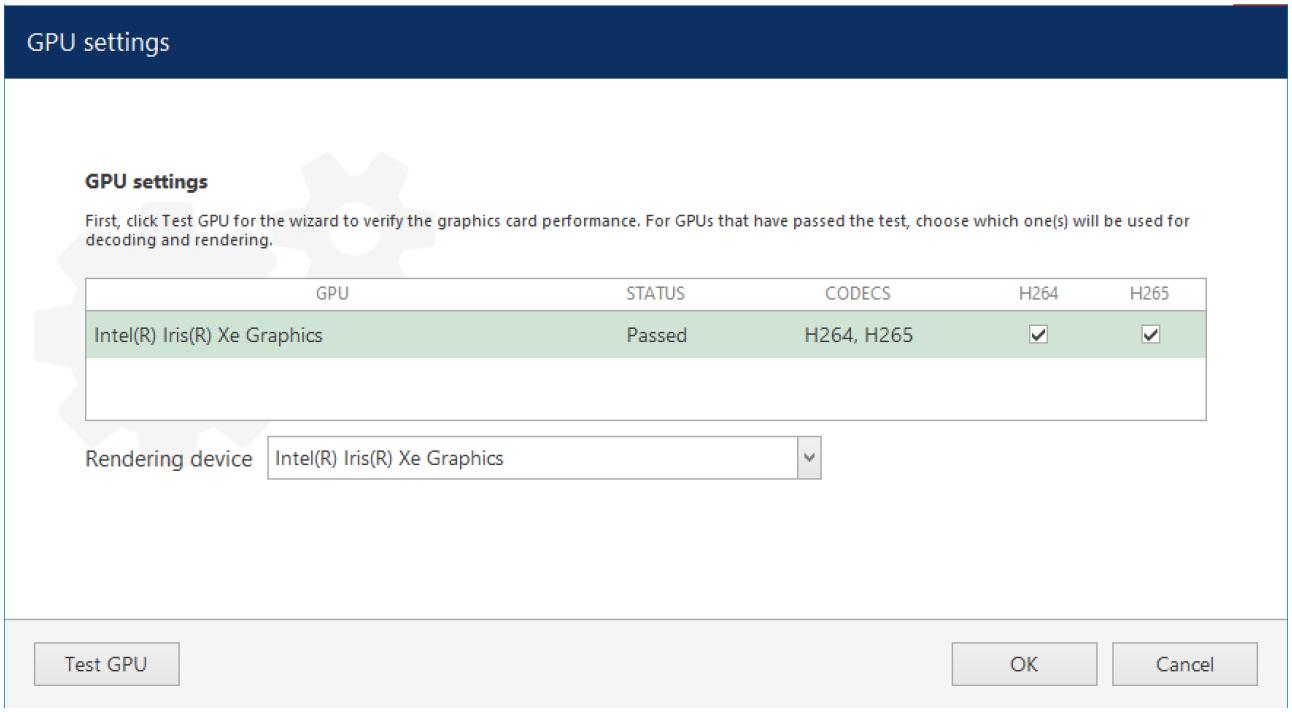
To run the **performance test**: hit the *Test GPU* button in the bottom left corner. In the list, mark all GPUs that you wish to engage by putting check marks in the *Test* column, then click *Test* below.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com



If you have already launched the test earlier, the *Status* column will reflect the last test results. For the GPUs that have passed the test, there is no need to re-launch it, unless you have made changes to that video card configuration (e.g., added memory for the integrated card, installed a different device driver etc.). The test may take some time. If your Macula Monitor application is open, the wizard will ask you to close it and re-open later (and offer to do so automatically).

During the test, click the *Show log* button to see how the test is going. After the test is finished, the wizard will automatically switch to the previous screen, and you still will be able to view the last test log.



Log colors:

- red: most important (errors, failures)
- yellow: warnings

- blue: information
- black: default
- grey: trace, details or low importance

Flags used in the test log indicate GPU capabilities:

- supported: graphics card is supported
- unsupported: hardware decoding is not supported by OS for this GPU
- legacy: video card is old or has old drivers, max resolution will be limited to 1080p
- canDecode: the GPU is OK to be used for decoding
- canRender: the GPU is OK to be used for rendering

As a result, the previously *Not passed* GPUs will change their status. GPUs that have passed the test, will be available for **decoding** (putting a check mark in the *Decode* column). Below the table, you can choose, which GPU will be used for **rendering**.

If you graphics card can decode both H.264 and H.265, you will have both codecs enabled after the test. However, you can deselect H.265 if you do not wish it to be decoded by GPU. Do not forget to restart Macula Monitor if you have just opened the wizard to change the settings (without running the test).

> Video output process on the Macula Monitor side consists of two stages: decoding frames and rendering for displaying them. After decoding, the frames are converted and passed for rendering. If decoding and rendering operations happen on different GPUs, CPU is used in between so its load may grow a bit. Therefore, if only one GPU is used for decoding, it may be wiser to use the same GPU for rendering. Same logic is to be applied for cases when one GPU takes the most decoding load (this can be deduced from the GPU test log). But, if you happen to have a GPU that does not support decoding, you may want to use it for rendering, so that the total load is split between GPUs.
>
> In general, according to our tests, **Intel GPUs have better decoding capabilities**, and Nvidia GPUs (hi-end) are good at 3D rendering.

Click *OK* to **save** the settings and exit. If you close the wizard by clicking *Cancel* or *X*, the GPU settings will not be saved.

> If you open the wizard and change **any settings** without running the test, please manually **restart** the Macula Monitor application for the changes to take effect.

You can re-open the wizard at any time to run the test again and/or change the settings.

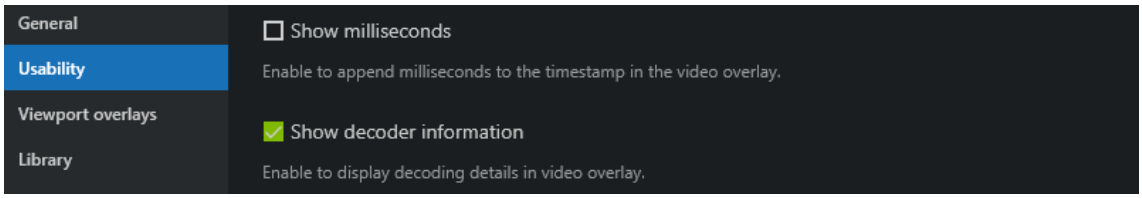
Usage in Macula Monitor

After you have enabled GPU settings via wizard, the Macula Monitor application on the same machine will be able to use GPU capabilities. Using GPU will significantly decrease the CPU load and will allow you to output more channels simultaneously on the same workstation. By combining GPU acceleration with substream usage you can gain even more, as using lower resolution streams for multichannel output is more efficient.

Macula Monitor will automatically use GPUs enabled via wizard, you do not have to enable anything else in the application settings. Limitations:

- **live** view and **DPTZ**
- **fisheye dewarp** (supported dewarp mode must be set in Macula Console, as described above)
- stream codec must be **H.264**
- stream **resolution** must be supported (see GPU test log for details), e.g., legacy GPUs will not be used for resolutions greater than FullHD

If you want to check whether the decoding is currently performed by GPU, enable rendering info in the Macula Monitor application settings. In the main menu, choose *Edit* > *Settings* > select the *Usability* tab > enable the *Show decoder information* option > *Save*.



After you have enabled this setting, each viewport in the live mode will have a **label next to the timestamp** (upper right corner):

- **CPU**: decoding is performed using CPU (GPU is not configured or overloaded, or stream codec/resolution is not compatible)
- GPU: the corresponding graphics card type will appear as a label - **Intel**, **Nvidia**, **AMD**, or **other GPU**.

> Macula Monitor will automatically switch to CPU decoding if the configured GPU is overloaded (more than 80% of its decoder, renderer or memory is used).
>
> Make sure you have at least 512MB of dedicated video memory per display (recommended minimum is 1GB per display).

Troubleshooting

If, immediately after enabling hardware acceleration, your Macula Monitor application behaves strangely, crashes, or causes other problems, try running it **without GPU** decoding. To do so a single time - for troubleshooting - use the *Macula Monitor without GPU decoding* shortcut from the Start menu (similar icon but in grey colors). This shortcut activates a so-called "**safe mode**" for the Macula Monitor application, which completely **ignores** the GPU settings configured via GPU test utility.

After launching the Macula Monitor application in "safe mode", check if the issue is gone. If the no-GPU mode helps, disable GPU decoding via *Renderer test utility* by de-selecting GPUs in the list (remove the check mark in the *Decode* column). If you have multiple graphics cards, the issue may be caused by one of them, so a wise approach would be to enable/disable the graphics adapters one by one in order to find out, which one is causing problems.

© GSF Corp. 2024 Macula Professional Administration Guide
www.gsfcorp.com