



ATEAS Security

user manual

ATEAS CZ

Na Dlouhém lánu 508/41 | 160 00 Prague 6 | Czech Republic

www.ateas.eu | info@ateas.net

CHAPTER 1 - INSTALLATION	14
1.1. GENERAL REQUIREMENTS	14
1.2. CONSISTENT INSTALLATION PROCESS	15
1.3. ADMINISTRATION SERVER SPECIFICS	18
1.4. CAMERA SERVER SPECIFICS	19
1.5. INSTALLATION FOLDER	20
1.6. AFTER INSTALLATION	21
1.7. CONFIGURATION PARAMETERS OF THE ADMINISTRATION SERVER	21
1.8. CONFIGURATION PARAMETERS OF THE CAMERA SERVER	22
1.9. CONFIGURATION PARAMETERS OF THE CAMERA CLIENT	24
1.10. AUTOMATIC UPDATES	24
1.11. MOBILE CLIENT INSTALLATION	26
1.12. NEURAL NETWORKS INSTALLATION	27
1.13. INSTALLING THE BROWSER COMPONENT	27
1.14. INSTALLATION OF OTHER ADD-ONS – LPR, UIC	28
1.15. IPV6 COMPATIBILITY	29
CHAPTER 2 - STARTING UP FOR THE FIRST TIME	30
2.1. FIRST LOGIN AND PROVIDING THE LICENSE KEY	30
2.2. MULTI-FACTOR AUTHENTICATION	36
2.3. ATEAS ID INSTALLATION IDENTIFIER	37
2.4. CERTIFIED INSTALLATIONS	37
2.5. BASIC SETUP WIZARD	39
2.6. CUSTOM SERVER NAMES	41
2.7. VERSION INFORMATION	42
2.8. PMA INFORMATION	45
2.9. APPLICATION MAIN MENU	45
2.10. APPLICATION AUTOMATIC STARTUP	46
2.11. SEARCHING, FILTERING AND SORTING	47
2.12. RENAMING ITEMS	48
2.13. TERMINAL CLIENT ACCESS	48
2.14. PROTOCOLS	49

CHAPTER 3 - HELP	50
3.1. DOCUMENTATION AND HELP	50
CHAPTER 4 - MONITORING	51
4.1. VIEWS	51
4.1.1. VIEWS ADMINISTRATION	51
4.1.2. NAME-BASED CAMERA SEARCH	62
4.1.3. DISPLAYING WEB CONTENT	63
4.1.4. VIEW LAYOUT DESIGNER	64
4.1.5. VIEWS ORGANIZATION	68
4.1.6. AUTOMATIC MODES	70
4.1.7. TOURS	72
4.1.8. OPENING ADDITIONAL WINDOWS	75
4.2. EVENTS AND ALARM LIVE VIEW	75
4.2.1. RECEIVING EVENTS	75
4.2.2. RECEIVING ACTIONS	78
4.2.3. SWITCHING EVENTS	79
4.2.4. WINDOW SUBDIVISION	79
4.2.5. SEPARATE EVENTS WINDOW	80
4.2.6. ALARM HANDLING	81
4.2.7. EVENT POSITIONS IN THE VIEW	82
4.3. INSTANT REPLAY	83
4.3.1. LIVE VIEW REPLAY	83
4.3.2. AUTO-REPLAY	88
4.3.3. DOWNLOADING RECORDINGS	88
4.3.4. CREATING BOOKMARKS	91
4.3.5. SMART SEARCH	92
4.3.6. SIMILARITY SEARCH	95
4.3.7. RESTRICTING ACCESS TO RECORDINGS	97
4.4. SELECTED CAMERA FUNCTIONS	98
4.4.1. CAMERA SELECTION	98
4.4.2. DISPLAYING DETAIL	100
4.4.3. SAVING SNAPSHOTS	101
4.4.4. PTZ DEVICE CONTROL	101

4.4.5. PTZ LOCKS	105
4.4.6. SPECIAL PTZ FUNCTIONS	106
4.4.7. PRESET POINTS	107
4.4.8. OUTPUT ACTIVATION	108
4.4.9. RECEIVING AUDIO	109
4.4.10. PUSH-TO-TALK	110
4.4.11. DIGITAL ZOOM	112
4.4.12. MANUAL RECORDING	114
4.4.13. FISH-EYE IMAGE DEWARPING	115
4.4.14. DISPLAYING METADATA	117
4.4.15. MOTION DETECTION AND ANALYTICS CONFIGURATION BY USERS	119
4.5. USING TRANSACTION DATA	120
4.5.1. LIVE VIEW	120
4.5.2. REPLAYING TRANSACTIONS	120
4.5.3. SAVING A TRANSACTION	121
4.6. COOPERATION WITH THE MAP WINDOW	122
4.6.1. SYNCHRONIZATION DURING CAMERA OR ELEMENT SELECTION	122
4.6.2. EVENT SYNCHRONIZATION	123
4.6.3. MAP SELECTION	124
4.7. WORKING WITH THE VIDEO WALL	125
4.7.1. SWITCHING CAMERAS	125
4.7.2. DISPLAYING METADATA	126
4.7.3. SWITCHING URLS	127
4.7.4. DETAIL DISPLAY	128
4.7.5. VIDEO WALL VIEWS	129
4.7.6. AUTOMATIC MODE	130
4.8. WORKING WITH COUNTERS	132
4.8.1. ZONE COUNTERS	133
4.8.2. COMPLEX COUNTERS	133
4.8.3. DISPLAYING THE VALUE OF COUNTERS	134
4.8.4. MANUAL RESET OF THE COUNTER	134
4.8.5. EVENT BASED RESET OF THE COUNTER	136
4.8.6. ZONE COUNTERS IN THE MAP	136

4.8.7. COUNTER VALUES IN WEB CONTENT	136
4.9. WORKING WITH THE FACE DATABASE	137
4.9.1. FACE PREVIEW	137
4.9.2. FACE DATABASE	137
4.9.3. ADDING IMAGES	139
4.10. VIDEO INFORMATION	139
CHAPTER 5 - WORKING WITH RECORDINGS	141
5.1. SEARCHING FOR A RECORD	141
5.1.1. RECORDINGS SUMMARY	141
5.1.2. DISPLAYING VIDEO OVERVIEWS	143
5.1.3. PREVIEWING AND SAVING RECORDINGS	146
5.2. META SEARCH	146
5.2.1. DEFINING CONDITIONS	147
5.2.2. DISPLAYING RESULTS	150
5.2.3. ADVANCED TEXT SEARCH	151
5.2.4. EXPORT FUNCTIONS	154
5.2.5. CHARTS	155
5.2.6. AUTOMATIC REPORTING	160
5.3. ALARM DATABASE	164
5.3.1. ACCESSING THE ALARM DATABASE	164
5.3.2. EXPORTING AND PRINTING THE LOG	166
CHAPTER 6 - USING THE DOWNLOAD MANAGER	168
6.1. INTRODUCTION	168
6.2. TASK MANAGEMENT	169
6.2.1. ADDING A TASK AUTOMATICALLY	169
6.2.2. ADDING A TASK MANUALLY	170
6.2.3. TIME LAPSE VIDEOS	171
6.2.4. TASK LIST CONTROL	173
6.3. DOWNLOADS SETUP	174
CHAPTER 7 - WORKING WITH SNAPSHOTS	176
7.1. SNAPSHOT MANAGEMENT	176
7.1.1. SNAPSHOT SUMMARY	176

7.1.2. ADDING INFORMATION	178
7.1.3. PRINTING SNAPSHOTS	178
7.1.4. SERVER CAMERA PREVIEW	180
CHAPTER 8 - LOCAL SETUP	181
8.1. BASIC SETUP	181
8.1.1. LANGUAGE SELECTION	182
8.1.2. MONITORS AND SCREENS	183
8.1.3. EVENTS	185
8.1.4. MAP	186
8.1.5. VIDEO SETTINGS	188
8.1.6. WORKSPACE	192
8.1.7. AUTO START OPTIONS	194
8.1.8. LOGIN HISTORY	196
8.1.9. TEXT DISPLAY SETTINGS	196
8.1.10. KEYBOARD	197
8.1.11. MESSAGES	198
8.1.12. CUSTOM INDICATORS	199
8.2. JOYSTICK SETUP	200
8.2.1. BASIC SETUP	200
8.2.2. BUTTON FUNCTIONS	202
CHAPTER 9 - ADDITIONAL TOOLS	204
9.1. LIVE GUARD	204
9.2. CUSTOM BUTTONS	205
9.3. PLATE LISTS	207
CHAPTER 10 - WEB ACCESS	208
10.1. RUNNING THE WEB CLIENT AND LOGIN	208
10.2. LIVE VIEW	209
10.3. SELECTED CAMERA FUNCTIONS	211
10.4. WORKING WITH RECORDINGS	213
10.4.1. REPLAYING RECORDINGS	213
10.4.2. EXPORTING RECORDINGS	214
10.5. CLIENT SETTINGS	214

CHAPTER 11 - SYSTEM ADMINISTRATION	215
11.1. ENTERING THE ADMINISTRATION SECTION	215
11.2. CAMERA MANAGEMENT	217
11.2.1. AUTOMATIC CAMERA DISCOVERY ON THE NETWORK	217
11.2.2. ADDING AND REMOVING CAMERAS IN THE SYSTEM	219
11.2.3. VIDEO CAPTURE CARD SUPPORT	230
11.2.4. BASIC CAMERA SETUP	231
11.2.5. VIDEO SETTINGS	253
11.2.6. BATCH CAMERA CONFIGURATION AND REMOVAL	260
11.2.7. ADDRESS AND LOGIN CHANGE	261
11.2.8. MOTION DETECTION ON THE SERVER	262
11.2.9. ANALYTIC SOURCES	266
11.2.10. ZONE MAP LOCALIZATION	280
11.2.11. VIDEO ANONYMIZATION	281
11.2.12. SERVER BASED STATIC MASKING	282
11.2.13. CONNECTING ANALYTICAL SOURCES TO PRESETS	282
11.2.14. DETAILED SETUP	283
11.2.15. EVENTS AND THEIR MANAGEMENT	284
11.2.16. DYNAMIC SOURCES AND ONVIF EVENT SOURCES	305
11.2.17. BATCH EVENT CONFIGURATION	309
11.2.18. DYNAMIC EVENT SCHEDULING	310
11.2.19. COMPLEX EVENT SOURCES	312
11.2.20. LOCATING CAMERAS IN THE MAP	318
11.2.21. EXPORTING AND IMPORTING CAMERAS	321
11.3. CUSTOM EVENTS AND OBJECT TYPES	322
11.3.1. CUSTOM EVENTS	322
11.3.2. SYSTEM NAMES FOR CUSTOM EVENTS	325
11.3.3. EVENT MANAGEMENT	326
11.3.4. CUSTOM OBJECT TYPES	326
11.4. SCHEDULED EVENTS	327
11.4.1. BASIC SETUP	327
11.4.2. EVENT MANAGEMENT	330
11.5. ALARM HANDLING MODE	331

11.5.1. MODE BASICS AND ACTIVATION	331
11.6. RECORDINGS MANAGEMENT	332
11.6.1. MEDIA STORES	332
11.6.2. RECORDING RULES	346
11.6.3. BACKUP	353
11.7. VIEWS MANAGEMENT	357
11.7.1. SHARING VIEWS	357
11.7.2. SYSTEM SHARED VIEW GROUPS	358
11.7.3. VIDEO WALL	358
11.8. LPR ENGINE ADMINISTRATION	363
11.8.1. SELECTING CAMERAS FOR DETECTION	363
11.8.2. MASK CONFIGURATION	369
11.8.3. WORKING WITH LP LISTS	370
11.8.4. LP RECOGNITION SETTINGS	372
11.8.5. EVENT MANAGEMENT	373
11.9. UIC ENGINE ADMINISTRATION	375
11.9.1. SELECTING CAMERAS FOR DETECTION	375
11.9.2. EVENT MANAGEMENT	378
11.10. SERVER AND USER MANAGEMENT	379
11.10.1. BASIC SERVER MANAGEMENT	379
11.10.2. CAMERA SERVER CONNECTION IN CLOUD MODE	386
11.10.3. USING A DOMAIN NAME FOR CAMERA SERVER	387
11.10.4. GPU ACCELERATION IN THE SERVER SERVICE	388
11.10.5. STARTING A NEURAL NETWORK ON THE SERVER	390
11.10.6. CLUSTER ADMINISTRATION	394
11.10.7. SMTP ACCOUNTS	397
11.10.8. DEVICE CERTIFICATION	397
11.10.9. NOTIFICATIONS	399
11.10.10. CONFIGURATION BACKUP AND RESTORE	401
11.10.11. DLNA STREAMING SUPPORT	404
11.10.12. SERVER MIGRATION	407
11.10.13. USER ADMINISTRATION	407
11.10.14. GROUP ADMINISTRATION	424

11.10.15. FOUR EYES PRINCIPLE	425
11.10.16. USER POLICY	426
11.10.17. USERS INTEGRATION WITH EXTERNAL SOURCES	429
11.10.18. AUTHENTICATION METHODS	433
11.10.19. ATEAS INTERLOGIN FEATURE	435
11.10.20. PRINT REPORTS	436
11.10.21. SYSTEM LOG	437
11.10.22. SYSLOG PROTOCOL SUPPORT	441
11.11. EXTERNAL	442
11.11.1. VIRTUAL STRUCTURE OF OBJECTS	442
11.11.2. CREATING EVENT SCENARIOS	446
11.11.3. LOCATING ELEMENTS IN THE MAP	448
11.11.4. COMMUNICATION CHANNELS	448
11.11.5. NETWORK TCP AND HTTP CHANNELS	449
11.11.6. NETWORK SNMP CHANNEL	451
11.11.7. WEB SERVICE AKV CHANNEL	453
11.11.8. SIA INTEGRATION CHANNEL	454
11.11.9. FILTERING IP ADDRESSES	456
11.11.10. USER BUTTONS	456
11.11.11. DOCUMENT INTEGRATION	460
11.12. LICENSING AND ACTIVATION	462
11.12.1. LICENSE KEYS AND THEIR ACTIVATION	462
11.12.2. SYSTEM EXTENSIONS	465
11.12.3. ACTIVATING NEW VERSIONS	465
11.12.4. AUTOMATIC LICENSE REACTIVATION	466
CHAPTER 12 - PLAYER	468
12.1. STARTING THE PLAYER	468
12.2. REPLAYING VIDEO IN ATS FORMAT	469
12.2.1. OPENING A FOLDER	469
12.2.2. FILE LIST	471
12.2.3. REPLAYING A FILE	472
12.2.4. INDEXED FOLDERS	478
12.2.5. FISH-EYE IMAGE DEWARPING	479

12.2.6. VIDEO EXPORT	480
12.2.7. AVI VIDEO EXPORT	481
12.2.8. MP4 VIDEO EXPORT	484
12.3. DIGITAL SIGNATURE	485
12.4. FILE PROPERTIES	487
CHAPTER 13 - MAP WINDOW	490
13.1. MAP WINDOW BASICS	490
13.2. MAP DATA DISTRIBUTION	492
13.3. MAP WINDOWS BASICS	493
13.3.1. MOVING AND ZOOMING THE MAP	493
13.3.2. SWITCHING LEVELS	495
13.3.3. SEARCHING THE MAP	496
13.4. ADDITIONAL MAP FUNCTIONS	496
13.5. DYNAMIC MAP LAYER AND VIDEO PREVIEW IN THE MAP	498
13.6. DISPLAYING MAPS DIRECTLY IN THE LIVE WINDOWS	502
13.7. GEOGRAPHICALLY LINKING THE MAP LEVELS	504
CHAPTER 14 - ACCESS FROM APPLE DEVICES	506
14.1. SUPPORTED FEATURES	506
14.2. LAUNCHING AND LOGIN	506
14.3. CAMERA LIST AND LIVE VIDEO	509
14.4. VIEWS OF MULTIPLE CAMERAS	511
14.5. REPLAYING RECORDINGS	512
14.6. SETUP	515
14.7. USING THE INTEGRATED CAMERA	517
CHAPTER 15 - ACCESS FROM ANDROID DEVICES	519
15.1. SUPPORTED FEATURES	519
15.2. LAUNCHING AND LOGIN	519
15.3. CAMERA LIST AND LIVE VIDEO	521
15.4. VIEWS OF MULTIPLE CAMERAS	523
15.5. REPLAYING RECORDINGS	523
15.6. SETUP	525
15.7. NOTIFICATIONS	527

15.8. USING THE INTEGRATED CAMERA	528
15.9. ANDROID TV	530
15.9.1. VIDEO WALL	531
CHAPTER 16 - APPLICATION FOR MONITORING THE SCREEN	532
16.1. INSTALLATION AND START-UP	532
16.2. CONFIGURATION	534
CHAPTER 17 - APPENDIX 1 – NETWORK CONFIGURATION	536
17.1. ADMINISTRATION SERVER	536
17.2. CAMERA SERVER	536
CHAPTER 18 - APPENDIX 2 – ATEAS API	538
18.1. COMMUNICATION BASICS	538
18.2. ATEAS API OF THE ADMINISTRATION SERVER	538
18.2.1. EXTERNAL EVENTS	538
18.2.2. VIDEO WALL	539
18.2.3. LICENSE PLATES	541
18.2.4. FACE DATABASE	542
18.2.5. USER AND GROUP MANAGEMENT	548
18.2.6. DEVICE MANAGEMENT	554
18.2.7. EVENT NOTIFICATIONS	558
18.2.8. USER NOTIFICATIONS	562
18.3. ATEAS API OF THE CAMERA SERVER	563
18.3.1. EXTERNAL EVENTS	563
18.3.2. METADATA	564
18.4. PARAMETERIZED APPLICATION LAUNCH	565
18.4.1. ADMINISTRATION SERVER	565
18.4.2. CAMERA SERVER	565
18.4.3. CAMERA CLIENT	566
CHAPTER 19 - APPENDIX 3 – EXTERNAL ANALYTICS DATA	568
19.1. PREREQUISITES	568
19.2. INTEGRATION WITH THE VTRACK SYSTEM	568
19.2.1. CONNECTING METADATA FROM SERVER	568

19.2.2. CONNECTING METADATA FROM CAMERA	569
19.2.3. LINKING EVENTS	570
CHAPTER 20 - APPENDIX 4 – OPENSTREETMAP SOURCES	572
20.1. CREATING MAPS FROM FREE MAP SOURCES	572
20.1.1. AREA SELECTION AND DATA DOWNLOAD	572
20.1.2. DATA CONVERSION	573
20.1.3. USING THE DATA	573
20.1.4. SUPPORT FOR VARIOUS LEVELS OF DETAIL	574
20.2. GENERATING MAPS FROM RASTER BITMAPS AND PLANS	574
CHAPTER 21 - APPENDIX 5 – JSON DATA INTEGRATION	576
21.1. PREREQUISITES	576
21.2. CAMMRA APPLICATION INTEGRATION	576
21.2.1. RECEIVING METADATA OVER TCP	576
21.2.2. RECEIVING METADATA OVER HTTP	577
21.2.3. METADATA AND EVENTS	577
21.2.4. CHARTS	578
CHAPTER 22 - APPENDIX 6 – AXIS BODY WORN INTEGRATION	579
22.1. CONNECTING TO ATEAS	579
22.2. ADDING CAMERAS AND USERS	582
22.3. SYSTEM OPERATION	583
CHAPTER 23 - APPENDIX 7 – CERTIFICATES	584
23.1. INTRODUCTION	584
23.2. PREREQUISITES	584
23.3. CERTIFICATES	587
23.3.1. ACME PROTOCOL	588
23.3.2. WILDCARD CERTIFICATES	589
23.4. USING AN EXISTING CERTIFICATE OF AN ORGANIZATION	590
23.4.1. OBTAINING THE CERTIFICATE	590
23.4.2. EXPORTING THE CERTIFICATE	592
23.4.3. INSTALLING THE CERTIFICATE	593
23.4.4. UPDATING DNS RECORDS	593

23.4.5. TESTING THE CERTIFICATE	593
23.5. USING A NEW CERTIFICATE	595
23.5.1. CREATING A ROOT CERTIFICATE	595
23.5.2. CREATING THE SERVER CERTIFICATE	596
23.5.3. INSTALLING THE CERTIFICATE	599
23.5.4. PRELIMINARY CERTIFICATE TEST	600
23.5.5. PROVING THE ORIGIN OF THE SERVER	601
23.5.6. FINAL CERTIFICATE TEST	604

Chapter 1 - Installation

1.1. General requirements

A Microsoft operating system is required to run ATEAS Security products. The entire ATEAS Security system installation is very simple and only takes several minutes. The installation requires you to be logged on as administrator under Windows. If required by the installer, .NET framework generation 4 needs to be installed with the minimum version of 4.8. The ATEAS Screen Recoder can cope with 4.0 version, which makes it possible to use it for older computers.

NOTE

In most cases the .NET framework will already be part of your operating system.

ATEAS Security system also comes with an automatic update engine. Downloading and installing the new administration server (ATEAS Administrator) directly from the client application is the only user action required. All other applications will be updated automatically.

Each edition of the ATEAS Security product requires the installation of three basic ATEAS Security applications:

1. ATEAS Security Administrator – ATEAS Security system server, central login to system or a central camera server and event management.
2. ATEAS Security Server – ATEAS Security camera server, communication with cameras or video servers. Responsible for video and audio stream management, recordings and event evaluation.
3. ATEAS Security Observer – client application, the only user interface application in the system. It provides full access to the system and its administration (completely adjusts the behavior of servers, cameras, recordings etc.).

Apart from these applications, several additional add-ons or components are offered, such as the ATEAS Screen Recorder application, emulating a camera on a standard computer, or the ATEAS Security LPR Engine for detecting vehicles license plates.

The HOME edition usually installs both server applications on a single computer. The client application can be installed to a location of your choice (on the same computer where both server applications are

installed). However, compared to the PROFESSIONAL edition, system access is limited to only two simultaneous accesses.

The PROFESSIONAL edition sees the ATEAS Administrator and ATEAS Server are generally installed on a camera system computer (server), where recording and event management will proceed. ATEAS Observer is then installed on a corresponding number of client workstations which will access the system.

The UNLIMITED edition installation is identical to the installation of the PROFESSIONAL edition, with the only difference being the ATEAS Server application can be installed on additional computers (servers), to which additional cameras or devices can be connected.

1.2. Consistent installation process

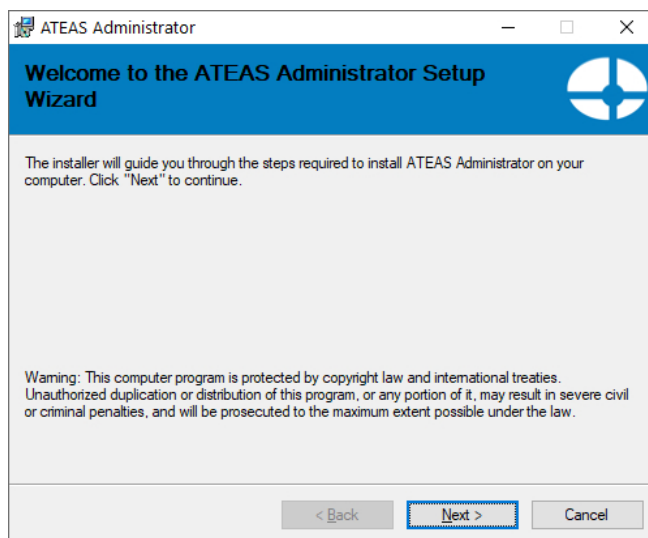
All three applications are installed identically using the same installation wizard. Links to the installation for all of these applications including other important links can be found directly on the page that automatically opens after inserting or connecting the installation media. The following links are available:

- first chapter of the product documentation on system installation,
- installing the system administration server,
- installing the system camera server,
- installing the client application,
- access to clients for iOS and Android in their respective stores (free),
- installing applications for computer monitoring.

Camera servers, client applications and all other applications can also be installed using the administration server web page. Compared to the links that are directly on the installation media home page, this page also contains links to important documents, complete product documentation in print quality and an ATEAS API demo application.

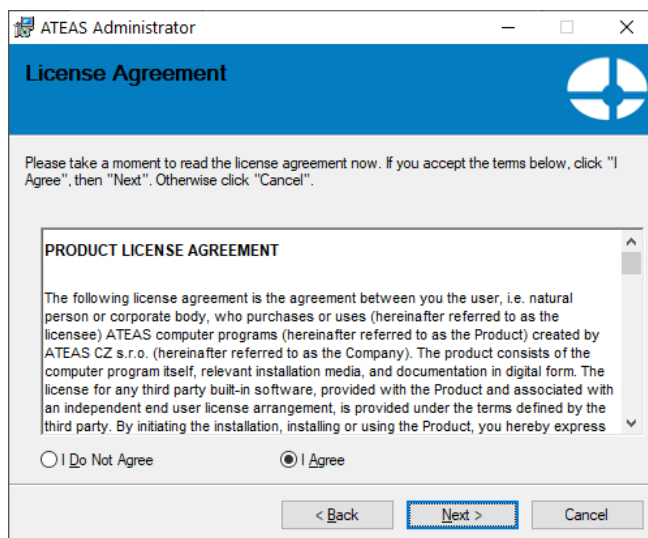
All three applications can be installed in any order. Now, we will go through the ATEAS Security Administrator installation process. The installation process of the two other applications is completely identical to this installation with only a few minor differences, described further in this chapter.

Step 1 – Installer welcome screen.



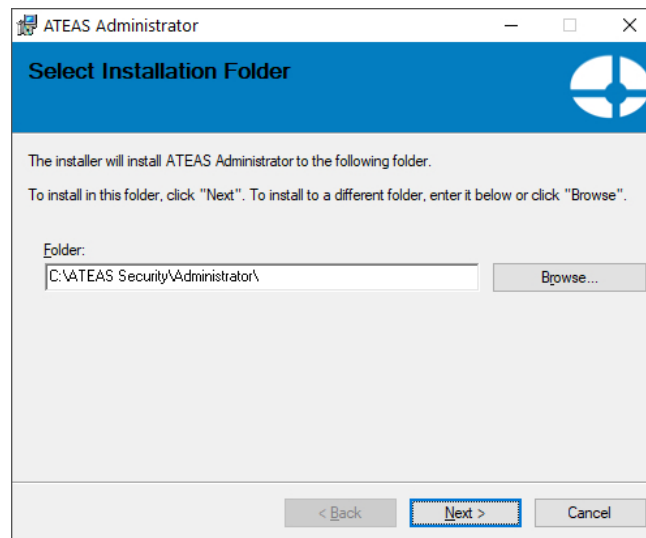
Continue installation by pressing the **NEXT** button.

Step 2 – License agreement.



Check the I agree radio button and continue with installation by pressing the **NEXT** button.

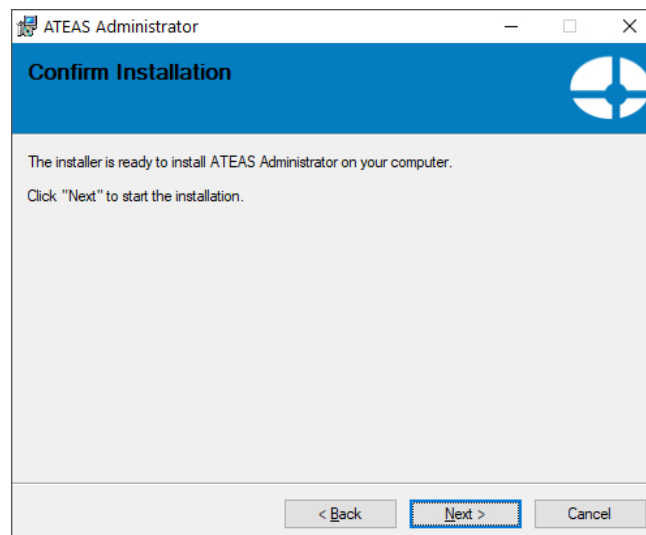
Step 3 – Installation folder selection.



This part of the installation requires selecting a destination folder, where the application shall be installed. Changing the hard drive can be easily accomplished by re-writing the beginning letter in the text field labeled Folder.

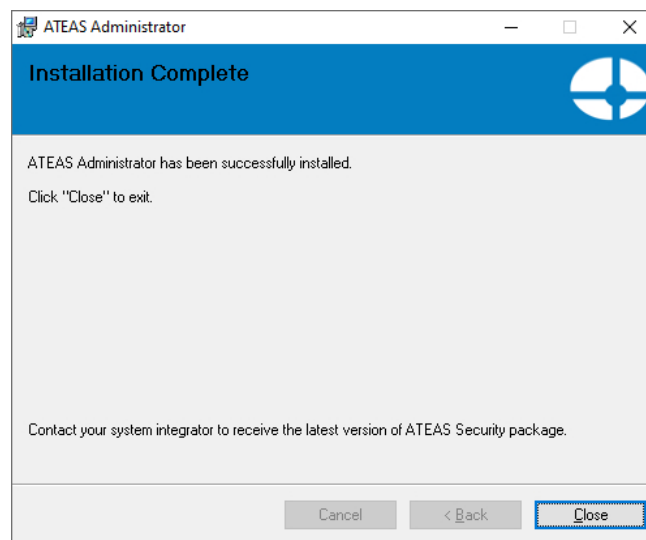
Continue the installation by pressing the **NEXT** button.

Step 4 – Installation confirmation.



Continue the installation by pressing the **NEXT** button.

Step 5 – Finishing installation.



The Installation is finished by pressing the **CLOSE** button.

1.3. Administration server specifics

When installing the administration server, an additional dialog appears before the start of the installation process, informing the user that if you are upgrading an existing installation the system cannot be activated if no ATEAS PMA service is active. Make sure that the ATEAS PMA service has been activated for the respective ATEAS ID before starting the installation process on an existing installation.

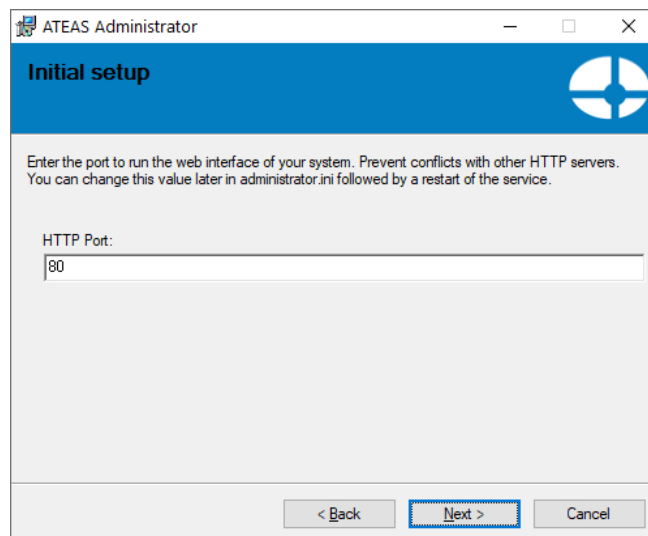
NOTE

In the trial version, new product versions can be installed without any restrictions.

A dialog box will appear during the administration server installation, where the user can enter a numerical value for the designated HTTP port, used by the administration server for communicating with web browsers. Both control or data communication ports are listed in the appendix. Nevertheless, a client application can be easily installed or downloaded from a web browser; therefore a CD is not required.

NOTE

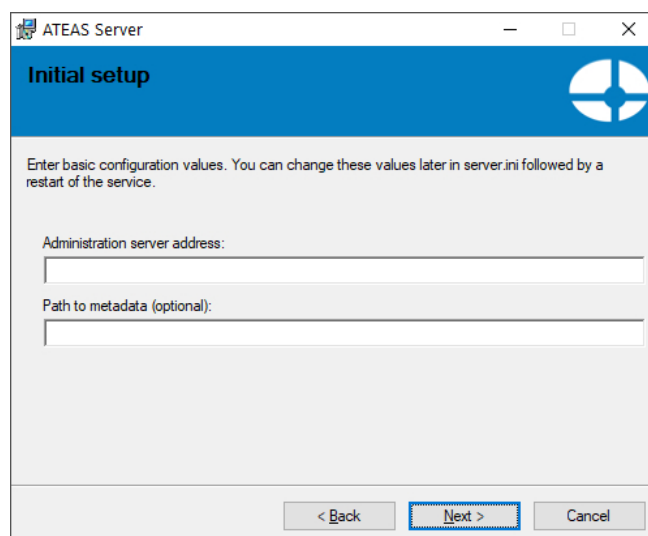
A camera server can be also downloaded or installed from a web browser. However, only an administrator can add a new camera server to the system.



The default value of the HTTP port is set to 80. In this case, the administration server can be accessed from the web browser using its address, e.g. 10.0.0.1. In case another port is used, the user must add this port to the address (e.g. 10.0.0.1:999). The HTTP port must not be used by any other application or server such as Apache, IIS, etc. This value can be changed at any time in administrator.ini, using the HTTPPORT key found in the installation folder. This action requires the ATEAS Administrator service be restarted.

1.4. Camera server specifics

The camera server installation will ask for the address or name (computer name or DNS) of the administration server. Every single camera server must be connected to the administration server. There is only one administration server in each system.



Please consider the following rules and recommendations when filling in the address:

HOME and PROFESSIONAL editions: The administration server address is consistent with the camera server address since both server applications are installed on one computer (server). Therefore, fill in the local IP address of the computer or server (e.g. 10.0.0.1 or 192.168.1.1, etc.).

UNLIMITED edition: A limitless amount of camera servers can exist in the local network, WAN or internet. Fill in the address to establish a connection with the administration server. This address may either be an address in a local area network or the WAN address of the NAT-enabled router, which redirects the communication to the administration server.

NOTE

For proper server service operation in the NAT environment, see network configuration. There are certain ports that need to be open for ATEAS Security applications.

This value can be changed in server.ini using the ADMIN key, found in the installation folder. This action requires ATEAS Server service to be restarted.

Optionally, a custom location for video analytics metadata can be specified during installation. This location can be changed later in the server.ini file.

1.5. Installation folder

The default location for installing the server services is set to ATEAS Security on the system disk. This location can be changed during install. For the client, the system folder for 64-bit applications is used by default. Every Windows account has a separate data folder with settings, exports or maps location in the system folder for local application data.

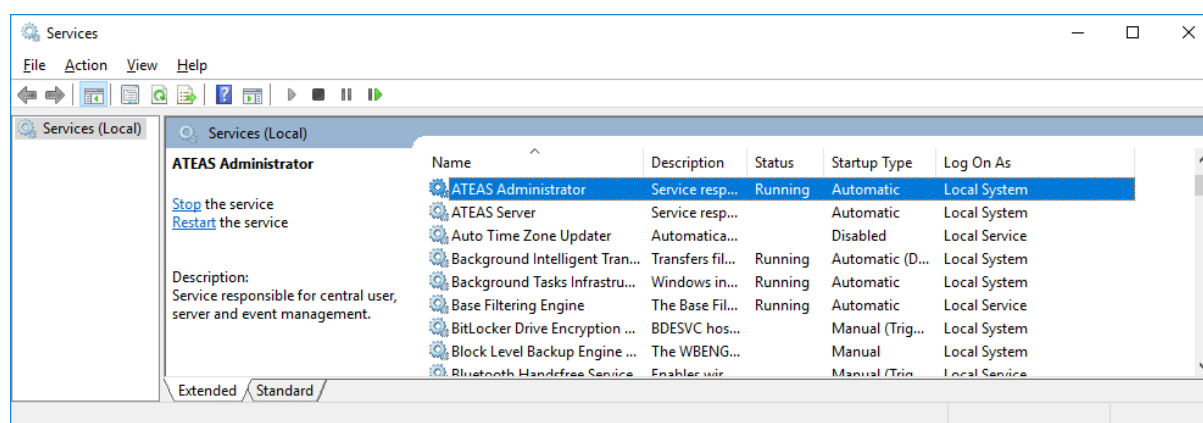
TIP

Therefore, every user can configure an automatic login according to his Windows account.

1.6. After installation

Server applications (ATEAS Administrator and ATEAS Server) are installed on your computer or server as services with no user interface. All system controls, system management and settings are executed within the ATEAS Observer client application environment. The installer will automatically create a corresponding program group in the Start Menu that will include the ATEAS Observer shortcut, also appearing on the desktop.

After the installation, both server applications are started automatically and their startup value is set to automatic (see the following picture), meaning both applications are started automatically at Windows startup (regardless of whether a user is logged on or not) and terminated at Windows shutdown.



This is how you navigate to the services window:

English operating system: Start – Control panel – Administrative tools – Services.

1.7. Configuration parameters of the administration server

The configuration parameters of the administration server are located in the administrator.ini file in the administration server installation folder. These parameters can be configured directly in this file using any text editor. The administration server service shall always be restarted for changes to be applied.

HTTPPORT (default value 80): This parameter is automatically set to the value entered during installation and specifies the port on which the administration server displays the home page of your camera system, runs the web client, and manages automatic system updates.

HTTPSSPORT (default value 443): This parameter specifies the port on which the administration server displays the homepage of your camera system and runs the web client via the secured http protocol.

WEBCCLIENT (default value OFF): Permits or denies web access to the system (value OFF or ON).

WEBFORCETLS (default value OFF): If the value is set to ON, sensitive parts of the web content will be forced to use the https protocol. This affects using the web client or automatic server and client updates. For this feature to work, a certificate must be set up. The configuration process is described in this documentation.

SERVICEUSER item (not used by default): Specifies the user name for the service to log in.

SERVICEPASSWORD item (not used by default): Specifies the password in an encrypted form for the service to log in.

REALTIME (default value 0): If set to 1, the service process will gain maximum priority on operating system level. This can help to fight some energy saving settings of the hardware if the service suffers from not getting enough CPU time to read networks packets.

NOTE

These service related items are only effective when a service is reinstalled, not just restarted.
The service uses the Local System account by default.

1.8. Configuration parameters of the camera server

The configuration parameters of the camera server are located in the server.ini file in the camera server installation folder. These parameters can be configured directly in this file using any text editor. The camera server service shall always be restarted for changes to be applied.

ADMIN item (default value 127.0.0.1): This parameter specifies the name or address of the administration server in the system, to which the given camera server shall connect and be a part of. This value is automatically set to the value entered during installation.

METADATAPATH item (not used by default): Specifies a full path for a location used to store video analytics metadata for forensic search purposes. By default, this will be directly in the server's installation folder.

SERVICEUSER item (not used by default): Specifies the user name for the service to log in.

SERVICEPASSWORD item (not used by default): Specifies the password in an encrypted form for the service to log in.

WANKEY item (not used by default): This item defines the unique camera server key for camera server connection in cloud mode.

HTTPPORT item (default value 8080): Specifies the http port number of the camera server service, which might be used by some other systems e.g. when downloading media from body worn cameras.

HTTPUSER item (default value root): Specifies the username when authenticating to the http server.

HTTPPASS item (default value pass): Specifies the password when authenticating to the http server.

REALTIME (default value 0): If set to 1, the service process will gain maximum priority on operating system level. This can help to fight some energy saving settings of the hardware if the service suffers from not getting enough CPU time to read networks packets.

DECODESTRICTMODE (default value 1): Specifies the strictness when decoding video. A value of 0 includes some lightweight bitstream checking only and enables corruption repair algorithms. A value of 1 adds some additional memory range checks and disables most video repair algorithms, a value of 2 adds more detailed bitstream checking, and a value of 3 requires full standards compliance, including cases where any error correction would be safe. Values of 2 and 3 may increase the CPU consumption. This value affects H264/5 CPU decoding only. GPU decoding and AV1 video format are not affected.

LOCALIP (not used by default): The parameter can be used to select the proper network interface for establishing a connection with the administration server of the system, which would ensure the camera server is properly identified. However, this is only used in rare situations when the camera server is unable to automatically determine the use of network interfaces. For more information see the Multiple network adapters chapter.

MULTICASTSOURCEIP (not used by default): This parameter allows you to select a network interface that will be used for multicast transmission. For more information see also the Multiple network adapters chapter.

DLNA item (not used by default): This item determines the network interface for broadcasting video via DLNA standard. If not populated, an interface is chosen automatically.

FORCEDSERVERID (not used by default): Camera servers are commonly identified within the system based on their address, which gives them a unique number in the system, assigned by the administrator. This parameter can be used to distinguish multiple server connections from the same address.

NOTE

These service related items are only effective when a service is reinstalled, not just restarted. The service uses the Local System account by default.

1.9. Configuration parameters of the camera client

The configuration parameters of the camera client are located in the observer.ini file found in the client installation folder. Updates can be made directly to this file via text editor. The client must be restarted with each update.

MUTEXLEVEL (default value 1): The item specifies that a mutex system object is used to prevent a duplicate launch of the client. If the client is launched in terminal mode (e.g. using desktop virtualization technology with GPU acceleration), depending on the selected virtualization depth, this protection may need to be disabled by setting the value to 0. For more information, see also the GPU acceleration chapter.

DECODESTRICTMODE (default value 1): Specifies the strictness when decoding video. A value of 0 includes some lightweight bitstream checking only and enables corruption repair algorithms. A value of 1 adds some additional memory range checks and disables most video repair algorithms, a value of 2 adds more detailed bitstream checking, and a value of 3 requires full standards compliance, including cases where any error correction would be safe. Values of 2 and 3 may increase the CPU consumption. This value affects H264/5 CPU decoding only. GPU decoding and AV1 video format are not affected.

1.10. Automatic updates

The installation of ATEAS Security applications installation is very quick and simple supporting comfortable automatic system updates. Automatic updates are available for both camera servers (ATEAS Server service) and system clients (ATEAS Observer). Only the system administration service (ATEAS administrator) requires reinstallation in terms of the full system update. The rest of the system will be updated automatically. The new version of the system (administration server) can either be obtained directly via ATEAS installation medium, available in ISO format, or can be downloaded

directly from the new system version check window. See Version information chapter for more information.

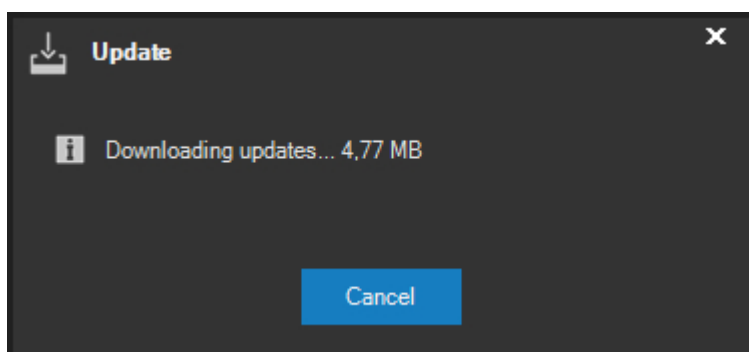
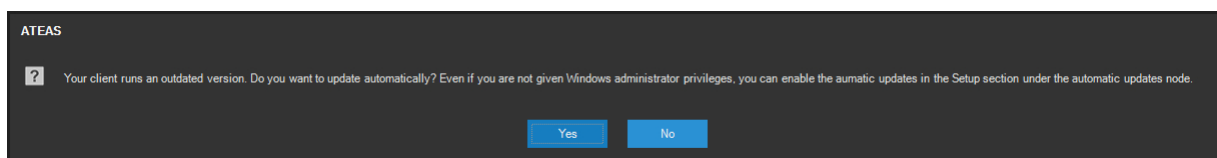
NOTE

When reinstalling the system administration server, the old version of the product is automatically replaced, thus a manual uninstall is not necessary.

Camera servers, disconnected during the system administration core installation (basic functions are not interrupted), are capable of downloading and executing updates, after automatic reconnection to the Administration server, followed by a restart of the service.

Automatic updates make life easier especially on large systems with many clients or for UNLIMITED edition users with many camera servers, capable of executing the update and restarting themselves automatically (after the administration server service has been updated).

System clients are disconnected during the system administration core reinstallation and need to be logged in again. After the login process, the client is capable of downloading and executing the automatic update. The client automatic update process is guided by a very simple update wizard as follows.



CAUTION

In order for the automatic update process to run successfully, the administration server requires the HTTP port be available, making it possible to download the update package. The port (see the network ports appendix) is implicitly set to 80 and may be changed in administrator.ini.

NOTE

If the computer involved is included in the video wall (i.e. the user currently logged in is created as a video wall account), the update will automatically start without having to confirm the dialog by pressing **YES**, because the video wall computers do not necessarily have peripheral devices connected.

1.11. Mobile client installation

The application for mobile access to the system can be launched or installed using the links on the installation CD or from your system's administration server address.

The iOS application requires the iOS operation system, installed on Apple devices - iPhone, iPad. The application is started after being downloaded from the App Store. The application is free to download.

The Android OS application requires the Android operating system, installed on various types of smart phone and tablet devices. The application is started after being downloaded from the Android application online store (Google Play). The application is free to download.

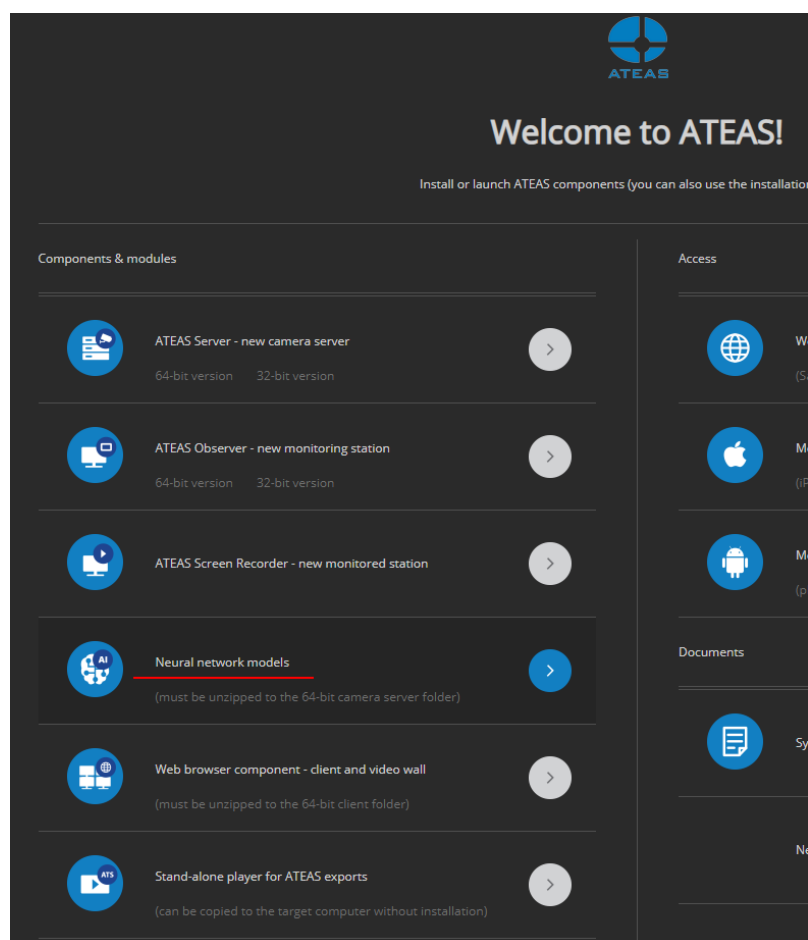
The Android application can also be installed on devices such as televisions or displays running the Android operating system, controlled via remote controller or as part of a video wall. The same APK used for the mobile phone or tablet can be used for the installation. If the application detects it has been launched on a television or other display, it automatically selects the optimized user interface.

NOTE

Some Android displays do not feature a display recognition option and the application will be launched with the phone interface. In this case, during the installation, you must use the APK, which includes the interface for televisions and display only.

1.12. Neural networks installation

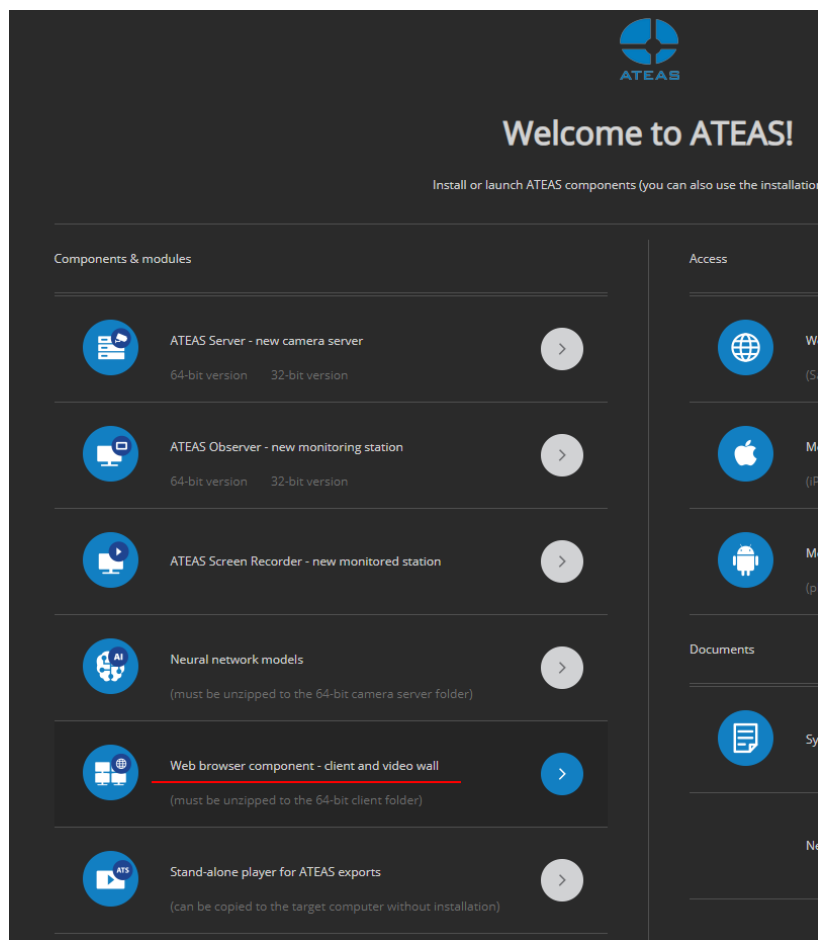
A neural network can easily be installed by downloading the archive directly from the system administration server website and unpacking the contents of the archive to the installation directory of the camera server designated to be equipped with artificial intelligence and analysis capability features.



After the installation, you can continue in server administration section by pressing the **DNN** button.

1.13. Installing the browser component

Apart from cameras ATEAS client or the video wall can also display any web based content. For this purpose, a web browser component must be added to the client that is available on the administration server website.



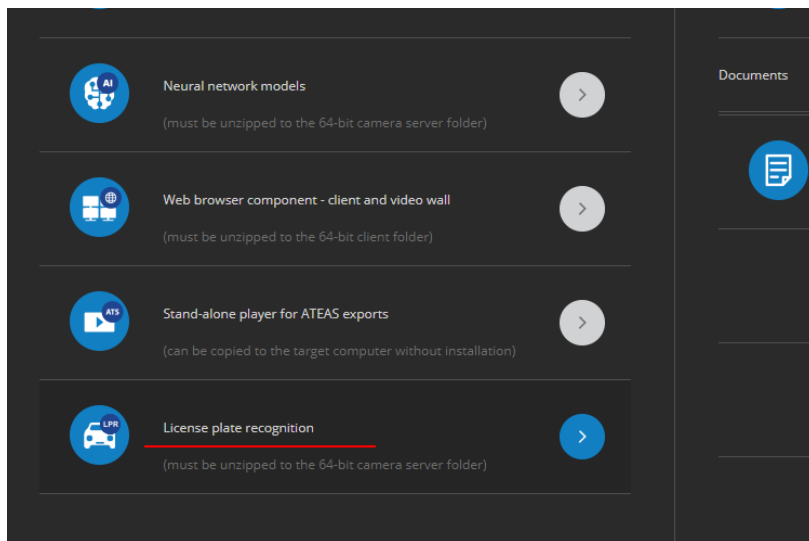
The archive must be unzipped to the ATEAS client installation folder.

NOTE

The web browser component can only be used with the 64-bit version of the client and can't be used with an Android powered display device, which can be part of the video wall.

1.14. Installation of other add-ons – LPR, UIC

Installing the license plate recognition engine, the UIC wagon number recognition engine or other engines is as easy as unpacking the installation package in the camera server's installation folder. The main webpage of your administration server contains all important installation links for downloading the engines. A link to the LPR engine is shown in the following image.



After the installation, you can continue in the add-on administration section.

NOTE

An additional license may be required for license plate recognition or other modules.

1.15. IPv6 compatibility

The actual exhaustion of public IPv4 addresses is the key driving force behind the evolving use of IPv6 addresses. The first to be affected by the transition to IPv6, in terms of camera systems, will be the users accessing the system from IPv6 (mobile) networks, in which IPv4 addresses will no longer be assigned to the devices. Therefore, ATEAS also supports the IPv6 protocol for communication between system components (users, servers, cameras).

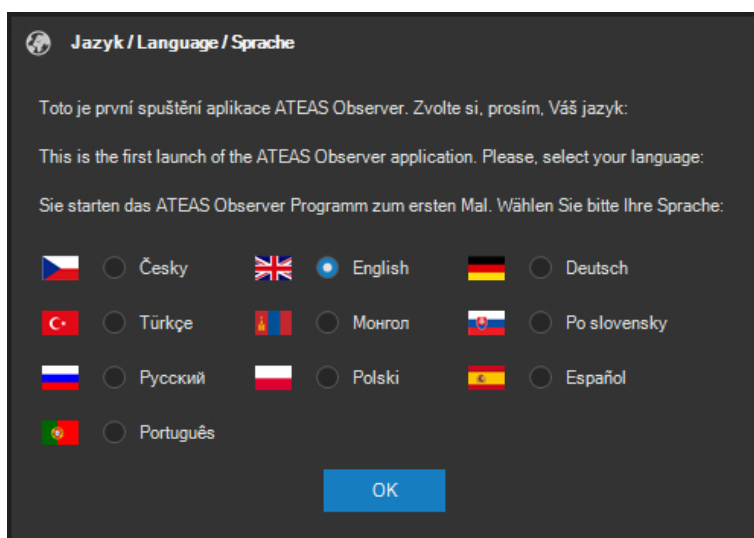
Chapter 2 - Starting up for the first time

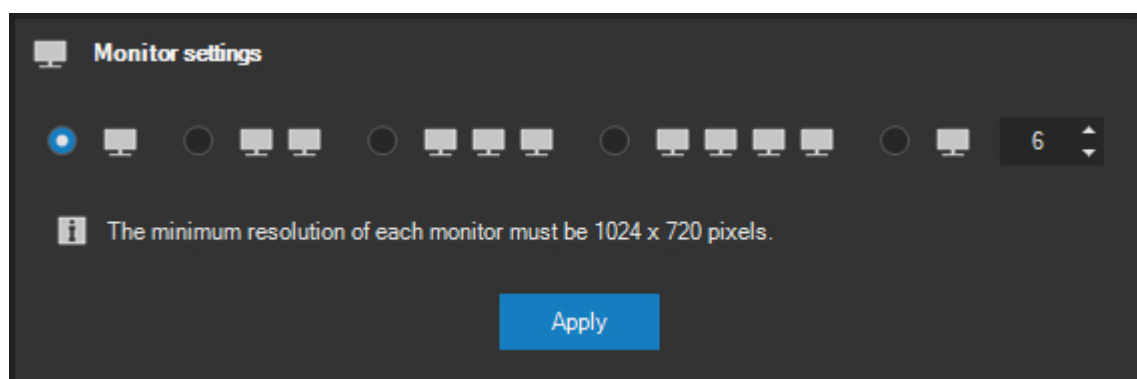
2.1. First login and providing the license key

NOTE

For more information about license activation and obtaining the activation key, please read the Product activation and license key upgrade subchapter (found under the administration section). If your system has not been activated yet, this information is available at the address of your administration server (using a web browser). This subchapter also includes information interesting to hackers.

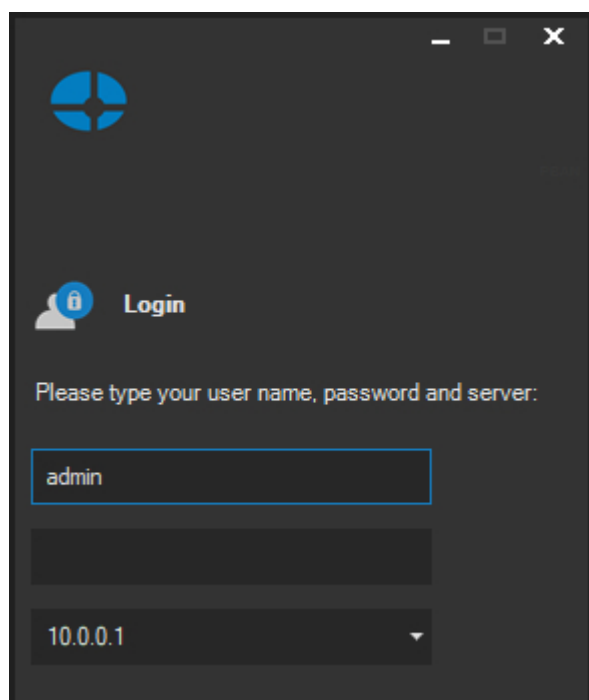
Several basic application setup dialogs are displayed when running the application for the first time on a given workstation (language selection and multiple monitor settings). In both cases, it is necessary to select one of the options and continue by pressing the **OK** or **APPLY** button (the language might be preselected according to your system's settings). Further information about monitor settings can be found in the documentation section regarding local application settings, where these options may be changed.



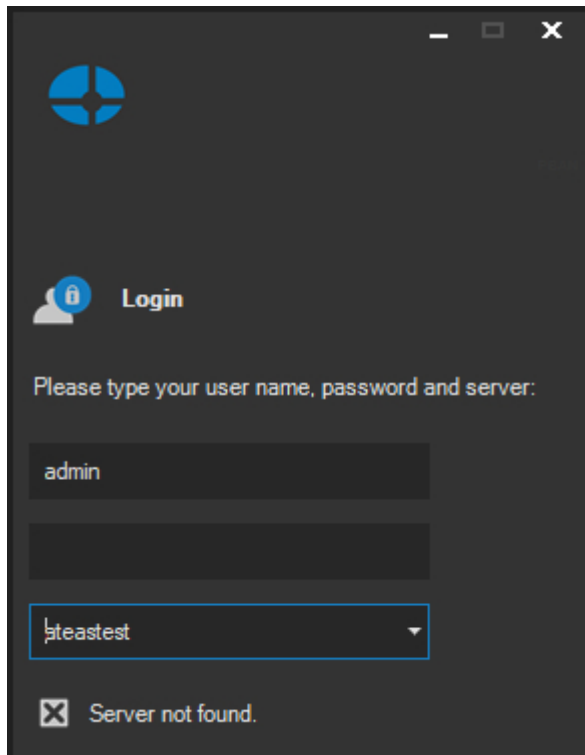


After the client application (ATEAS Security Observer) is started, the system will require the user to enter his username, password and server to log in. The system uses a predefined administrator account **admin** with the password **admin**. The system does not accept identical usernames and passwords, so the user must change his password after the first login. You can enter either the IP address or the name of the server where the ATEAS Security administration server is currently running. After the user is successfully authenticated, the server name or address is saved and does not need to be entered again in the future.

The client application remembers the last login. When logging on again, not only is the server information automatically filled in, but a list of recently used servers is also available. It is possible to select any given item from the list or use the auto-complete function when typing via the keyboard. The drop-down list is always sorted according to the server login dates, in descending order starting with the most recently used names or addresses.



The application always states the cause of an unsuccessful login, as seen in the following picture:



The most common reasons for unsuccessful authentication include:

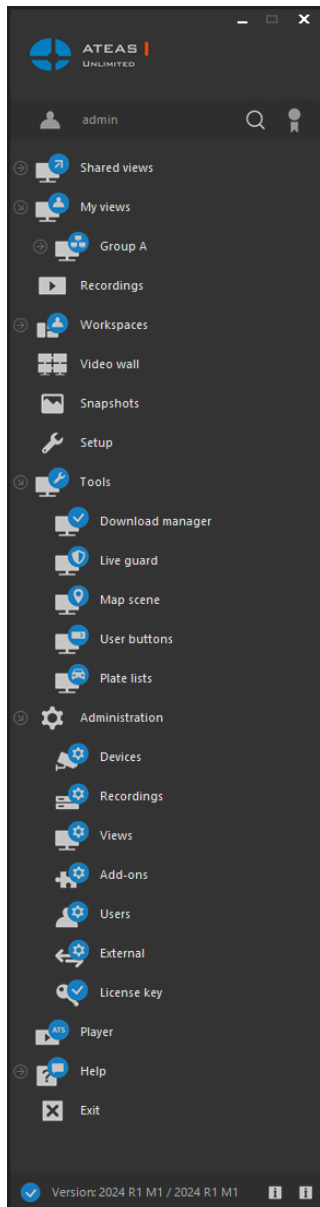
- incorrect username or password, note that passwords are always case sensitive,
- incorrect address or server name,
- network connection problems,
- exceeding the limit of simultaneous client accesses as per the actual license,
- invalid (outdated) client application version,
- duplicate login (with the option to log off ourselves from another desktop client).

The system does not accept identical usernames and passwords and will ask the user to change the password following the first login as admin (this also applies to passwords reset by the administrator or logging on with a new user account for the first time). The following is an overview of rules that shall be considered when creating a new system password:

- the minimum password length is 4 characters (providing the system administrator did not modify the user policy, which requires the minimum length to be higher or for the required password to be strong),
- passwords are case sensitive,

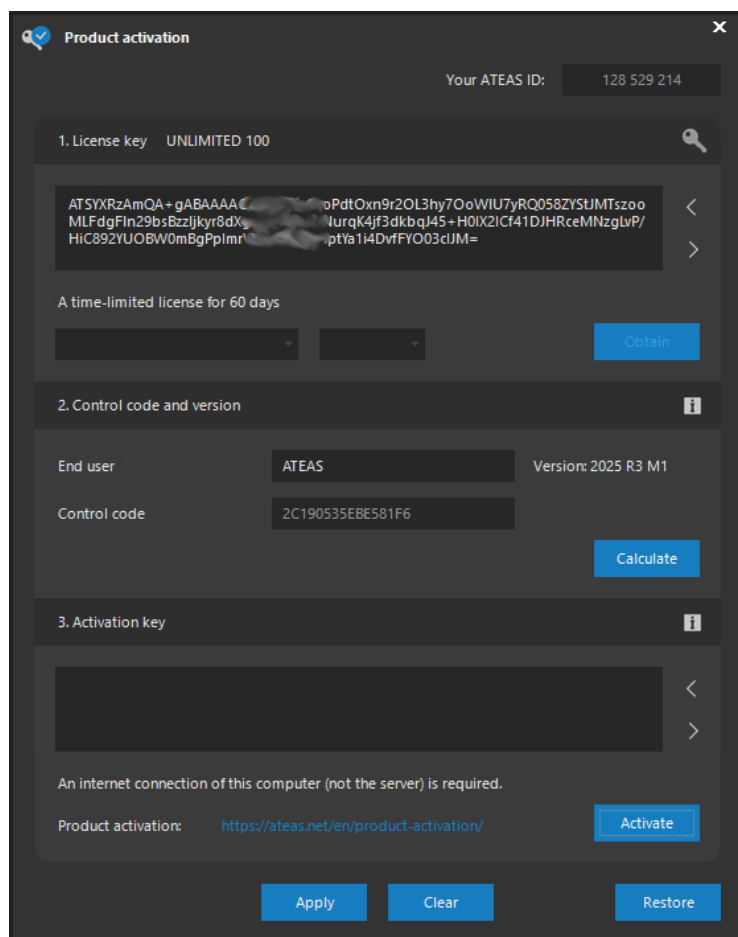
- entering a password identical to the username is not possible (regardless of case sensitivity).

The application main menu will appear after the login is successful. You will also see a logo corresponding to the currently installed product edition (HOME, PROFESSIONAL, UNLIMITED) and a small administration server connection indicator will appear at the bottom.



Connections to all camera servers and to the administration server are maintained automatically and can be recovered on break up. The administration server connection status is indicated by a symbol located in the bottom left corner of the main menu window.

After the initial client application startup, the administrator shall enter a license number, otherwise it will not be possible to continue working with the system.



The screenshot shows the 'Product activation' window with the following sections:

- Header:** 'Your ATEAS ID: 128 529 214'
- 1. License key:** 'UNLIMITED 100'. It displays a license key: 'ATSYXRzAmQA+gABAAAAE...'. Below it, a note says 'A time-limited license for 60 days'. There are dropdown menus for selection and an 'Obtain' button.
- 2. Control code and version:** 'End user: ATEAS', 'Version: 2025 R3 M1', 'Control code: 2C190535EBE581F6'. There is a 'Calculate' button.
- 3. Activation key:** A large empty text box for the activation key. Below it, a note says 'An internet connection of this computer (not the server) is required.' and a link for 'Product activation: https://ateas.net/en/product-activation/'. There is an 'Activate' button.
- Footer:** 'Apply', 'Clear', and 'Restore' buttons.

The license key number you purchased shall be entered in the License key section. This license number can be copied or inserted from the license file that was attached to the activation e-mail. Importing the license key from the license file can be performed via the white arrow button. More information is provided in the product activation documentation section in the full version of this document, which is also available at your administration server address.

If you have not purchased a license number, you can automatically obtain a trial license for 60 days. To do this, simply select the edition, number of cameras and use the **OBTAIN** button. You can upgrade from a trial license to a commercial license without any time limit at any time.

CAUTION

It is not possible to downgrade the system license to a lower edition or number of cameras. This should be kept in mind if you plan to upgrade to a commercial license later.

After entering the license key, the name of the license end user shall be entered followed by pressing **CALCULATE** to generate the control code.

CAUTION

A valid end user name must be entered. System users can display the name at any time and, provided the name is incorrect, they shall request the name to be corrected. A system with an invalid end user name is considered to be improperly licensed.

NOTE

The end user name is a precaution that increases the security of providing licenses. The end user names are not monitored or saved in any way, nor are they transmitted to the licensing server during system activation.

NOTE

Besides the end user name of the license, the control code calculation also includes basic information about the computer on which the administration server is installed.

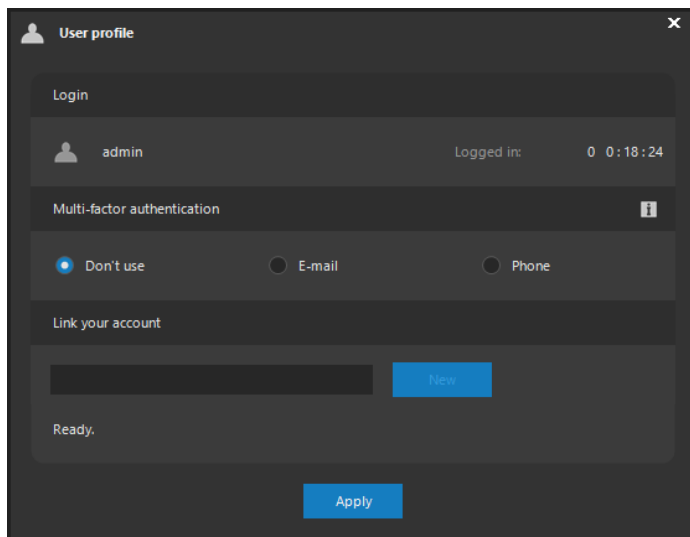
Apart from the license number, it is necessary to obtain the activation key. This can be done either online by clicking the **ACTIVATE** button or using the links at the bottom of the window. You must have an internet connection to access ATEAS servers (not necessary for computers with ATEAS software equipment installed).

The license dialog also includes a **RESTORE** button that allows you to restore the system configuration after a clean installation. You can learn more about configuration backups and restores in the chapter on server administration.

This dialog can be closed without entering a license number by clicking the **CANCEL** button.

2.2. Multi-factor authentication

As a part of the user policy, system administrator can activate the possibility or obligation of multi-factor user authentication. In such a case, the user can (or will be forced to) click his username in the main window to display the multi-factor authentication dialog.



The user's uptime is displayed in the upper part of the dialog. To activate the multi-factor authentication, it is necessary to select one of the supported (and allowed by the administrator) methods and use the **NEW** button to initiate the association process.

In the case of the e-mail address, it is necessary to click on the link in the verification e-mail sent by the server. In the case of the mobile verification, it is necessary to log in from a mobile app. The dialog always displays the remaining time to complete the association process.

CAUTION

Multi-factor authentication is an effective way of protection against disclosing users' credentials. However, it must be configured before the disclosure, not after.

Once the account has been linked, a multi-factor authentication will require you to confirm a link in the verification e-mail or authenticate the login in the mobile app. The mobile app always displays the username, the address of both the client and the system and the login time together with the **CONFIRM** and **IGNORE** buttons.

TIP

Using an iOS device, the notification can also be handled without actually launching the app by long-pressing it and displaying its options.

2.3. ATEAS ID installation identifier

After the license key has been entered and the system has been activated, the ATEAS ID will be displayed in the top right corner of the license dialog. This ID serves as a unique and permanent identifier of your software copy and shall be used for all technical and process matters regarding your installation. The ATEAS ID is a nine character numerical identifier.

The ATEAS ID also facilitates installation management for installation companies, for ATEAS ID stays the same for all standard system operations:

- The license key (along with the activation key) is updated when the system is expanded, nevertheless, the assigned ATEAS ID remains the same.
- When the system is moved to a different hardware configuration and the license is deactivated, the control code for your license (along with the activation key) is updated, nevertheless, the assigned ATEAS ID remains the same.
- Upgrading to a newer version of the system results in the activation key changing with the reactivation process, nevertheless, the ATEAS ID remains the same.

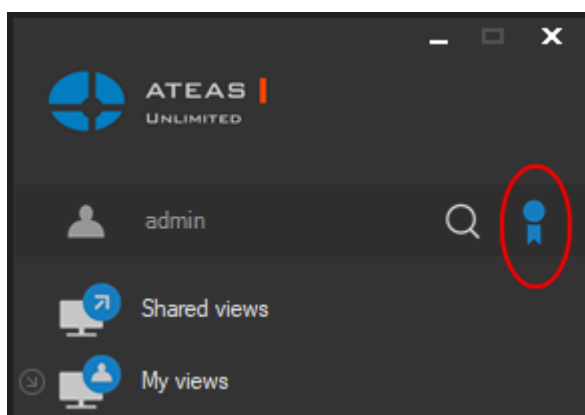
2.4. Certified installations

Your installation can be certified. This indicates the installation was carried out by a company that meets the requirements for performing certified installations, which in particular include undergoing various levels of authorized administrator ATEAS training sessions. An installation certificate is generated and automatically uploaded to the system during the license key activation process. The certificate is an XML file uploaded to the certificates subfolder under the installation folder of your administration server.

NOTE

A certificate is also generated for manual license key activations performed on the ATEAS webpage. A download link is created to download the certificate. This file must be placed in the folder stated above. This must then be followed by a restart of the administration server.

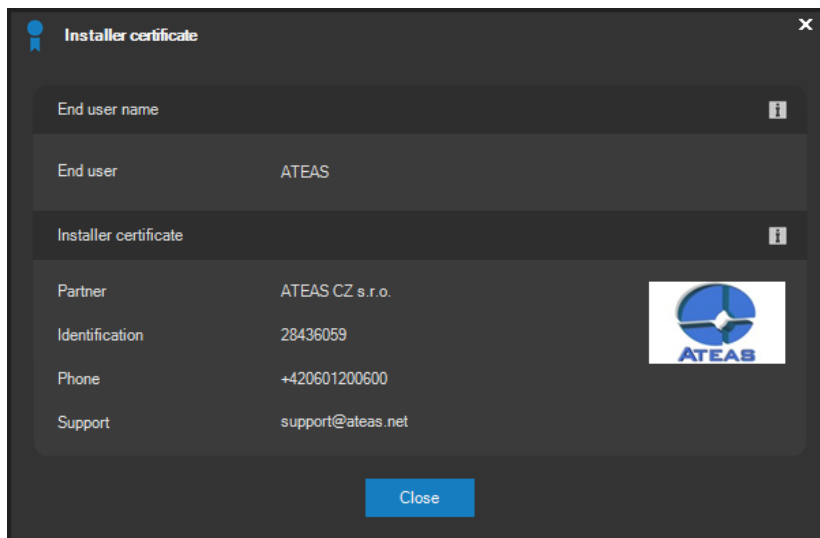
A bold certificate symbol in the top left corner of the window with the application main menu indicates your system is a certified installation.



In addition, the certificate includes the following features:

- The certificate is digitally signed directly on ATEAS servers and cannot be created by anybody else.
- A certificate is linked and issued to a specific ATEAS ID and is non-transferable.
- The certificate contains the installation partner's credentials as well as their ID including logo. Optional data includes phone or online support contacts.

This data can be displayed at any time by clicking on the certificate icon.



Besides the certificate of the installation partner, this dialog also displays the end user name. In order to create a control code for your installation, a valid end user name shall be entered during system activation.

CAUTION

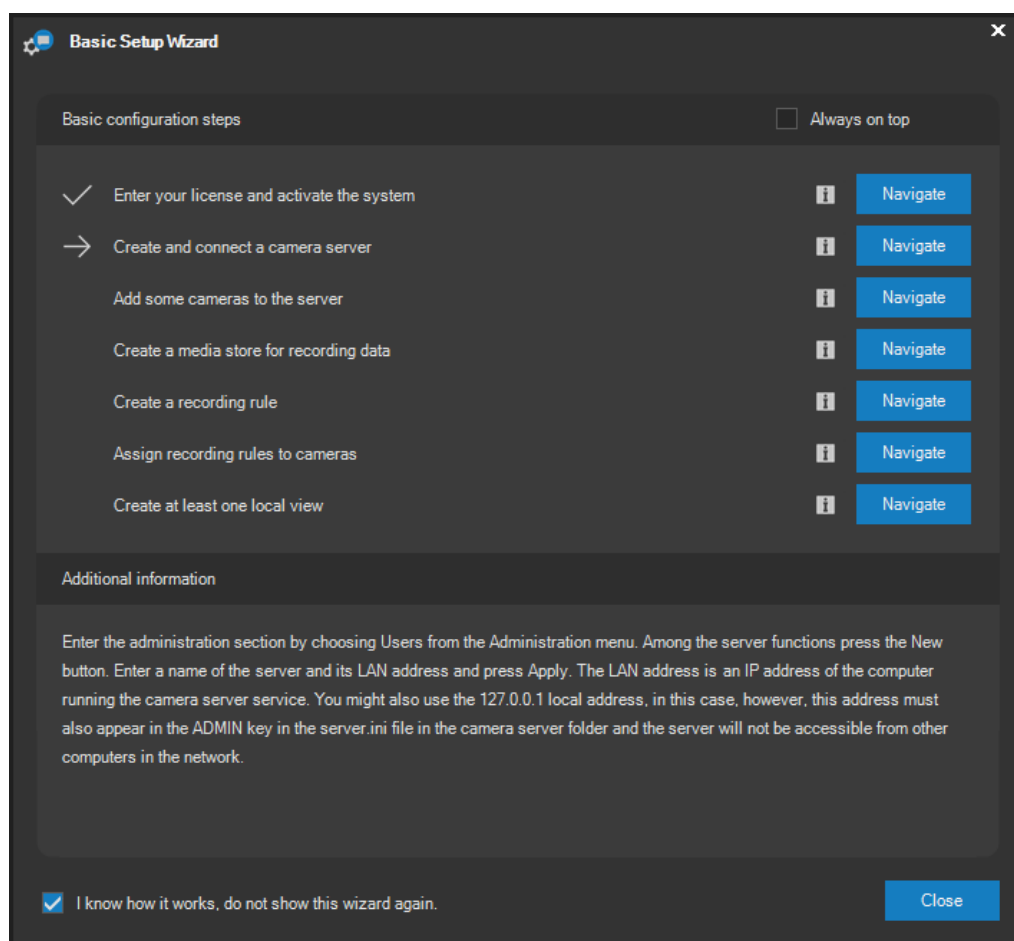
If your installation shows a different end user name, you should contact your installation partner to rectify such situation. A system with an invalid end user name is considered to be improperly licensed.

NOTE

If the installation partner's certificate is not available in the system, the certificate icon in the main menu is grey and no certificate can be displayed. However, end user data will always be visible.

2.5. Basic Setup Wizard

The Basic Setup Wizard will automatically be launched after the user successfully logs in to the system for the first time. This wizard will guide you through several basic steps normally required to get the fundamental functions of the camera system up and running. These functions, for example, include adding cameras, setup recordings or creating a live view.



The setup wizard is well organized into several basic steps covering license entry and system activation, creating a camera server, adding cameras to the server, creating a media store for recording data and creating a recording rule, assigning recording rules to cameras and creating at least one local camera view. During the setup process, the wizard displays information stating which steps have already been carried out and which step is the next to be performed.

Detailed information on how to perform each step is displayed at the bottom of the wizard window. A **NAVIGATE** button is also available for each step, which automatically opens the respective window with the settings required for the given action. The blue button with the information icon will provide additional information for any of the steps.

If you do not wish to use the wizard for system setup, it can be deactivated by activating the checkbox on the bottom edge of the window. In this case the wizard will no longer appear.

NOTE

The wizard can be reactivated at any time by manually selecting Setup Wizard from the Help menu.

NOTE

The wizard is shown automatically only for the master system administrator (administrator number 1), authorized to perform all steps in the installation wizard. This is only the case should any of the setup steps not be carried out. If all steps have been carried out, the wizard will not appear.

NOTE

The wizard can be loaded by other system administrators manually, but will not appear automatically. The wizard cannot be opened by standard system users.

The wizard window is displayed in front of all other opened windows, ensuring you always have the current setup step in front of you. However, the wizard on top feature can be disabled by deactivating the Always on top option.

2.6. Custom server names

When logging in, the text field for entering the server supports both the server IP address, as well as the server name (e.g. DNS name or local network name). These names are then displayed in the drop-down list, which shows the history of recent successful logins sorted in chronological order with the names of the most recently used names shown first.

NOTE

The history can contain up to 25 login items.

Based on experience, logging in to various camera systems using a single client can create a confusing list of IP addresses, which seemingly cannot be assigned to specific systems. These can be substituted with aliases.

NOTE

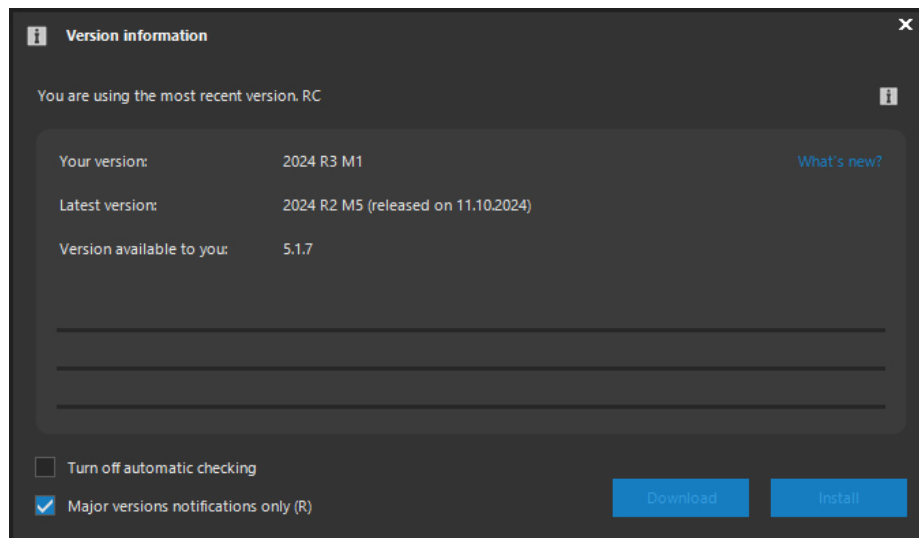
In this case we mean logging into multiple different camera systems, each of which has a custom licensed administration server. We are not referring to the situation in which multiple servers exist within a single camera system. Here, the users of course perform a single sign on, granting them access to all servers in an UNLIMITED edition simultaneously.

Custom logon server names (alias names) can be created under Settings, in the Login history section, where this feature is described. In addition to this, the alias can also be created by direct entry immediately when logging in by adding the alias into parentheses behind the actual network name or server address, e.g. 10.0.0.10 (alias).

The alias names created in local settings section or by following the procedure specified in the previous paragraph can then be used in the same manner as network names. The alias names just need to be entered into the server field when logging in.

2.7. Version information

Icons with an information symbol are located in the bottom part of the main menu window in the right bottom corner (besides the connection with administration server status and current version information). Providing the computer running the client application is currently connected to the internet, it is possible to verify the newest available version of the ATEAS platform by clicking on icon on the right.

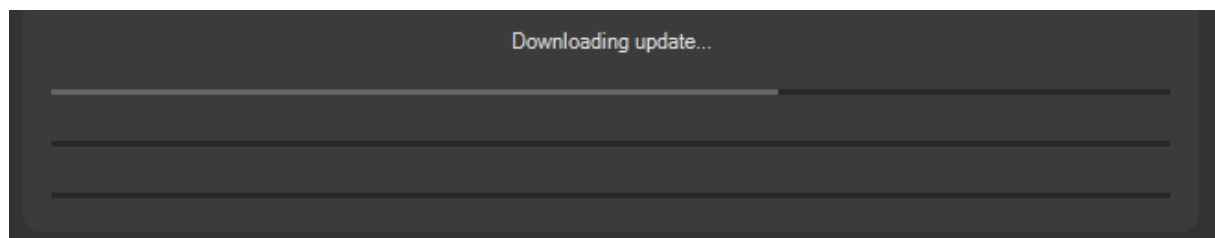


The client application contacts ATEAS servers and determines the currently newest version available along with its release date. Furthermore, it will also display information whether or not you are using the current product version and the latest version available to you.

The client application is configured to automatically check for a newer version by default. You will be notified of a newer version. This automatic control can be switched off by checking the relevant option on the bottom edge of the window.

By default, you will only be notified of major ATEAS versions with a different year or R number. If you also wish to be notified of any minor version changes with a different M number, you might deactivate the Major versions notifications only option.

If a new system version is available, a user with master administrator rights can download the new version by clicking the **DOWNLOAD** button. The first row shows the downloading progress.



NOTE

The latest system version will be downloaded, only if your ATEAS PMA entitles you to do so and you can activate it. The automatic update feature can also resort to downloading an older version if it is at least 2023 R1 M1.

After the downloading process is complete, the integrity of the downloaded file is checked. The progress of this check can be seen in the second row. The third row shows the progress of uploading the update to the system administration server.

NOTE

Therefore camera system servers do not need to be connected to the internet during the auto-update process.

After the update has been uploaded to the administration server, click the **INSTALL** button to initiate the reinstallation of the system administration server. The reinstallation process disconnects the client. After the client is automatically connected, the client may require an update along with the need to activate the new version of the system. The Automatic updates chapter describes this process together with the auto-update process of all camera servers.

NOTE

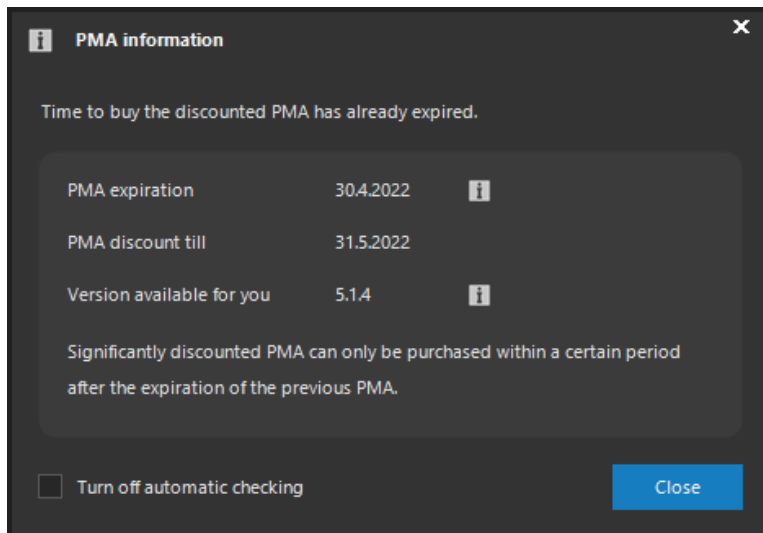
You can successfully activate the new version upon installing only providing you have the right to do so (free update by purchasing a license number or independent contract on PMA product support).

NOTE

The client application version is displayed on the bottom of the application's main menu window followed by the version of the system the client has logged on to. The client application has backward compatible and can access older system versions.

2.8. PMA information

The symbol on the left, within the group of information symbols located in the bottom right corner of the window displaying the main menu, is used for verifying the PMA status of your installation.



ATEAS PMA guarantees updates for your system to the most recent version available. In order to update the system, an ATEAS PMA service must be active. More favorable conditions are available to those who renew PMA on a regular basis. Thus, if the application is connected to the internet, you can check the PMA expiration date and the PMA renewal date directly in your application. With every new license purchase there is a 2-year PMA included.

The client application is configured to automatically check for expiration by default. You will be notified prior to the expiration date. This automatic control can be switched off by checking the relevant option on the bottom edge of the window and by clicking the **CLOSE** button.

Version available for you displays the maximum system version that you can install and activate. Had your ATEAS PMA already expired, this version can be lower than the most recent system version.

2.9. Application main menu

The application main menu will appear after a successful login. It contains the following items:

Shared views – views defined by administrators with access granted to all users.

My views – views defined by users with no access for other users.

Recordings – access to camera recordings.

Workspaces – this option includes the layout of several live windows including views or the map window, it is activated within the workspace setup section.

Video wall – this option enables access to the video wall or to remote monitors providing a video wall is configured by the administrator.

Snapshots – opens a window with the saved snapshots.

Setup – local workstation setup.

Tools – contains additional tools like the download manager, the live guard, map, custom buttons, face database or the vehicle LP lists.

Administration – camera management and setup, recordings, views and video wall, add-ons, users, rights and server management, integration possibilities and license number upgrade (activation).

Help – opens the product documentation.

Exit – closes the application.

The current user is displayed above the main menu as well as a button for activating the menu search. This is especially handy, when there are many shared or private live views possibly organized in a multi-level tree structure.

2.10. Application automatic startup

The startup value for ATEAS Administrator and ATEAS Server services is set to automatic by default and does not require user action to be run (except for restarting).

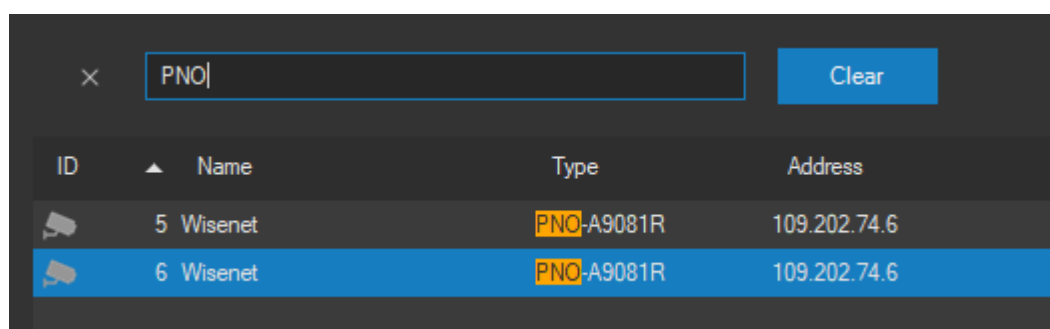
Using the local setup, the ATEAS Observer client application may be started automatically after Windows startup and can automatically authenticate a specific user. Automatic workspace loading also enables the opening of predefined views and their correct positioning on relevant monitors. See the local settings chapter for more information.

CAUTION

Be very careful when using the automatic login feature. Users logged in automatically do not have to enter their password, which can lead to their account being abused. Therefore, it is highly recommended to only use the automatic login function for universal users with low permission levels.

2.11. Searching, filtering and sorting

Various segments of the client application produce system data lists – e.g. list of cameras, users, servers, events, external elements and many more. The data is presented either in table view or list view with tree structure. The CTRL-F key combination can be used in all of these structures to activate searching via the integrated search panel.



The screenshot shows a search interface with a search bar containing 'PNO' and a 'Clear' button. Below the search bar is a table with four columns: ID, Name, Type, and Address. The table contains two rows, both of which are highlighted in blue. The first row has ID 5, Name Wisenet, Type PNO-A9081R, and Address 109.202.74.6. The second row has ID 6, Name Wisenet, Type PNO-A9081R, and Address 109.202.74.6.

ID	Name	Type	Address
5	Wisenet	PNO-A9081R	109.202.74.6
6	Wisenet	PNO-A9081R	109.202.74.6

By entering text into the search field, data rows in the table are automatically filtered. Only the data rows that meet the search criteria will be displayed. The following rules apply for searching and filtering:

- All table columns are automatically searched for the entered text.
- Entering multiple words separated by a space, searches for all data rows with at least one column containing at least one of the search words (logical OR).
- To search for data rows containing multiple words, the word should be prepended with a + symbol (logical AND).
- An entire phrase containing spaces can be searched by adding quotation marks to the entire searched phrase.
- To restrict the search to a specific column, enter the column name followed by a colon before the search phrase.
- The searched phrases are automatically highlighted within the filtered data rows.
- All entered search words can be removed by pressing **DELETE**.

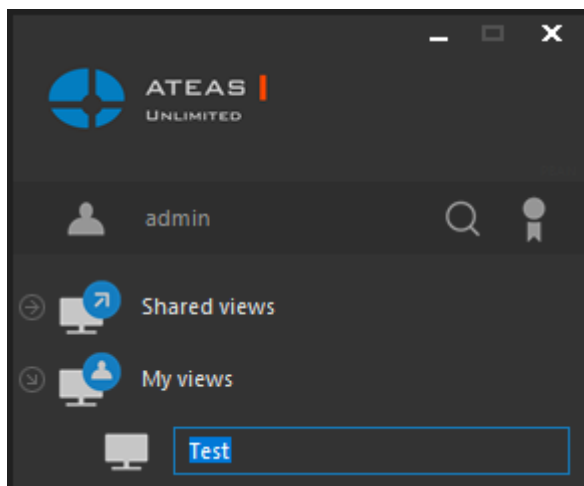
Lists can be sorted by simply clicking on the header of the relevant column. Clicking the column header again will change the sorting from ascending to descending and vice versa. Use the SHIFT key to select and sort according to multiple columns.

TIP

It is possible to select and copy the texts in the tables by repeatedly clicking a cell.

2.12. Renaming items

Based on your permissions, some items in the main menu can be renamed using the edit symbol. For example, you can rename local or shared views or workspaces.

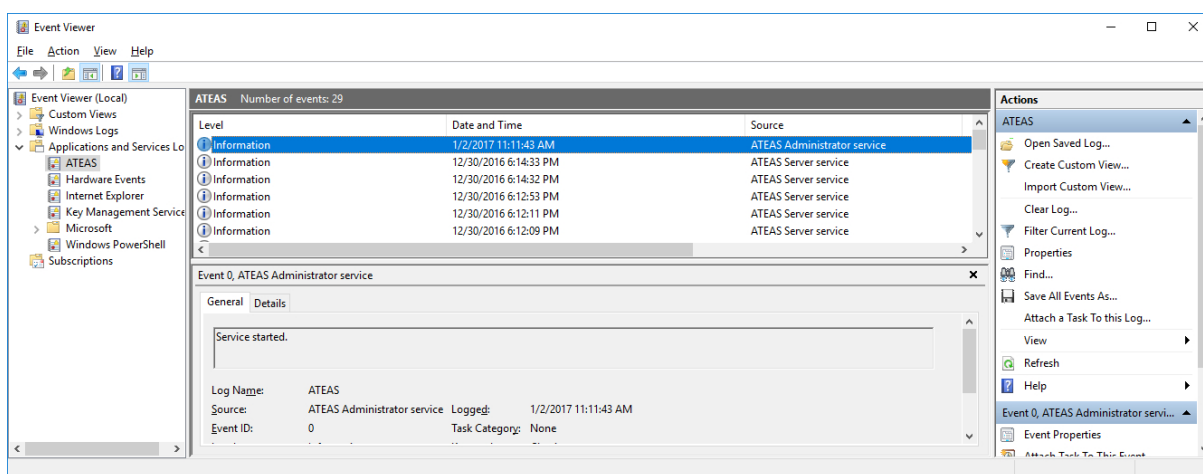


2.13. Terminal client access

Desktop virtualization technology indisputably has great benefits for the operation of information systems within enterprise solutions. Since ATEAS applications support GPU acceleration technologies (client and server), camera systems can now also be fully integrated into the architecture. The client application can utilize the acceleration via server GPUs (Tesla) and can be run for a larger number of clients with GPU acceleration. Without this acceleration, multiple launches of the client, demanding smooth high definition video, would immediately overload the server processors. For more information, see the GPU acceleration chapters.

2.14. Protocols

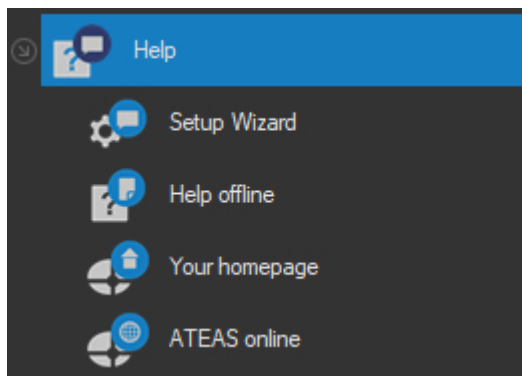
A new event protocol labeled ATEAS is created upon finishing the installation of any ATEAS Security application. All significant circumstances related to the application run are recorded to this protocol. The protocol can be found in the Control panel – Administrative tools – Event Viewer section. In case of any suspicious or non-standard behavior, this protocol may contain important diagnostic data. Besides the system protocol logging, managed by the Windows operating system, ATEAS Security writes its own system log related to the camera system, available in the user administration section. The log contains a history overview, filtering and a live spy window feature.



Chapter 3 - Help

3.1. Documentation and help

There are several links available in the submenu as follows.



System administrators can run the Setup Wizard to guide them through basic steps for the initial setup.

The Help offline link opens the complete offline product documentation in PDF or CHM file format. Your homepage opens the administration server homepage in your default web browser (internet connection is not required), where besides the complete press quality documentation, other documents and system applications installers can be found.

The last link will redirect you to the manufacturer's homepage (internet connection required), providing contact information and enabling users to log into the partner section.

Chapter 4 - Monitoring

4.1. Views

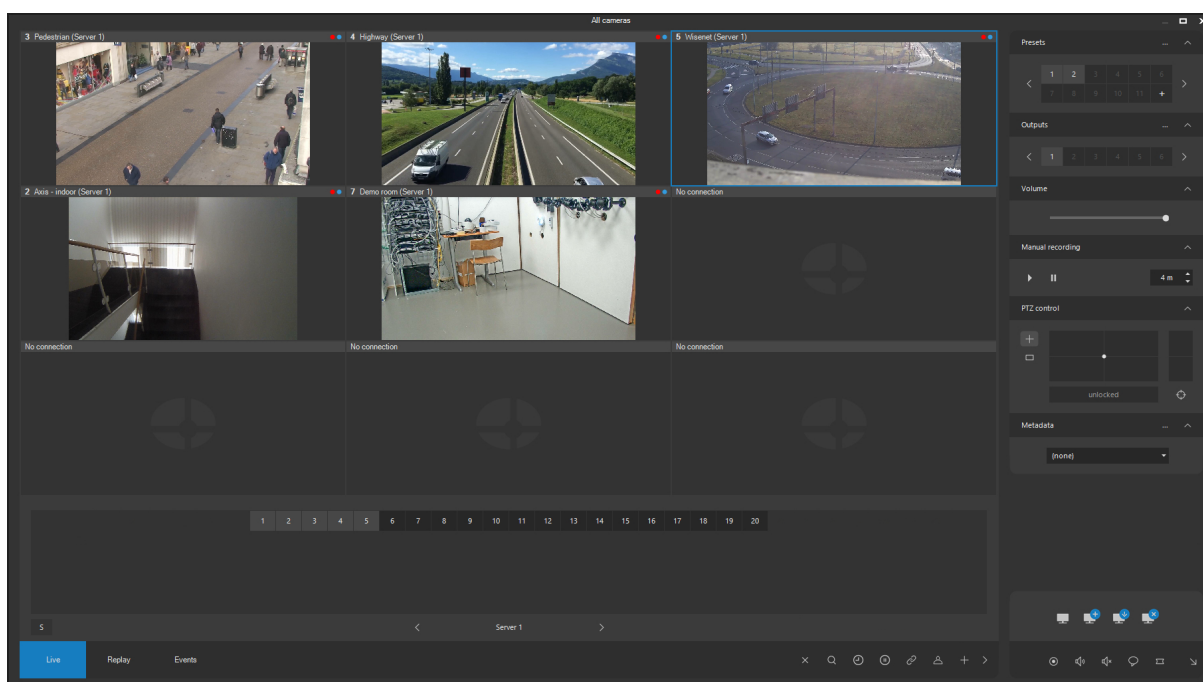
4.1.1. Views administration

A view is specified as a defined layout of cameras on a computer screen (in a live window).

While one or more live windows are open, users can easily switch between views and change the number of cameras and their layout on the monitors with a single click.

There are two items in the main menu that open the views submenu.

Shared views contain views visible and available for all system users, **My views** contain views which are created by the user from cameras available to him. These views are not visible to other users. One live window can contain up to 100 cameras, the maximum number of live windows is 16. The built-in video wall feature can be used to display more cameras in detail (see relevant chapters).



Live window control

The live window can be either maximized (controls not displayed) or assume its standard form with the controls displayed. The live window can be maximized by clicking the control in the bottom right corner

of the side control panel and is switched back to standard view by sliding the mouse cursor into the bottom right corner of the maximized window. The F12 key can also be used for switching between maximized and standard view.

If the live window is displayed in standard form with controls displayed, you can switch between the following groups of controls (tabs):

View related functions are found on the **Live** tab. Events are available on the **Events** tab and switching between events can be executed here. The **Replay** tab plays the live view from recorded video and audio data. The side control panel provides access to camera functions for the selected camera.

Switching views

Views can be easily switched by selecting a view from either the **Shared views** or **My views** menu. The selected view is switched to the last active live window. This is important when you have several live windows opened (see opening additional windows).

If the primary live window (view management window) is not opened, it will open after a view is selected, independent of other live windows.

NOTE

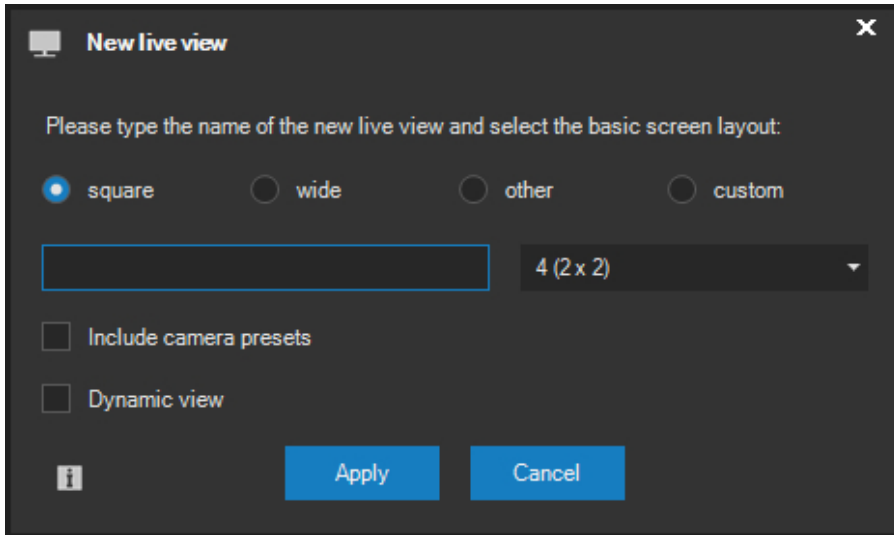
If no view is created, a primary live window will be opened directly upon clicking the **My views** menu item.

Creating new views



Use the Create new live view button on the Views tab to create a new view. A dialog box will appear asking you to enter the name of the new view and its basic layout (i.e. the number of cameras the new view will contain). A specific layout view can be selected from the list for each layout type (square, wide, and other). Square layouts always contain the same amount of cameras in the horizontal and vertical direction, wide layouts offer modes with a greater number of cameras in the horizontal direction than in the vertical direction (about a 16:9 ratio) and other layouts offer various window sizes

for individual cameras. The largest square layout is 11 x 11 consisting of 121 cameras, the largest wide layout is 13 x 9 (or 14 x 8), which is 117 (or 112) cameras.



The other views group contains so called centric views. Centric views are always in 1 + N mode with one larger camera window in the centre of the view and N windows for cameras arranged around the centric view. Besides this orientation, centric views have other specifics, increasing the user features of these views:

- If the camera located along the perimeter of the view is switched to detail by double clicking on its header, the detail will be displayed directly in the centre of this view instead of applying the hotspot monitor settings.
- The primary frame rate is used for displaying video in the centre window of the view.

When a centric view is opened, the option of having duplicate cameras in the view is activated. When a different view type is opened, this option is deactivated again. The current state is indicated by the button with the 1 symbol positioned to the right of the camera numbers overview which is interpreted as a lock for having duplicate cameras in a view. This lock, however, can be manually modified at any time.

NOTE

We might need to turn off this lock even in a non-centric view, when we need to display the same camera in two different digital zoom levels beside each other.

Besides views available among other views, it is also possible to create custom views. When creating custom views, we do not choose from available view layouts. Instead, we create a new custom layout using a layout editor. The layout editor is started upon selecting the Custom option and pressing the **EDIT** button. The following subchapter describes how the layout editor is used.

Use the **APPLY** button to confirm the dialog box. The view will be created and automatically switched to primary live window. The new view will be also displayed as a menu item in the main menu, from where you can perform a quick selection of this view.

When creating a new view, you can check the Include camera presets option. If this option is checked, the view will keep track of the preset positions for PTZ enabled cameras. This view is then saved together with the last preset positions to which all PTZ enabled cameras were sent. Upon activating this view, cameras will be automatically positioned to the saved preset positions. This feature enables the user to define many different views consisting of the same cameras (PTZ enabled cameras are automatically sent to different preset positions after the selection of each view).

Activating the Dynamic view feature changes the behavior of the created view provided the respective view is identified as shared by the system administrator. Changes in behavior include the view automatically changing its layout according to how many cameras from the view can be accessed by the user displaying the view. Thus, various users can see the same view in various layouts. See subchapter Views Administration in chapter System Administration for more on shared views and view groups.

Editing views

For cameras to be displayed, it is necessary to switch them to the view. The camera switching (selection) process is only performed when editing the view. The view is saved along with camera information and layout.

NOTE

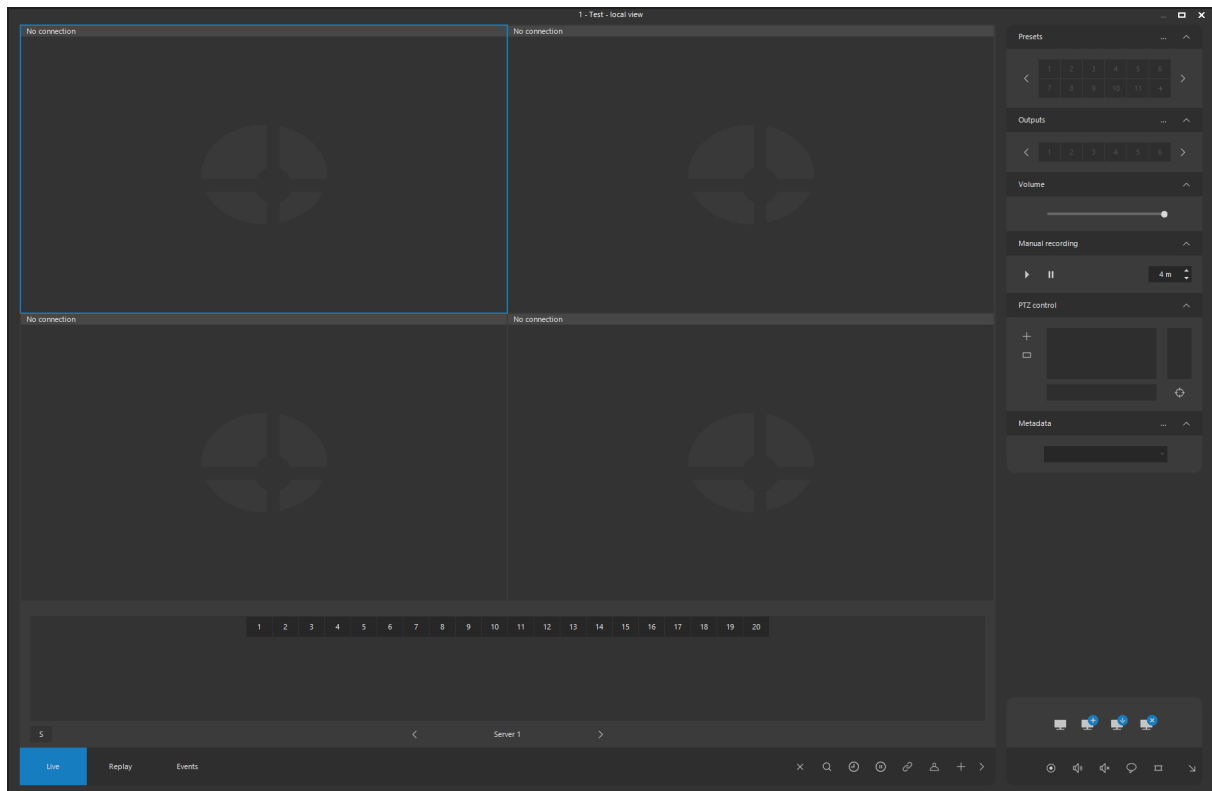
Automatic or tour modes can also be defined in terms of the view, as described in further subchapters. Here, you will only find information about basic camera switching to view.

There are two ways to switch cameras in the view. The first way is to select the position followed by selecting the camera. This way you will always be able to switch one camera. The second method is dragging the mouse or touching, allowing switching multiple cameras at a time. The auto-fill view feature is also available and is described further in the text.

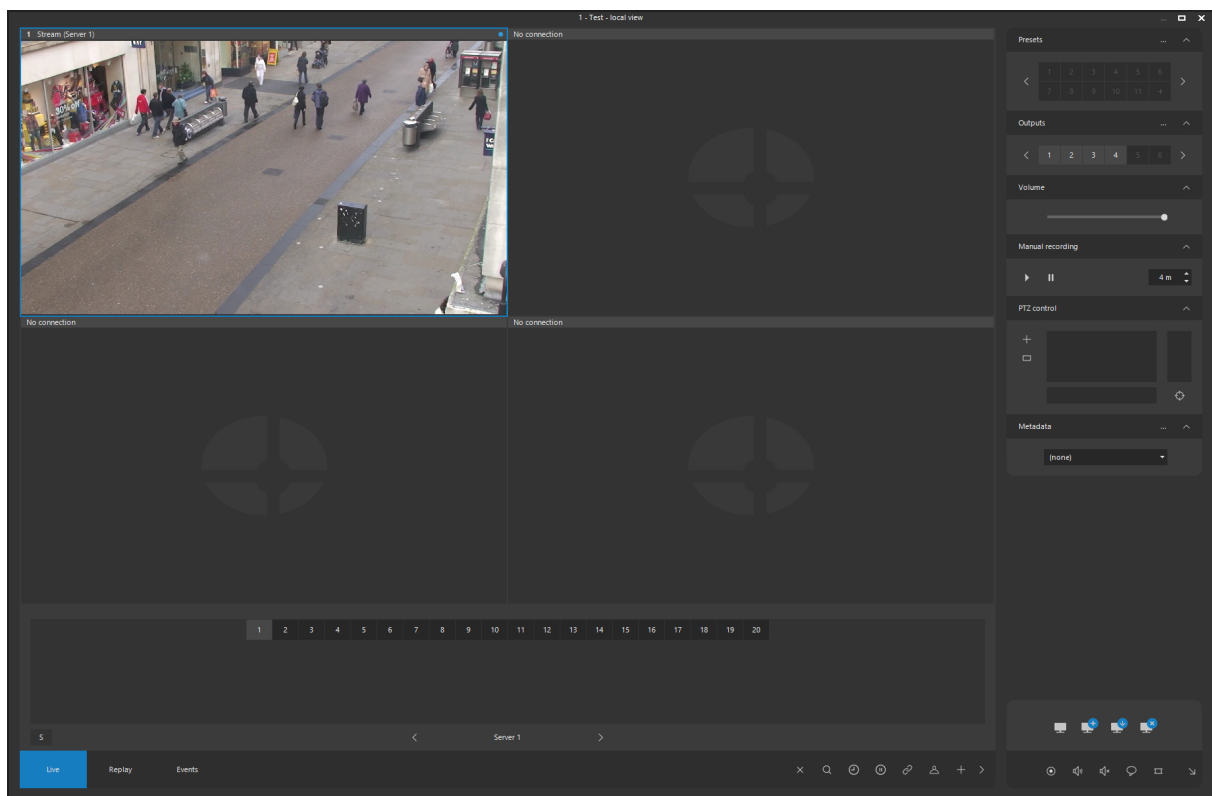
Switching one camera

You can switch a camera to a given camera window as follows:

- Select any camera window in the view. A selection rectangle will appear around the selected area.

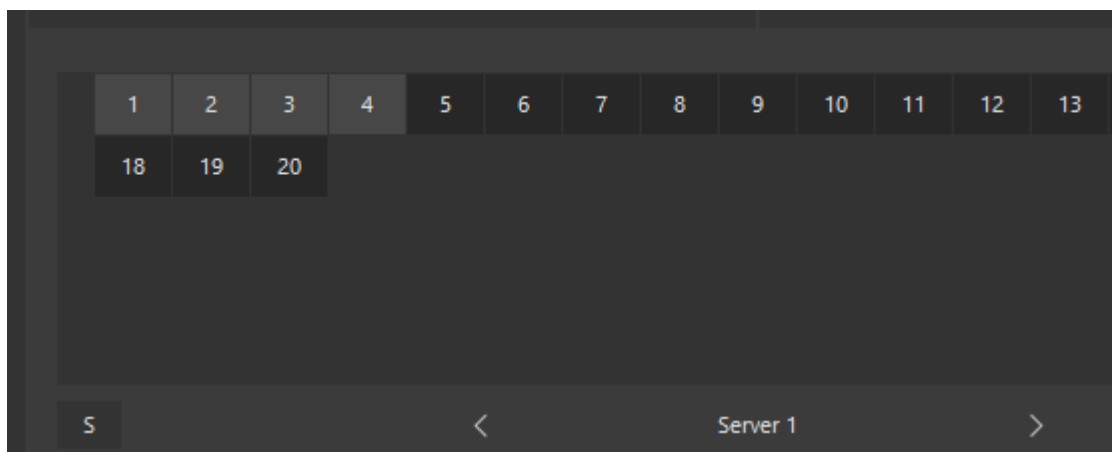


- Next select a camera on the Live tab by clicking on the camera number (the selection is made easier by displaying tooltips with camera names and – if the user is granted the permission – addresses), the camera will be switched to the selected view position.



All camera windows in the view can be filled by repeating the steps described above. Moving a camera is as simple as dragging its header to a different position within the view. By default, the primary stream is used. To use the secondary stream, you need to activate the secondary switch labeled S in the left bottom corner.

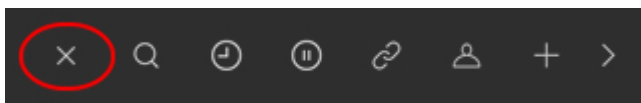
Camera numbers are displayed in ascending order starting with number 1. Empty positions are inserted for missing camera numbers for better orientation. All cameras already being part of the view are marked with a distinctive color as illustrated on the following picture.



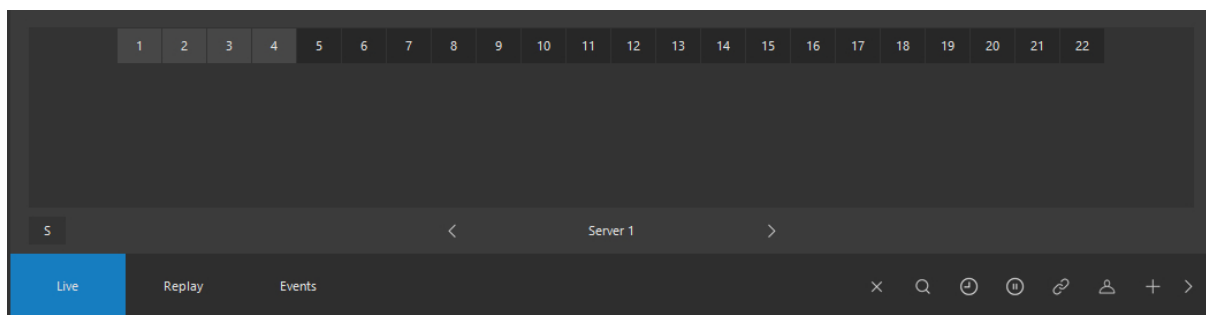
NOTE

This way you can easily create camera sections or groups based on the grouping of camera numbers.

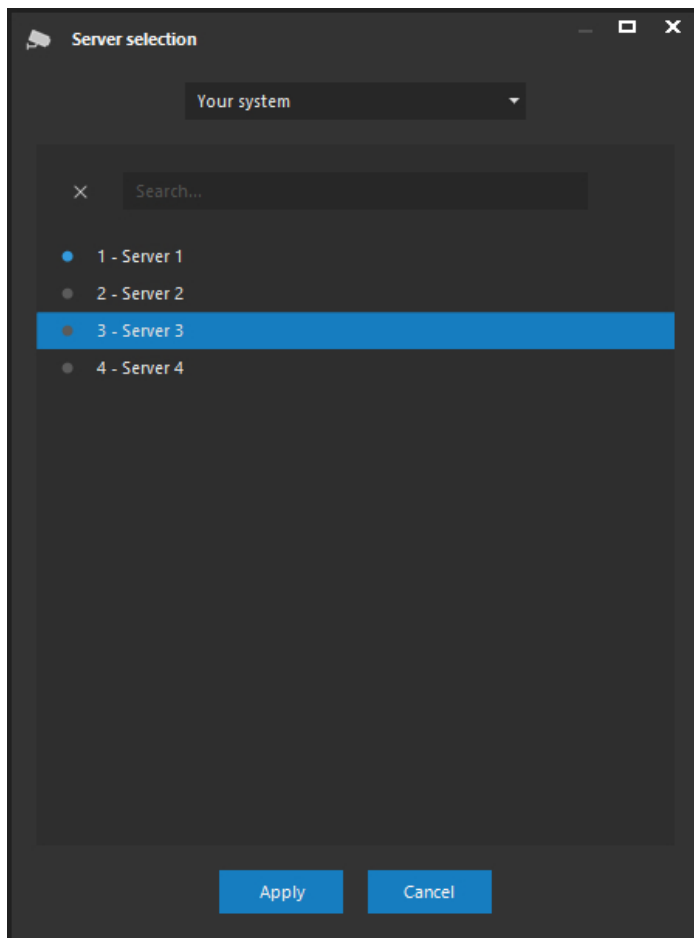
If you want to clear the camera window without moving the camera to another camera window, use the Turn off button after selecting the desired camera window.



Combining cameras from different servers in a single view is possible. Based on your ATEAS Security product edition, the camera server can run directly on your computer, where the monitoring itself is performed, or on a specialized server anywhere throughout the network. Up to 999 cameras can be connected to one server. However, your administrator may configure the system to accept feeds from several servers for various reasons. If this is the case, you must switch between them to display a different camera set after each switch.



By clicking on the server name, you can display a complete server list (more precisely, only the servers available to you) or you can use the list arrows. From there, you can switch to any server by selecting the server from the list and pressing the **APPLY** button or by simply double-clicking it. The server window also shows the current status of each server (online or offline).



If your system administrator activates the multiple login feature (ATEAS Interlogin), you will be able to select other systems from the system list than just Your system.

NOTE

While selecting another camera server belonging to the same camera system only displays different camera numbers of the new server, selecting another camera system also closes the current view.

Switching by drag & drop

Camera switching can also be performed by dragging the camera numbers using the mouse. This is a standard way of pressing and holding the camera symbols and dragging the cameras to the position of choice in the view. During this operation, the color frame will indicate the target position in the view, where the camera will be displayed upon releasing the mouse button.

Using the CTRL key will allow selecting multiple cameras. Using the SHIFT key will also select multiple cameras, the selection will, however, always include all cameras between and including the marked numbers.

NOTE

Dragging multiple cameras at once also displays the corresponding number of color frames indicating the target position.

If the target positions are already occupied by other cameras, using a standard drag & drop operation leads to the cameras being replaced by new ones, i.e. the selection will be overwritten. Should you wish, however, to place the cameras into the view using insert mode (instead of overwriting) in such a way, that free space is allocated at the target position and the cameras are shifted, you can perform the drag & drop with right mouse button.

Cameras can also be dragged directly between each other. This action will cause the camera positions to be swapped.

View layout expansion

Using the camera mouse drag and drop feature described above, you can also automatically expand the view by adding new rows, columns, or both. To automatically expand by adding a new column (or row), simply place the mouse cursor near the beginning of the first or end of the last column (or row) while dragging, and the new column (or row) will automatically be offered as an option for camera placement.

NOTE

However, this expansion cannot be performed for views with a custom layout from the designer, or for centric or other views. Using expansion, it is also not possible to exceed the maximum of 121 view positions.

Auto fill feature

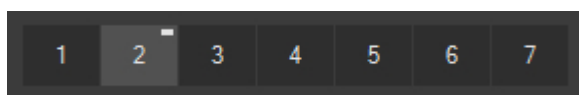
This function automatically fills the current view with cameras from the selected camera server. Automatic camera filling is always starts from the focused camera window and continues with the following views (or until the highest camera number from the selected server is reached). The auto fill

feature is especially useful for a greater number of cameras in the system when a single click is enough to use up all view positions available.

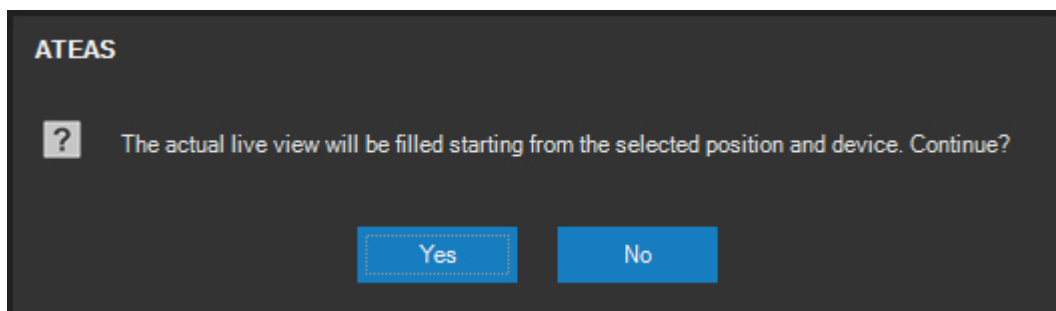
CAUTION

Camera windows already filled with cameras will be switched to different cameras during the auto fill process.

If you want to start the automatic filling process from a particular camera, click the fill symbol located above the number of the active camera (see the following picture).



The automatic filling starts upon confirming the following message dialog.



NOTE

The auto-fill process is automatically interrupted if the filling process reaches the last position in the view, the last camera displayed or it runs into a gap between cameras on the panel displaying camera numbers.

Saving views



The view shall be saved after layout for all cameras has been arranged. To save the view, click the Save live view button.

If you forget to save the view after changes have been made and the view needs to be closed or switched, the application will ask you to save the view, therefore no changes will be lost.

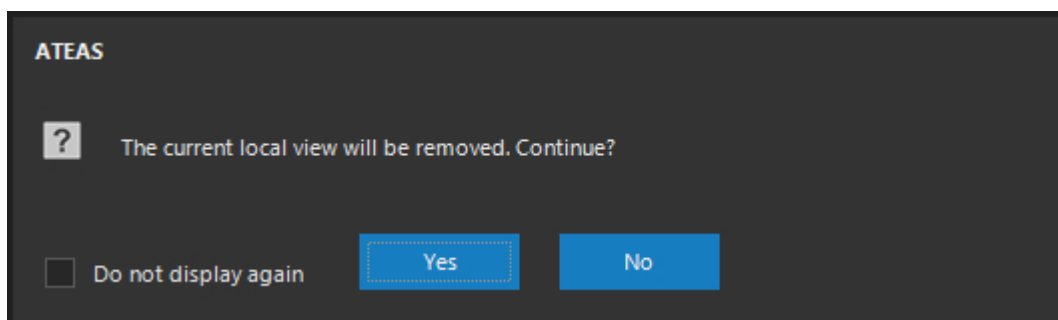
TIP

If the current view is not a local or shared view (e.g. map or event view), before saving the view, it will be possible to enter a view name.

Removing views



You can also remove the active view in the primary live window. To do so, click the Remove current live view button. The view will be removed upon confirming the following message dialog by clicking the **YES** button.



NOTE

Using the very same method, administrators can remove shared views as well.

Indicators

Each window, a camera is switched to within the view, is equipped with its own synchronization indicators. These are small color symbols along the right window heading border containing the camera name. There are three indicators available.



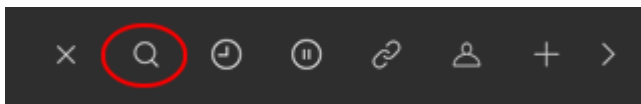
The right indicator displayed in blue means the video is live. During replay, it indicates video is available for the time being replayed.

The middle indicator displayed in red means recordings are active. If they are not, but a server pre-alarm buffer is being maintained, it is displayed in yellow.

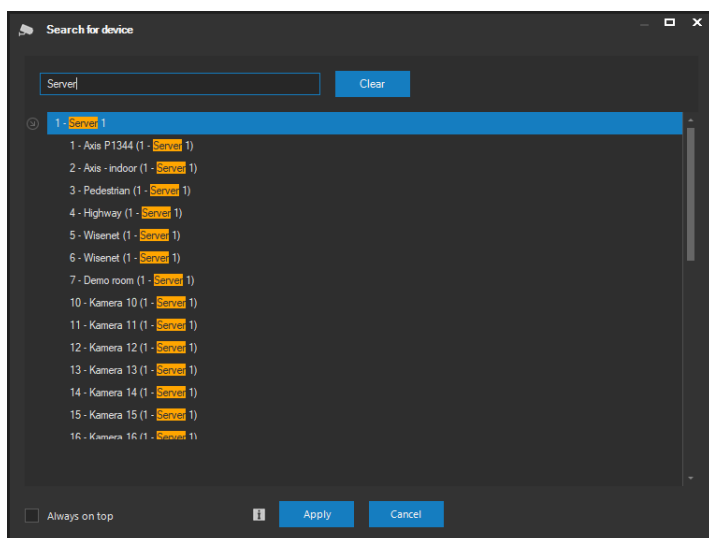
The left indicator displayed in white indicates an encrypted transmission from the server. For https protocol, a violet color indicates the device certificate has been successfully validated. When both facts apply, the indicator is displayed in green.

4.1.2. Name-based camera search

Server identification and camera numbers are primarily used for orientation when adding cameras in the view. For larger systems, searching for cameras across all servers based on their name could be helpful. To start the search, press the search button.



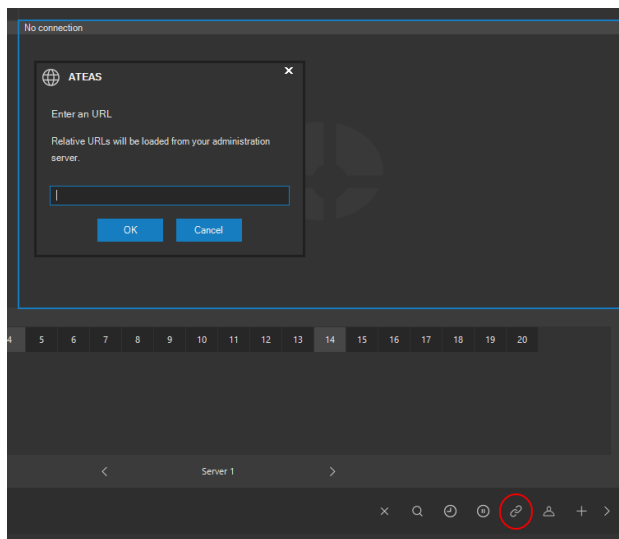
The search dialog allows the user to start typing the camera name that will be searched among all cameras on all servers which the user can access.



After selecting a specific camera from the returned result, the respective camera is shown in the view. You can switch cameras into the active view without closing the window by double-clicking a camera.

4.1.3. Displaying web content

Apart from cameras you can also display any particular web content in a given position of a view. The live windows supports the most recent web content technologies including HTML5, CSS3 or JavaScript. You can display the web content using the web button, as illustrated in the following picture.



NOTE

The ability to include web content in a view is bound to the corresponding user permission.

Any given address can be used starting with http or https protocol. If a relative address is used (i.e. one without the protocol), it will be evaluated in administration server context.

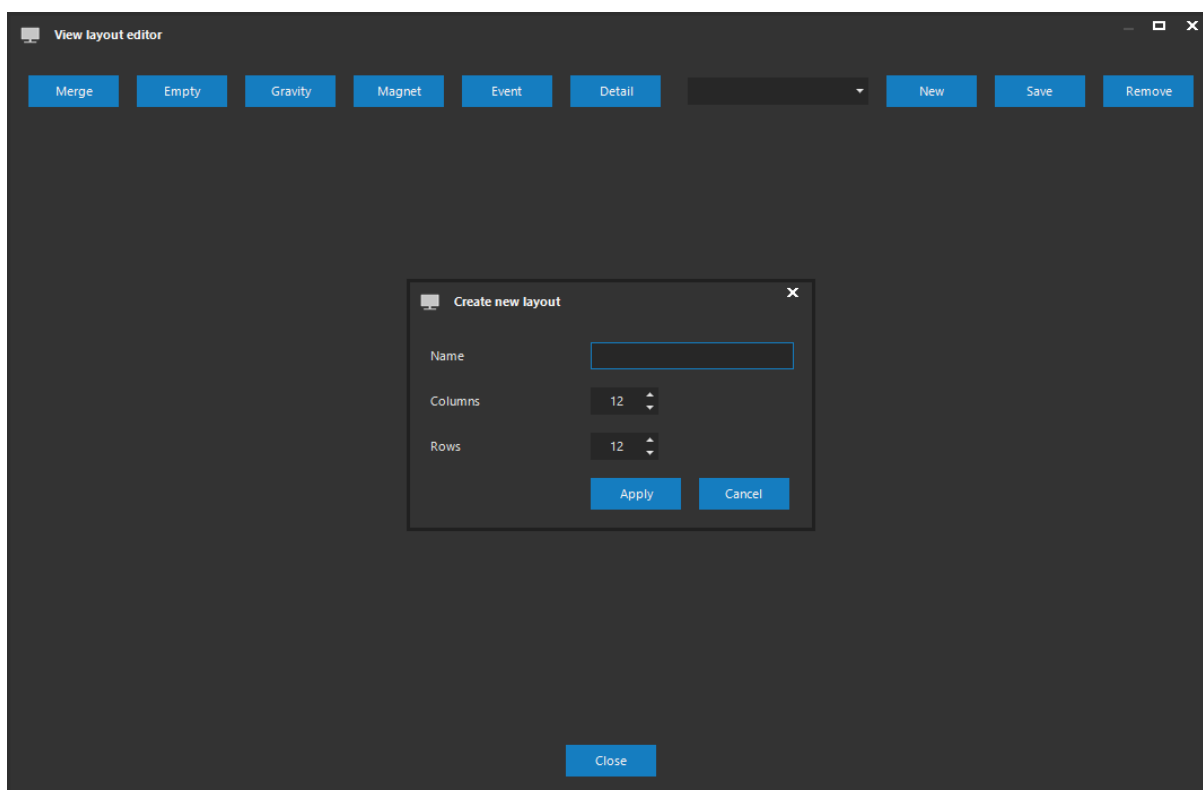
After saving the view, the web content is a fixed part of the view and can also be shared and made available to other users.

NOTE

The video wall has a very similar feature for displaying web content.

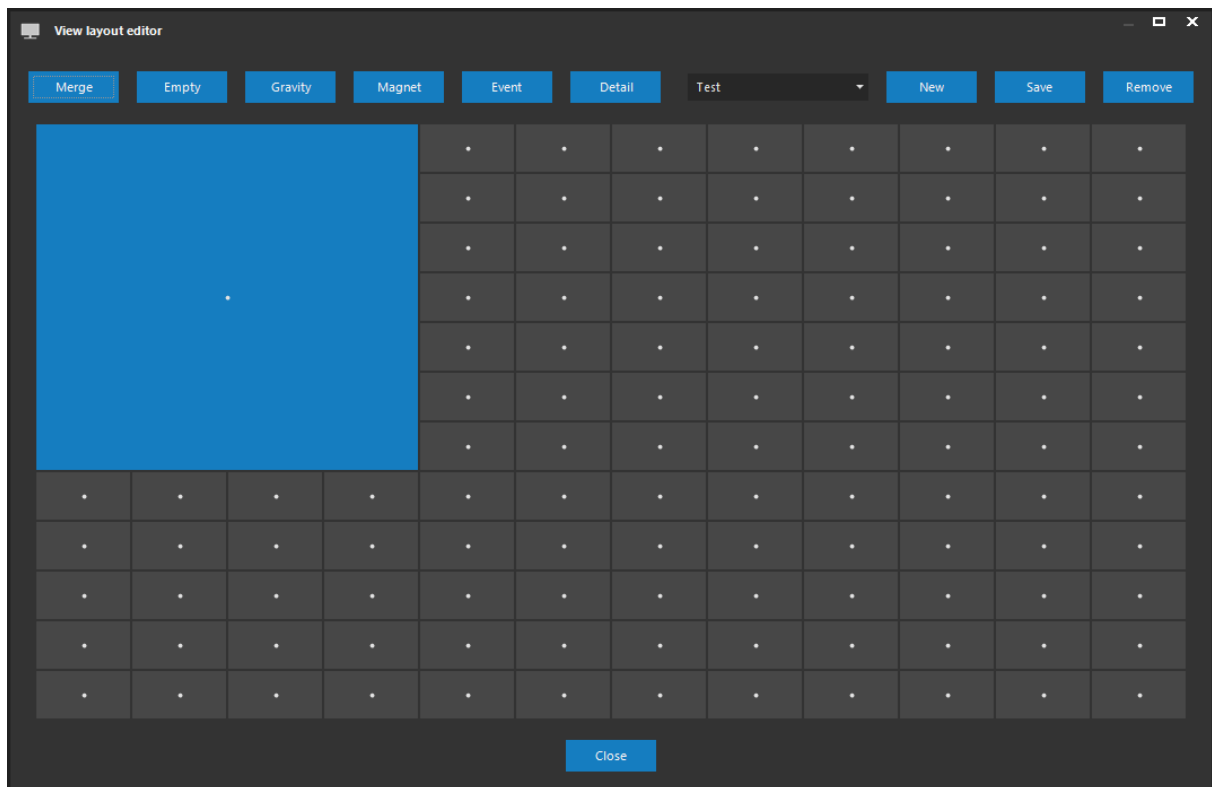
4.1.4. View layout designer

View layouts are not selected from predefined layout groups (such as square or widescreen layouts) when creating custom views. This layout is custom created using the layout editor directly. Press **NEW** to create a new layout.



The first step prompts the user to specify the name of the new layout and the default number of columns and rows the layout will consist of. The available range for these values is 1 – 20. Therefore, the default matrix can be divided into a maximum of 400 windows before making additional changes to the layout.

The layout can be edited further by selecting several windows from the displayed matrix and pressing **MERGE** to merge them into a single window. This procedure can be repeated as many times necessary until the final layout is achieved. During the selection of the windows, the editor always adds other windows to the selection automatically to create the smallest rectangle possible.



The user can return to the default layout at any time during the process of merging windows in the layout. The **EMPTY** button restores the layout to have the original default number of columns and rows.

A finished layout can be saved at any time by pressing **SAVE**, or deleted by pressing **REMOVE**.

CAUTION

Despite the option of initially dividing the layout into 400 positions, we can only save a layout containing a maximum of 121 positions. This is linked to the maximum limit of cameras displayed in a single view.

Modifying the physics of the view

Each camera windows in the layout editor contains a dot symbol, which specifies the gravity applied within the respective window. The gravity is set to center by default. The gravity within the camera window determines to which position the video area in this window will be pulled. This applies not only in situations when the native video resolution is less than the video display area, but also in opposite cases when the maintain aspect ratio option is enabled. Unused vertical or horizontal areas next to the video area often arise in this case.

By adjusting the gravity, you can achieve the effect of displaying the video either in the center or attached to any of the following window positions: left center, top left, top center, top right, right center, bottom right, bottom center or bottom left.

The gravity can be changed by pressing **GRAVITY** and clicking into the camera window for which you intend to adjust the gravity setting. The gravity will be set to the value with the closest match to the point of clicking.

NOTE

Changing gravity can especially be helpful for creating views that will include video from cameras equipped with multiple lenses capable of comprising a single scene.

MAGNET button can be used to configure the next aspect of displaying the camera within the view. Only the horizontal magnet is supported. If enabled, the width of the window displaying the video is automatically adjusted to the video size while ensuring no vertical areas without video content and the camera windows to the left and right of the magnetized window are pulled as close to the given window as possible.

A window is magnetized by selecting the given window with the **MAGNET** button pressed. Two vertical lines near the edges of the window indicate a window is magnetized.

NOTE

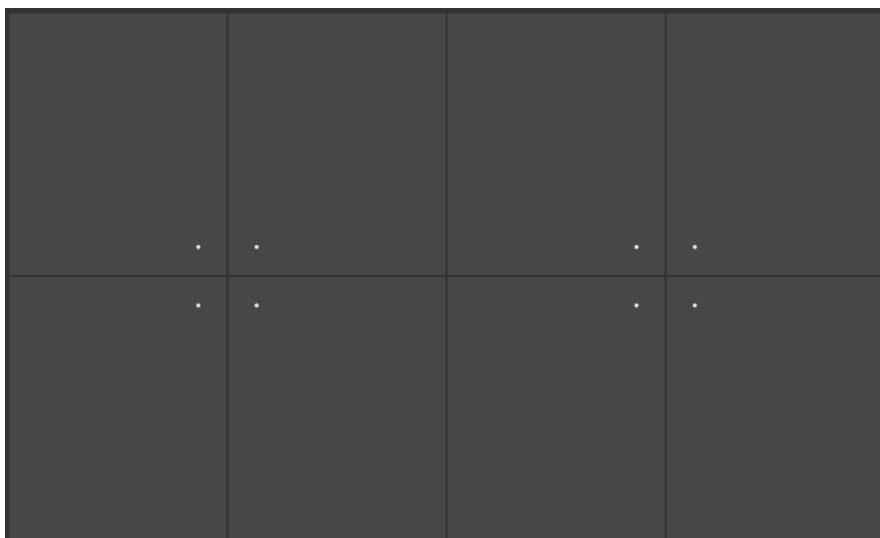
If multiple vertically adjacent windows are magnetized, the magnet is transferred all the way to the first window, which is not magnetized, if such a window exists. If no such window exists, the magnet is transferred to the edge of the live window. However, if the magnet is transferred to both edges of the window, it is applied evenly, and the effect will not be visible.

NOTE

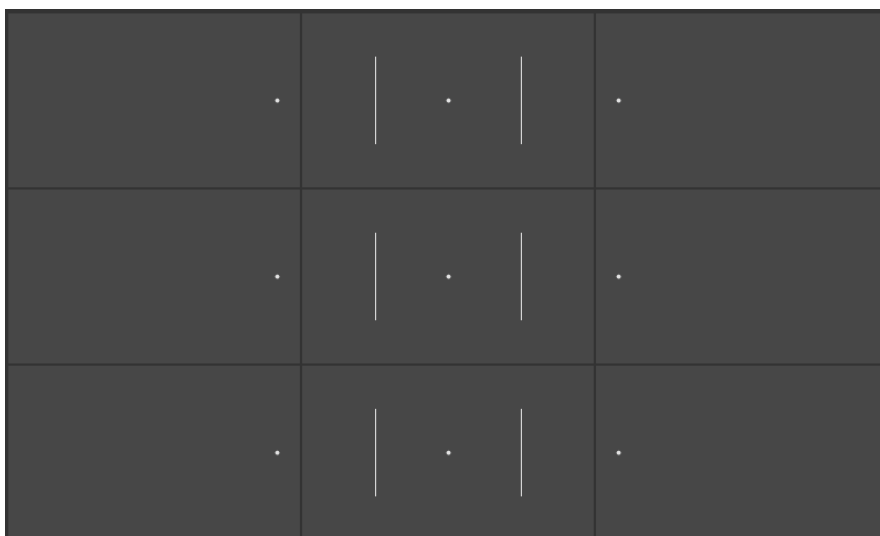
The gravity or magnet button shall be released to finish the respective setup.

Examples of modified physics

Example of an 8 camera view with 4 cameras in each group:



Example of a 9 camera view with each row within the view containing cameras belonging to a device with three lenses:



NOTE

When setting the window gravity to the top edge of the window, to improve the visual perception the camera caption containing the camera name is automatically hidden. In this (and only) case a double-click in the video area is necessary to switch to detailed view.

NOTE

Modified physics is, of course, applied for views that have been shared for other users as well.

Using the **EVENT** button selected positions can be configured as event monitors. If the current view contains at least one event position, different rules apply for displaying an event. Instead of opening an event view in the current or a new live window (according to your local settings), the event positions are used to display all the cameras configured to be included in the event view without changing other positions in the view.

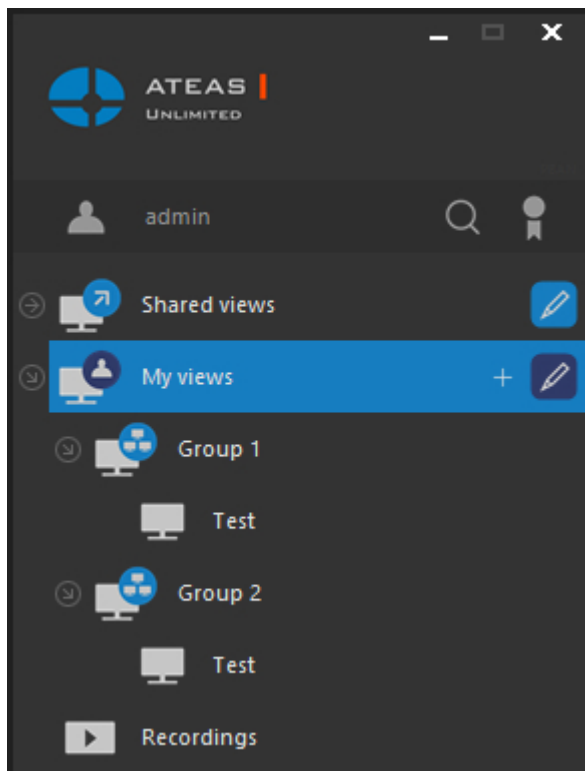
In such case, previous events are moved to subsequent event positions and multiple events can be displayed. This is a similar effect to video wall event monitors, where an event based shift is also applied across the event monitors.

The event positions are indicated by a horizontal line in the designer and might use a custom colored indicator in the view as configured in local settings.

Using the **DETAIL** button you can pick some positions to be the target positions for detailed view. This produces the same effect as centric views have with one larger position in the middle of the view to display the detail. The positions marked as detail positions will be used consecutively to display the detail.

4.1.5. Views organization

We recommend organizing your views if the total amount of all views created exceeds the limit, where orientation within the application main menu is still smooth. Organizing views is one way of dividing individual views into groups providing a better overall overview. The main menu considers the organization of views by creating an additional menu level displaying the groups of views. The view list will become available upon selecting a group, as you can see in the following picture.



Organizing views can be intuitively performed directly in the views menu. To start editing, you have to activate the edit button next to the My views or Shared views menu item.

Using the plus symbol, you can create and name a new group on the current level, using the minus button, groups can be removed.

Based on user permissions, views or entire groups of views can be moved or copied within the entire local and shared views tree structure. You can move or copy a view or group by dragging it with the mouse and dropping in over the target location. When dragging within local or shared views, items will be moved by default, when dragging across local or shared boundaries, items will be copied.

TIP

You can override this behavior by holding a CTRL or SHIFT key.

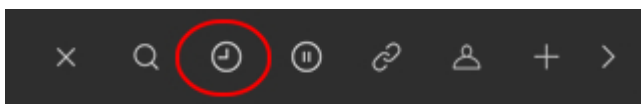
TIP

You can drop a view or group over their direct container. This is a quick way of creating a copy of the selected view or group.

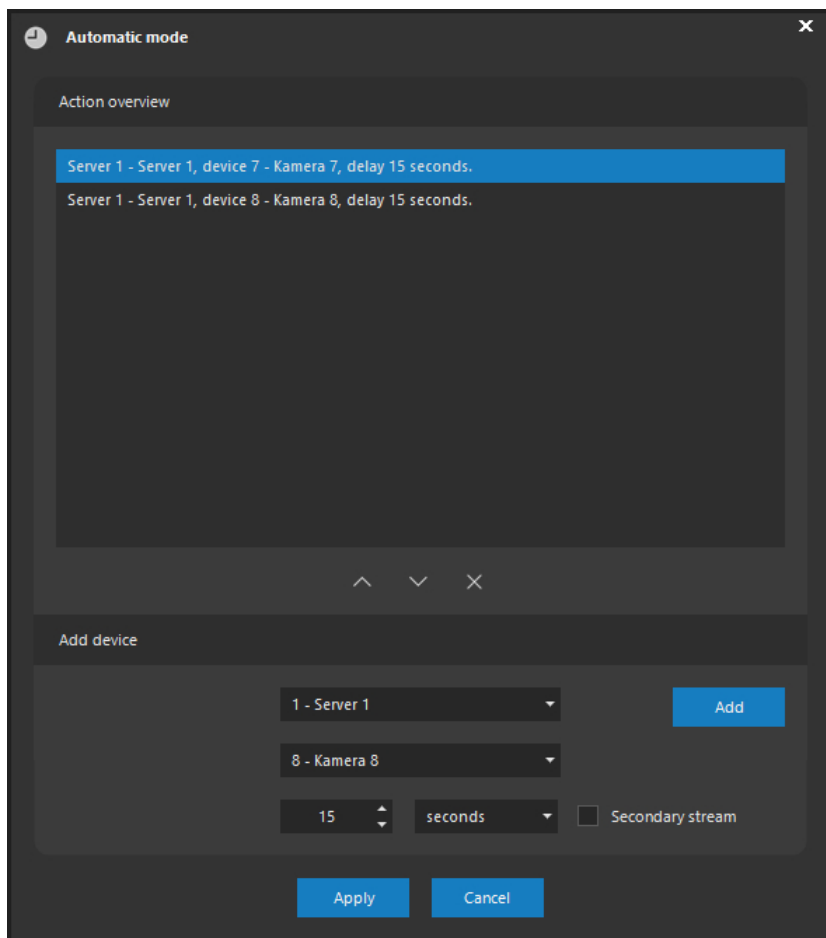
4.1.6. Automatic modes

Automatic modes are used to expand view options. Instead of one static camera directed to an assigned place of the view, you can assign an automatic mode to that place. The automatic mode will ensure periodic camera switching.

The automatic mode assignment is executed by pressing the Automatic mode button.



In the following dialog, you can create an automatic mode, which will be applied to a selected place of the view by pressing the **APPLY** button. The automatic mode is saved together with the view. That means that all automatic modes will be started with the next switch to this view.



Each automatic mode has an unlimited amount of actions, switching assigned cameras to defined places of view, where the automatic mode is applied. An action can be added by filling in the fields in

the Add device section and pressing the **ADD** button. If the Secondary stream option is active, the automatic mode will contain the secondary stream of the respective device.

NOTE

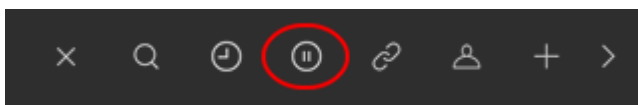
The minimum time delay is 4 seconds, maximum is 1 hour.

To delete an action from the automatic mode, select it and press the delete action button. Using the move arrows you can change the order of actions already added to the list.

Using the **APPLY** button, the automatic mode will be applied to the selected position in the view. To turn the automatic mode off, switch any other camera to the place where the automatic mode is currently used, or just close the window (where the automatic mode is applied).

Controlling automatic modes in the view

Automatic modes are saved at their respective positions in the view together with the view itself and automatically re-opened when the view opens. If a camera, which is part of the automatic mode, is switched to detail (within the same live window), automatic mode will automatically be paused. Leaving the camera detail will resume automatic mode from the paused position. It is possible to use the pause automatic mode button in order to pause automatic mode without switching to camera detail.



Clicking the button again resumes automatic mode.

NOTE

Using the right button temporarily pauses automatic modes for all positions of the view at once. Using the right button repeatedly, all automatic modes are resumed again. In case automatic modes are in different states, all states are updated according to the selected (or first) automatic mode in the view.

4.1.7. Tours

Tours are another way of extending static live views besides automatic modes. Tours always relate to a certain camera (not to a certain window as is the case for automatic modes). Tours always define a constant movement for each camera assigned.

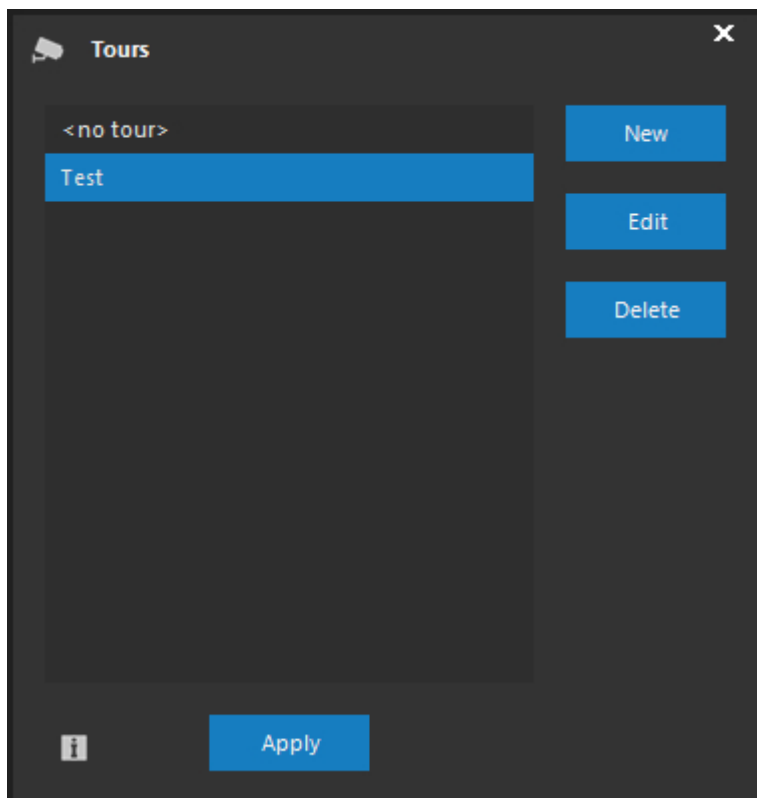
NOTE

Tours may only be accessed by authorized users. However, it is possible to distinguish which users can only run tours and which can also create, edit or delete the tours.

The number of tours created (and saved), for each PTZ device in a system, is unlimited. However, only one tour can be active at a time. The list of tours for a specific camera can be displayed by pressing the Tour button placed next to the presets overview.



Upon pressing this button, a tour summary will be displayed. The tour, currently assigned to the camera, is automatically selected.



To create a new tour, press the **NEW** button and enter a name. After that, the tour will appear in the list. To delete a tour, press the **DELETE** button. To applying the selected tour, use the **APPLY** button. To end a tour, select the first item from the list.

You can only apply a tour to a camera if it has at least one defined action, otherwise a warning message will appear and the tour will not be applied.

CAUTION

If a camera is set to a tour mode and a user intends to control the camera, the tour will be stopped. It will be automatically activated after the given time interval from the previous manual camera operation elapses. This interval is configured in the edit tour dialog.

NOTE

Tours are controlled by the relevant camera server and are not dependent on the user who activated them (users must be authorized to activate tours). Tours are reset after a server restart or failure.

NOTE

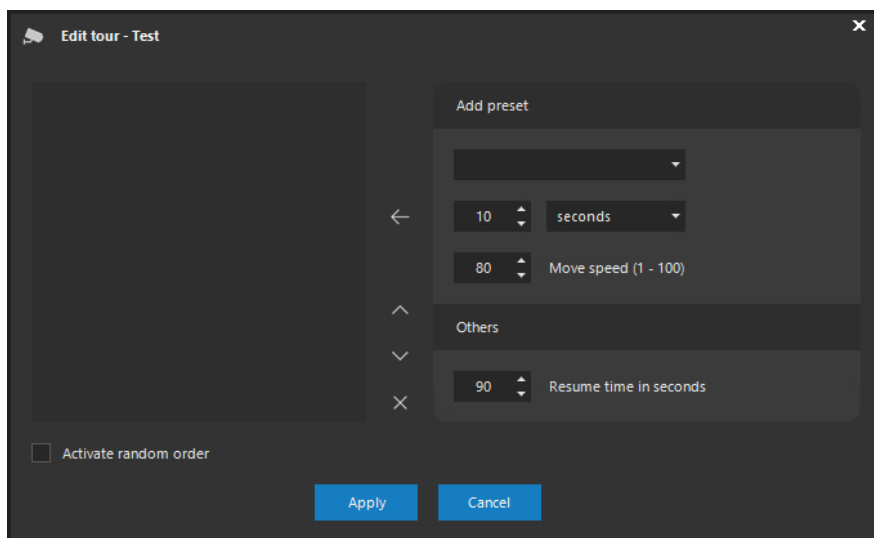
The tour will also be temporarily suspended when the camera is included in an event scenario and it is instructed to move to a preset position or switch to another (alarm) tour.

NOTE

By creating a tour, which will contain a single camera preset, it is easy to ensure PTZ devices return to their default (home) positions.

Editing a tour

To use a recently created tour, you must edit this tour. To edit a tour, press the **EDIT** button.

**CAUTION**

Preset points must be defined prior to creating a new tour.

A summary of all preset points is shown in the action list. The camera will cycle between these preset points. The action consists of a number of preset points, the speed of movement ranging from 1 – 100 and the time delay before the next action.

CAUTION

The speed parameter might not be supported by all camera models.

An action can be added by filling in the fields in the Add preset section and pressing the arrow button. You can use the remaining buttons to delete a selected action or change their order.

A time period can be set for every tour, during which the tour will be stopped if an authorized user controls the camera manually (a time period which elapses between the last manual control command from the user (from the view, joystick etc.) and an automatic reset of the tour). The time interval is set in seconds ranging from 10 seconds to 60 minutes and is set to 90 seconds by default.

An Activate random order option is available under the list of events. If this option is activated for a selected tour, individual events (moves to a preset position) will not start in the defined sequence but in random order. Viewers then never know where the camera will move or where it will be positioned next.

4.1.8. Opening additional windows

Additional live windows can be opened using the button shown below up to the maximum amount of 16 live windows. The selected view is switched onto the last active live window. Location and size of all live windows as well as the currently active views can be saved as a workspace so that a single click from the main menu can be used to reopen all live windows.



4.2. Events and alarm live view

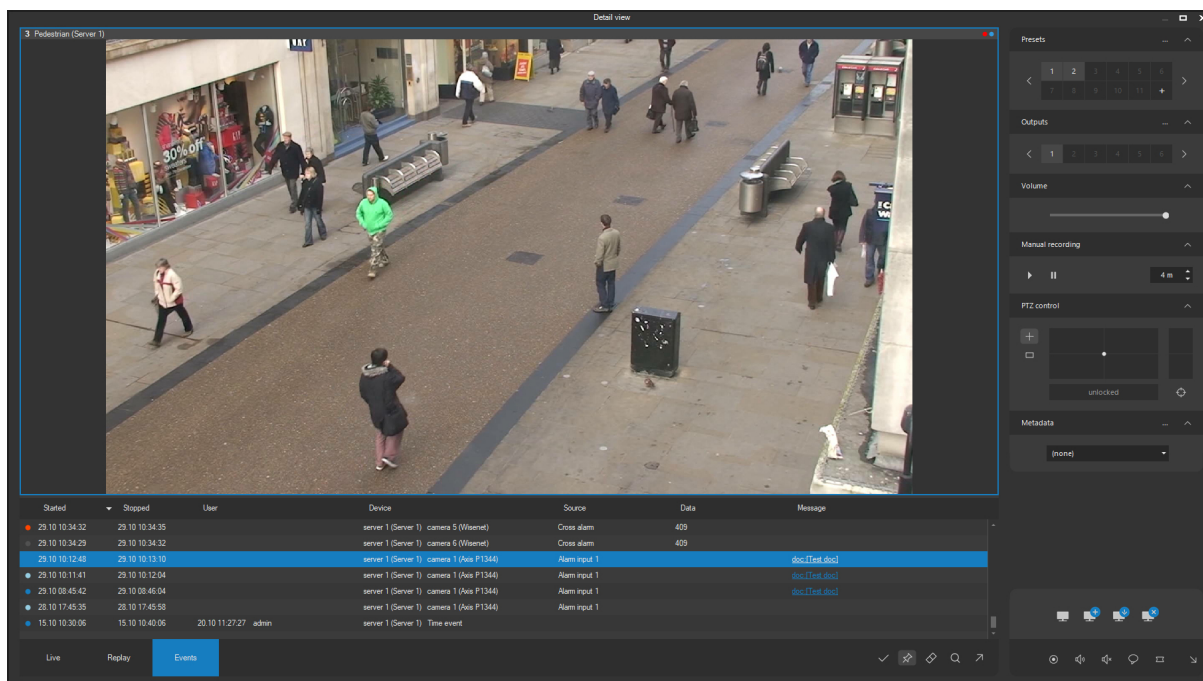
4.2.1. Receiving events

Any live window can be configured to receive events. When an event is received, the current live view may be switched to the event live view which is defined by the administrator and only displays the assigned event.

A system event is initiated by activating one of the currently monitored event inputs. An event input can be, for example, motion detected within the defined area, the activation or deactivation of an alarm input or the activation of a connected sensor.

When an event is received, the application behavior is influenced partly by the administrator (determining the event live view), partly by the user (selecting the live window) and partly by the existing system situation (see description below). A user can select a live window to display system events on the **Events** tab.

When an event is received, a new line holding the event description will be displayed on the **Events** tab.



Information displayed on the **Events** tab includes:

- The level of significance specified by the symbol at the beginning of the line. The system normally distinguishes between events and alarms (common events not causing an automatic view change in the live window). The user can also filter out common events so that they are not displayed within live windows. However, alarms are always displayed. For example, breaking a door contact during the day can be considered as a common event whereas in the night, it can be considered as an alarm, and the system will react differently in both cases.
- Date and time of event start and end, provided the end of the event already occurred.
- The camera (or any other source of events), that invoked the event. A camera unit is defined by server and camera unit identification.
- The time of accepting or closing the alarm together with the user, provided extended alarm handling has been activated.
- The Source of events on the given camera unit. For example, the source can be a connected sensor or motion detection etc. The event source can be identified by either its default name (e.g. alarm input 1) or its symbolic name (e.g. hall door contact).
- Additional event data. This contains either additional information or specifies the event source (e.g. LP of the vehicle).
- A user message, which in case of this event can contain additional information such as instructions for operators etc.

TIP

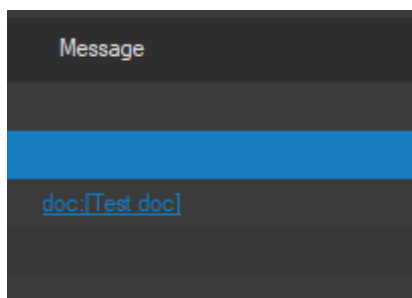
Unused columns can be hidden using the context menu, the order and width of the columns can be updated using a mouse drag operation. These settings remain vital in a saved workspace.

Receiving an event can also invoke automatic changes to the live view on a corresponding live window and can also be accompanied by a signal, alerting the operator. The live view will not be automatically switched to the event live view if only a simple event occurs or at least a minimum configurable amount of seconds have not passed since the last switch invoked by an event. This ensures the view does not persistently switch throughout the process of receiving many events in a short period of time, which would lead to overloading the operators. However, the actual event receiving process is assured every time, so that the user is always informed when an event occurs (without automatic switching of the live view). All events on the **Events** tab are classified according to date and their number can be modified. Sorting of the rows can be updated at any time by clicking on the header of a specific column or multiple columns.

NOTE

An event live view, defined for an assigned event by the administrator, can consist of a random number of cameras. Therefore, it is not a precondition that the camera causing the event is displayed to the user, for the camera does not necessarily have to be the most suitable for monitoring the event. It is also efficient to switch to other cameras that could be essential for evaluating the current event.

Besides a user message, the user may see a link to a PDF document that can contain additional text and graphic information for the event.



Clicking the link opens a window in which the respective document will be shown.

NOTE

The document window remains open after returning to the live window, therefore, the operator sees both the document and the live window at the same time. Clicking on another document link will replace the contents of the window with the last document requested.

The user can lock the currently selected event live view on the screen, preventing automatic live view switching, even after the protected duration for basic event evaluation has lapsed. This is executed by pressing the Hold current view button.



This button will remain active upon pressing it once and automatic live view switching will be reset after pressing it again.



Using the rubber symbol button it is possible to clear the current list of events which always displays the configured number of the most recent system events given by the permissions of the user or group.

NOTE

By cleaning the list it is not possible to remove any open alarms configured to be handled, which always require an action from the operator.

4.2.2. Receiving actions

Besides events or alarm status events, the client application can also receive and display other facts within the events receiving window. These facts lack an event status and it is neither possible nor logical to define a camera scenario according to which the system would react to such facts. These facts are called system actions and are displayed for the purpose of informing operators.

Currently displayed system actions include:

- camera server failure or connection loss (with the alarm status),

- administration server failure or connection loss (with the alarm status),
- camera server connection re-established (with the event status),
- administration server connection re-established (with the event status).

4.2.3. Switching events

You can switch between events displayed on the **Events** tab. Selecting a line holding a particular event will switch the current view to the event view which is assigned to this event by the administrator.

NOTE

The switchover will always be performed, regardless of how serious the situation is and time elapsed since the last switchover.

Started	Stopped	User	Device	Source	Data	Message
15.10.10.30.06	15.10.10.40.06	20.10.11.27.27 admin	server 1 (Server 1)	Time event		
28.10.17.45.35	28.10.17.45.58		server 1 (Server 1) camera 1 (Avis P1344)	Alarm input 1		
29.10.08.45.42	29.10.08.46.04		server 1 (Server 1) camera 1 (Avis P1344)	Alarm input 1		doc/Test.doc
29.10.10.11.41	29.10.10.12.04		server 1 (Server 1) camera 1 (Avis P1344)	Alarm input 1		doc/Test.doc
29.10.10.12.48	29.10.10.13.10		server 1 (Server 1) camera 1 (Avis P1344)	Alarm input 1		doc/Test.doc
29.10.10.41.16	29.10.10.41.37		server 1 (Server 1) camera 1 (Avis P1344)	Alarm input 1		doc/Test.doc
29.10.11.00.58	29.10.11.01.03		server 1 (Server 1) camera 6 (WiseNet)	Cross alarm	17	
29.10.11.01.03	29.10.11.01.05		server 1 (Server 1) camera 6 (WiseNet)	Cross alarm	18	

4.2.4. Window subdivision

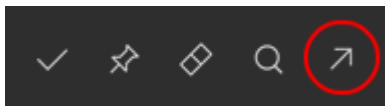
The live window is divided into the view area and some control panels. Between these parts active areas are placed which can be used to change the size ratio of these window parts. This way you can enlarge the control with camera numbers of the list of events. This change will be very beneficial for lists that contain a significant amount of events or if we perform some additional searching or filtering.

NOTE

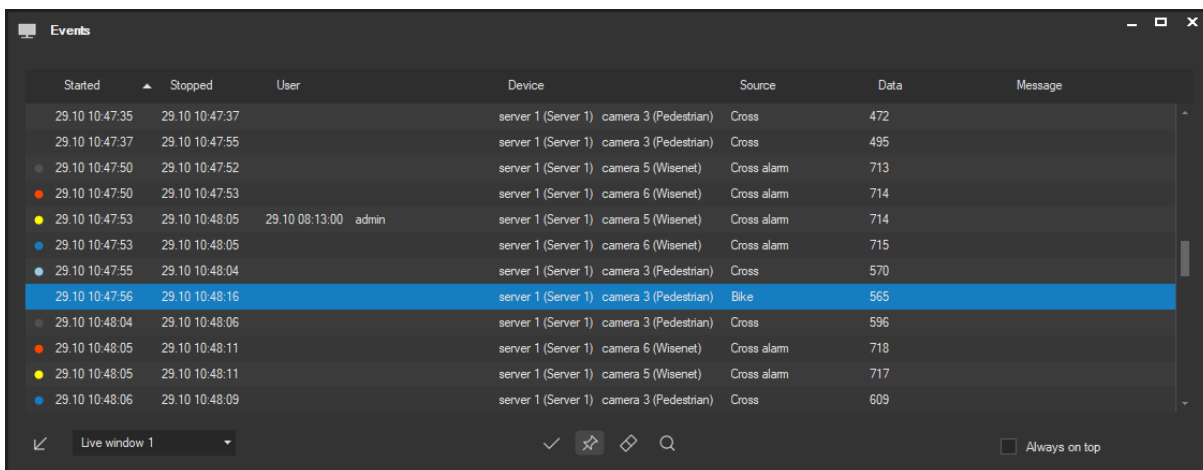
The control panel can also be quickly enlarged by double-clicking the active area intended for changing the display size. If the control panel has its initial default display size, double-clicking will change the size of the view and the control panel to fit exactly one half of the window. Double-clicking a second time will reset the display size ratio to the initial default value.

4.2.5. Separate events window

Using the button for releasing the events from the view it is possible to move the list of events to a separate window.



A separate events window behaves much like the events displayed in a live window. Basic features like selecting the events, replay time synchronization, map synchronization, searching for events etc. all function in the same way. In a separate events window there are also the same buttons for closing an alarm, fixing an event view or cleaning the list of events as above the list of events in a live window.



Started	Stopped	User	Device	Source	Data	Message
29.10 10:47:35	29.10 10:47:37		server 1 (Server 1) camera 3 (Pedestrian)	Cross	472	
29.10 10:47:37	29.10 10:47:55		server 1 (Server 1) camera 3 (Pedestrian)	Cross	495	
29.10 10:47:50	29.10 10:47:52		server 1 (Server 1) camera 5 (Wisenet)	Cross alarm	713	
29.10 10:47:50	29.10 10:47:53		server 1 (Server 1) camera 5 (Wisenet)	Cross alarm	714	
29.10 10:47:53	29.10 10:48:05	29.10 08:13:00 admin	server 1 (Server 1) camera 5 (Wisenet)	Cross alarm	714	
29.10 10:47:53	29.10 10:48:05		server 1 (Server 1) camera 5 (Wisenet)	Cross alarm	715	
29.10 10:47:55	29.10 10:48:04		server 1 (Server 1) camera 3 (Pedestrian)	Cross	570	
29.10 10:47:56	29.10 10:48:16		server 1 (Server 1) camera 3 (Pedestrian)	Bike	565	
29.10 10:48:04	29.10 10:48:06		server 1 (Server 1) camera 3 (Pedestrian)	Cross	596	
29.10 10:48:05	29.10 10:48:11		server 1 (Server 1) camera 6 (Wisenet)	Cross alarm	718	
29.10 10:48:05	29.10 10:48:11		server 1 (Server 1) camera 5 (Wisenet)	Cross alarm	717	
29.10 10:48:06	29.10 10:48:09		server 1 (Server 1) camera 3 (Pedestrian)	Cross	609	

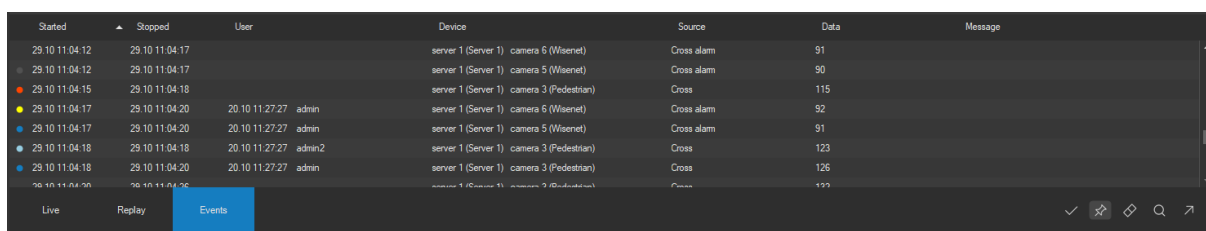
A separate events window can be set to always reside On top or can be brought back to any selected live window using the controls in the bottom part of the window.

NOTE

Switching events between regular live windows and a separate events window affects the local setting in the Monitors and screens section. A separate events window is also part of a saved workspace and can be reopened at its original location and with its original size while loading a workspace.

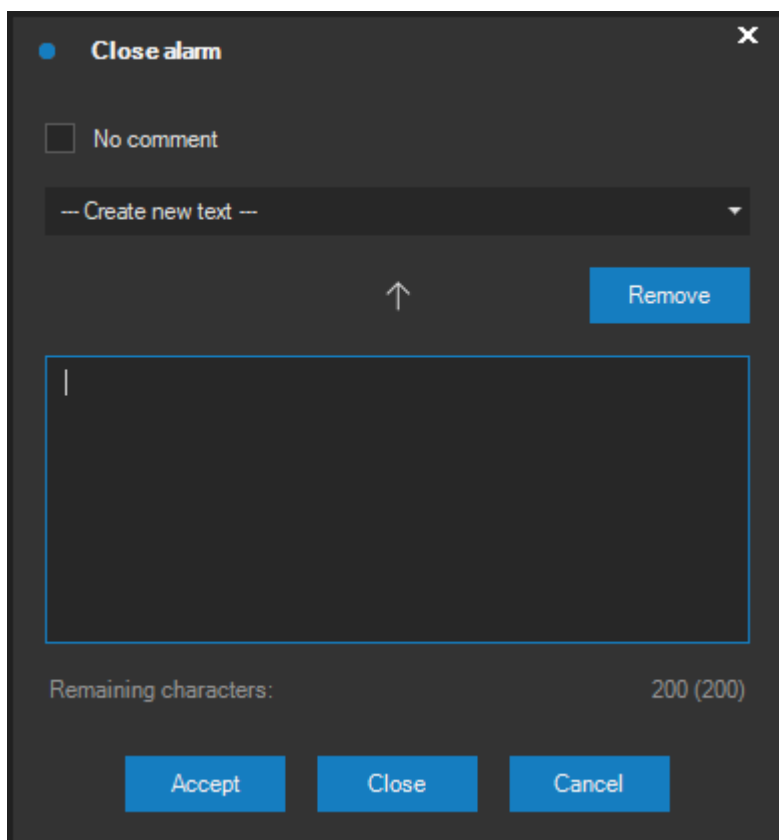
4.2.6. Alarm handling

If the administrator activates the alarm handling mode for any event sources, each alarm with the active alarm handling mode must first be handled in order to be subsequently removed from the live window. A handled alarm (by you or another user) changes the color of its icon to blue. The picture below shows all color options for icons in the event list – common event, alarm, alarm with extended handling mode active, an alarm accepted by you but not yet closed, an alarm already closed and an alarm accepted by someone else.



Started	Stopped	User	Device	Source	Data	Message
29.10.11.04.12	29.10.11.04.17		server 1 (Server 1) camera 6 (Waernet)	Cross alarm	91	
29.10.11.04.12	29.10.11.04.17		server 1 (Server 1) camera 5 (Waernet)	Cross alarm	90	
29.10.11.04.15	29.10.11.04.18		server 1 (Server 1) camera 3 (Pedestrian)	Cross	115	
29.10.11.04.17	29.10.11.04.20	20.10.11.27.27 admin	server 1 (Server 1) camera 6 (Waernet)	Cross alarm	92	
29.10.11.04.17	29.10.11.04.20	20.10.11.27.27 admin	server 1 (Server 1) camera 5 (Waernet)	Cross alarm	91	
29.10.11.04.18	29.10.11.04.20	20.10.11.27.27 admin2	server 1 (Server 1) camera 3 (Pedestrian)	Cross	123	
29.10.11.04.18	29.10.11.04.20	20.10.11.27.27 admin	server 1 (Server 1) camera 3 (Pedestrian)	Cross	126	
29.10.11.04.18	29.10.11.04.20	20.10.11.27.27 admin	server 1 (Server 1) camera 3 (Pedestrian)	Cross	127	

To handle the selected alarm, you must double-click the respective alarm row, or use the Close alarm button. The following dialog requires the user to enter a comment for the alarm handling, or explicitly check the option to close the alarm without a comment.



Close alarm [X]

☐ No comment

-- Create new text --

↑ Remove

|

Remaining characters: 200 (200)

Accept Close Cancel

An alarm can be either accepted or immediately closed in this dialog. After the alarm has been accepted or closed, the color indicator will automatically change for all users having this alarm displayed (colors are different).

Accepting an alarm tells other users (or anyone checking the alarm database), that the user actively deals with the alarm situation and is going to close the alarm sooner or later. This is especially suitable, when there is not enough information to close the alarm right away. The relevant time for evaluating operator's activity is the time of accepting the alarm (if the alarm was accepted before closing). Accepted alarms (by you or someone else) are assigned different colors, see the aforementioned color overview.

For quickly clearing an alarm, you can use any of the predefined texts found in the drop-down list above the comment field. If the user is granted rights for advanced event functions, the user can also edit, delete or create new predefined texts.

Text entered in the comment field can be stored among the predefined texts via the white arrow located to the right of the text field. If a specific text is selected from the drop-down list, the text will be replaced. If the first value in the list is selected, a new text will be created. Predefined texts can be deleted by pressing the cross symbol button next to the drop-down list.

NOTE

Integer values are automatically assigned to individual predefined texts. A text item can be quickly selected from the list by directly entering a code via keyboard.

NOTE

Alarm handling information including information about the user and handling time are available in the alarm database in the Recordings window, where additional alarm comments can also be added.

4.2.7. Event positions in the view

Using the custom layout designer, event positions can be created in a view (see the layout designer description for more). Once event positions are created, they will be used for displaying the event without otherwise interfering with the rest of the view. Older events are automatically shifted to subsequent positions in the view.

A configuration of a view with event positions is especially beneficial for single-monitor configurations and can be used as an alternative to the return from event views feature.

TIP

Event positions are designated by a custom indicator whose color can be changed in local settings.

4.3. Instant replay

4.3.1. Live view replay

Any live view (local, shared, event, detail) can be switched to replay mode, providing instant access to currently viewed camera recordings. This switch is performed by selecting the Replay tab from the bottom control panel.

NOTE

Only views containing no more than 16 windows can be switched to recording mode, making it possible to replay a maximum of 16 cameras at once.

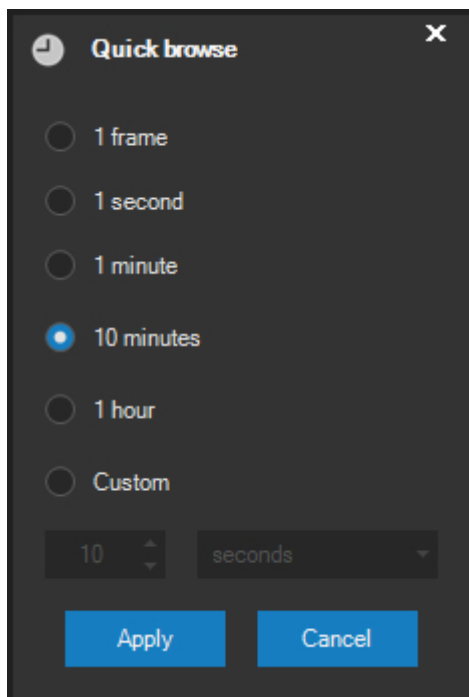
All camera outputs will be stopped after switching to the Replay tab and recorded data can be replayed online. Both date and time are displayed on the right part of the Replay tab. If available, audio is also automatically replayed for the selected device.

In view replay mode, the replay time is automatically set to the last value of the previous replay process. However, if an event view is switched to replay mode, the time will always be automatically set to the start of the last selected event.

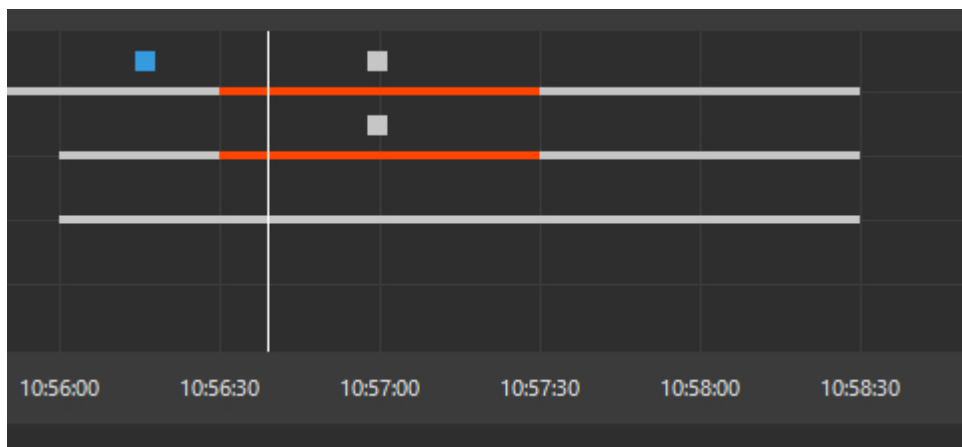
Replaying with player control



The player control feature enables replaying a recording from the current live view. The two smaller buttons on the left side of this control allow the user to change the replay speed ranging from sixteen times slower to sixteen times faster. The three bigger buttons in the middle of this control change the direction or stop the replay. The two smaller buttons on the right can be used for fast scrolling (forwards or backwards) by increments of a specified time interval. This interval can be changed by clicking on its current value. The user can either select a predefined interval or create a new one in the following window. To assign a selected interval to the scrolling buttons, press the **APPLY** button. Value 1 frame is time independent and allows moving between individual video frames.

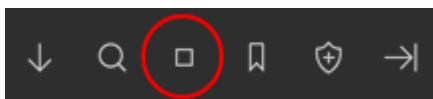


Replaying with timeline



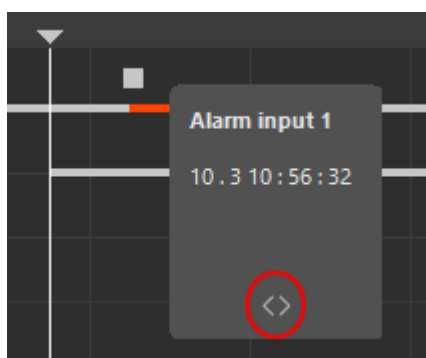
This control graphically shows the time in which the record is available for the viewed cameras. Each row shows the availability of recorded data for each camera, that is part of the replayed view. Event recordings (recordings made during an event), i.e. a situation where the respective camera responds to an event by making a recording, are distinguished by color. If there are several rows on this control, they are sequenced accordingly to their appearance in the view (first by rows, then by columns). Up to 9 rows can be simultaneously displayed. If the replayed view consists of more than 9 cameras (16 at most), only one row is displayed for the currently selected camera.

Individual time rows can also display additional description of events and bookmarks. These descriptions are connected to square colored indicators and will show up once you hover with the mouse over them. This function can be activated using the corresponding button for displaying the events.

**TIP**

Individual camera or external events can be assigned different colors for an improved look and orientation on the time axis.

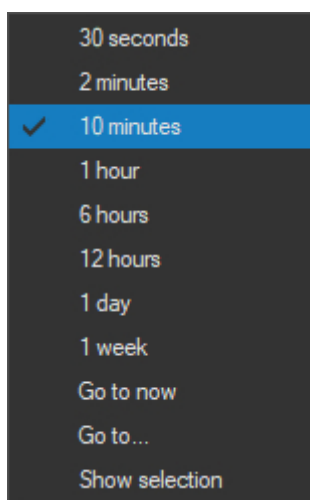
The detailed information displayed over an event or bookmark contains a button for using the event determined by the server, camera and event type or the bookmark determined by the server and camera as a filter for browsing the recordings.



After pressing this button, the skipping arrows of the replay control will navigate the time axis to skip to the next or previous occurrence of this event or bookmark until a new event or time interval or frame is selected.

The vertical white line in the middle shows the time of the recording. This time always corresponds to data displayed on the **Recordings** tab. You can use this control to perform fast scrolling in time by moving the mouse while the left mouse button is pressed (dragging the mouse).

This control has an adjustable time resolution. The time resolution can be changed by displaying the context menu of this control (by pressing the right mouse button), where any of predefined time resolutions can be selected. A quicker and easier option for changing the time resolution (zoom) is using the mouse wheel.

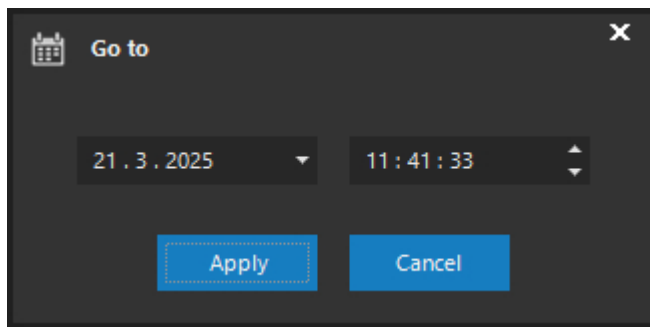


The Go to now option enables a quick jump to the current date and time, therefore to the most recent recording.

NOTE

This function is useful particularly because when activating the recording replay on the Replay tab, the date and time of the recording are automatically set to the last segment replayed, and therefore a quick jump to the last recording available may be required.

The next option within this context menu is the Go to item, the selection of which opens a simple dialog where the user can directly enter the date and time or choose a date from a calendar, taking him to a specific moment.



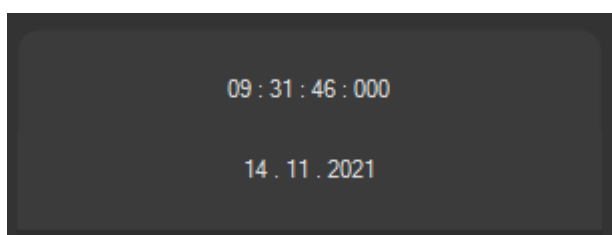
The Show selection option allows you to display the interval boundaries directly in the replay timeline and it also moves the boundaries into visible area. The same effect can be achieved by double-clicking the timeline.

NOTE

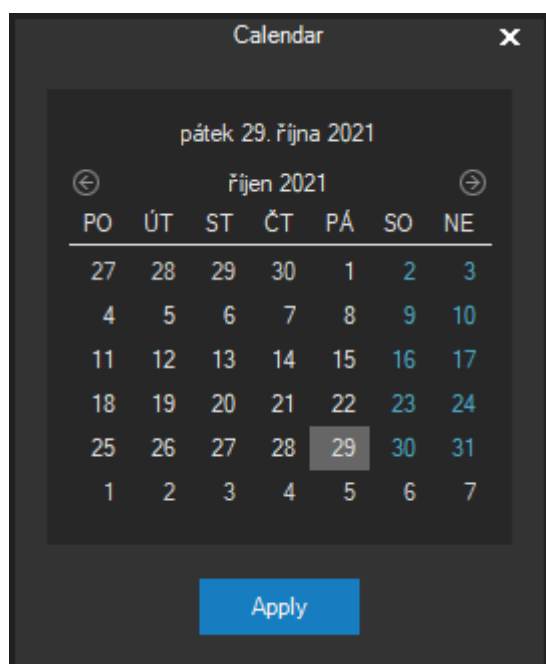
As is the case in the live view, during the replay, it is also possible to display the camera detail by double-clicking on the camera window heading and switch back to the view by double-clicking again.

Date and time selection using the date and time labels

Clicking on the clock symbol accompanying the time label has the same function as the Go to... option.



Clicking on the calendar symbol allows the user to comfortably select a different date while maintaining the current replay time.



4.3.2. Auto-replay

If the auto-replay function is activated, the view can be easily replayed even when recordings are not available for certain intervals for the selected camera. In other words, intervals without recordings will be automatically skipped during the replay process in both directions and at any given replay speed setting.



This function is particularly beneficial for camera recordings made only during an event.

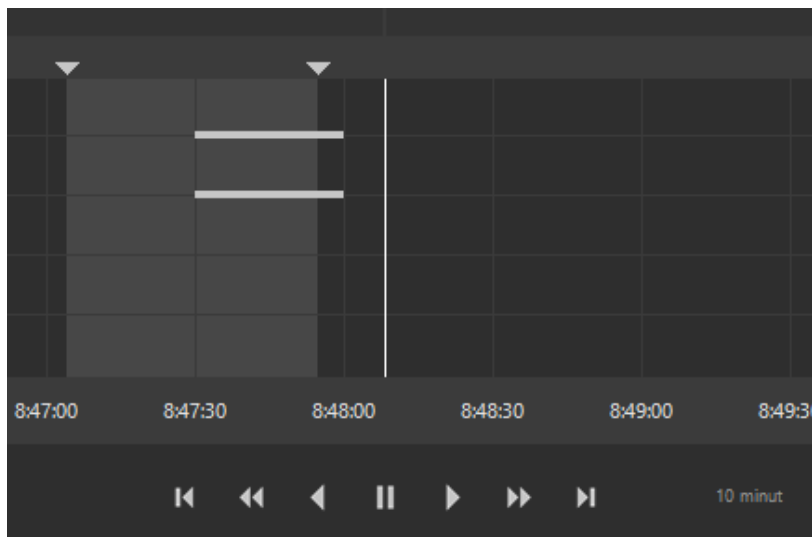
NOTE

If the replayed view consists of multiple cameras, the auto-replay feature is always applied to the selected camera.

4.3.3. Downloading recordings

It is possible to export data from the camera server media stores directly from the live window. During the export process, a new media sequence copy is created on your local hard drive (beyond the camera server media store). The exported media sequence is saved permanently and can still be replayed, edited or exported to other file formats.

The download interval can be configured directly on the time axis using the interval arrows.



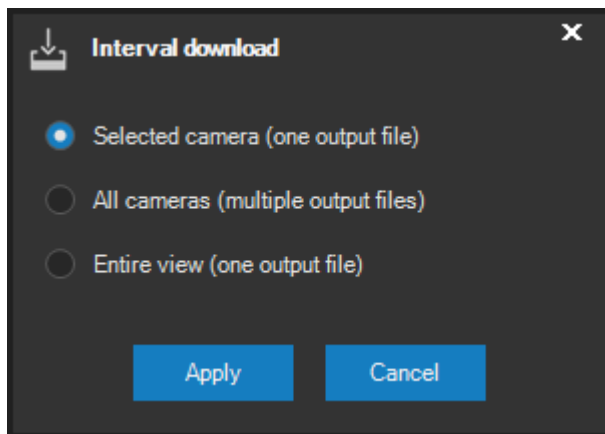
For maximum comfort, the entire view of cameras is synchronized and the corresponding time is displayed when moving the interval arrows. For an exact time configuration, the arrows can be double-clicked which activates the Go to feature.

If the interval borders are outside the visible area of the time axis, double-clicking the time axis resets the interval to appear in the visible area. The Show selection option of the context menu of the time axis has the exact same effect.

Downloading can be initiated using the following button.



The way used to store data can be selected from the dialog displayed after pressing this button.



The first option downloads data for the selected camera. The second option downloads the defined interval for all cameras in the view, where a separate output file is created for each camera. The third option downloads the defined interval for all cameras as well, however, just one single output file will be created containing data for all cameras. The output file created for the last option also maintains the view layout with the exception of custom layout views.

NOTE

Should you select the third option (download all cameras in the view to a single output file), Custom folder shall be selected as the download target in the Download manager window and all cameras in the view must be connected to one server.

NOTE

Each live window stores the previously selected option and will automatically pre-select the respective option as the default option for future downloads.

TIP

The exported data may also include text data of transactions if transactions are displayed at some positions in the view.

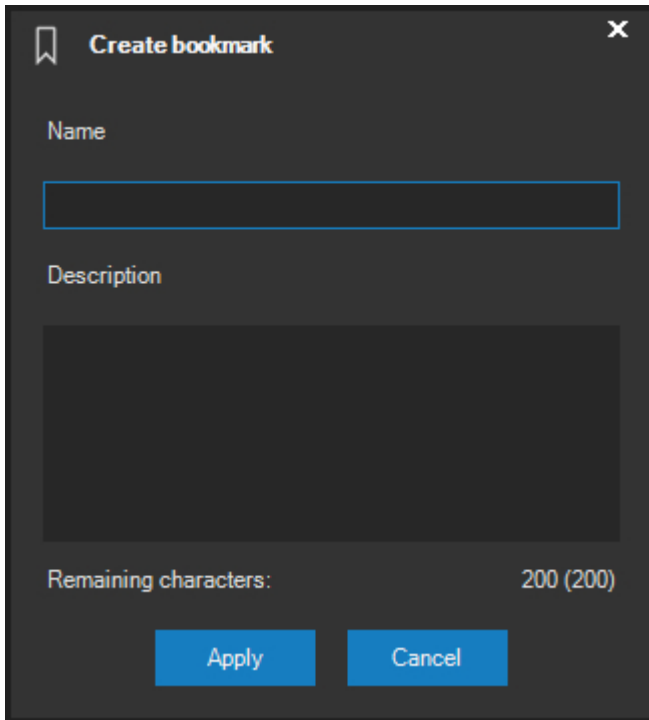
The selected interval for record media sequence downloading must be within 5 seconds to 40 days, otherwise the application will display a warning message and you will not be able to start the media download.

If the time interval for downloading takes longer than 30 minutes, the interval will be split automatically to make handling the downloaded data easier.

Data downloads from the media stores of individual camera servers are performed using a smart download manager, described in a separate chapter. The download manager registers download requests as its tasks and executes these one by one or in parallel.

4.3.4. Creating bookmarks

The insert bookmark button is located in the replay view function button group. Bookmarks contain user information referring to a specific moment in the recorded video. The following dialog for creating a bookmark will appear upon clicking the button.



The image shows a 'Create bookmark' dialog box with a dark background. It has a title bar with a bookmark icon and a close button. The dialog contains two input fields: 'Name' (a single-line text box) and 'Description' (a multi-line text area). Below the description field, it shows 'Remaining characters: 200 (200)'. At the bottom, there are two buttons: 'Apply' and 'Cancel'.

Each bookmark must contain a name and an optional description with a limited number of 200 characters.

NOTE

Bookmarks can only be created by users who are authorized to access the bookmarks features.

NOTE

Bookmarks can only be inserted providing there is data recorded on the server close to the time for inserting the bookmark for the selected camera.

4.3.5. Smart search

If any live window is in replay mode, a smart search can be conducted on the recorded data. Smart search allows the user to perform fast searches for objects of different types, counts, direction, staying time in a zone, colors etc.

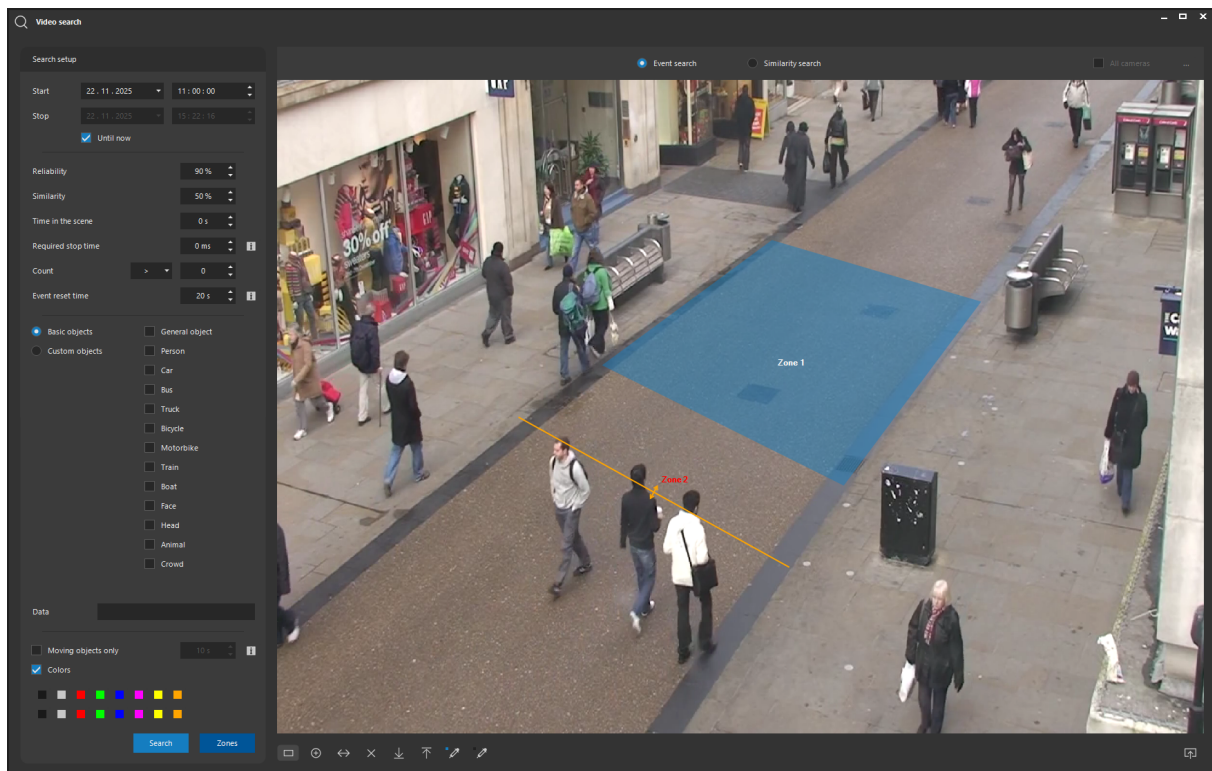
CAUTION

For smart search to be able to generate results, the system administrator has to activate a neural network and metadata storing for selected cameras.

You have to select a camera first and activate the search feature with the corresponding button.



Pressing the Video search button opens the following window from which the search function can be started. If the window is already open, its background image will be updated that can be used to define the event or select an object. The upper part of the window contains options for an event search (condition definition) or a similarity search (sample definition).



NOTE

If a preset is active on a dome camera, the search will be limited to objects bound to this preset only.

In the Search setup section it is possible to limit the time interval for the search. If the Until now option remains activated, the search runs up to the current time.

The Reliability, Similarity, Time in the scene, Required stop time, Count and Event reset time options have the exact same meaning as when configuring the analytical event sources. Using a smart video search however, these settings are applied to stored neural metadata during the search. In any particular zone, it is possible to search for objects satisfying the configured reliability, stay time in the zone, the count of objects in the zone etc.

In the Objects section you can select the types of objects to be searched for. Objects are divided into two groups, it is possible to select from both at the same time. The basic group contains objects that are supported by freely available ATEAS neural networks, the custom group displays object types that you can create by yourself. For more information, see the chapter on custom object types.

The first General object option searches through metadata generated by the advanced motion detector, not by the neural networks. For this feature to work, it is sufficient to activate the generation of this type of metadata.

NOTE

When searching, general objects cannot be combined with the neural network objects.

You can restrict the search for selected object types to those appended with some specific data in the Data section. For instance, you can search for the face object type where the face belongs to people with specific names or to specific groups.

The Moving objects only option restricts the searched incidents to those based on moving objects only. The time value specifies the amount of time an object must be at rest to not be considered a moving object.

In the Colors section you can limit the search to objects satisfying the prevalent color or colors combination (for persons) condition.

Using the **ZONES** button you can activate the drawing options for creating or modifying zones or lines, where the search will be performed. All buttons for creating and editing the zones under the video preview are exactly the same as when configuring the analytical event sources. There you can also find their description. The **SEARCH** button is used to initiate the search process.

All matched results can be viewed by using the **PREVIOUS** and **NEXT** buttons, the preview control under the search results can be used to quickly preview the time before and after any matched event. Double-clicking the result opens a live window in replay mode to replay the event. The time of the very first search result is displayed under the search results.

TIP

Using the CTRL key, multiple search results can be selected. Thus, after a double-click, a view of multiple cameras can be opened at the time of the search result double-clicked last.

4.3.6. Similarity search

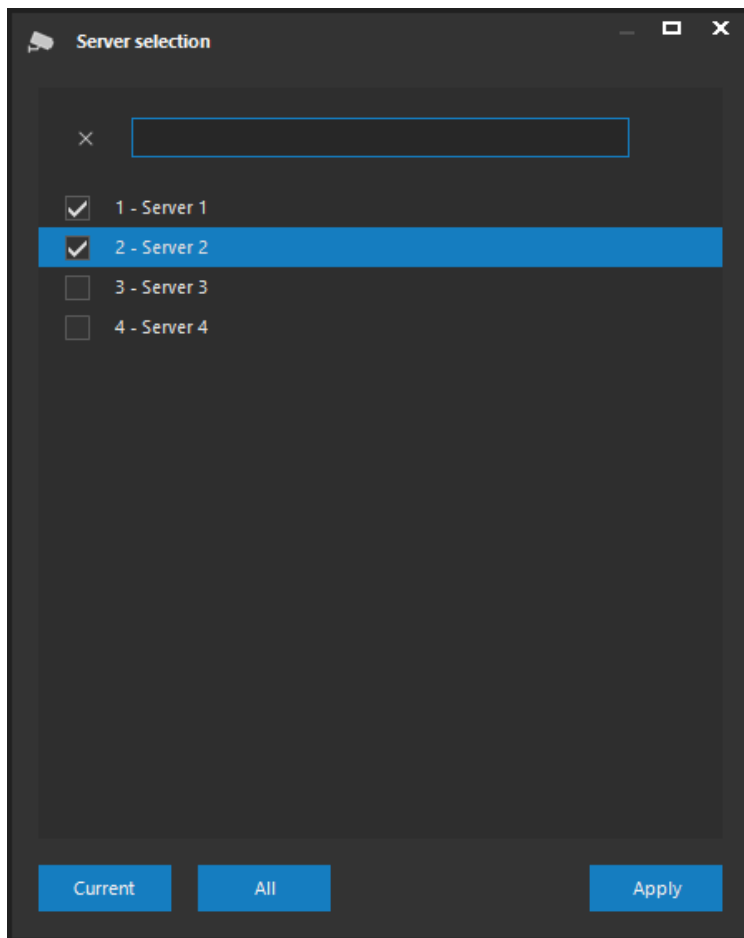
If an event has been raised based on a similarity trigger (face recognition), it can be found among regular metadata including the name of the person or group. If a similarity trigger happened in the past while neural network metadata were being saved, it can be found by entering the name of the person in the Data field while still having the Event search option active.

If neither of these methods can be used, the Similarity search option can be activated in the upper part of the window.

After activating this option, one (and only one) closed zone must be selected where a visual search sample is located. Subsequent search will use the specified reliability and similarity parameters looking for occurrences matching the selected sample. You can search e.g. for faces or whole persons, the type of the object will be detected automatically.

If the visual sample of interest is not part of the server recordings, you can import a jpeg or bmp image into the window, which can be used to select a sample to look for. The button in the right bottom corner of the window can be used to import the image.

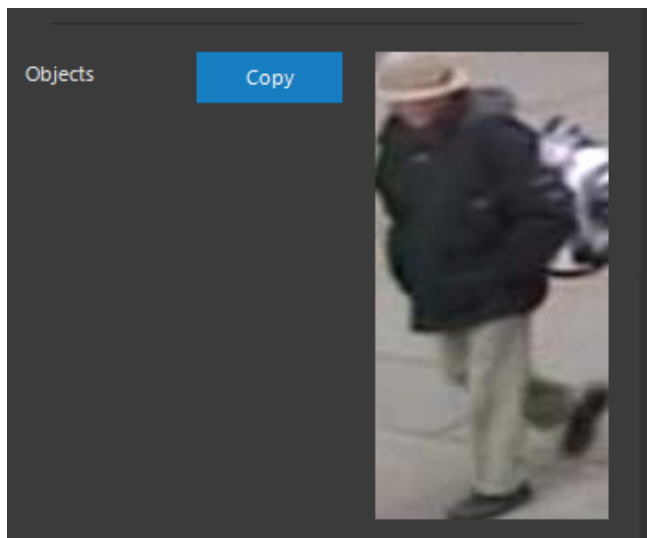
For visual searches, the All cameras option can be used to extend the search to all cameras on a particular camera server or to all cameras in the system (all camera servers). You can select camera servers to be included in the search using the following dialog.



The **ALL** button activates all camera servers, the **CURRENT** button activates just the server to which the camera in the search window belongs.

The search results are affected by whether or not the neural network has tracking enabled. If on, it will be possible to better filter the search results by not repeatedly offering e.g. the same person as soon as the event reset time elapses, because the system will be aware that it is still the same person who has not yet left the scene.

When performing a similarity based search, the visual sample is displayed and can be copied e.g. into the face database or into the Live guard feature. If the Zoom results option is active, all search results are zoomed automatically.

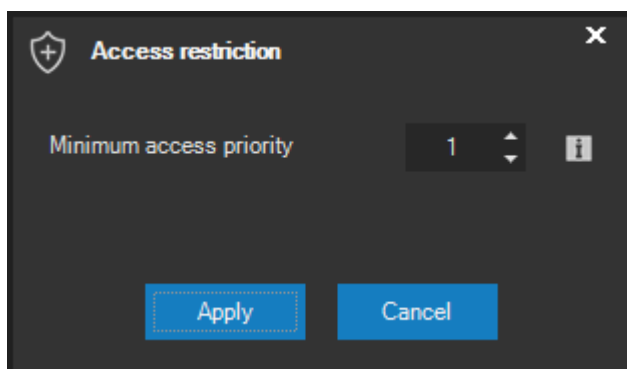


4.3.7. Restricting access to recordings

A system administrator has various tools to restrict user access to camera recordings. The basic tool is controlling access to cameras by specifying rights and restrictions. Another option is to limit the time of the recordings, to which the user has access, for example, only the last hour or day. Instead, the access restriction tool can be used in situations where we would like to limit user access to specific recordings.

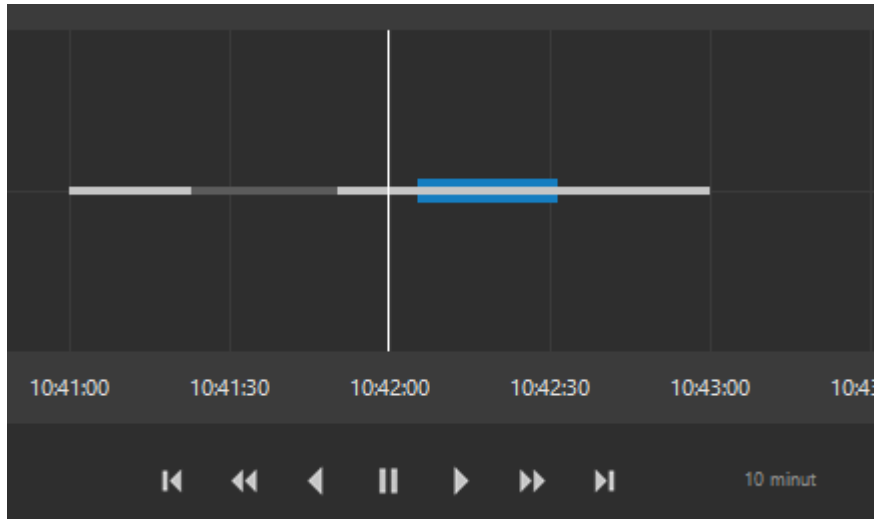


Prior to applying this tool, the camera and recordings interval must be selected with one of the methods described in the Media sequence saving chapter. The following dialog is displayed once the access restrictions are being applied to recordings.



By determining the minimum access priority to a given recordings interval, you can ensure that users with a lower recordings access priority (for the given camera) will not have access (replay or

download) to specific parts of the recordings. The timeline shows which parts of the recording have been restricted and also whether or not the configured access priority allows viewing the recordings.



NOTE

Setting the minimum access priority to 0 removes the restriction for the given interval. Of course, this only applies when our priority is higher than the priority of the user who configured the restriction.

NOTE

Any user can use this tool based on his maximum access priority to recordings, granted by the administrator. By default, however, this priority is set to a value of one, meaning the restriction can be configured, but it will not be effective.

4.4. Selected camera functions

4.4.1. Camera selection

Any camera can be selected from the view by clicking anywhere within assigned camera window. A camera window is determined by its title including a number, name and other camera data, a surface for displaying the view and the camera image itself (if available at the given moment). A blue border will always be displayed around the selected camera. Functions on the side control panel only apply to the selected camera.

NOTE

If the current view contains a single camera, it is selected automatically.

CAUTION

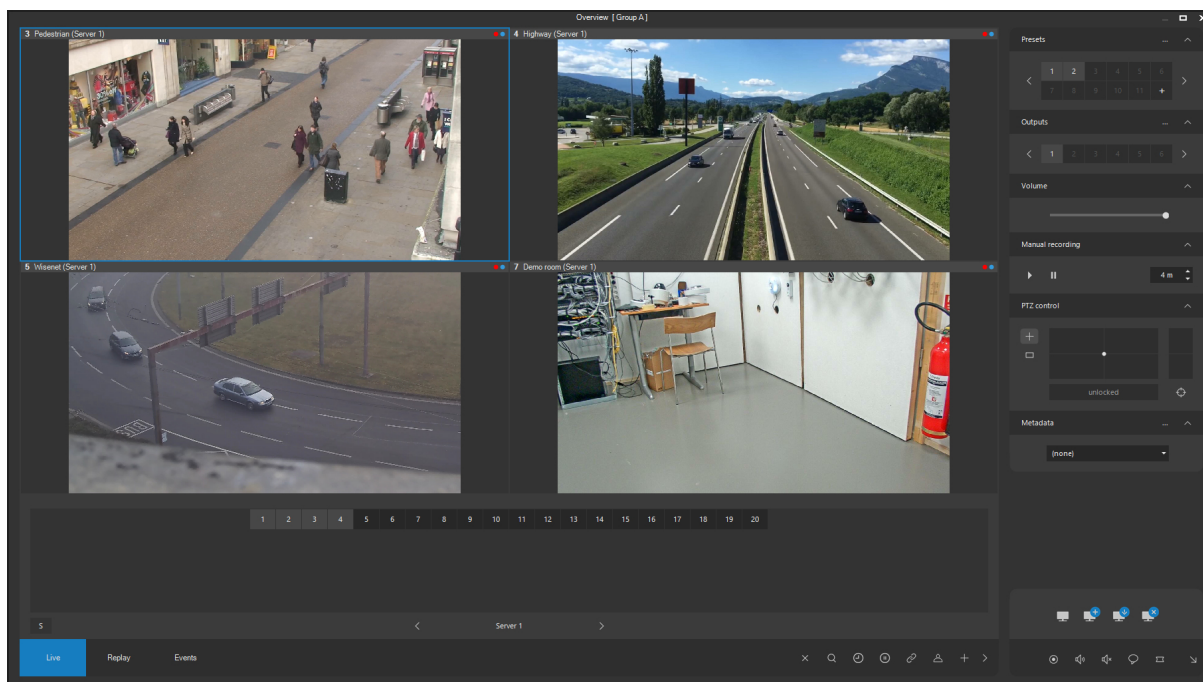
We recommend selecting cameras by clicking on their header instead of clicking directly in the camera window. Considering the fact that PTZ devices can be controlled from the camera window, clicking in the camera window may lead to the camera starting to move (if configured as a PTZ device).

A camera may also be selected by specifying its number on the numerical keyboard, similar to special camera keyboards. To select, press all digits the camera number consists of on the numerical keyboard (e.g. 1, 2, 3 for camera number 123), and confirm by pressing ENTER. The camera selection is made for the currently selected position in the view.

NOTE

Keys in the numerical part of the keyboard by default are used for PTZ camera control. In order to use the numerical keyboard for making a camera selection, the numerical keyboard settings must be changed in the local client settings. Cursor arrows can then still be used for PTZ camera control.

4.4.2. Displaying detail



Any camera (with an available camera view) within the current view can be switched to the detail view, displayed always for a single camera. The camera view will be available with the maximum possible resolution (with regard to the native camera and monitor resolution) and also with enhanced (maximum) frame rate for the detail view. This is ensured automatically and based on administrator settings.

The camera can be switched to detail view from any live window by double-clicking on the header of relevant camera window. You can switch back to the default view by double-clicking on the relevant camera header again, this time in the detailed view. The detail view will be closed if another view is selected from the main menu or if the user switches to the event view.

The target live window, to where the detailed view will be switched, can be configured in Setup. The current view will be replaced with the detailed view by default, if detailed view is selected. The detailed view will then be displayed in a current live window. This behavior can be modified in Setup.

There is one exception here, if the currently opened view is a centric view (camera layout with multiple cameras around a bigger central camera position), the detail switch is made into this central camera window.

4.4.3. Saving snapshots

Snapshots can be saved for each camera selected. A snapshot is referred to the current state of a camera view converted into image format, generally supported by all platforms (JPG, BMP etc.). A snapshot from a selected camera can be saved by pressing the Take shot button. This button is on the side control panel and always applies to the camera selected.



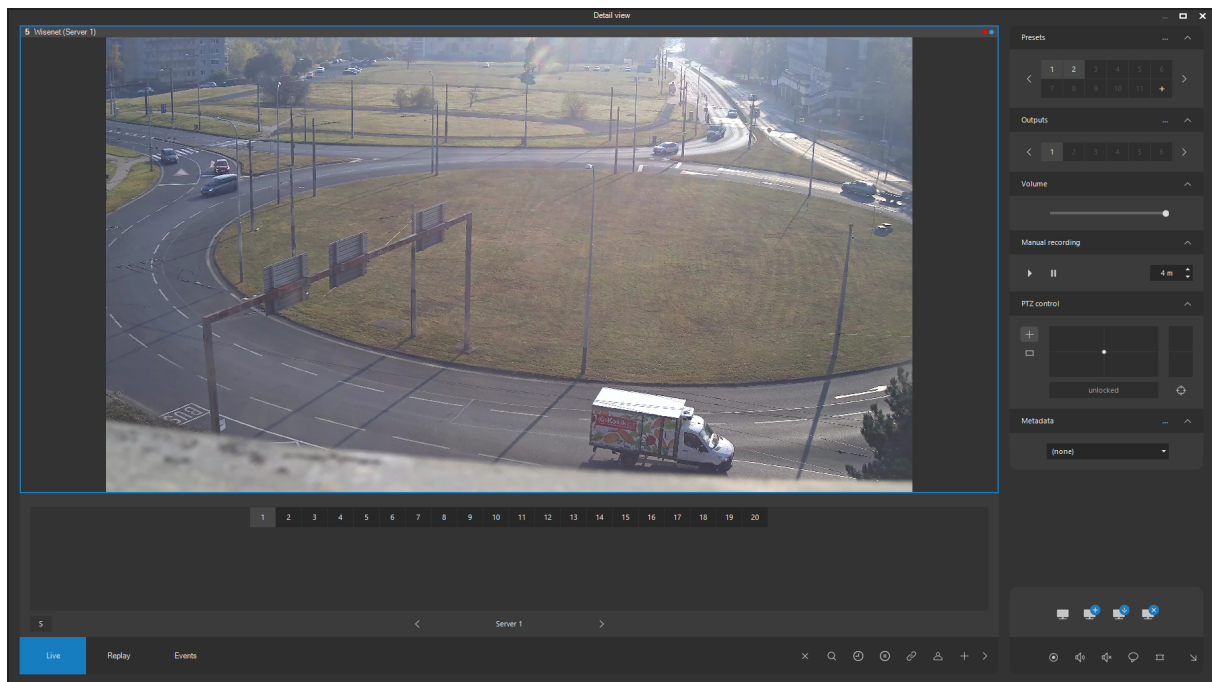
After the snapshot is saved, a window containing the snapshot database will open. Operations related to this window are discussed in a separate chapter.

4.4.4. PTZ device control

PTZ device control is one of the basic functions for cameras selected. The ATEAS Security system offers full-featured and very sensible controls and mechanisms. Controllable cameras (i.e. PTZ and DOME devices) can be controlled in several ways.

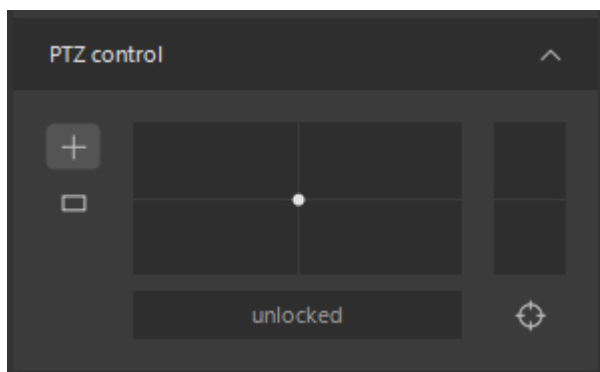
Controlling a camera within the camera window

Controlling a camera directly within its view is a very intuitive control method, where the camera always moves from the middle of the view to the mouse cursor. The movement speed depends on the distance between the cursor and the middle of the view. You can move the camera along two axes and in all directions at variable speeds. Transitions are perfectly smooth.



To rotate a camera by mouse, press and hold the left mouse button while the cursor is positioned on an assigned location within a camera window. The camera will stop moving as soon as you release the left mouse button.

If available, the mouse scroll wheel can be used for zoom control (even while controlling the camera within the camera window). All operations in all three axes are projected into the camera positioning control in the bottom part of the side control panel.



Controlling a camera using the camera positioning control

The control showed above basically simulates a tri-axial joystick, which makes it possible to position the camera directly by using a mouse. The camera can be rotated by pressing the left mouse button and moving the mouse. Similar to clicking within the view, both the horizontal and vertical movement speeds depend on the distance between the mouse cursor (point 1) and the middle of the control

(point 2). The direction is set by the vector between both points. The right part of this control is intended for zoom control. The zoom speed depends on the vertical distance between the mouse cursor and the central line segment.

Controlling a camera using a joystick

Cameras can also be controlled using joysticks connected via the USB interface. If the joystick is equipped with all three axes, smooth movement is achieved at variable speeds for each of the three axes (pan, tilt, zoom). If a joystick is not equipped with a third axis, you can zoom in or out using the joystick buttons. Joystick button functions can be configured in Setup on the joystick tab.

CAUTION

Not all joysticks are suitable for controlling cameras (often is the case that cameras are difficult to control due to low sensitivity and large dead and saturation zones on cheap models designed for gaming).

NOTE

Special high-sensitive tri-axial joysticks for controlling cameras may be included with your camera system order.

Controlling a camera using a computer keyboard

PTZ devices can also be controlled by a computer keyboard, or by the numeric keyboard arrows to be more specific, with both horizontal and diagonal movement available. The plus and minus keys can be used for zooming. Cursor arrow buttons can also be used. This can be convenient, for example, when using the numerical keyboard for camera selection (see local settings). Of course, diagonal direction control is missing with the use of cursor arrows.

Focus control

The Focus button can be used to adjust the camera focus manually, provided we are not satisfied with the result of auto-focus. This may occur in situations, when the camera cannot objectively decide on how far it shall focus with respect to the actual scene.

Pressing the focus button allows the user to control the focus in the same manner as zoom, using all of the methods described above including, for example, joystick control. Proportional focus speed is also supported as is the case with zoom control. In order to return to zoom control you need to release the button again by pressing it once more.

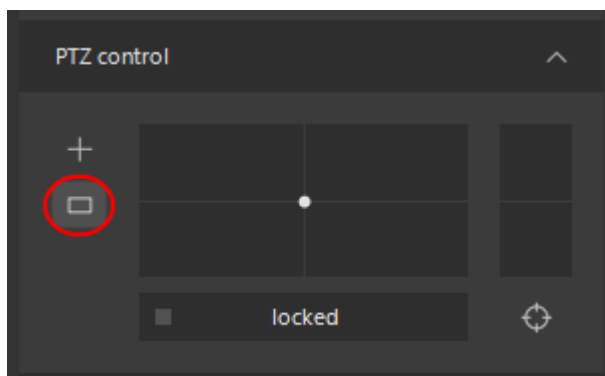
NOTE

If focus control is active, a different transition color is used in the PTZ user control to distinguish from camera zoom.

Area zoom feature

The default method of controlling the PTZ camera by touching or clicking in the camera image described above can be switched into a different PTZ control mode by clicking the area zoom button.

A faster way of using the area zoom feature is leaving the PTZ symbol in its default state (proportional control) and using the Ctrl key, which activates an instant possibility to select a rectangle to perform the area zoom operation.



A rectangle can be drawn in this mode and the camera will automatically pan, tilt and zoom in to capture the selected area as best as possible.

CAUTION

This feature is not supported by all camera types.

Some special types of fixed cameras (e.g. Axis Q6000) enable to calibrate an associated PTZ camera, allowing the zoom area feature to be used even in the image of fixed cameras and thus achieve an area zoom by the associated PTZ camera. Together with these special cameras, this feature allows zooming in on the scene detail without losing the overall situation awareness given by the fixed cameras.

NOTE

The live window keeps track of the last used control mode for a PTZ camera and this mode will automatically be selected when the next PTZ camera is selected.

4.4.5. PTZ locks

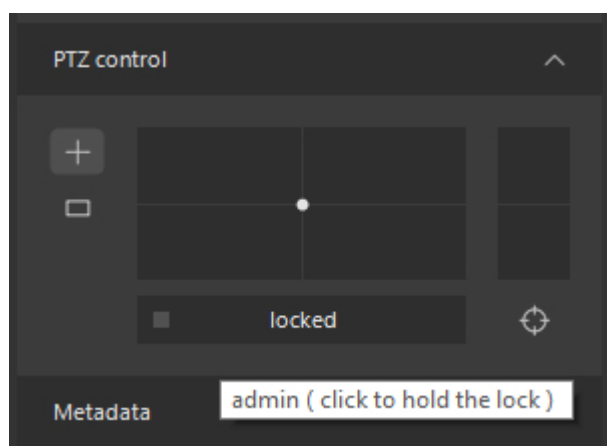
ATEAS camera servers use an advanced set of smart rules for managing multiple user access to camera control. Control priority settings (PTZ priorities) for individual users and generating so called PTZ time windows are crucial. PTZ time windows are described in subchapter User administration under PTZ rights and priorities settings. The basic principle of the time window rests in the camera being still under the control of the user who controlled the camera last for a certain period of time (the duration of the PTZ time window is tens of seconds), in order to ensure the continuity of PTZ camera control. The time window can be interrupted only by a user with higher PTZ priority to the respective camera.

Providing the user needs to control a camera explicitly himself for a longer period of time and restrict other users from controlling the camera even after the PTZ time window duration has lapsed, he can apply the PTZ lock.

NOTE

For example, if the user needs to direct a camera to a certain point of interest, leave it idle for a longer period of time, and at the same time, restrict another user from directing the camera elsewhere.

For the user to be able to apply the PTZ lock, he must have a PTZ time window generated for the given camera, i.e. he must first acquire camera control. In this case, besides the information stating camera control is locked for the user with his name, the button for activating the PTZ lock is also enabled. The name of the user is displayed when hovering with the mouse over the lock area.



After pressing this button, the PTZ lock is applied to the camera and no other user with the same or lower priority will be able to control the camera, not even after the PTZ time window duration has lapsed. A user with higher priority for using the given camera can of course cancel the PTZ lock and create his own PTZ time window, or potentially his own lock.

NOTE

The PTZ lock can be applied to an arbitrary number of cameras. The PTZ lock, however, requires user presence in the system, if the user logs out or otherwise concludes his action, the PTZ locks will be cancelled on camera servers and camera control will be open to other users.

The PTZ lock can be disabled by pressing the lock button again on the camera the lock was applied on.

4.4.6. Special PTZ functions

Using the user control for controlling PTZ cameras (see previous subchapter), it is possible to activate special PTZ camera functions, if supported by the given camera type. If any type of special PTZ function is supported, it will be possible to activate these functions by clicking on the graphic symbol and to switch them using arrows. The function activation itself must however be executed using the left mouse button. The right mouse button deactivates the special PTZ function selected.

The following special functions are available:



Auto tracking function – if activated, the camera is switched to auto tracking mode and reacts to movement in the image by monitoring moving objects or vehicles by itself.

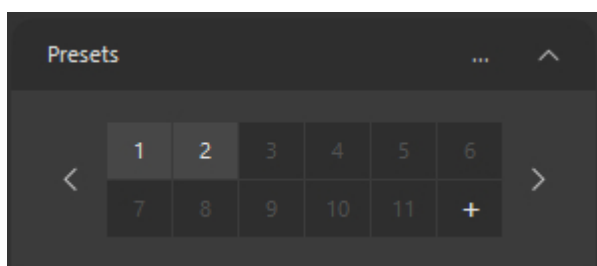
CAUTION

There are no special rights under user administration connected with the use of special PTZ functions. These special functions, however, may only be used by users authorized to control the given camera and at the same time have the highest control priority (at least priority 10).

4.4.7. Preset points

A common function for PTZ devices is saving the values for all three axes (pan, tilt, zoom) for a specific point. This point is known as the camera preset point and can be used to instantly shift to a specific location.

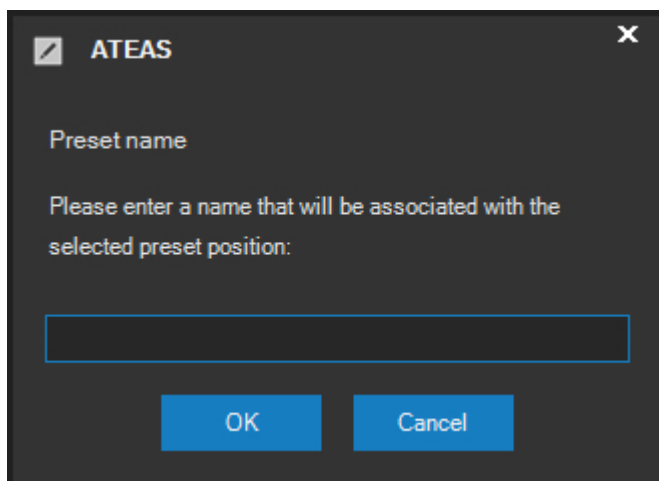
Switching cameras to preset points



Each camera can have up to 100 predefined preset points. . You can tell filled positions apart from free positions by their lighter shade of grey. If you move the mouse cursor over individual preset points, the names of each point are displayed. The selected camera is positioned to a preset point by clicking on the number of the preset point. You can use the arrows to move to the right or left to display additional presets.

Preset points setup

If you want to fill or re-write a certain preset point, you must first position the camera to a target point and then click the setup button, which will then be highlighted. After clicking on a destination position (from 1 to 100 based on the currently displayed set of preposition points), a dialog requesting the name of the preset point will be displayed.



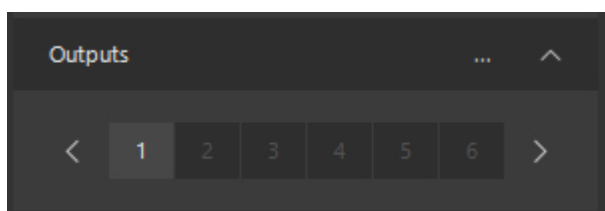
Upon confirming with the **OK** button, the current camera position will be saved and assigned a number. The preset point setup button on the preset points control will be automatically disabled (standard preset point operation remains in tact).

Deleting preset points

Preset points can be deleted similar to the way they are created, the only difference being that you have to click the particular preset point, to be deleted, using the right mouse button (the setup symbol must be highlighted demonstrating an active state). The preset point will be deleted upon confirming the displayed message dialog.

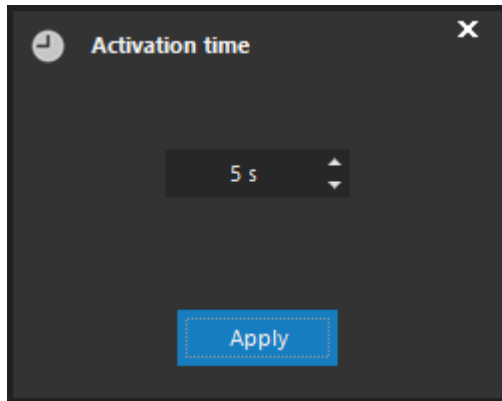
4.4.8. Output activation

Outputs can be connected to certain cameras or video servers. These outputs can control, for example, door locks, tollgates etc. and can be activated manually in the live window (they can also be activated automatically during events). Selected camera outputs are part of the output control.



Available outputs have a light grey color, unused outputs blend with the application background. If you move the mouse cursor over the output numbers, the name of each output is displayed. This name can be either default (e.g. Output 1) or symbolic, defined by the administrator (e.g. Gate etc.)

Activating an output for a certain number of seconds can be executed by clicking on the assigned output number. The default pulse time is 5 seconds, this value can be configured for each camera separately by clicking on the three-dot configuration button.



NOTE

If the time delay value is set to 0 (zero), the output will be permanently activated – it will not automatically switch to an inactive state. Manual output deactivation is possible by setting the time pulse value to -1, or by clicking the right mouse button on the output, which deactivates the output independently of the time pulse value.

NOTE

The application remembers the last values used to activate individual camera outputs and automatically sets the respective time interval upon selecting the same camera (even if selected in a different live window). This information is stored throughout the entire client application session. By restarting the application, the information will be deleted and set to default.

4.4.9. Receiving audio

If an audio source is available for the selected camera and the administrator allows audio transmission for this camera, you will automatically hear a live audio feed after selecting a camera. The only precondition is a working sound device (sound card) and connected speakers.

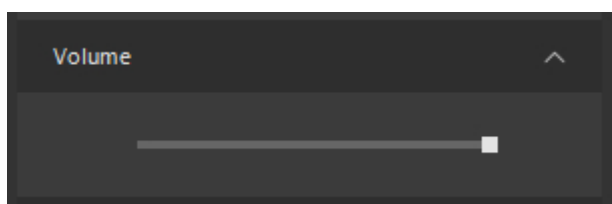
Audio can only be played from one selected camera per live window. If more than one live window are opened, you need to manually detach the audio feed from the window you are not interested in listening. To attach/detach audio, use the relevant buttons on the side control panel.



NOTE

If the system contains a video server with several video inputs and one audio input, it depends on the administrator settings, to which video inputs audio will be allocated. Audio can be allocated to a random combination of video inputs, this for a random video format. For some video formats, however, it might be necessary to allocate audio to video inputs also directly in the video server settings, depending on the type of camera.

Volume can be adjusted using the control showed below. The volume is set to maximum by default.



Receiving audio for a selected camera is available for both live view and replay from a recording.

4.4.10. Push-to-talk

Providing the selected device supports two-way audio, you may speak directly into the camera from the live window meaning that if a camera is equipped with an audio speaker, the station operator, equipped with a microphone, can establish audio transmission with the camera. A button enabling this function is available on the selected camera functions panel.

This function depends on whether or not the camera supports two-way audio and also if audio transmission is enabled by the system administrator. You can only talk to a device on port 1 if the device is multi-port (devices with several video inputs) and have only one audio input (and most often only one audio output).



NOTE

If you want to speak into the camera, press this button and release it after the audio transmission by pressing it once more.

If the push-to-talk feature is already in use for the selected camera by another user with equal or higher priority, talking to the camera will not start and the user will be notified with a message.

Talking to multiple cameras simultaneously

Your client application can transmit audio from your microphone to multiple cameras or special IP speakers at the same time. If you right-click the button to activate the audio transmission instead of left-clicking it, the audio transmission will automatically be activated for all cameras in the view.

NOTE

When transmitting audio to all cameras in the view, the user permission to this feature is of course respected for cameras in the view and the transmission will only be possible to cameras, which the current user can access and for which he is granted the two-way audio permission.

NOTE

It is not possible to transmit audio simultaneously to multiple cameras connected to different servers (the target server for multiple audio transmissions is specified by the server of the selected camera). It is however possible to activate the audio transmission function in multiple live windows at the same time, thus making it possible to simultaneously transmit audio to a maximum of 400 cameras connected to 4 servers.

If the push-to-talk feature is already in use for any camera by another user with equal or higher priority for the given camera, talking to the camera will not start for all cameras. The user will be notified with a message. Cameras that were not receiving any audio, or that were receiving audio from users with lower priority, can be used.

Auto-mute feature

Audio from the camera is often captured by its microphone when working with two-way audio transmissions. This situation is referred to as audio feedback. Feedback can be caused on both the camera's end and client's end. ATEAS introduces a simple way to prevent this situation. Simply double-click the button for transmitting audio to the camera to automatically disable audio on client's side. This function may also be used for the simultaneous transmission to multiple cameras by double-clicking using the right button.

NOTE

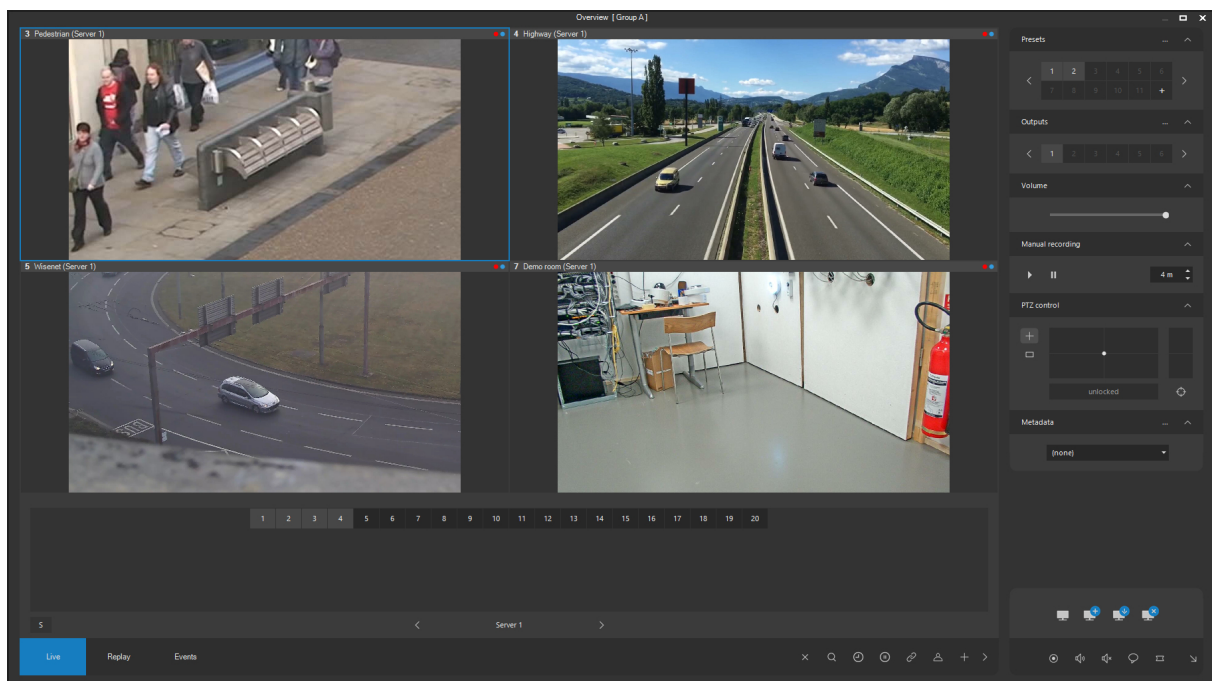
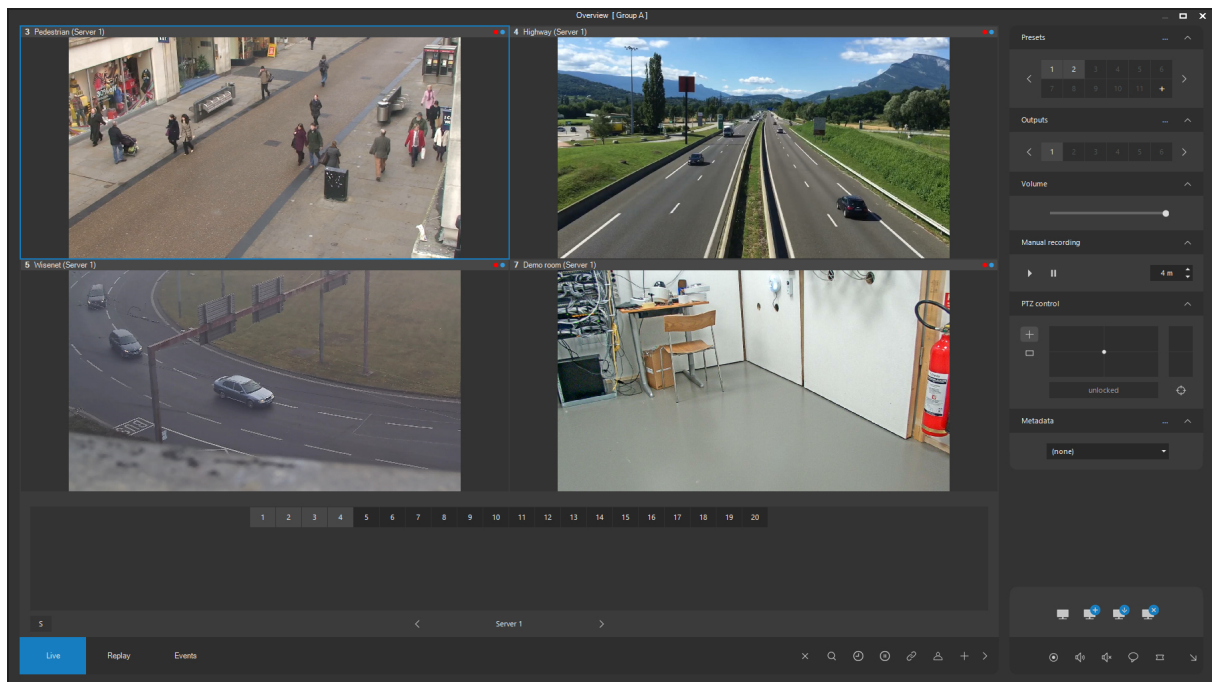
The audio transmit to camera function including auto-mute can also be enabled by pre-set keys, which can be arbitrarily selected in the local client settings. See the keyboard local settings chapter for more information.

4.4.11. Digital zoom

ATEAS Security software offers digital zooming for each selected camera. A digital zoom is referred to as enlarging image details within a window of constant size. This function is especially suitable for devices with megapixel resolutions (can be used for all resolutions). The precondition for using this function is that you can display a view in a larger size than the current one. To some extent, this is regarded as an alternative to the detail view function which switches the selected camera to a new detail live view. The digital zoom function displays a selected view in detail without opening a new view window. This function can additionally be used in many other parts of the system, for example:

- in a detail view, for sufficient camera resolutions,
- in a record preview,
- when replaying a recording,
- in a snapshot preview and browsing,
- in the ATS Media Player application.

The following pictures show the utilization of digital zoom with a fixed camera positioned in the top left corner of the view.



Digital zoom (or zoom out) is entirely controlled by the scroll wheel. If the view is digitally zoomed, you can digitally move around the whole view in the same way as you would manually rotate a PTZ device, directly from the view. Therefore, a joystick or a simulator cannot be used for digital zooming.

By clicking the middle button (mostly a mouse wheel) you can quickly reset the digital zoom to its default.

NOTE

If you switch to another view or if you adjust the window size, digital zoom is reset to its default value (i.e. the whole view is displayed).

Digital zooming also can be used for PTZ devices. Considering scroll wheel operations and clicking into the view are automatically assigned to PTZ control, you must first disable all PTZ operations. To disable PTZ operations, click the PTZ control button currently active.

NOTE

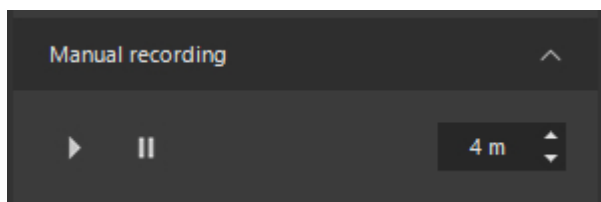
The default system settings only allow digital zoom up to the native resolution of the displayed video. Increasing the digital zoom does not improve the quality of the displayed graphical information (the number of pixels is finite), nevertheless in some cases, you can benefit from increasing the zoom. The digital zoom can be increased above the native resolution of the video by activating it in the local settings of the Video settings.

NOTE

The speed at which picture digitally moves during the digital zoom depends on the distance of the mouse cursor from the centre of the picture, but it also intelligently adapts to the digital zoom level to achieve smooth and expected movements.

4.4.12. Manual recording

Since release 3.9.6, all authorized users can perform manual recording, the controls of which are available in each live window in the right part of the window.



NOTE

This function relates to the provision of relevant rights by the system administrator, this function will not be available to users without these rights.

The principle of manual recording rests in the user's capability of invoking a manual recording event with the press of the button containing a blue arrow symbol. This concerns a special event, which can initiate recording or increased recording frame rate. This event is subsequently available in the system on the list of events when viewing camera recordings.

Depending on the current camera settings, initiating manual recording events for a selected camera can have various affects. If at the given moment the camera records only events, the initiation of manual recording will cause recording to begin (with the option of saving a pre-alarm recording, if configured). If a camera records with a low or medium frame rate (see creating recording rules) and if increased frame rate is permitted during an event, the initiation of manual recording will increase the frame rate of recording as specified.

CAUTION

Therefore, the operation of this function requires the camera to have an assigned recording rule, which permits recording during events or at least an increased recording frame rate during an event.

The user control for controlling manual events also enables configuring the duration of an event. After the duration (specified in minutes) has lapsed, the event will be automatically concluded. The event can also be concluded even before the expiration of this duration by pressing the respective button.

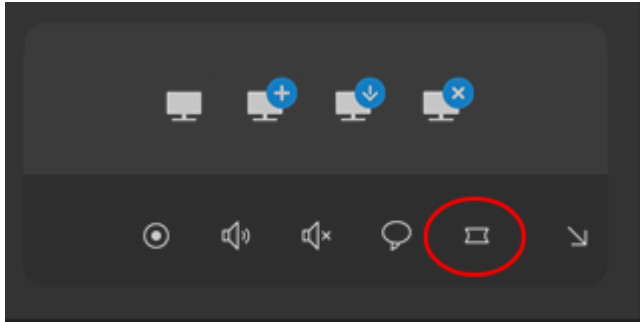
NOTE

Multiple initiations of manual recording are not possible, the previous event must be concluded (duration has lapsed or manually) before starting a new event.

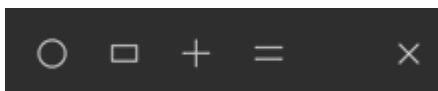
4.4.13. Fish-eye image dewarping

If the system administrator configured the selected camera as a fish-eye video source (fish-eye cameras with a special 360 degree lens), the Dewarping modes button can be used to activate the

dewarping mode selection. Dewarping is used because the basic fish-eye image, displayed in the rectangular area of your view, is naturally deformed.



A new set of buttons for activating image dewarping modes appears when the button with the fish-eye symbol is pressed.



The following image dewarping modes can be activated with these buttons:

- 360 degree image (no dewarping),
- single PTZ view (dewarping into one view with PTZ camera control option),
- "quad" view (dewarping into four views in various sections also with PTZ control option),
- panoramic view (single or double panoramic view).

NOTE

In simple view mode, the image can be zoomed out to full overview (360 degrees), correction is smoothly applied as necessary.

The buttons for switching between image dewarping modes can be hidden via the white cross symbol.

Modes that support PTZ control can be controlled in the same way as actual PTZ cameras, directly by clicking into the camera image.

NOTE

The single or double panoramic view is automatically selected based on the camera orientation set by the system administrator. See the basic camera setup chapter for more information.

Any given selected image dewarping mode set for a selected position in the view is always stored together with the current view. This indicates the image dewarping mode is automatically activated when this view is opened and of course also when the view is shared.

NOTE

The view not only contains the information about the selected dewarping mode, but also the information about the PTZ position. If a single PTZ view or a quad view is subsequently moved to a different position, this information will be stored together with the view. Unlike the image dewarping mode, however, a changed PTZ position itself does not trigger a dialog for saving changes when the view is closed without saving.

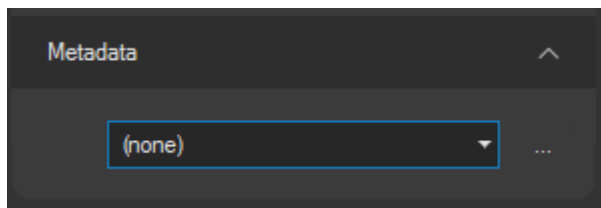
NOTE

The selected dewarping mode and PTZ position is also automatically used for a detailed view of the camera displayed in the same or separate window.

The fish-eye image dewarping mode can be changed in the live view even during playback. If a full fish-eye image (360 degrees) has been recorded in the system, we can access the recordings at any time in a PTZ camera mode in the sense that we can freely look around the recorded scene.

4.4.14. Displaying metadata

Provided the system administrator connected neural network metadata or an external source of analytical data to the camera, the names of these sources will be displayed after selecting the respective camera.



Once a data source is selected, analytical metadata will immediately begin to appear in the camera video, regardless of whether or not an event occurred. Displaying, for example, object analysis results adds value in situations when an event has not yet occurred based on the configured rules.

NOTE

The selected metadata source for the given camera is saved together with the view including a shared view.

NOTE

If storing of neural network metadata is enabled, when selected from the list, the metadata can also be replayed together with the camera video.

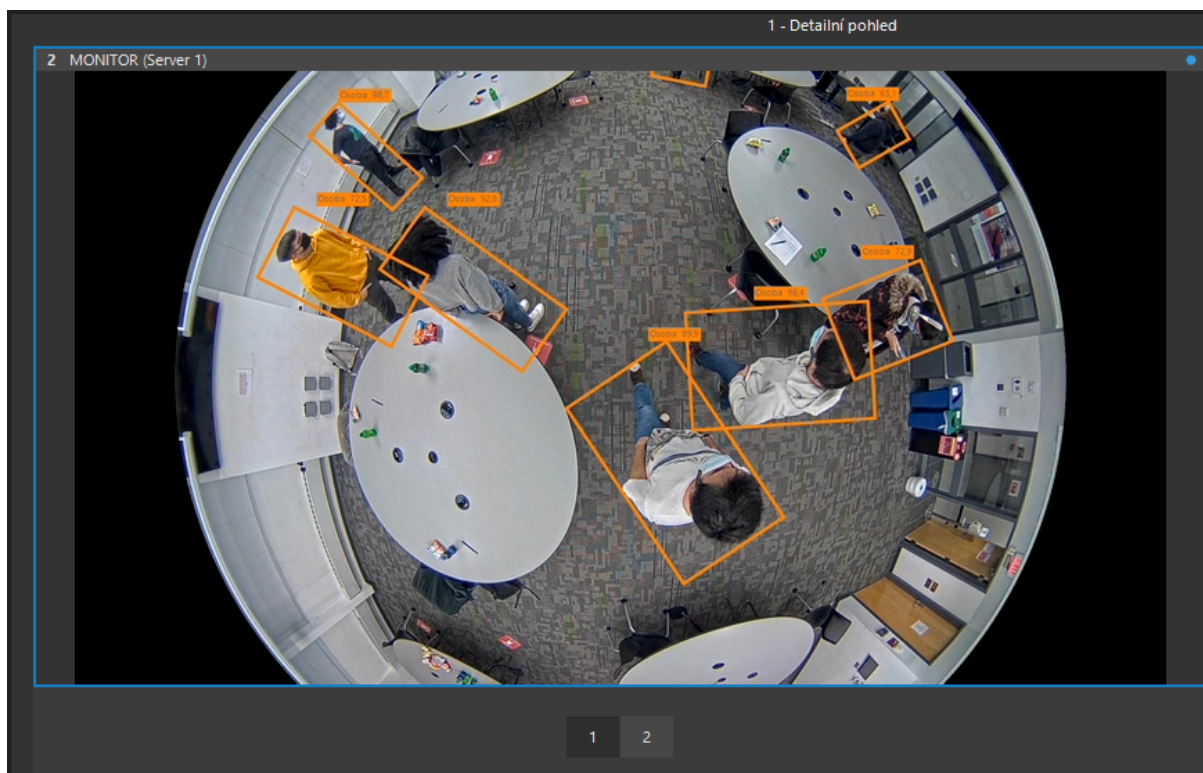
NOTE

The pen width for metadata rendering can be configured in the local client settings. This width remains the same while digitally zooming (unlike the situation when the metadata is rendered directly by the camera).

Networks capable of predicting additional object attributes or extended object location information can display additional visual elements. For example, the WD model, thanks to also predicting the angle, can display rotated bounding boxes.

NOTE

To be able to display rotated boxes, acceleration of metadata rendering must be activated.



4.4.15. Motion detection and analytics configuration by users

Privileged users, who have been assigned the necessary permission by system administrators, can use the button to the left of the metadata groups combo box (see previous subchapter) to configure server motion detection and video analytics settings. This includes changing the motion detection parameters like sensitivity, editing existing or adding new detection zones for neural networks, or changing the event source parameters.

NOTE

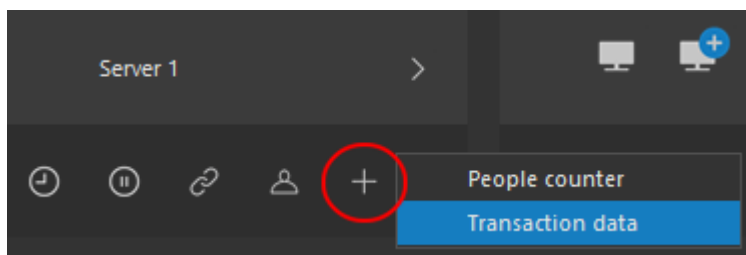
As opposed to entering this configuration from system administration section, it is not possible to add new event sources. This is because users cannot access the event scheduler, neither are they allowed to configure the event scenario.

The way of configuring all these settings is described in detail in the relevant system administration chapters; the user interface and overall logic stay absolutely the same.

4.5. Using transaction data

4.5.1. Live view

If the system administrator linked some cameras to transaction data (e.g. with point of sales data), this transaction data can be displayed live and replayed directly in the live window. Displaying transaction data for any selected camera can be done using the additional data camera menu.



Receiving transaction data from cameras can be an integral part of camera views (local and shared). Live video from the camera, its associated transaction data together with a cash desk terminal screen captured by the ATEAS Screen Recorder application can be combined in one view.

NOTE

You can create a complete system for all types of stores with a high added value by combining video monitoring features, cash desk terminal screen integration into the camera system and transaction data integration.

NOTE

The presence of a specific item anywhere in the transaction can also be a reason for an event to be generated. For more information, see the chapter about custom camera events.

4.5.2. Replaying transactions

Replaying transactions follows the same principles as replaying video from cameras. The transaction data of one or more cameras is automatically synchronized during the replay process or while moving along the time axis. During the replay process, the current row of the displayed transactions is always highlighted with respect to the actual replay time.

1 Axis P1344 (Server 1)		
ATEAS transaction		
549780	Oranges	15.20
005890	Milk	19.90
479055	Potatoes	49.00
789475	Eggs	25.00
497528	Bread	16.50
210591	Whiskey	764.50
No connection		

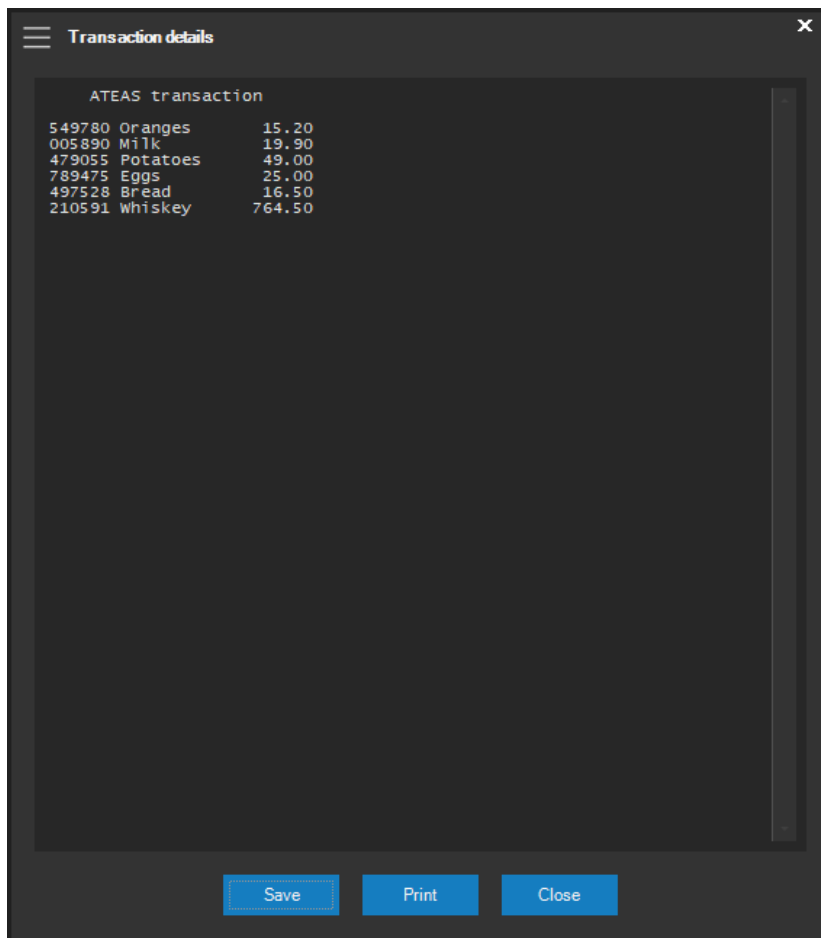
CAUTION

Transaction data must be received in real time to ensure the automatic row selection and selection moving. When receiving entire transactions at one moment in time, this feature will be disabled by design.

The displayed transaction also offers a new way of synchronizing the replay time in the live window. Clicking on a particular item in the transaction sets the replay time to the occurrence of this item. Video or transactions data will therefore become synchronized on all other positions of the live window.

4.5.3. Saving a transaction

A transaction can be saved using the button commonly used for saving the current snapshot in the window.



In this window, a transaction can be saved to a text file or sent directly to a selected printer for printing.

4.6. Cooperation with the map window

4.6.1. Synchronization during camera or element selection

If the automatic map synchronization is set to full under local setup, the entire map scene will be synchronized after selecting a camera or element. This will automatically select a map level (centering and zooming in and out according to current setup and zoom).

Automatic synchronization will also be used if the camera automatically switches to detail view or if the automatic mode is activated. The map is synchronized if the activated automatic mode window is selected. Therefore, it is possible to perform virtual tours of the object along with automatic map synchronization.

CAUTION

Automatic synchronization is not possible if the map window is not opened. In other words, automatic map synchronization does not open the map window, if closed. The map window always has to be opened using the respective button.

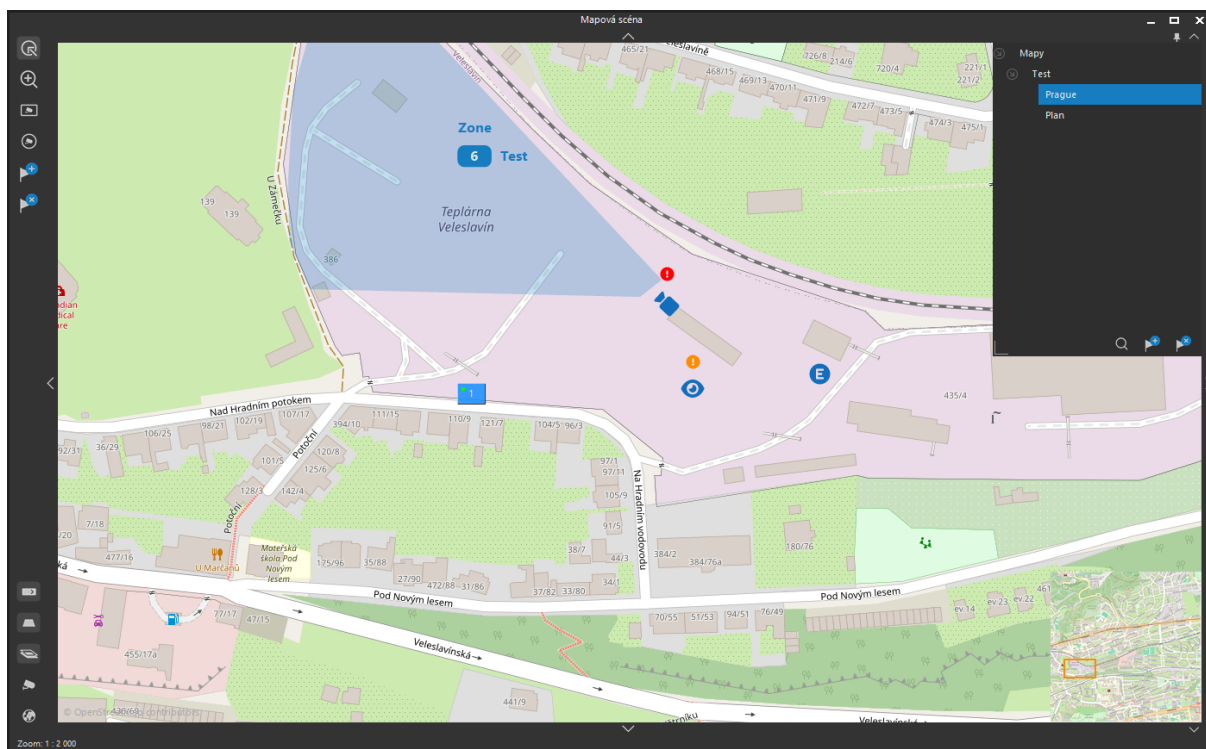
NOTE

The camera symbol in the map will flash for a couple of seconds for better orientation.

4.6.2. Event synchronization

If automatic map synchronization is configured to full or event and an event occurs, the map scene will be synchronized the same way as in the previous case, meaning that if an event occurs, the map will be centered and the place where the event occurs will be zoomed optionally. Automatic map synchronization will always be performed (even if the view is not switched to an event view because of two quickly subsequent events, or if the switch of the view is evaluated as overloading the operator). In case an overload is detected due to an excess amount of events, the view will not be switched to the event view, however, the map will be automatically synchronized (though only if the place where the event occurs can be pinpointed – the camera which detects motion has specific coordinates). A new line will also be added to the list of active events.

Events are indicated by an additional exclamation mark symbol. Depending on their age, events will change their color until they disappear completely from the map scene. The following picture contains cameras showing different events, each with a different age. Time delays between individual age groups can be configured in local setup.



Automatic map synchronization will also be executed (providing at least automatic synchronization is active) for a selected line and event. If this is the case, the view is automatically switched to event.

CAUTION

Here we do not synchronize the event view cameras. Instead, the source camera or element is synced which might be a different camera from those added to the event view.

NOTE

In case of an external event, which is not localized, the map will at least be synchronized according to the first camera in the event scenario, which is localized. This way the user can get some information about the location of the external event.

4.6.3. Map selection

Cameras selected using map window functions (described in a separate chapter regarding map window control) can be projected into live windows (according to local setup). Selected cameras are marked with a different color in the map and the newly formed view is referred to as Map selection.

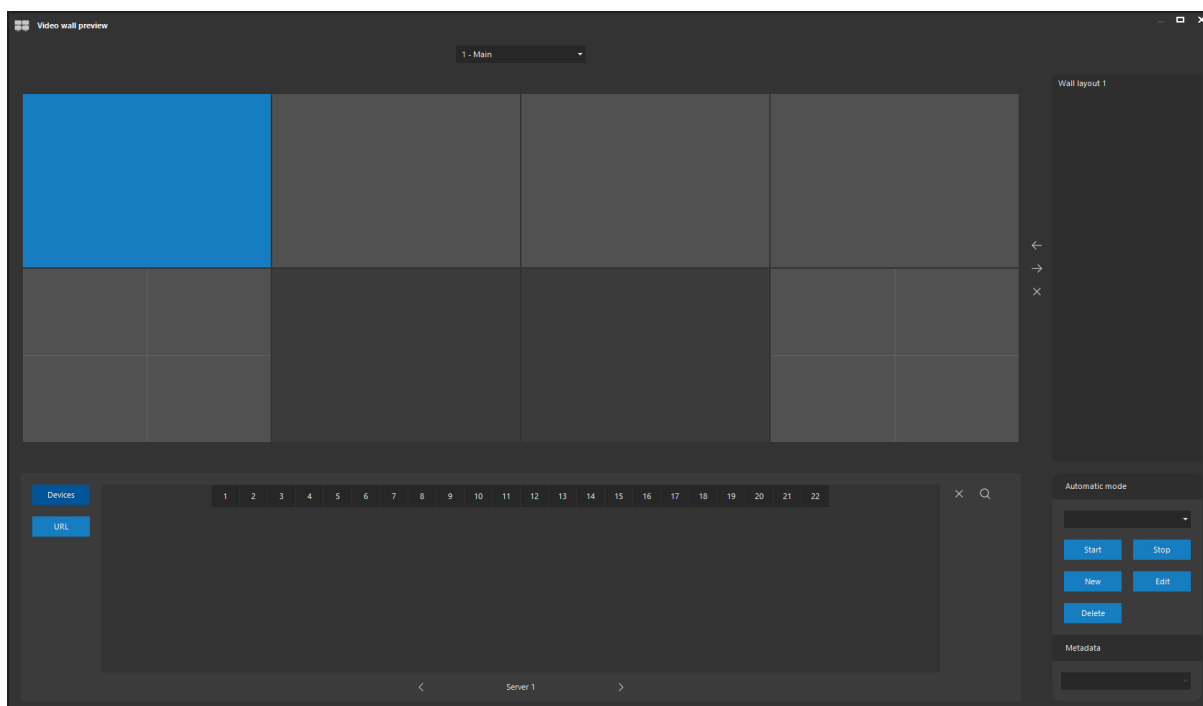
4.7. Working with the video wall

4.7.1. Switching cameras

A video wall is a physical or virtual group of monitors connected to several slave stations in the system. The video wall can be controlled from other authorized client workstations. If your main menu includes the Video Wall item and you are authorized to run and control the wall, you will also have access to all remote monitors that have been configured by the administrator.

NOTE

Video wall configuration and functioning processes are described under administration in the views section of the Video wall tab.



The video wall we intend to use can be selected from the drop-down list in the top part of the window. There is virtually no limit to the number of video walls, they can represent independent groups of external monitors in various locations.

All video walls, created and configured by the system administrator, are available in this window. Any camera in the system (available to the user) can be switched to another active (light) monitor. The switch itself is very easy. First of all, select an active monitor from the video wall by clicking on the

monitor (indicated by a blue background). Then select a corresponding camera from any server by clicking on the camera in the control panel in the bottom part of the window. To select a server by scrolling or by selecting it from the list, proceed the same way as you would with switching within live windows or creating event scenarios. If a camera is successfully switched to a remote monitor, both the camera and server IDs will appear in the monitor symbol. To turn the camera off from a particular monitor, press the button with the cross symbol, located next to server and camera controls.

A video wall preview is updated depending on the operations of users who have access to the video wall (also depending on the occurrence of alarm events). Therefore, if another user (or the system itself) switches a camera to a remote monitor, you will be notified in your video wall preview.

Monitors marked with a white dot symbol belong to the group of event monitors. The system automatically positions and moves cameras that display system alarm events (with the Include in alarm view attribute assigned) to these monitors.

Monitors, visibly separated into 4, 9, or 16 parts are referred to as Quad, Triple, or Sixteen type monitors. These monitors can display up to 4, 9, or 16 cameras. If a Quad, Triple, or a Sixteen type monitor is selected, one of its parts (besides the entire monitor) is selected to perform a manual camera switch.

Same as in the live window, using the search device button you can quickly search for cameras according to their numbers or names and send them to the video wall.

NOTE

The video wall has all mechanisms for restoring connection implemented just as the standard client (camera failure, connection to camera server failure). It additionally features the option to restore connection to the administration server. After restarting the video wall (computer or client software), it will automatically restore to the previous state.

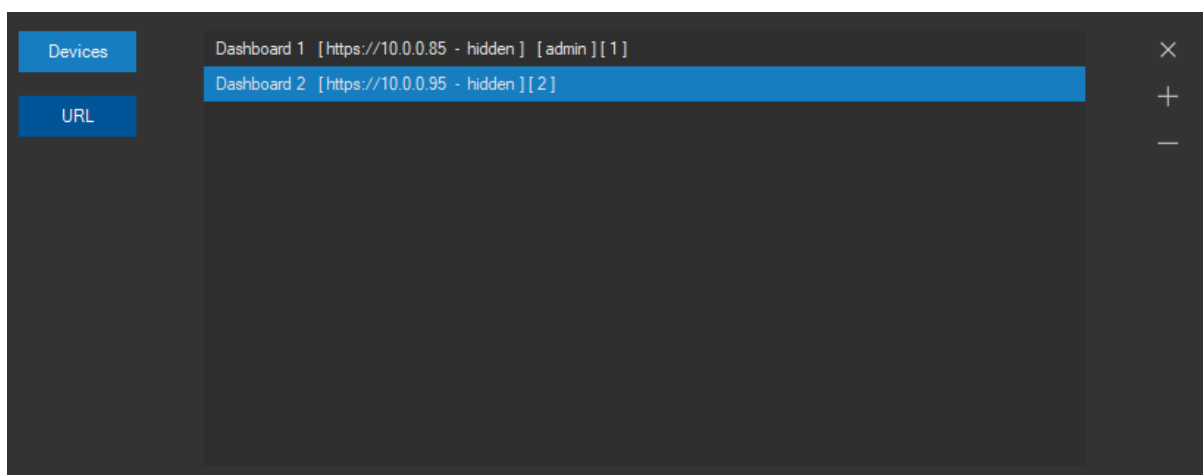
4.7.2. Displaying metadata

You can activate displaying of analytical metadata coming from ATEAS neural networks or from the cameras on the video wall much in the same way as in regular local or shared views. To display metadata on the selected wall position, use the Metadata drop-down list in the right bottom part of the window.

When displaying large numbers of cameras in full frame rate on one video wall computer, you should activate GPU acceleration for video rendering in local video wall client settings. When many objects are detected in the scene, the GPU accelerated metadata rendering should be activated as well.

4.7.3. Switching URLs

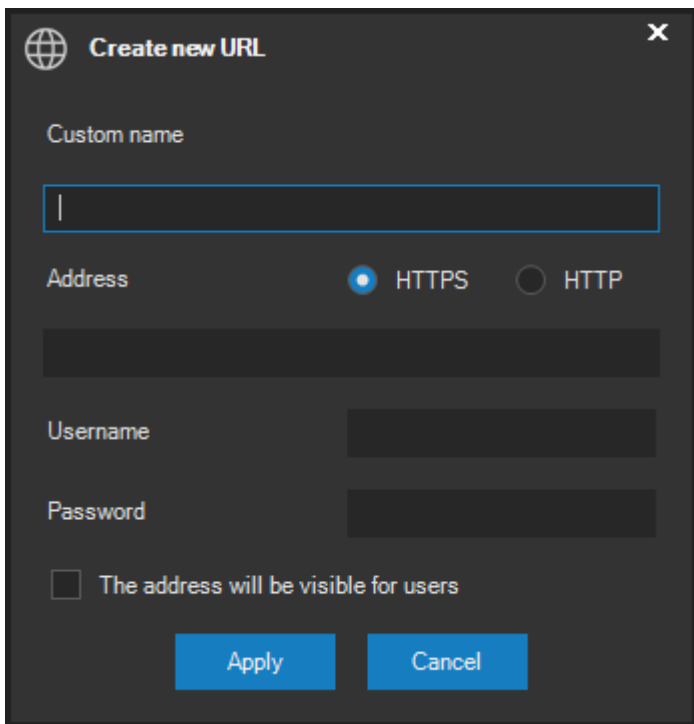
A video wall supports displaying modern HTML 5 based web content with latest CSS etc. Much like a camera, you can switch a webpage to any particular place on the video wall, which has been added to the system by an authorized user. The URL selection can be activated with the **URL** button.



The list displays the custom names for the URL as well as its address, provided the user is authorized to view it. If the address is hidden, the user may switch the URL to the video wall but can't see its real address. If the user is authorized to view the addresses, he always sees them, if they are configured as hidden, this information will be displayed behind the address.

At the end of the URL authorized users are shown a numeric value identifying this URL for ATEAS API purposes.

A URL can be added by clicking the plus button symbol. Then, following dialog needs to be filled in.



A custom name and address (with http or https protocol selected) must be filled in. If a given URL requires authentication, it is possible to also enter the username and password. The video wall would then authorize itself and display the protected web content.

Using the corresponding option, the address of a URL can be configured as hidden for users without the necessary permission.

The minus symbol button is used to remove any given URL from the list.

You can inject the current value of counters into the web content in the same way as into the web content displayed directly in the live windows. Read about creating complex event sources and counters to get more information on this.

4.7.4. Detail display

Quick access to a selected camera from the video wall is considered an interesting and significant function. By double clicking on an active monitor with a switched camera, you can promptly display a standard local live view in a detail live view focused on a selected camera. This function can be used with all types of monitors, including Quad monitors.

NOTE

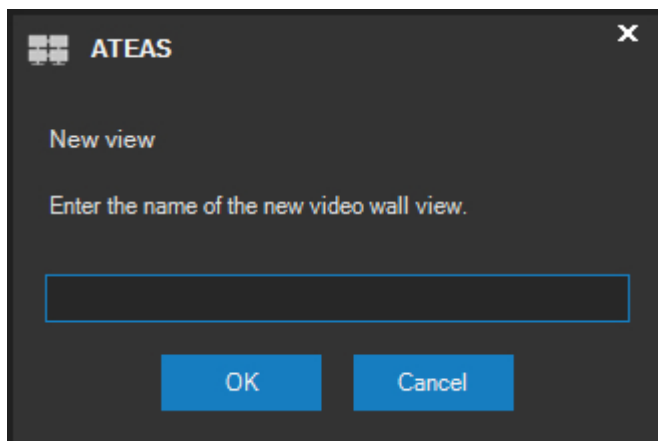
You will use this function as soon as you need to work with additional camera functions. This, for example, concerns camera control, switching to a preset point, audio reception, output activation, preview, downloading records etc.

4.7.5. Video wall views

Switching cameras to a video wall is completely identical to switching to local live windows. Saving local views and video wall views also works on a similar principle. Video wall views are controlled by a group of buttons that are between the video wall preview and the list of video wall views.



The current state of the video wall (meaning the camera layout on the monitors) can be saved as a video wall view by pressing the middle button. Only the name needs to be entered before saving.



Saved video wall views are displayed in the list found in the right part of the window. Any video wall view can be reactivated by selecting the desired view and clicking the top left arrow button. This way, you can achieve a layout with any number of cameras on the video wall with the click of a button.

NOTE

Video wall views are local for each user and cannot be shared.

Any locally saved video wall views can be deleted by clicking the cross button found in the video wall views control panel.

Despite obvious analogy between local and video wall views, there is one significant difference. Switching between video wall views is not invasive and results in the following behavior. If a local view contains empty positions, they will be created during the process of switching to the local view (i.e. cameras at their respective positions will be turned off). However, original cameras remain on unoccupied monitors when switching between video wall views, meaning that you can create views that will, for example, only change the top or bottom part of the video wall, or specifically selected monitors.

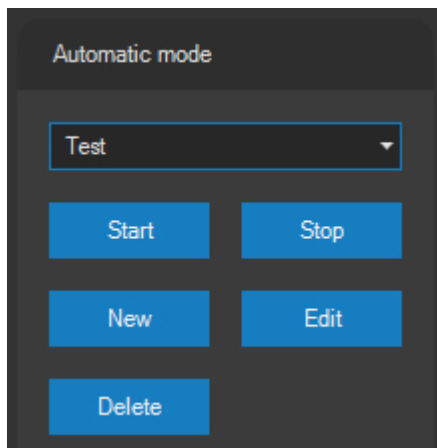
4.7.6. Automatic mode

Video wall views can be used to create automatic modes (automatic changes to video wall views).

NOTE

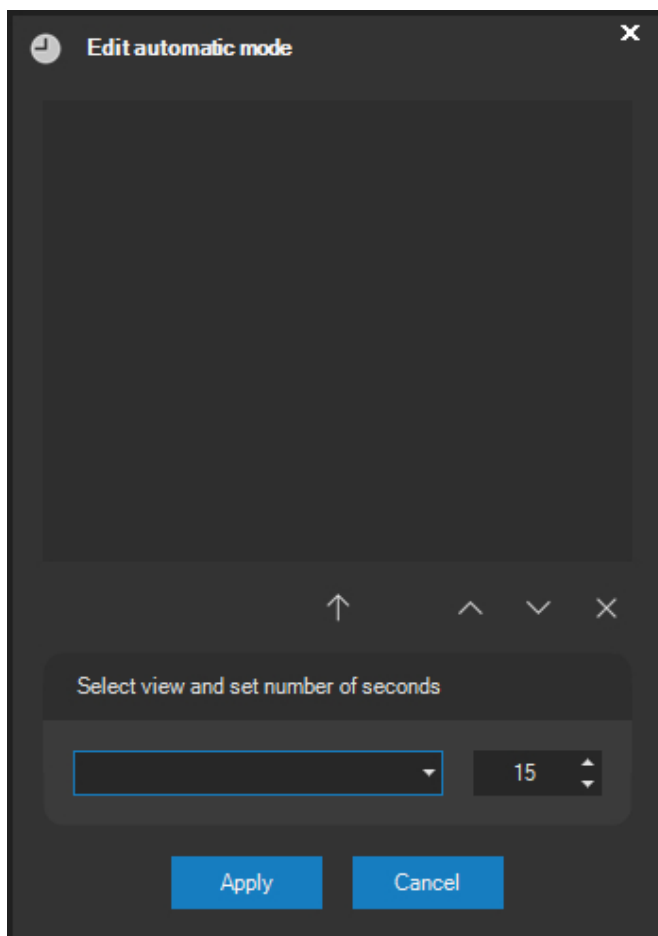
Just as video wall views are identical to user local views, the automatic mode of the video wall is similar to local automatic modes in the live window with the only difference being the video wall automatic mode is composed of individual views while the automatic mode in the live window is created from an optional position within the live window, directly from individual cameras on one or more servers.

Use the group of controls in the bottom right corner of the window to create, manage and run automatic modes.



The list of all automatic modes created is available as a drop-down list. As is the case for video wall views, video wall automatic modes are saved on a particular workstation and cannot be shared.

A new automatic mode can be created by pressing the **NEW** button. After entering a name for the new automatic mode, a dialog will be displayed where the user can edit the automatic mode. It is the same dialog displayed for a selected automatic mode upon pressing the **EDIT** button.



You must select a video wall view and a time delay in seconds. A view is added to the end of the automatic mode, into Video wall views list, by pressing the green arrow button. A time delay (during which a view is displayed on the video wall) can be set within the range of 5 seconds to 10 hours. After this delay, the following view in the list will be activated (or the first view in case the last list item has been reached). The selected view can either be moved in sequence or deleted using the buttons to the right of the view list. A single view can be part of the automatic mode more than once. The total amount of views is virtually unlimited.

NOTE

Non-invasive video wall views switching can enable creating automatic modes that will change only a specific part of the video wall.

The selected automatic mode can be deleted by pressing the **DELETE** button.

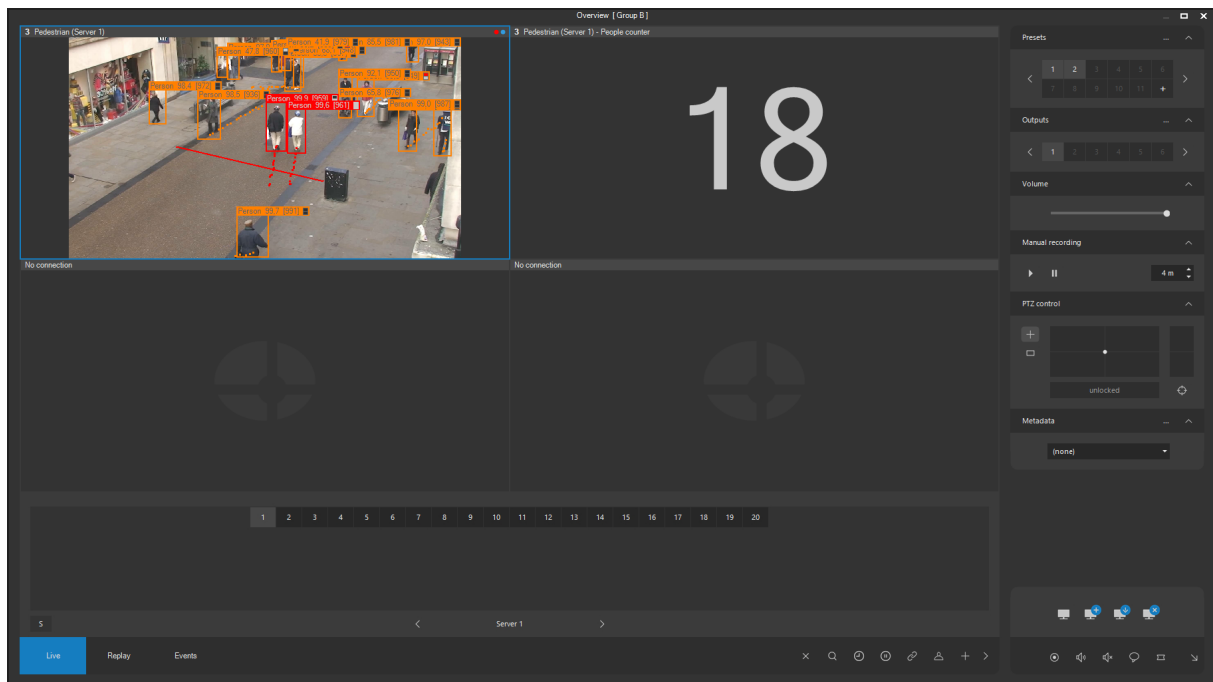
Any automatic mode can be run or stopped by pressing the **START** and **STOP** buttons. The selected automatic mode can be activated by pressing the **START** button (the currently activated automatic mode concludes). If the selected automatic mode is already active, it will be restarted. This method of restarting the automatic mode is used when an active mode has been configured and you need the changes to be applied. If another authorized user starts a different automatic mode, the current mode is replaced with the new mode.

NOTE

Once started, the automatic mode is stored on the server and will be active until deactivated by an authorized user. The automatic mode continues to run even if the video wall window is closed or the user logs out.

4.8. Working with counters

Using counters, it is possible to display the number of occurrences of any particular event or a combination of events. For example, combining the events of a person crossing a line for all entrances and exits makes the counter display the current occupancy of a building or area. If a line happens to be an entrance and exit at the same time, two event sources can be created according to the crossing direction.



NOTE

For a statistical view of any event source occurrences the metadata chart reporting tool is the right tool to choose. A counter, however, displays the current value for the event source combination.

4.8.1. Zone counters

Zone counters are created automatically in the system and correspond to existing video analytical event sources that are bound to closed zones. A value of a zone counter thus represents the total amount of objects of all types selected for this event source.

4.8.2. Complex counters

For any given camera, a counter can be created as a complex event. By its nature, a complex counter is an equivalent entity to a complex event source. Though we are not interested in the logical result of the entire event, we make use of connecting the sources from different cameras or servers.

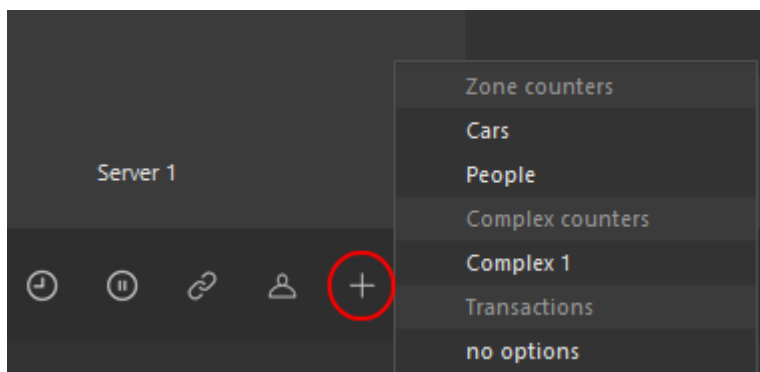
When creating a counter (complex event), all event sources without the logical negation will increase the value of the counter. The logical negation decreases the value of the counter as shown in the following image.

3 Pedestrian (1 Server 1) Entrance 1	NEG	×	A	1
3 Pedestrian (1 Server 1) Entrance 2	NEG	×	A	1
3 Pedestrian (1 Server 1) Leaving area line 1	NEG	×	A	1
3 Pedestrian (1 Server 1) Leaving area line 2	NEG	×	A	1
3 Pedestrian (1 Server 1) Cross	NEG	×		

A counter can, of course, embrace events from multiple cameras of even servers including external events.

4.8.3. Displaying the value of counters

Displaying the value of a counter for any selected camera can be done using the additional data camera menu, where all zone and complex counters appear automatically.



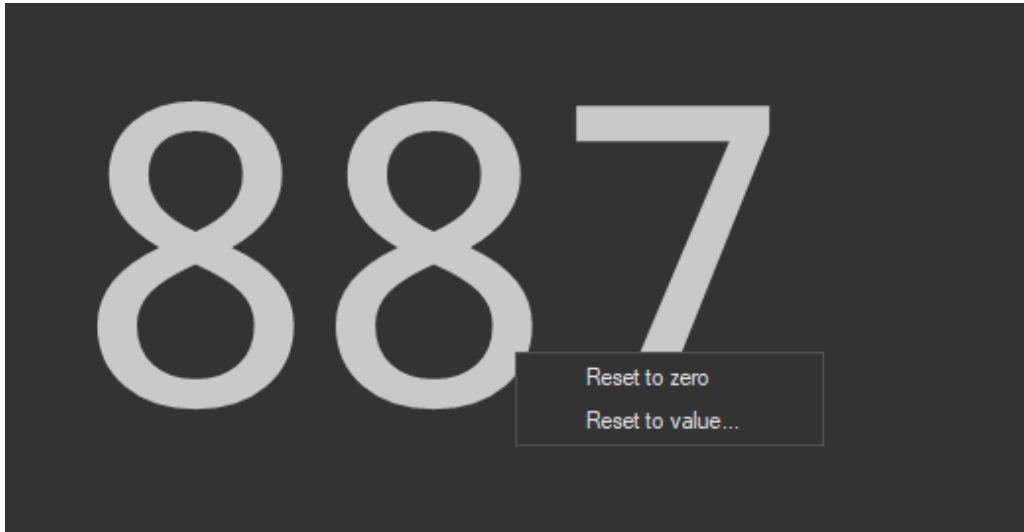
The list of the counters is always populated for the selected camera, the contents of the selected position is then replaced by the value of the counter. In live mode, counters display their real-time values. In replay mode, counters display values that were valid at the replay time given by the time axis.

4.8.4. Manual reset of the counter

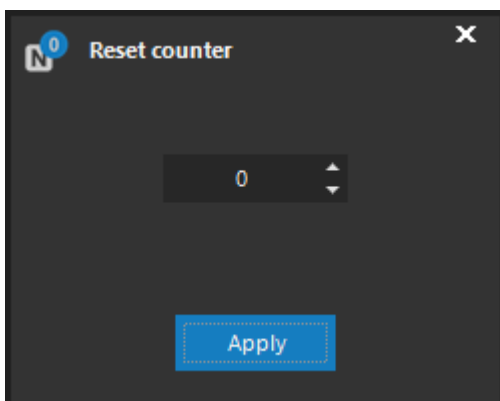
Authorized users can reset the counter to zero or another integer value at any time. The permission in charge here is named Additional event features. The reset is performed using the context menu of the counter.

NOTE

Only a complex counter can be reset, not an automatic zone counter.



When selecting the second option, a dialog window is displayed to select a value as follows.

**TIP**

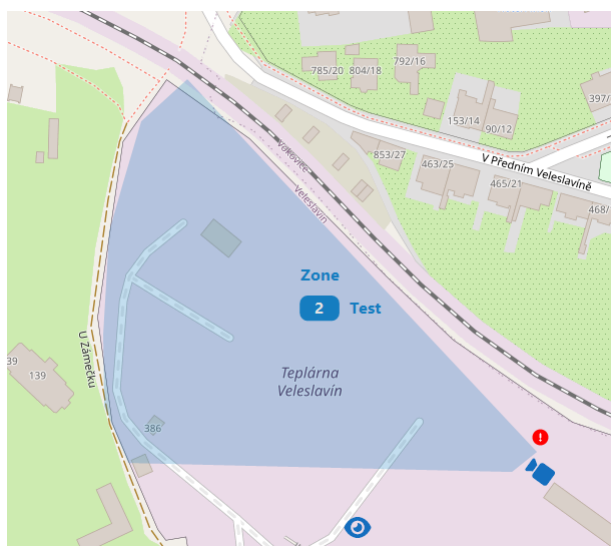
You can reset a counter inserted in a web page in the exact same way provided the counter is web page is opened directly in an ATEAS client.

4.8.5. Event based reset of the counter

Resetting a counter to zero or another integer value is also possible within any system event if the reset action is configured to be part of the event scenario. Therefore, it is easy to reset the value on a regular basis (with a scheduled event) or based on any other event including external events. Head to the event management description for more.

4.8.6. Zone counters in the map

Once a zone is localized, automatic zone counters bound to this zone are automatically displayed in the map.



4.8.7. Counter values in web content

The current counter values may be injected into any active web content. In this case, multiple counters can be displayed within one web page or view position. A counter can be injected with any html tag using the corresponding ID parameter. Read about creating complex event sources and counters for more information. Values of the counters displayed in a web page are always real-time including the situation, when the window is switched to replay mode.

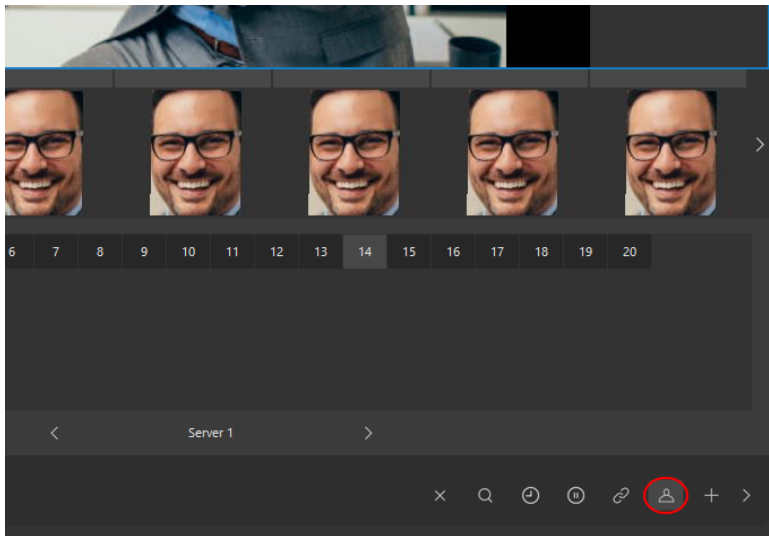
NOTE

You can display historical counter values by putting a counter directly in a view.

4.9. Working with the face database

4.9.1. Face preview

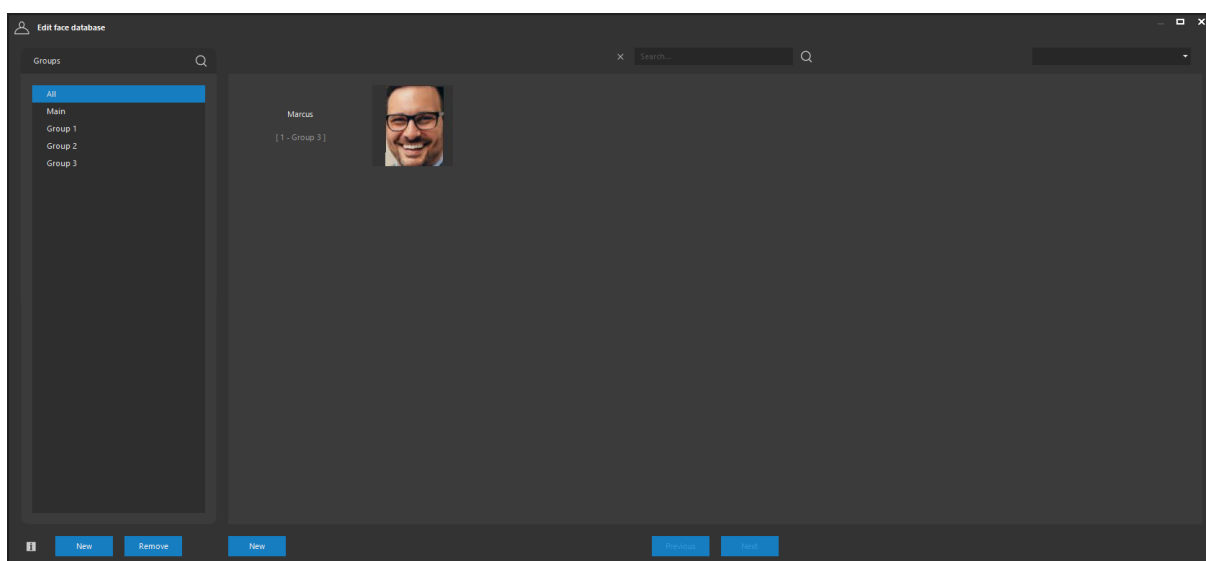
If video from the selected camera is being analyzed by the Face recognition network type, you can activate a live or recorded face preview in the canonical (base) form. The face button is used to achieve that.



If the face is assigned a specific person, the person and group names will appear above the preview. To be able to display the face preview, the metadata display permission must be granted.

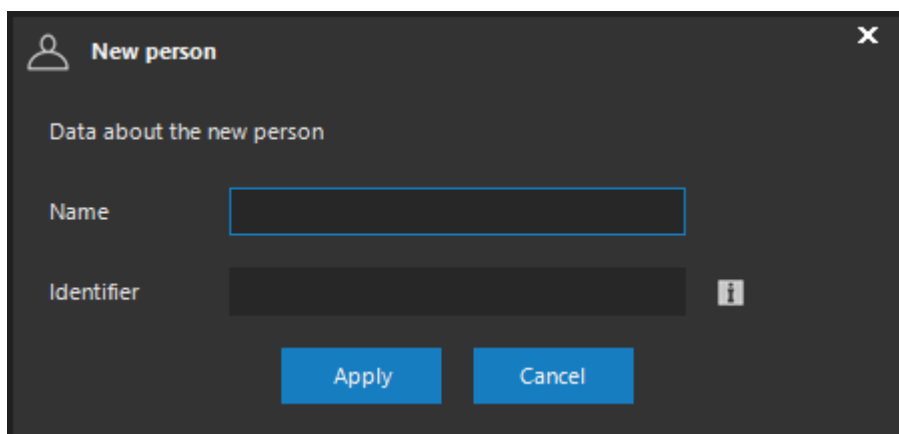
4.9.2. Face database

Users who have been granted the edit face database permission, can right-click the face preview area to display a context menu. From there, the selected face can be copied or the face database can be entered. The database can also be opened quickly from the Tools in the main menu.



All detected faces are checked against the face database in real time and based on the similarity parameter of the neural network they might be assigned person and group names. All persons must belong to a group, which can be created or removed using the **NEW** and **REMOVE** buttons in the left part of the window. A new person record can be created by using the **NEW** button. You can use the search text fields in the upper part of the window to search through both groups and persons. Use the **PREVIOUS** and **NEXT** buttons to move between pages.

When adding a new person, an optional identifier can be entered in addition to the full name, which can be used for integration purposes and becomes part of the ATEAS API event notifications.



Any person can be deleted by clicking on the cross symbol that is displayed while hovering with the mouse over a person's name. You can rename a group or person by double-clicking its name. People can be moved to different groups easily by a drag and drop operation.

4.9.3. Adding images

Any person can be assigned up to 10 canonical face images. The order does not matter. This can be done in several ways:

- by copying a face in a live window and inserting it on the selected database position using the context menu invoked by a right-click with the mouse,
- easily by dragging the face image from the live window to the database,
- by directly inserting a jpeg image.

When inserting face images directly, a conversion into the canonical form must be performed which requires a camera server running a Face recognition network type to be selected. If possible, the camera server will be selected automatically.

NOTE

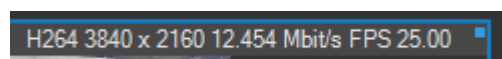
If no or more than one face are found in the image with the reliability specified, this image can't be used.

The images can be moved simply by dragging to a new position. Use the cross symbol to delete a particular image from the database.

Thanks to advanced technologies it is possible to check faces in real time against a database containing millions of face images using common hardware. This requires, however, an increased RAM consumption on the ATEAS administration server, approximately 1GB RAM per 100 thousand persons.

4.10. Video information

We often require accurate information about the video format or resolution of the camera video streams received by the client. This information can be obtained using the basic diagnostics information feature and can be activated for any given view. The feature can be activated for the entire view by pressing the SHIFT – S (statistics) key combination. This basic information will be regularly updated in the right corners of each camera window.



This information contains the video format, resolution, actual bandwidth and frame rate. Having this data available facilitates the quick assessment of camera settings, the ability of cameras to produce the declared frame rate or network load.

NOTE

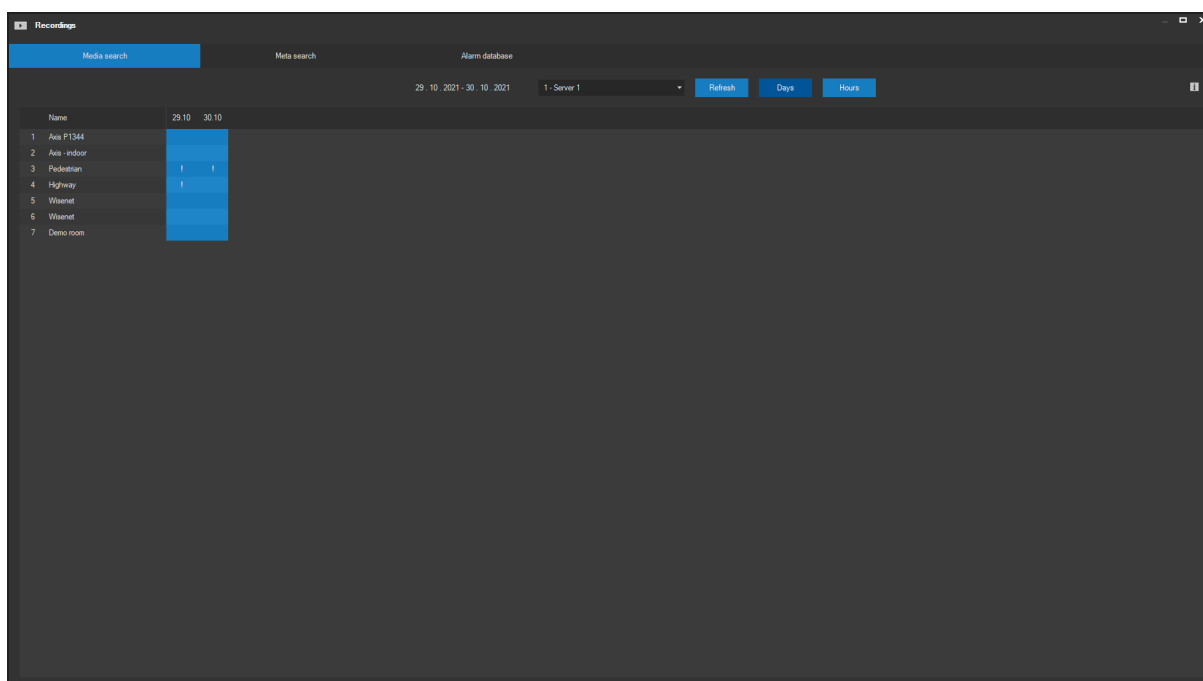
The data is obtained from the video, which is transmitted between the camera server and client. Results are therefore also affected by the video settings on the server output side (e.g. primary and secondary frame rate).

Chapter 5 - Working with recordings

5.1. Searching for a record

5.1.1. Recordings summary

Besides replay directly in the live windows, all recordings can be accessed under Recordings in the main menu. Upon selecting a camera server, you can instantly retrieve information about time, all cameras in the view and as well as the time both insignificant and alarm events took place. This table will be displayed after selecting a server from the drop-down list, and can be updated by pressing the Refresh button, found next to the drop-down list. All these actions can be performed on the **Media search** tab.



The screenshot shows the 'Recordings' window in the ATEAS software. It features a 'Media search' tab, a date range selector (29.10.2021 - 30.10.2021), a server dropdown (1 - Server 1), and buttons for 'Refresh', 'Days', and 'Hours'. Below these controls is a table with columns for 'Name', '29.10', and '30.10'. The table lists seven cameras: 1. Ais P1344, 2. Ais - indoor, 3. Pedestrian, 4. Highway, 5. Wiseret, 6. Wiseret, and 7. Demo room. The '29.10' and '30.10' columns show colored backgrounds (blue and orange) indicating recorded data, with some cells containing exclamation marks (!) to denote alarm events.

Name	29.10	30.10
1 Ais P1344		
2 Ais - indoor		
3 Pedestrian	!	!
4 Highway	!	
5 Wiseret		
6 Wiseret		
7 Demo room		

Table columns are created according to individual days (or hours) in the recording database. Table rows are made up of cameras from a selected camera server. These cameras have an assigned name and a number. If a table cell corresponding to a specific camera and day (or hour) is empty, there is no recorded data available for this camera for the given interval. If the cell has a colored background, the camera record is available for the entire day or part of the day (or hour). Also, if there is an exclamation mark symbol in the colored background, events or alarm situations are available for this interval.

	Name	29.10	30.10
1	Axis P1344		
2	Axis - indoor		
3	Pedestrian	!	!
4	Highway	!	
5	Wisenet		
6	Wisenet		
7	Demo room		

The table is displayed in day mode by default (the table columns are created according to days). Use the two respective buttons to switch between Day and Hour modes. The current extent of days (Days mode) or the current day (Hours mode) is displayed next to these buttons.

29.10.2021 - 29.10.2021	1 - Server 1	Refresh	Days	Hours
-------------------------	--------------	---------	------	-------

The **HOURS** button can be only if a specific day is selected from the table (any cell in a certain day column is selected). Otherwise, switching to Hours mode is not possible. You can also switch to Hours mode by double clicking on a random table cell with a colored background, indicating that a record is available. After doing so, the table will be reorganized to show columns, each representing one hour of the selected day. The significance of rows and table data remains the same.

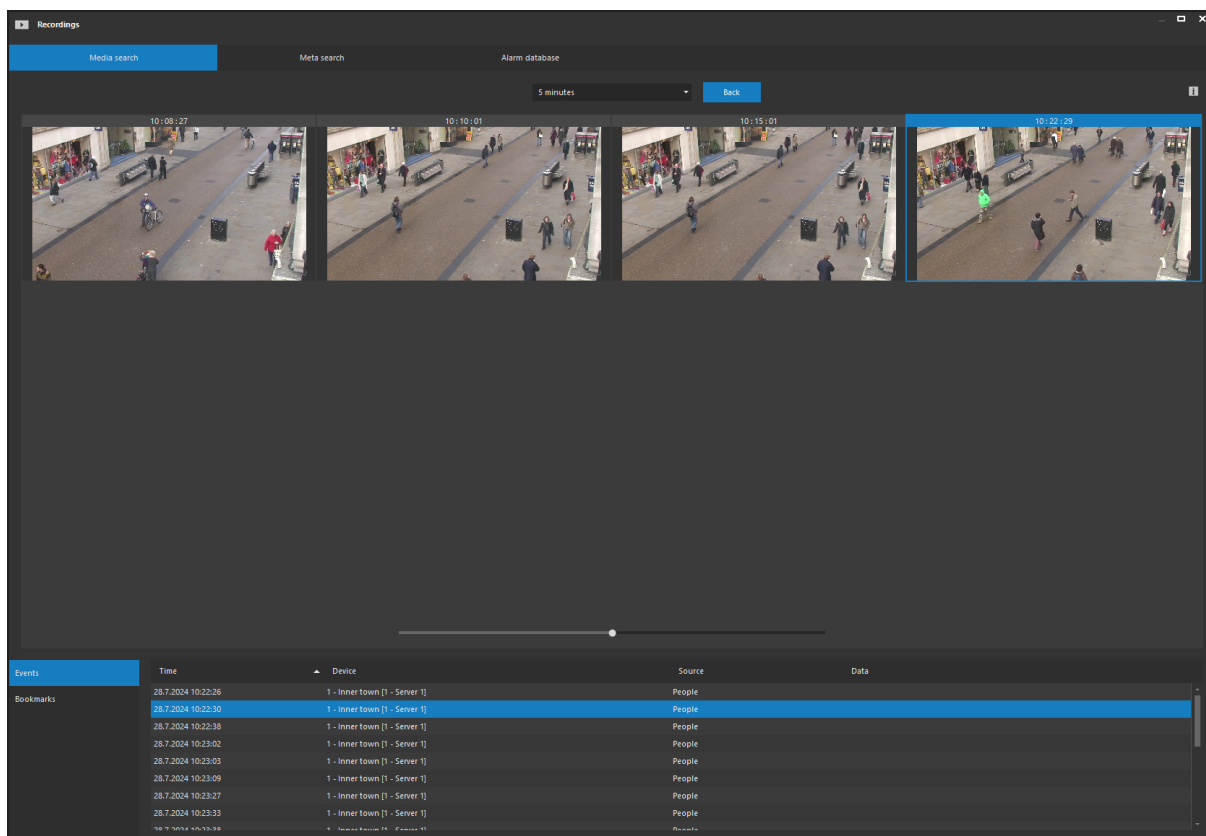
NOTE

While the amount of columns corresponds to the number of days included in the recording database for the daily summary, the hour summary always has 24 columns (separated into hours).

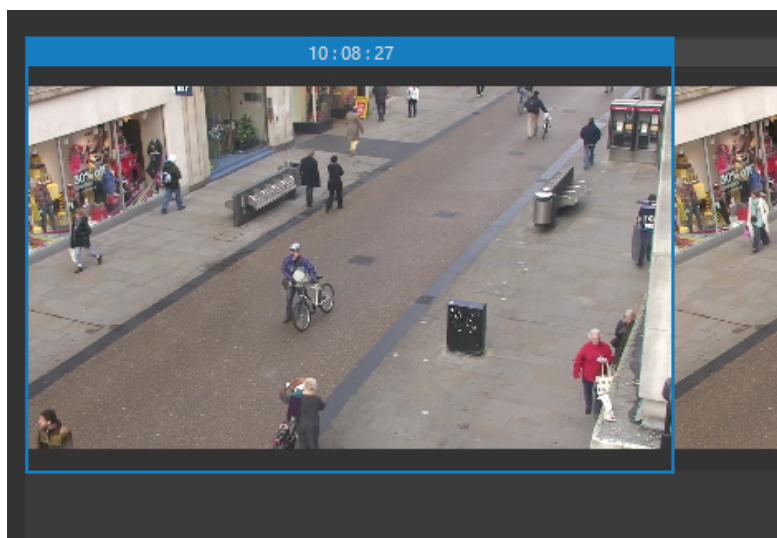
If a cell in Day mode has a colored background (or has an exclamation mark), at least one cell (hour) with a colored background (or with the exclamation mark symbol) must be available for the given camera after switching to Hour mode.

5.1.2. Displaying video overviews

For fast orientation in recorded data, you can display the record of a selected hour in terms of a preview display. Double-clicking on a cell with a colored background in Hour mode leads displays the video overview for the selected hour. Therefore, you can quickly identify the time frame the user is interested in.



You can return to the hour summary by pressing the **BACK** button and display another hour or the same hour for a different camera. The video overview is displayed with a 5 minute resolution by default, meaning that up to 12 preview recordings per hour can be displayed. This resolution can be changed and the client adapts the layout for an optimized preview of video. The header of each recording preview of the overview contains the exact time.



Individual recording previews can be selected using the left mouse button. A blue border will be displayed around the selected interval. Selected intervals can either be displayed in the form of a preview or downloaded (exported from the recording area of the camera server to a local hard drive).

NOTE

To ensure a better preview, operations such as digital zooming or movement are enabled for the selected interval. These operations are performed by using a mouse (scroll wheel and clicking into the view).

If a selected hour includes event or alarm situations (an exclamation mark has been assigned to the cell), a list of these events will automatically be added below the video summary.

Events	Time	Device	Source	Data
Bookmarks	29.10.2021 17:36:36	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	LBT 77-77 (C2) (C2)
	29.10.2021 17:36:44	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	PY 58-57 (C2) (C2)
	29.10.2021 17:36:48	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	9U0 0486 (C2) (C2)
	29.10.2021 17:36:52	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	PY 58-57 (C2) (C2)
	29.10.2021 17:37:01	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	SAU 8878 (C2) (C2)
	29.10.2021 17:37:35	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	SAU 8881 (C2) (C2)
	29.10.2021 17:37:50	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	AKM 44-56 (C2) (C2)
	29.10.2021 17:38:01	server 1 (Server 1) camera 4 (Highway)	LP - unregistered	AKV 86-40 (C2) (C2)

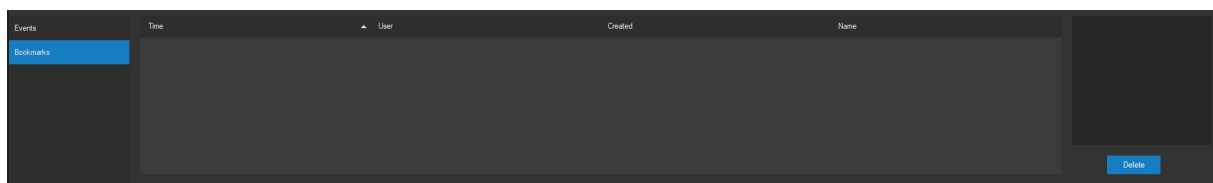
This summary includes the exact date and time of an event, the device that invoked the event, the source of the event for the given device (motion detection, alarm input etc.) and additional information or specifications pertaining to the event source (e.g. License plate).

CAUTION

Events displayed under the video summary are events which make the camera react to them with an event recording (can also start recording or increase the frame rate according to setup). Therefore, the device which invoked the event does not necessarily have to be consistent with the camera recording currently being viewed.

By clicking on any event in the list, the respective interval will automatically be selected from the view (a blue border will appear). The time will also be synchronized to the beginning of the event via the quick view control (see below).

If the selected hour contains bookmarks (the cell has a triangle symbol indicating a comment), a list of bookmarks will automatically be added under the video overview.



This overview contains the precise date and time of the bookmark, name of the user who created the bookmark, time created and name of bookmark.

By clicking on any bookmark in the list, the respective interval will automatically be selected from the view (a blue border will appear). The time will also be synchronized to the beginning of the bookmark via the quick view control (see below). The full text of the bookmark will also be displayed in the text field next to the list.

NOTE

The list of events and alarms is shown first by default. You can switch between the list of events and alarms and the list of bookmarks using a dropdown list.

A bookmark can be deleted by pressing the **DELETE** button next to the list of bookmarks. A user must have the respective permission to be able to insert bookmarks into the recordings and delete them.

NOTE

Even if the user is authorized to insert and delete bookmarks, he can only delete a bookmark created by himself, unless he is a system administrator. In this case, he can delete the bookmarks of all users.

5.1.3. Previewing and saving recordings

Intervals can be downloaded to a local computer. This is the only option available for protecting record media sequences from being rewritten on a record server. Basic strategy when recording is the cyclic rewriting of record media sequences. Although alarm situations (for example) are located in special areas, which are not rewritten immediately after reaching capacity, downloading the sequence is the only way to achieve a permanent record.



This scrollbar can be used for a quick interval preview. Its left and right ends represent the beginning and the end of the selected interval. The video is synchronized by moving the scrollbar. A media sequence can therefore be replayed at any speed while previewing an interval.

NOTE

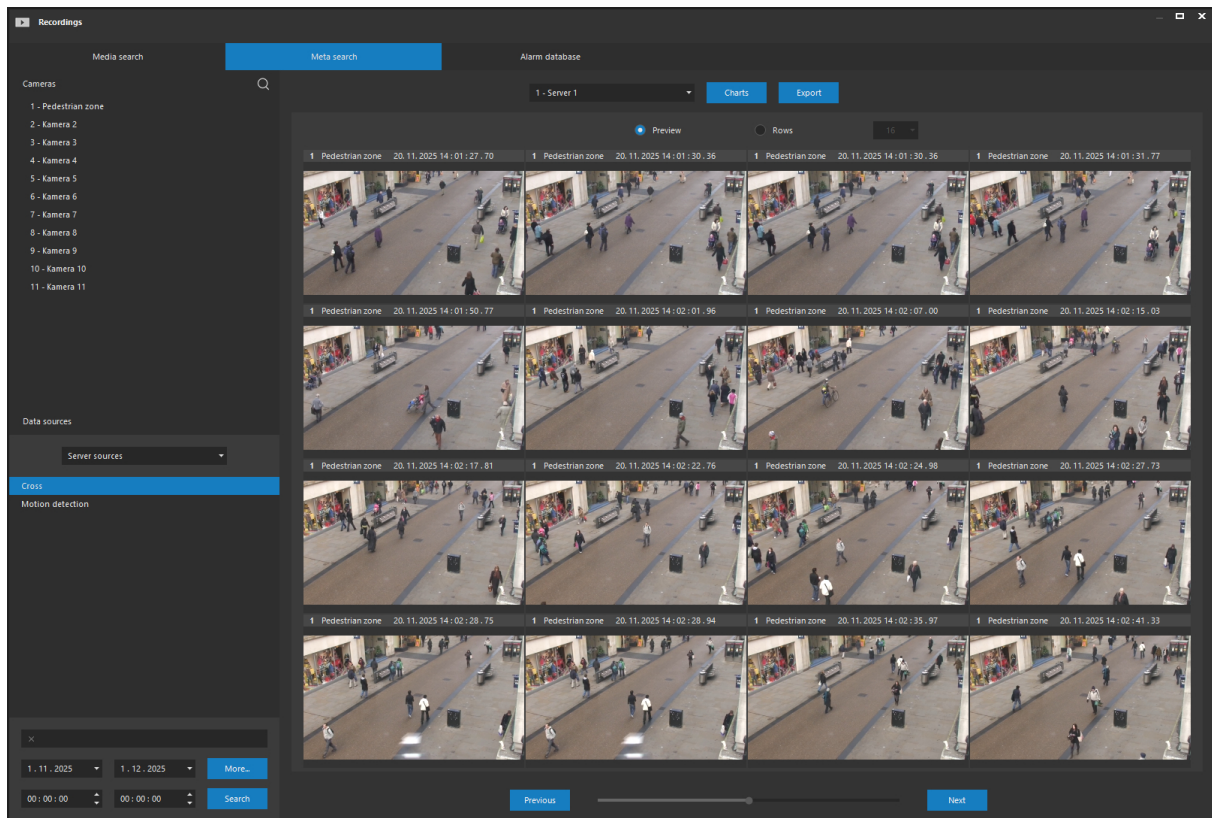
A live window can be automatically opened and configured to replay the selected time by double-clicking the header of the window containing the video camera preview or an item in the list.

The interval preview can be double-clicked to start downloading it.

Downloading data from the media stores of individual camera servers is performed using an intelligent download manager, described in a separate chapter. The download manager registers sequence download requests as its tasks and executes these one by one or in parallel. Double-click to assign a new task to the download manager.

5.2. Meta search

The meta search can be used to search for an event source or any additional data.



NOTE

Besides camera data sources, meta search can also be used to search external event sources by selecting the External objects item.

5.2.1. Defining conditions

First, you need to select a camera server, whose cameras will then be displayed in the camera list. The list also includes the External objects item for searching among external event sources from objects and their elements.

NOTE

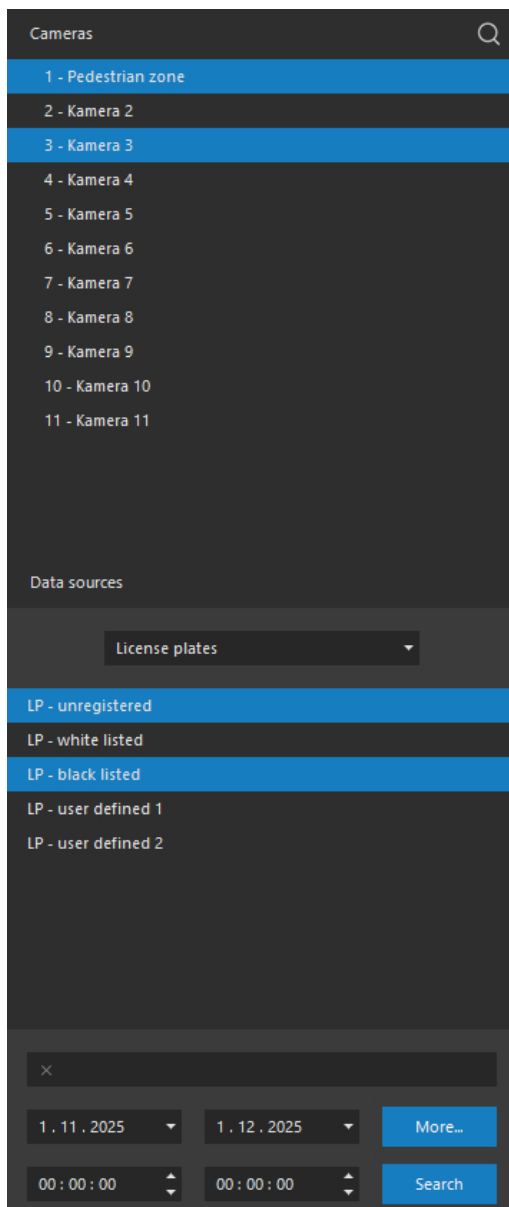
If metadata centralization is enabled on your system, you will also be able to select the All servers item.

In the camera list, you can select any number of cameras. If you search in centralized metadata, you can select camera servers. Multiple selections are possible, for example, using the CTRL key.

TIP

If no camera is selected, all cameras will be automatically included in the search.

In the Data sources section, you must select at least one source to include in the search. Again, you can select multiple sources. If you want to select sources across multiple groups, select Show all from the drop-down list.



The screenshot displays a search interface with two main sections: 'Cameras' and 'Data sources'.

Cameras section: Features a search bar with a magnifying glass icon. Below it is a list of 11 items, each with a selection checkbox and a label: '1 - Pedestrian zone', '2 - Kamera 2', '3 - Kamera 3', '4 - Kamera 4', '5 - Kamera 5', '6 - Kamera 6', '7 - Kamera 7', '8 - Kamera 8', '9 - Kamera 9', '10 - Kamera 10', and '11 - Kamera 11'. Items 1, 2, and 3 are currently selected, indicated by blue highlights.

Data sources section: Includes a dropdown menu currently set to 'License plates'. Below this is a list of six data source options, each with a selection checkbox: 'LP - unregistered', 'LP - white listed', 'LP - black listed', 'LP - user defined 1', and 'LP - user defined 2'. Items 'LP - unregistered', 'LP - white listed', and 'LP - black listed' are selected, shown with blue highlights.

Search filters: At the bottom, there is a search bar with a clear 'X' button. Below the search bar are two date range selectors: '1 . 11 . 2025' and '1 . 12 . 2025', each with a dropdown arrow. To the right of these is a 'More...' button. Below the date selectors are two time range selectors: '00 : 00 : 00' and '00 : 00 : 00', each with up and down arrows. To the right of these is a 'Search' button.

NOTE

Dynamic sources offer all sources provided by the cameras including cameras connected via ONVIF interface.

NOTE

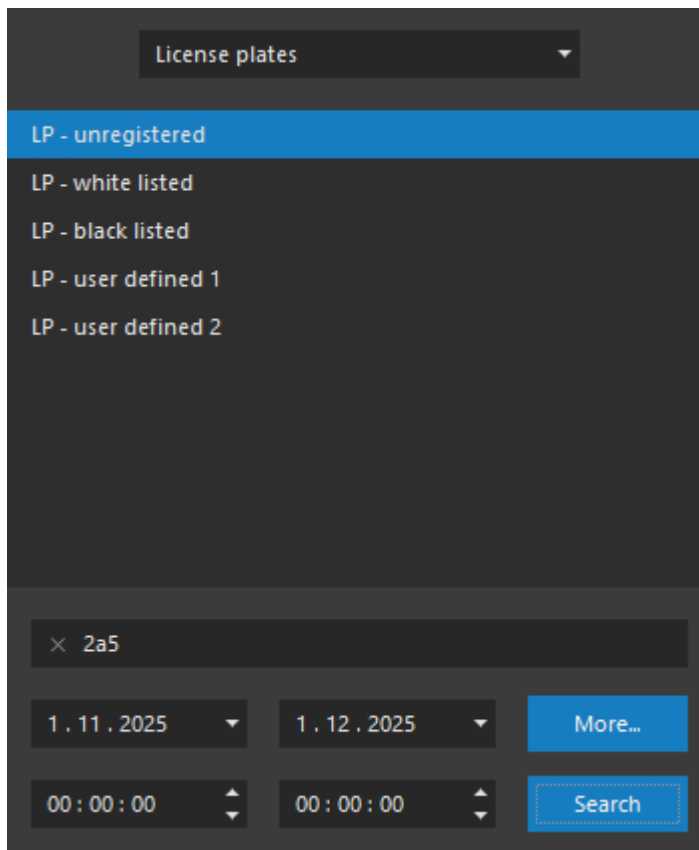
When selecting multiple cameras, the event sources incl. server, dynamic or complex sources are automatically consolidated according to their names.

External objects

When searching through external objects, we can see elements of the selected object, which are not further divided into subgroups. The search can be made for a specific object and for one or more of its elements, or also simultaneously for multiple objects. When selecting multiple objects, all elements of the selected objects are always included into the search.

Additional data

For most sources, it is possible to enter additional search data in the corresponding text box below the source list.

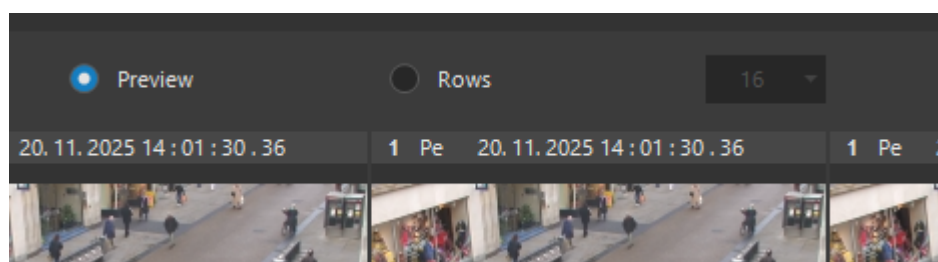


Entering a word or multiple words will produce results that contain all the groups of characters you've entered, regardless of their order. You can use the **MORE** button to perform more advanced searches, as described below in a separate subchapter.

The current month is automatically set as the default search interval. Using the user-friendly date and time pickers, it is possible to select a different start and end date for the search, up to a total interval of one year.

5.2.2. Displaying results

After entering all search criteria, press the **SEARCH** button. The default search result layout offers a video preview precisely synchronized to a specific point in time.



The results can be switched to a row view, for which you can choose the number of rows displayed on one page. In both result layouts, you can use the **PREVIOUS** and **NEXT** buttons to move between pages. In the video preview layout, you can additionally use the slider below the results to preview video around the time of the search result for a total interval of one minute.

Double-click on a video or row to open the associated event view, if it exists.

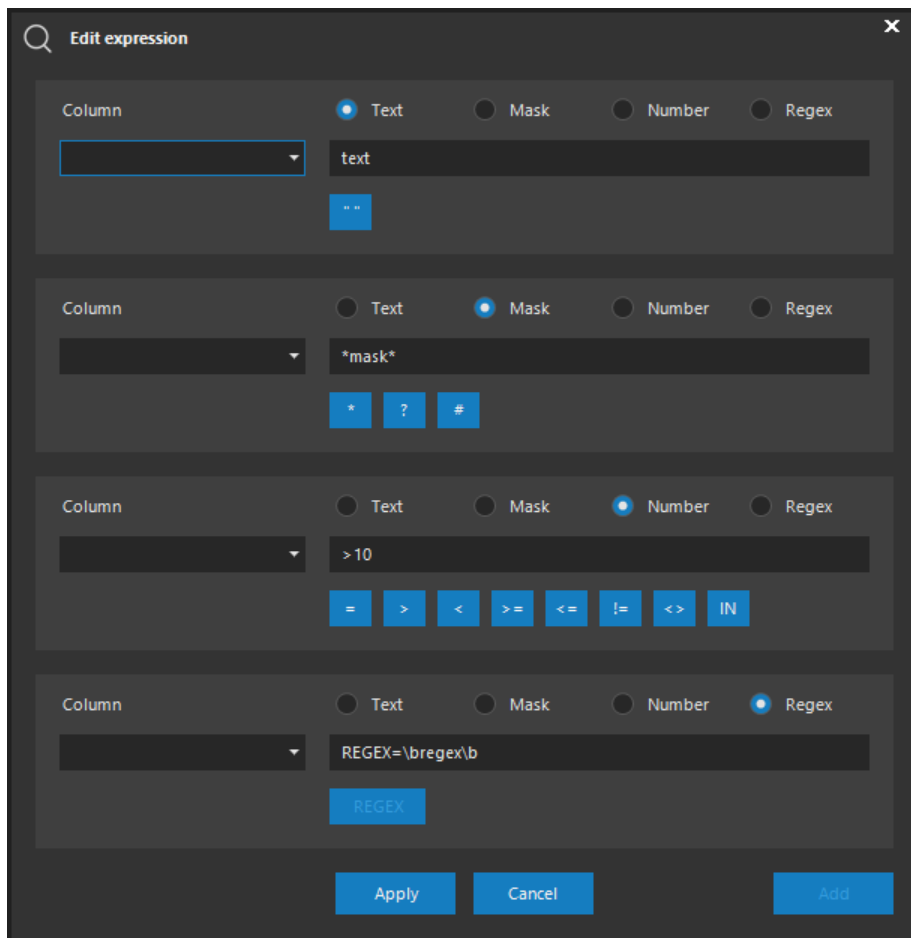
TIP

The event view can also contain other cameras that we want to display automatically.

If you intend to display just the camera displayed in the search result, you can double-click the result header instead of double-clicking the video area.

5.2.3. Advanced text search

A basic text search works in such a way that all groups of characters must be found in the result, regardless of their order. However, using the **MORE** button, these options can be expanded significantly.



The 'Edit expression' dialog box is shown with four sections, each representing a different search method. Each section has a 'Column' dropdown, a search field, and a set of auxiliary buttons.

- Text:** The 'Text' radio button is selected. The search field contains 'text'. There is a single auxiliary button with two dots '.. '.
- Mask:** The 'Mask' radio button is selected. The search field contains '*mask*'. There are three auxiliary buttons: '*', '?', and '#'.
- Number:** The 'Number' radio button is selected. The search field contains '>10'. There are seven auxiliary buttons: '=', '>', '<', '>=', '<=', '!=', '<>', and 'IN'.
- Regex:** The 'Regex' radio button is selected. The search field contains 'REGEX=\bregex\b'. There is one auxiliary button labeled 'REGEX'.

At the bottom of the dialog are three buttons: 'Apply', 'Cancel', and 'Add'.

In this dialog, you can select the following search methods; for each of them, auxiliary buttons are displayed to quickly insert the given function into the search field.

NOTE

All of these methods can also be used by manually entering the search term into the text field. The dialog is only a helper in creating the search term.

Text: Text search allows you to search for all groups of characters separated by spaces, regardless of their order. If we search for a group of characters that contains a space, we can use quotation marks.

Mask: The default text search essentially offers a mask behavior, as groups of characters are found if they are at the beginning, in the middle or at the end of a word. However, in mask mode, we can customize this behavior by using the wildcard characters * (represents any number of characters including none), ? (represents exactly one character) and # (represents exactly one digit).

Number: This mode allows for numerical comparison of values using all the operators displayed below the text field. This involves equality or inequality tests or a test whether a number belongs to an interval.

NOTE

Numeric comparison supports decimal numbers with both dot and comma symbols.

TIP

The system can also process numerical values followed by text. This is especially useful when defining conditions for numerical data coming with a unit, e.g. 50 km/h, etc.

Regex: This method supports very fast regular expression searches with all the possibilities regular expressions offer.

If the data is not organized in columns, the search term is always applied to the entire data record. However, if the data contains multiple items (e.g. vehicle LP, vehicle type, speed), it is possible to combine multiple columns and multiple conditions by prepending the column name to the condition followed by a colon. For example:

plate: 2A5 speed: > 50

When using this syntax, the results must always match all criteria. Dynamic event sources that provide additional data often include multiple data items (columns) that can be added and stored, allowing these advanced search methods to be applied later.

You can include multiple columns by repeatedly pressing the **ADD** button.

NOTE

Although the number of columns in the dialog is limited to four, more columns can be entered manually.

TIP

After performing a meta search, the system analyzes the results and offers all detected columns in the dialog automatically, which greatly simplifies searching.

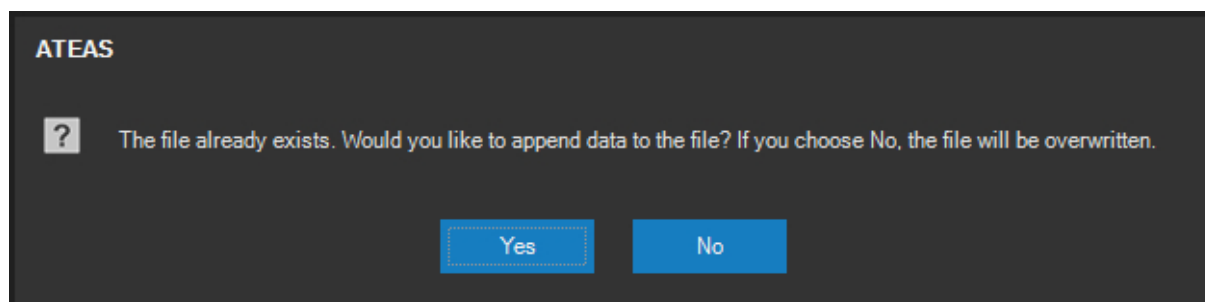
While editing the conditions in the text fields of the dialog, the expressions are being analyzed and the radio button for the currently active search method is activated automatically. After pressing the **APPLY** button, the expression is copied into the search field and the search is started. The cross symbol in the search text field can be used to reset it.

NOTE

Column notation uses the colon character. If you want to search for this character in your data, the escape sequence `\:` must be used to suppress the special meaning of the colon.

5.2.4. Export functions

Metadata can be exported into a text file using the **EXPORT** button. You can select any given new or existing file with a txt extension as the output file. If the selected file already exists, the application will show the following dialog:



In this case, you can either overwrite the file or add the list to the end of the existing file.

The output text format used is CSV (comma-separated values), which is a simple format for the export and potential import to random database formats, where each row contains one record and individual items are separated by a comma.

This way, data can be exported for entire days or months and for a random number of cameras at once.

5.2.5. Charts

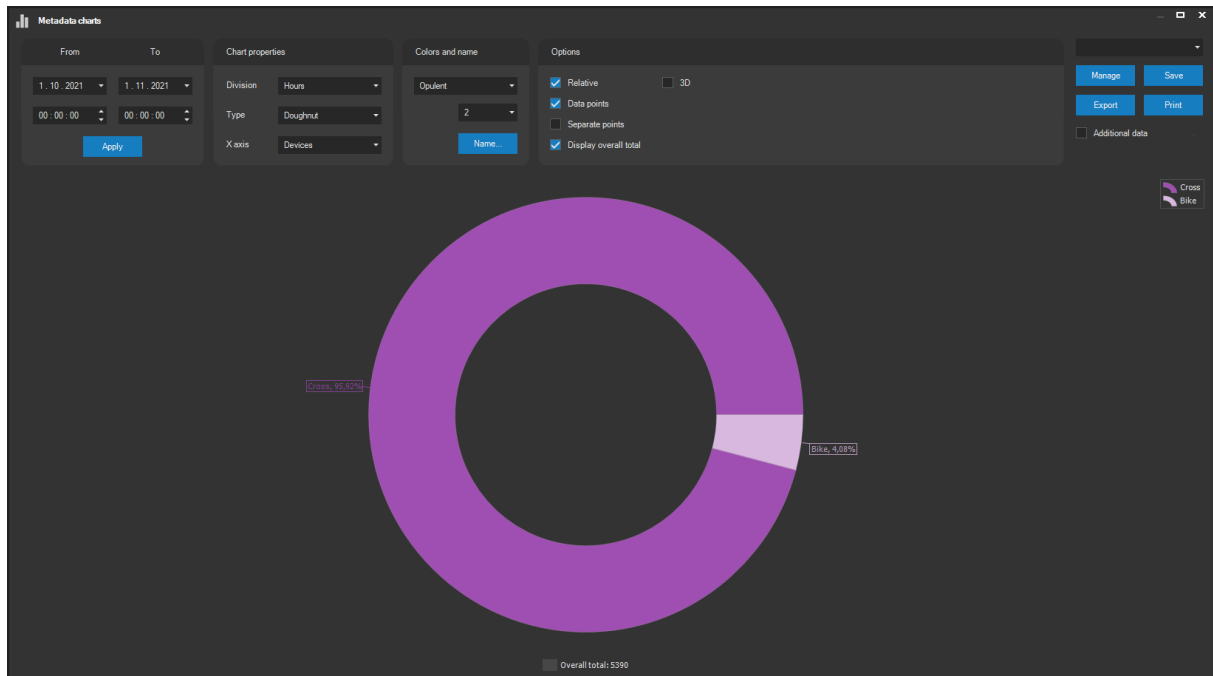
The current selection of metadata, based on selected filter, can also be expressed in the form of a chart. A chart is a statistical visual representation of the metadata selection and serves as the best available tool for data presentation within the system in the form of summary reports.

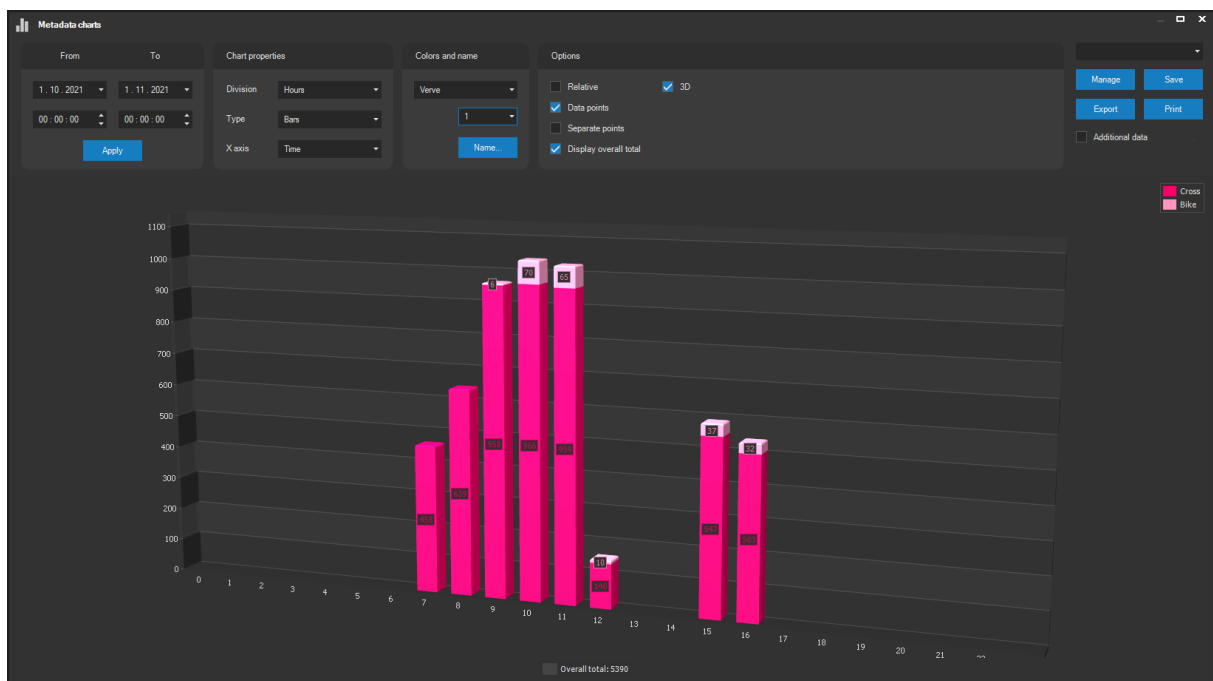
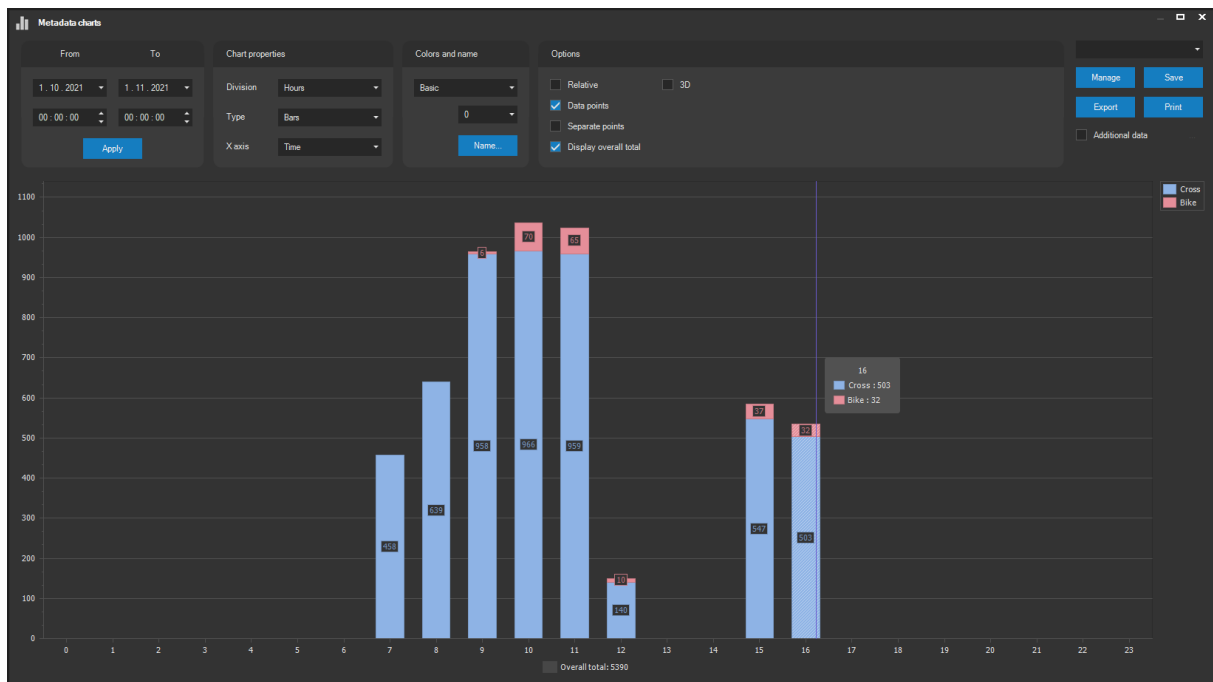
Charts can be opened by pressing the button with the chart symbol in the top right corner of the window.

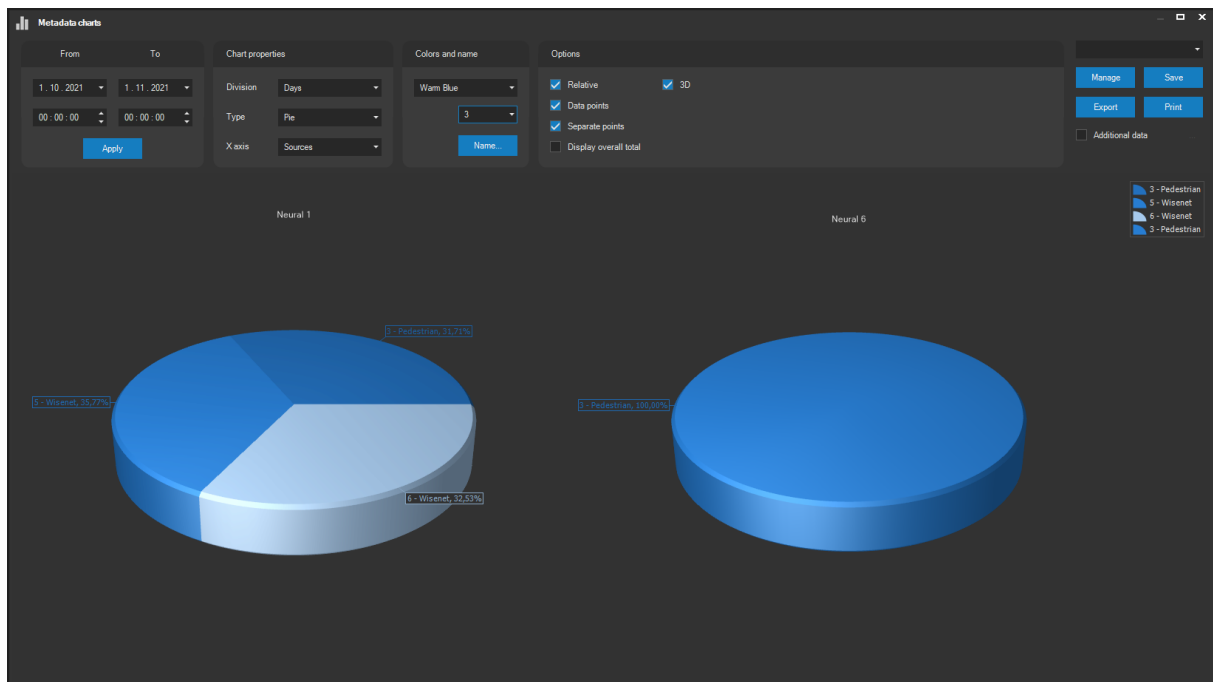
NOTE

Similar to export, at least a monthly time interval must be selected first.

You can use bar, pie and other chart types to analyze all types of metadata including vehicle LP frequency by the hour over the course of a month, camera outages, person or vehicle counting and statistics based on events captured by the neural network, as well as many others. The following is a sample of charts.







All items for selecting the type of chart and its settings are described below.

The From - To setting is used to select the days and exact times for which the chart will be generated. The maximum length of the time interval is 90 days, the date range can be adjusted independently of the originally selected interval in the metadata search.

Division specifies whether the graph will be created by the day or by the hour.

NOTE

Division only makes sense for bar charts.

If an interval longer than a day was selected prior to opening the chart window, a daily chart will automatically be used. Otherwise, an hourly chart will be used.

NOTE

The hourly chart is significant even for periods longer than one day. For example, it can display traffic statistics by the hour for a selected month.

Chart type allows the user to choose between bar or pie charts, including additional modifications of these basic types. Checking the Display overall total option displays the total sum of all data points at the bottom of the chart.

The X axis setting allows you to select how the data will be displayed. The default division for bar charts is always the time. You can then select (for individual time points of the bar chart or for individual pies), whether they are to be divided according to cameras and then according to metadata type or first according to metadata and then according to cameras. In both cases, a different view of metadata in the system is always achieved.

The Color scheme option allows the user to select from many predefined chart color schemes, as well as sub-schemes. Overall, you can create about 100 different color combinations to use for charts.

The Relative option has the following effect:

- It switches bar charts to relative view (evens out bar heights and displays percent values).
- It toggles displaying of data point values between absolute and relative for pie charts, which already express data in relative form.

The Data points option displays the numerical values of data points directly in the chart.

The Separate points option separates data points within one bar or pie into sub-points (according to the X axis settings). Independent sub-points will therefore be created for cameras or metadata.

NOTE

If a single camera is selected, separating data points actually separates the individual event sources, which would not be possible under multiple camera selection.

The 3D option enables the three-dimensional look of charts without changing the color scheme.

Chart name

The **NAME** button can be used to create a custom name for the chart. This name will be displayed above the chart. Basic HTML formatting such as bold or underlined font (, <u>) or color changes (<color=red>) are supported for the chart name entry.

Chart control

The mouse wheel can be used to zoom in or out on any 3D chart or 2D bar chart.

A 2D chart that is zoomed in on can be moved by using the sliders or by dragging with the mouse.

A 3D chart that is zoomed in on can be moved by dragging the mouse while holding down the mouse wheel. Regular dragging with the mouse is used to rotate the 3D chart.

Chart subdivision according to data items

The metadata sources of selected cameras are usually used to build up a chart. Provided the type of metadata is appended with additional data items, this data may be used for an additional finer subdivision of the chart. E.g. it is possible to create a chart of vehicle LP according to the countries or (provided the data source contains this type of data) according to the vehicle brand or model. In general, it is possible to separate any categorizable data, i.e. data which comes as an enumeration type (type of personal cards, product category etc.).

To activate this option, you should check the Additional data option and select a data column from the following dialog, according to which the subdivision will be performed.

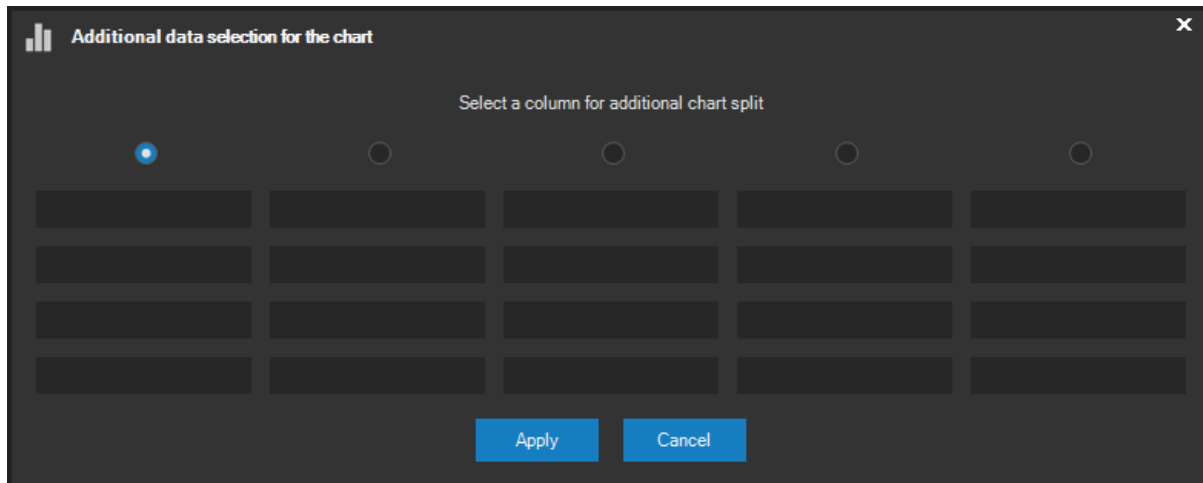
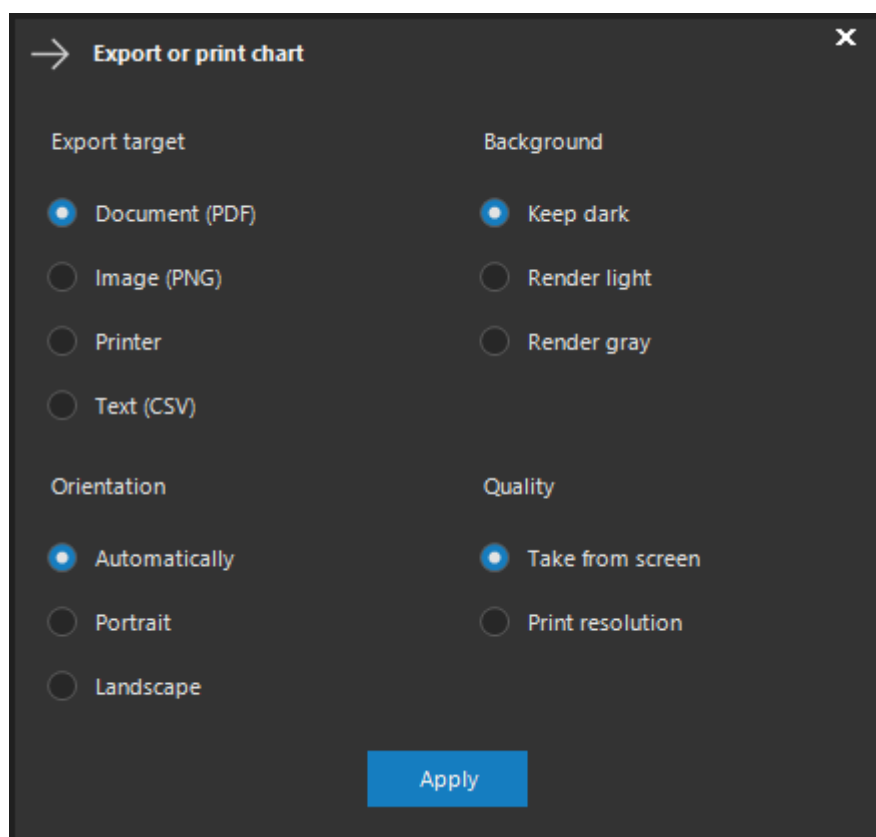


Chart export

Pressing the EXPORT button allows you to initiate the export process of the displayed chart.



The chart can be exported into a PDF document, a PNG image, or sent directly to the printer. Portrait and landscape orientation is available. If Automatically is chosen from the orientation settings, the orientation will be based on the current size of the chart.

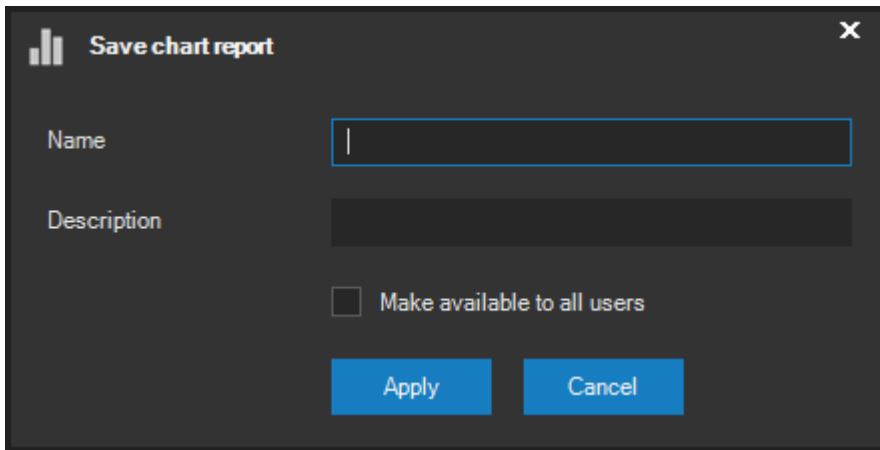
Because charts have a dark background in the application, they can be rendered with light or grey background during the export process. The Quality section allows you to increase the chart resolution for printing.

Data in its aggregated form can also be exported to a CSV text file. Such file can directly be imported to an Excel sheet to create some similar looking chart types for further editing.

When the **PRINT** button is pressed, the export dialog automatically opens with options suitable for standard printing – the export target will be set to the printer with the Render light and Print resolution options selected.

5.2.6. Automatic reporting

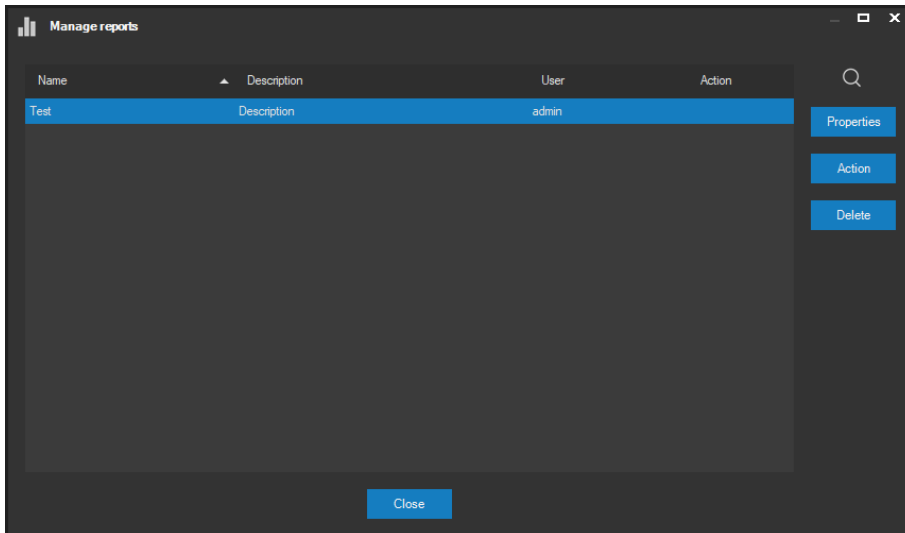
Any chart with all its settings, a suitable name and basic description can be saved to be recalled back later. This can be done using the **SAVE** button.



The 'Save chart report' dialog box is a dark-themed window with a title bar containing a bar chart icon and a close button. It features two input fields: 'Name' with a single character placeholder and 'Description' which is empty. Below these fields is a checkbox labeled 'Make available to all users'. At the bottom are two blue buttons: 'Apply' and 'Cancel'.

By clicking the corresponding option, an administrator has the option to save the chart as a public chart to make it visible to all users. Regular users don't have such option, however, they can see all charts saved by themselves and the one made public by administrators. For the chart to be recalled later, a single-click selection from the dropdown placed in the upper right corner of the window is sufficient.

Use the **MANAGE** button to see all the charts available to you.



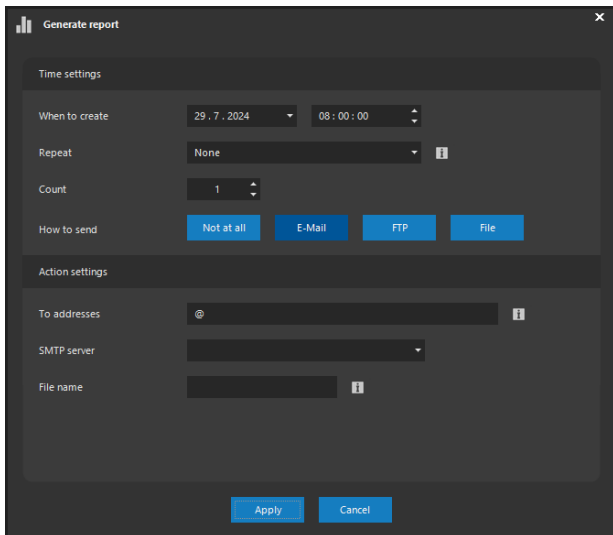
The 'Manage reports' window is a dark-themed interface with a title bar containing a bar chart icon and window controls. It features a table with columns: Name, Description, User, and Action. The first row shows 'Test' as the name, 'Description' as the description, and 'admin' as the user. To the right of the table is a search icon and three buttons: 'Properties', 'Action', and 'Delete'. At the bottom center is a 'Close' button.

Name	Description	User	Action
Test	Description	admin	

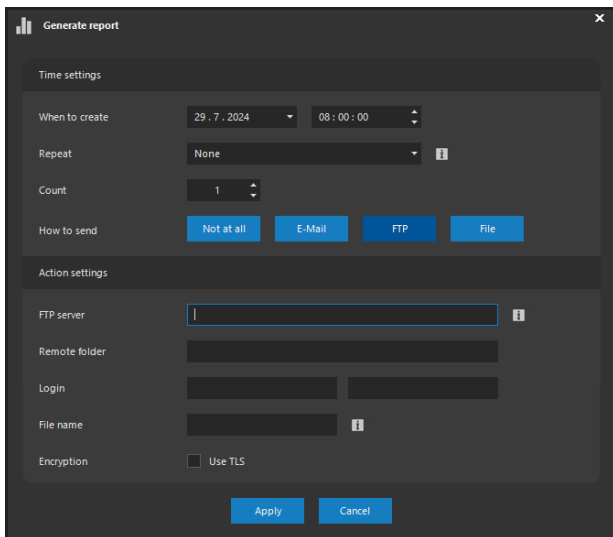
The master administrator sees all reports here including those saved by other users. Reports can also be deleted in this window. Besides the report name and description, the creator of the report is also listed here, as well as the current automatic action, if any.

Administrators can use the **PROPERTIES** and **ACTION** buttons to configure automatic report creation and distribution. Using the first button, the exact same settings can be performed as described above

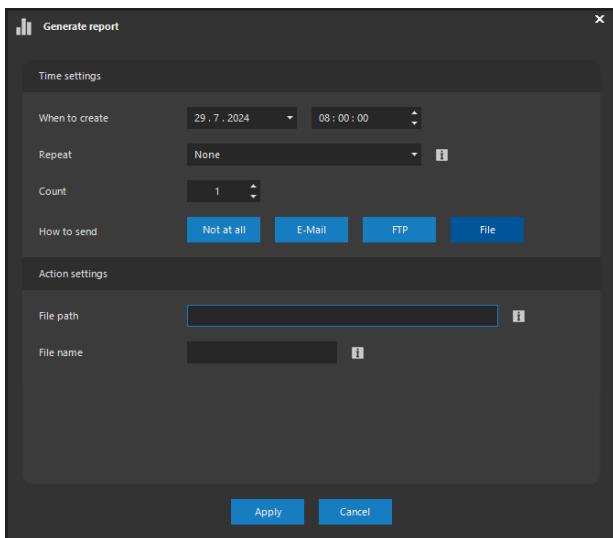
when exporting the chart, i.e. export format, background color or page orientation. The second button opens a dialog window with automatic creation and distribution settings.



The screenshot shows the 'Generate report' dialog window. It has a title bar with a close button. The window is divided into two main sections: 'Time settings' and 'Action settings'. In the 'Time settings' section, there are fields for 'When to create' (set to '29. 7. 2024' and '08:00:00'), 'Repeat' (set to 'None'), and 'Count' (set to '1'). Below these are four buttons: 'Not at all', 'E-Mail', 'FTP', and 'File'. The 'Action settings' section contains fields for 'To addresses' (with a placeholder '@'), 'SMTP server', and 'File name'. At the bottom are 'Apply' and 'Cancel' buttons.



This screenshot shows the 'Generate report' dialog window with the 'FTP' button selected. The 'Action settings' section now includes an 'FTP server' field, a 'Remote folder' field, a 'Login' field (split into two sub-fields), and a 'File name' field. There is also an 'Encryption' checkbox with the label 'Use TLS'. The 'Time settings' section remains the same as in the previous screenshot. The 'Apply' and 'Cancel' buttons are at the bottom.



In the upper part of the window the exact date and time can be configured when to create the chart as well as the repetition period. If a period is set, the time interval used to retrieve the source data for the chart will be shifted as well.

NOTE

This way you will always get your chart based on current data.

Report distribution can be either turned off completely or set to an e-mail, ftp or file action. In all cases, the communication channel settings must be filled in including the option to secure the communication. When using e-mail distribution, multiple comma or semicolon separated recipients can be entered.

In case of saving the report to a file, a local or network path on the administration server can be used. If using a network path, the administration server service must log in under a different user account.

The chart is created by the administration server based on data either already saved in its databases (external objects, centralized camera server metadata) or downloaded from the camera servers when creating the report. Should the camera server needed to deliver the data be offline, the system will try several times before eventually giving up the chart creation.

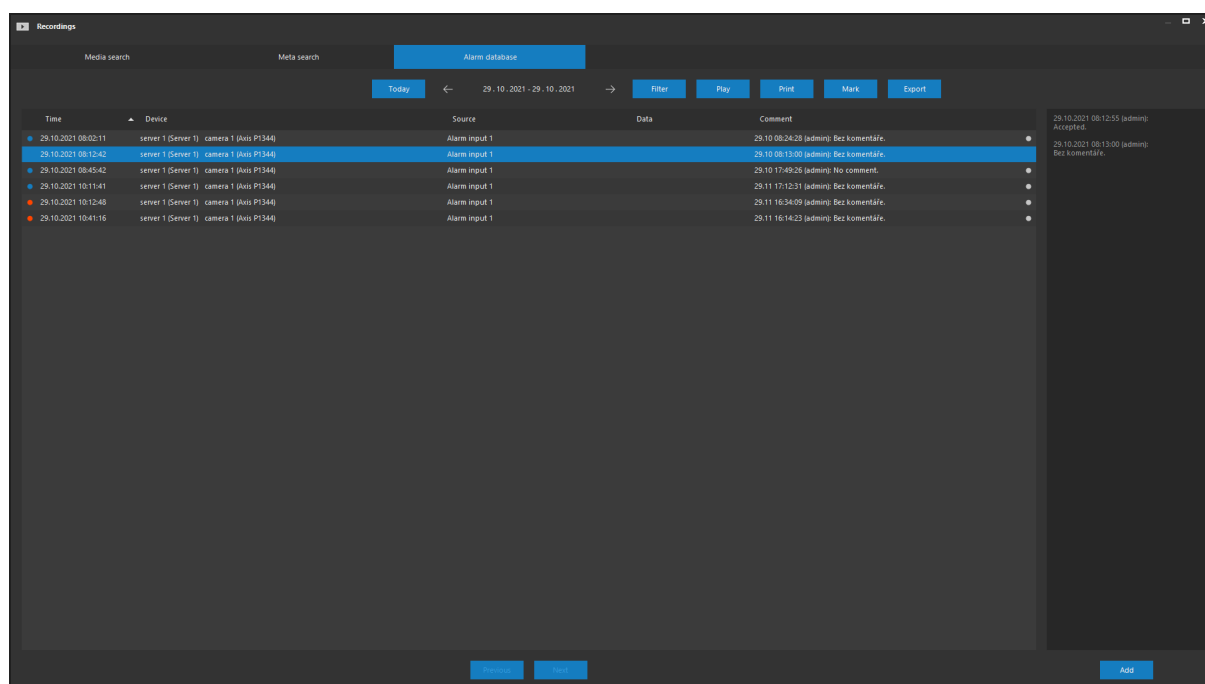
5.3. Alarm database

5.3.1. Accessing the alarm database

All alarms, for which the extended alarm handling mode was activated by the system administrator including those received using the ATEAS Interlogin feature, are automatically stored in the alarm database. The alarms can be displayed by selecting the Alarm database tab in the main Recordings window.

NOTE

The system administrator must provide the corresponding permission in order for you to access the alarm database.



The screenshot shows the 'Recordings' window with the 'Alarm database' tab selected. The interface includes a date range selector (Today, 29.10.2021 - 29.10.2021) and buttons for Filter, Play, Print, Mark, and Export. A table of alarm records is displayed with columns for Time, Device, Source, Data, and Comment. The table shows several alarm entries from 29.10.2021, all from 'camera 1 (Axis P1344)' and 'Alarm input 1'. The comments indicate various alarm states like 'Accepted', 'No comment', and 'Dec komentáře'.

Time	Device	Source	Data	Comment
29.10.2021 08:02:11	Jeniet 1 (Server 1) camera 1 (Axis P1344)	Alarm input 1		29.10.08:24:28 (admin): Dec komentáře.
29.10.2021 08:12:42	Jeniet 1 (Server 1) camera 1 (Axis P1344)	Alarm input 1		29.10.08:13:00 (admin): Dec komentáře.
29.10.2021 08:45:42	Jeniet 1 (Server 1) camera 1 (Axis P1344)	Alarm input 1		29.10.17:49:26 (admin): No comment.
29.10.2021 10:11:41	Jeniet 1 (Server 1) camera 1 (Axis P1344)	Alarm input 1		29.11.17:12:31 (admin): Dec komentáře.
29.10.2021 10:12:48	Jeniet 1 (Server 1) camera 1 (Axis P1344)	Alarm input 1		29.11.16:34:09 (admin): Dec komentáře.
29.10.2021 10:41:16	Jeniet 1 (Server 1) camera 1 (Axis P1344)	Alarm input 1		29.11.16:14:23 (admin): Dec komentáře.

Once you have entered the alarm log, all alarms with the handling mode active (handled and not handled) for the current day are automatically displayed. You can easily return to the current day at any time by pressing the **TODAY** button. If no specific date interval is selected, the arrow buttons shift the alarm database view by one day in the selected direction.

Press the **FILTER** button to display additional options for the search. The **DAYS** buttons opens a calendar for selecting any date range for displaying the alarms. If too many alarms are returned, page buttons below the list are activated. Once a new interval is selected, the date shift buttons above the

list will reflect the new value as opposed to shift by the default value of one day. So you can quickly move to the next week or month.

You can further limit the search by entering text into the individual text fields above the list. The search results will be refreshed as you type. When entering multiple words in one field, the server will search for all occurrences of these words as opposed to the exact word phrase. You can also use the * and ? wildcards representing any number of characters or exactly one character.

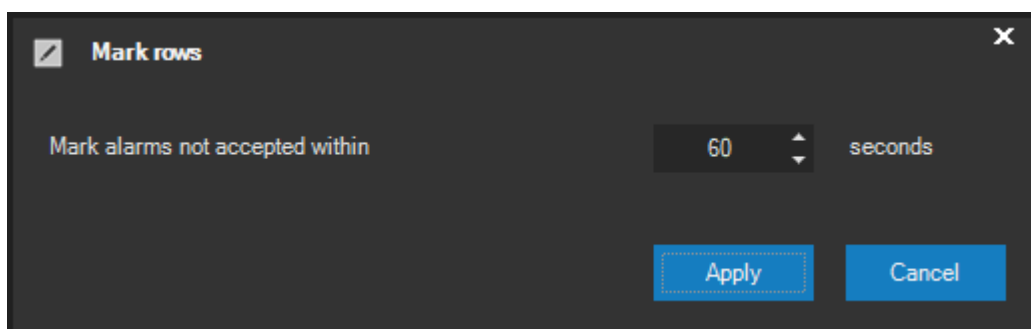
NOTE

Just like throughout the entire system, you can apply the CTRL-F key combination to further refine the search results.

Clicking the **FILTER** button one more time will restore the list of all alarms from the currently configured time interval.

The alarm list displays information about the current status of the alarm, device that fired the alarm, the event source, additional data and the last comment for handling the alarm. Alarms that are not handled are indicated by a red exclamation mark, handled alarms have the same icon with a blue color.

Alarms not accepted by the operator within the defined limit are automatically highlighted in the list. This limit can be changed via the **MARK** button. The newly defined limit will immediately be applied to the alarm list. Only alarms not accepted within the preset interval are actually highlighted disregarding the time when the alarm was finally closed which may depend on other circumstances.

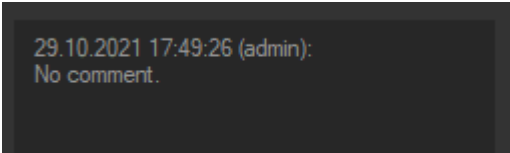


Any alarm from the list can be played by double-clicking on the alarm row or pressing the **PLAY** button.

NOTE

Playing the alarm will open the event view for this alarm. This means the view from one or multiple cameras can be automatically replayed, depending on which cameras have been assigned the Include in alarm view option by system administrator while setting up the event scenario.

After selecting any alarm from the list, the complete handling procedure for the given alarm will be displayed in the right part of the window. The first record always corresponds to the closure of an alarm from the live window; other comments can be entered directly in the alarm database window using the **ADD** button. Of course, each comment contains information about the precise time the comment was added, the user name and text.



29.10.2021 17:49:26 (admin):
No comment.

5.3.2. Exporting and printing the log

The alarm log can be printed on any printer (including e.g. PDF printers) by pressing the **PRINT** button. The log is printed including all information, exactly as seen on the computer screen in the alarm list.

Print alarms
×

Print
Close



Alarm log: 29.10.2021 - 29.10.2021

29.10.2021 08:02:11	1 - Server 1	1 - Axis P1344	Alarm input 1	29.10 08:24:28 (admin): Bez komentáře.
29.10.2021 08:12:42	1 - Server 1	1 - Axis P1344	Alarm input 1	29.10 08:13:00 (admin): Bez komentáře.
29.10.2021 08:45:42	1 - Server 1	1 - Axis P1344	Alarm input 1	
29.10.2021 10:11:41	1 - Server 1	1 - Axis P1344	Alarm input 1	
29.10.2021 10:12:48	1 - Server 1	1 - Axis P1344	Alarm input 1	
29.10.2021 10:41:16	1 - Server 1	1 - Axis P1344	Alarm input 1	

1 Printed: 29.10.2021 16:27
Printed by: admin

Export to XML format can be used for the purpose of automated or batch processing, or as a foundation for developing custom user printing systems, statistics or overviews. The export to XML button is located directly next to the **PRINT** button.

NOTE

The final XML document also contains the complete handling procedure of each alarm including all comments.

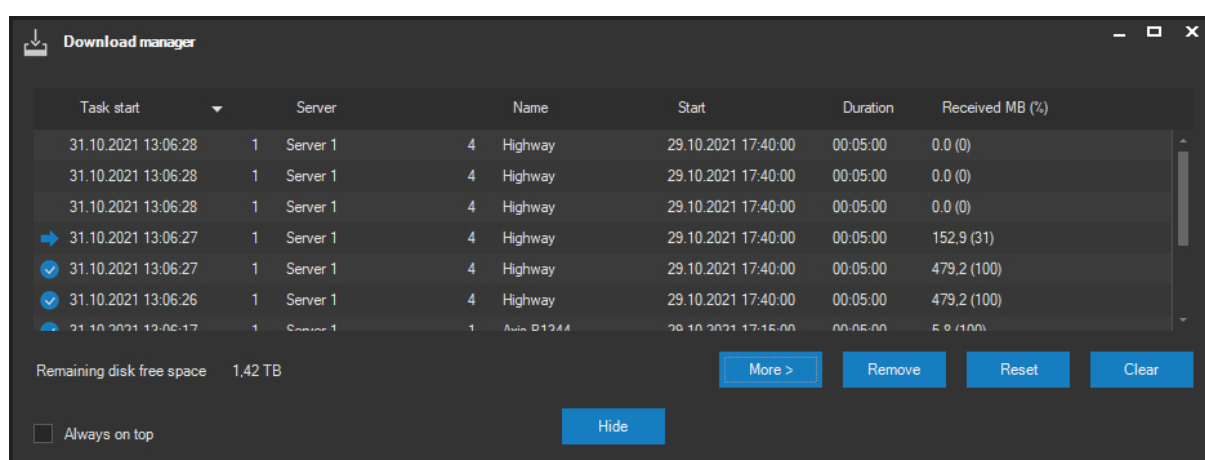
NOTE

If a search filter is applied to the list of alarms by entering a search phrase, the print and export features will be based on the displayed (filtered) data rows only.

Chapter 6 - Using the Download manager

6.1. Introduction

The Download manager is a smart tool used for downloads from the media stores of individual camera servers, which registers and processes all user-created tasks one by one or in parallel. The download manager window can be opened from Tools in the application's main menu, or automatically by creating a new task in a live or recordings window.



CAUTION

Closing the download manager window does not interrupt or stop the task flow. In this case, the manager runs in the background of the application and continues processing each task one after another.

All downloads use the ATS container format which guarantees maximum security providing a password protection option or digital signature and supports all other advanced features like dynamic video resolution or frame rate changes. All major video and audio codecs are supported.

Unlike the usual course of downloading from media stores, the download manager is equipped with many smart features, helping users with their downloads.

- Automatic notification for lack of available disk space.
- Automatic download pause prior to running out of disk space and continuing the download upon freeing up space.

- Option of creating an unlimited amount of download tasks, which will be processed one by one.
- Status preview for individual tasks and automatic one by one task restart for tasks which were not processed successfully.
- Simultaneous data download from different camera servers.
- Automatic or manual task creation.
- Postponed start of task option for manually created tasks (for example overnight when the network load is reduced etc.).

6.2. Task management

6.2.1. Adding a task automatically

The download manager list registers and displays all significant information for individual tasks such as the date and time for beginning the task, the number and name of server, number and name of camera, start of the downloaded sequence, length of the downloaded sequence and the amount of downloaded data expressed in MB and also as a percentage in relation to the overall interval for downloading.

The newest tasks are always displayed at the beginning of the list, nevertheless, the task order can be adjusted at will by clicking on the header of individual columns (clicking on the header again changes the manner of filtering from descending to ascending).

The current state is displayed by each task. The basic states include: task awaits being started (no icon is displayed), task is being processed (blue arrow icon displayed) and task was successfully processed (green confirmation icon displayed).

NOTE

Tasks can of course be filtered or grouped using the header of the first column, i.e. according to their state.

NOTE

You do not have to create tasks which are not processed successfully again, for the download manager will restart them automatically over time.

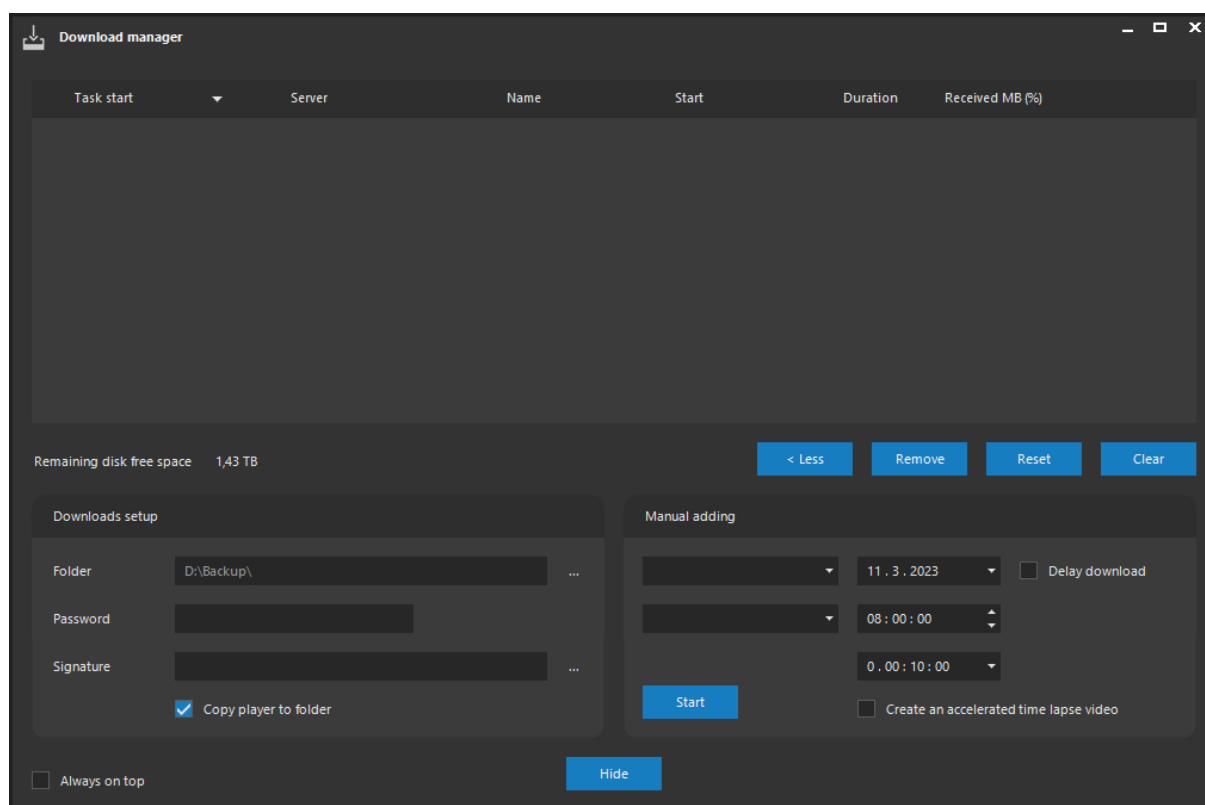
A new task can be automatically added to the task list by marking or selecting the relevant camera and sequence for the data download in the live window or recordings window. These procedures are described in the chapters regarding the control of individual parts of the application. After a task has been added, its start date and time is set to the current date and time or to the predefined value in the extended options section.

NOTE

However, this does not mean the task will start immediately under every circumstance. If another task is still being processed (on the same server), the start of this task is postponed until the task underway is completed.

6.2.2. Adding a task manually

Besides options for automated task entries into the download manager, new tasks can also be created manually. To do so, you must display the advanced settings and additional controls of the download manager by pressing the **MORE** button. You can go back from this view at any time by pressing the **LESS** button.



In the Manual adding section a manual definition of a new task can be performed. To achieve this, a camera server and a camera (or all cameras) as well as the date and time of the recordings and the time interval must be selected. Using the Delay download option, the task can be scheduled to start at a later timer.

NOTE

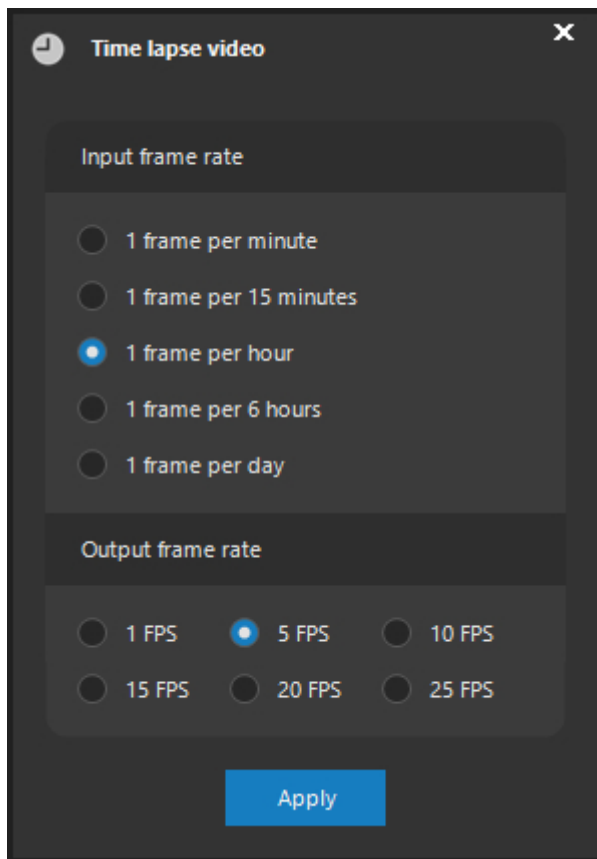
By delaying the task you can schedule larger data or longer interval downloads to take place e.g. during night hours when the network load decreases.

If the time interval for downloading takes longer than 30 minutes, the interval will be split automatically to make handling the downloaded data easier.

6.2.3. Time lapse videos

If the download manager shows the advanced settings by pressing the **MORE** button, you also have the option of checking the Create an accelerated time lapse video checkbox. This option allows making the necessary changes to the timing of each image while downloading to achieve an accelerated time lapse video. A time lapse video typically shows a longer period of time (weeks, months or years) accelerated within several minutes or tens of seconds. The result is an impressive display of slow flowing events (for example buildings etc.).

To create a time lapse video, all you need to do is select the respective option within the download manager window. For optimal results, you can modify the input and output frame rate.



In the Input frame rate section, you can specify the frame rate for images loaded from the server recordings for creating an accelerated video. In the Output frame rate section, you can specify the frame rate for images after downloading, which is indirectly proportionate to the duration of the video file.

NOTE

An accelerated time lapse video will never contain an audio track, even when server recordings contain audio.

NOTE

If the selected type of storage, from which the download will take place, is set to the Camera value, an accelerated time lapse video cannot be created. In this case, the application will respond with a warning message.

NOTE

If you are performing camera recordings for the sole purpose of creating a time lapse video, you can use the minimum frame rate for recording, which is one frame per minute. If this frame rate is also unnecessarily high for your needs, you can perform the recordings via scheduled events with a defined period with an even lower frame rate.

NOTE

Generating time lapse videos is available starting with ATEAS Security PROFESSIONAL edition.

6.2.4. Task list control

Several buttons are available under the task list used for controlling selected tasks or the entire list. Their brief definition is provided below.

REMOVE: This button removes the selected task from the list. If the task has not been successfully completed, this task will be immediately interrupted prematurely (and will not be restarted). The incomplete sequence download will not be available in the list of downloaded sequences and the associated data will be deleted from the local computer.

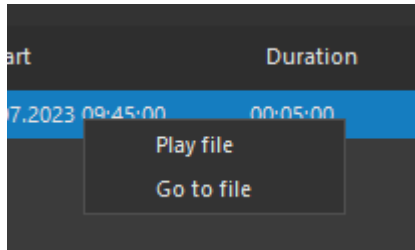
NOTE

Any given number of items can be selected from the task list using standard Windows methods (using a mouse, CTRL or SHIFT keys, CTRL-A hotkey). Thus, multiple items can be removed at once.

RESET: This button performs a complete reset and clears all tasks from the list. The button fulfils the same function as does **REMOVE**, the only difference being it is used on all tasks in the list. You must confirm a dialog before performing a reset.

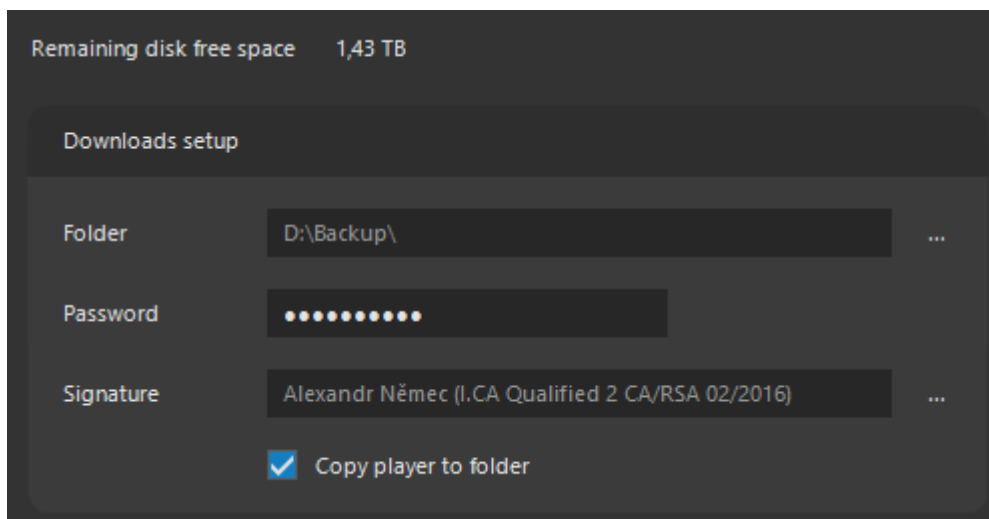
CLEAR: This button clears the task list. All successfully completed tasks will be removed from the list. The list will only contain tasks currently being processed and tasks which finished with an error and wait for being restarted.

Each download task has a context menu enabling a fast way to replay the downloaded file and a fast way to open the folder containing the file.



6.3. Downloads setup

In the Downloads setup section, available in the expanded part of the manager, the target folder for downloaded recordings in ATS format as well as the password and digital signature can be specified. The signature will be applied automatically for each download.



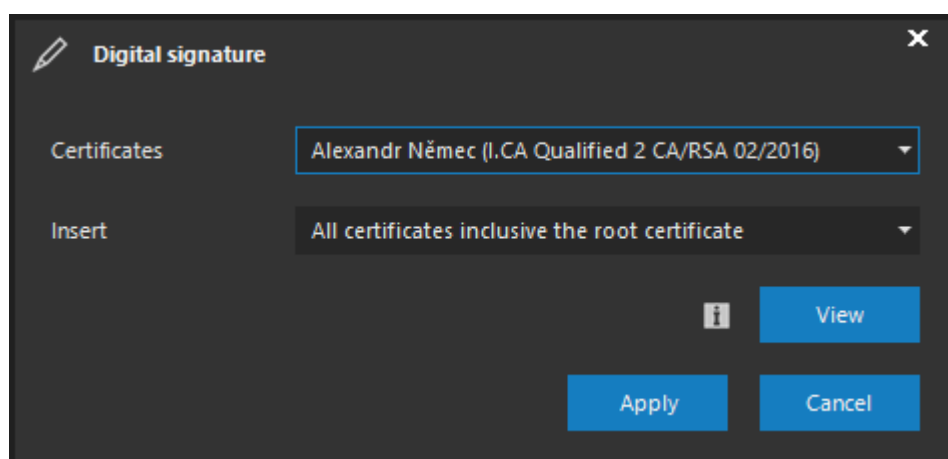
Similarly to camera server data backups, the target folder for downloaded recordings uses an easy-to-read folder structure according to servers (or views), cameras and days. File names include the time.

You might not be able to enter a password, if an administrator has activated a password protection for all data downloads and you have not been granted the permission for exporting data outside the system.

NOTE

Encrypting ATS files is available starting from the ATEAS Security PROFESSIONAL edition.

If you want your downloaded data to be signed automatically, select a signature in the dialog containing all signature certificates.



You may find it useful to automatically add a stand-alone ATEAS media player to the export folder, which can be launched on the target computer without the need to install anything. By checking the respective option, the player will be exported directly to the target folder.

CAUTION

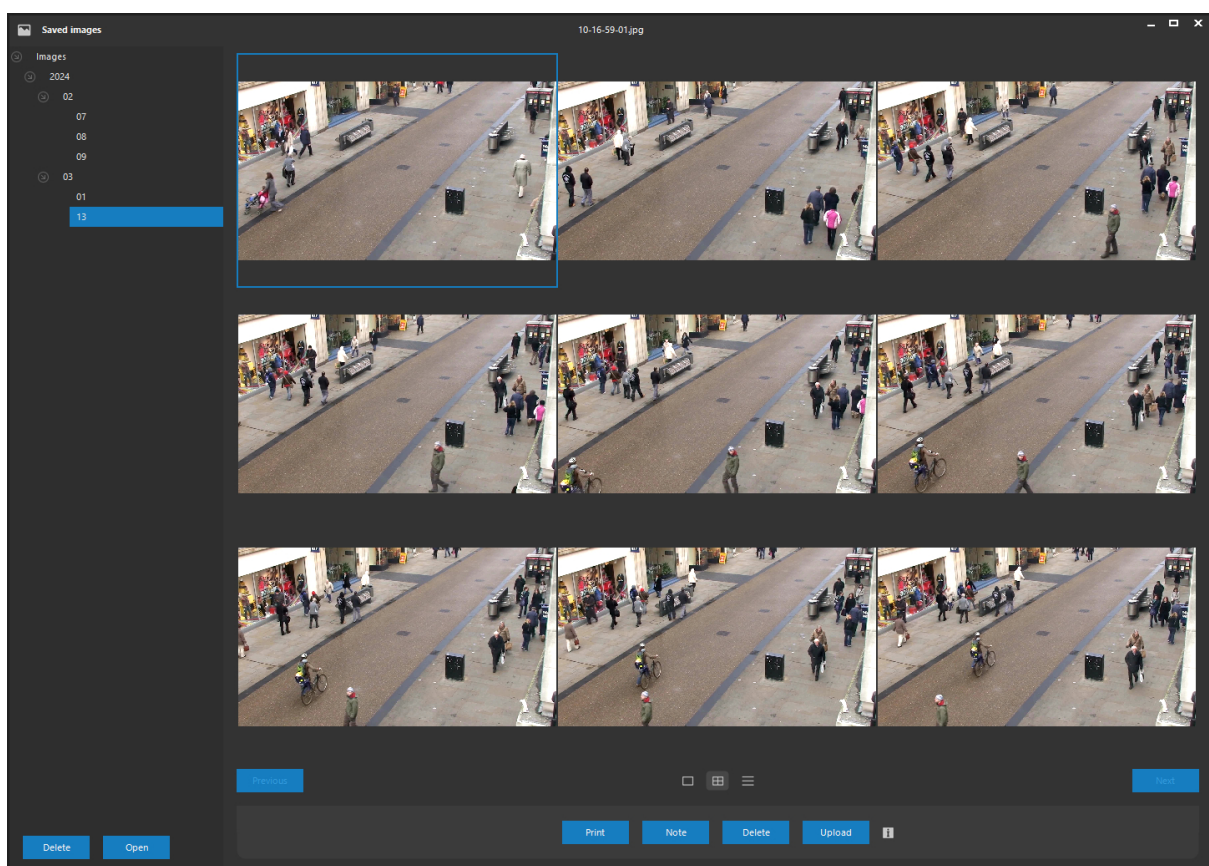
In order for the player to be exported together with data, your client will first download the player from the ATEAS administration server. Once downloaded, a new download process is not required for repeated exports. The first download, however, requires your administration server to have its http port accessible.

Chapter 7 - Working with snapshots

7.1. Snapshot management

7.1.1. Snapshot summary

A separate snapshot database window will open upon saving a snapshot from either the live view or recorded video and all snapshots will be displayed in the preview.

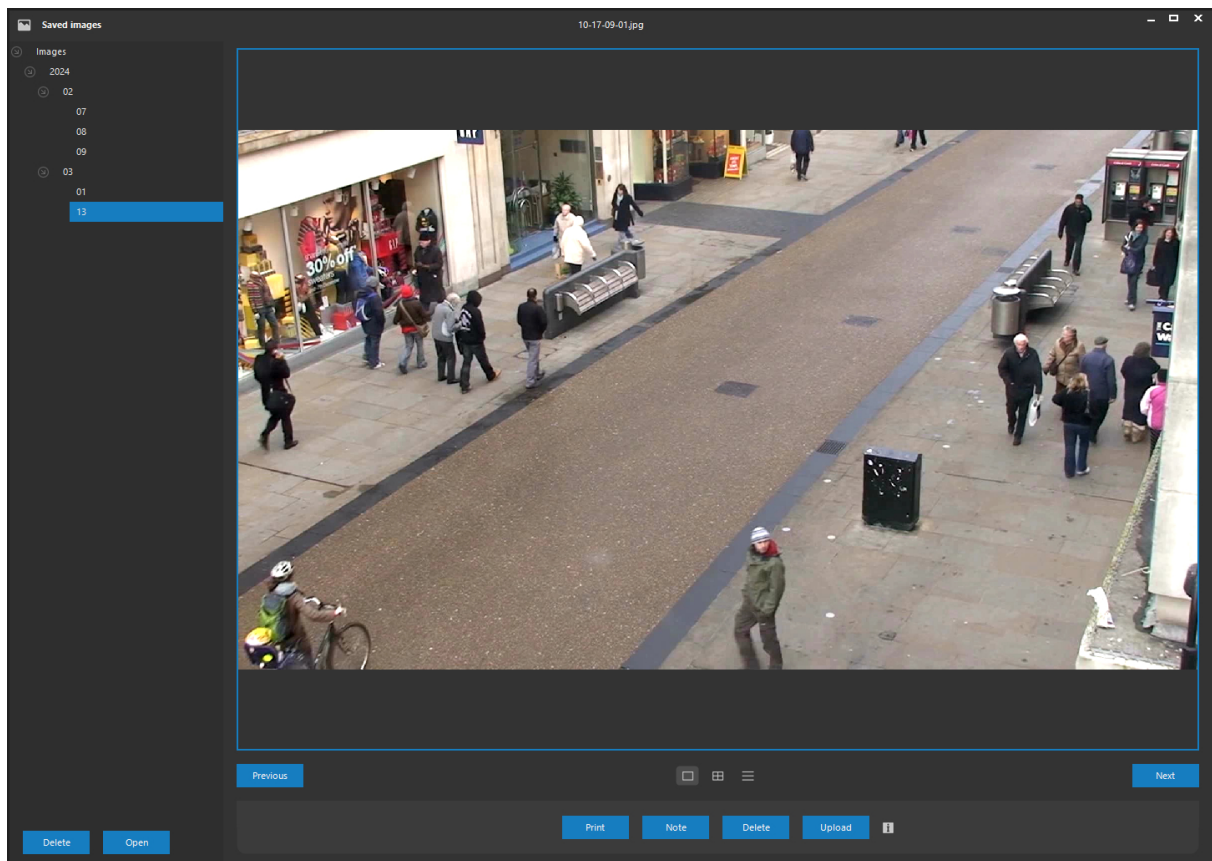


Snapshots for a particular day can be displayed in different sizes. Three buttons in the bottom part of the screen allow the user to select the display mode. If in the given display mode the number of snapshots exceeds the value that guarantees a good viewing experience, the Previous and Next buttons will appear to allow the user to easily navigate between pages.



Individual snapshots are available in JPEG format under the Shots folder found in the application installation directory and can be viewed by any external browser. Metadata can be linked to the image files by using JSON files with the same file name.

Double-clicking a selected snapshot performs a switch into a detail view.



NOTE

Operations related to digital zooming and movement can be performed for a selected snapshot using the mouse scroll wheel and by clicking directly into the view.

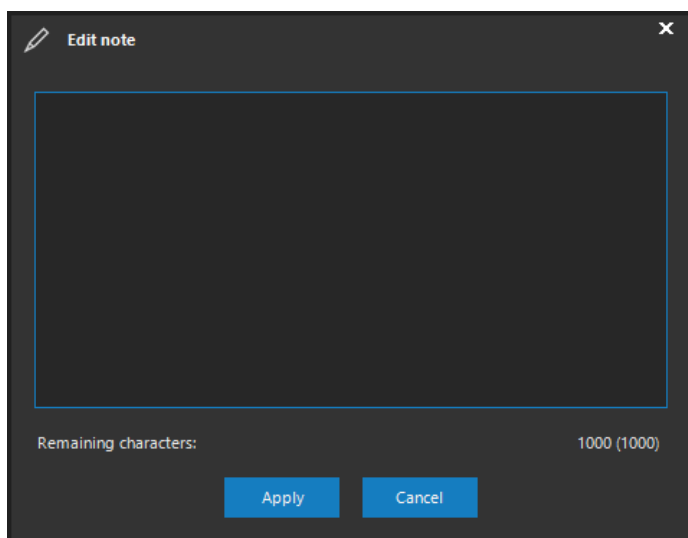
The snapshot display can be filtered according to time by selecting a group from the list to the left of the window. This control automatically creates time folders in the tree structure. Years, months and days are listed in the created first, second and third levels respectively.

Any snapshot can be deleted by pressing the **DELETE** button in the bottom part of the window. To delete all snapshots in the given time folder (year, month or day), select a folder and press the

DELETE button located under the folder tree. The **OPEN** button is a convenient way to open the folder with the snapshots.

7.1.2. Adding information

A closer description relating e.g. to what the snapshot actually depicts can be saved with each snapshot. This description is then printed part of the print report. You can add a description using the **NOTE** button.

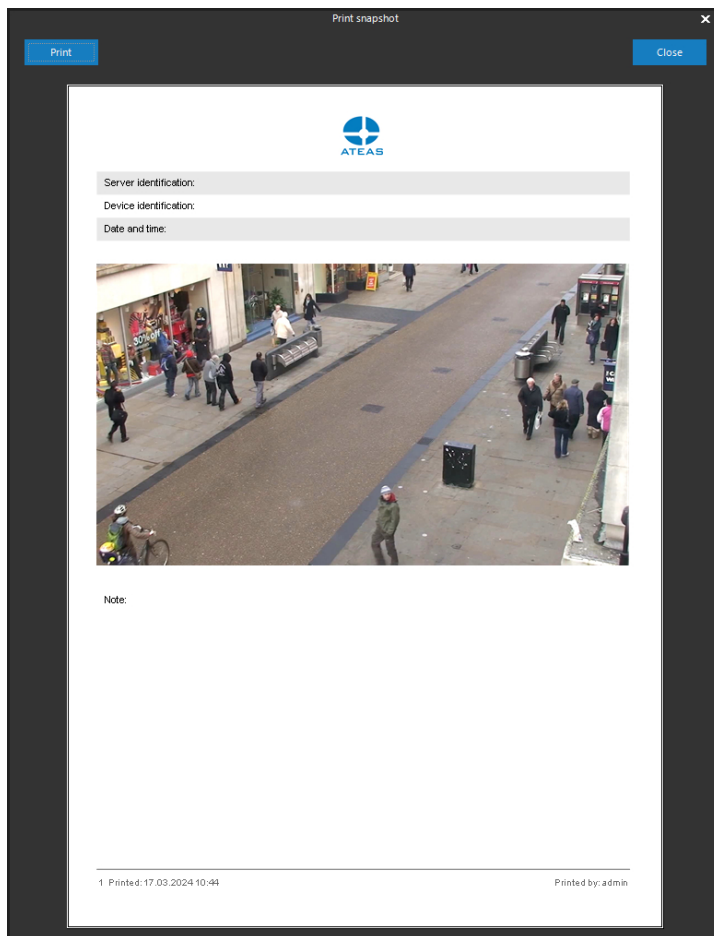


7.1.3. Printing snapshots

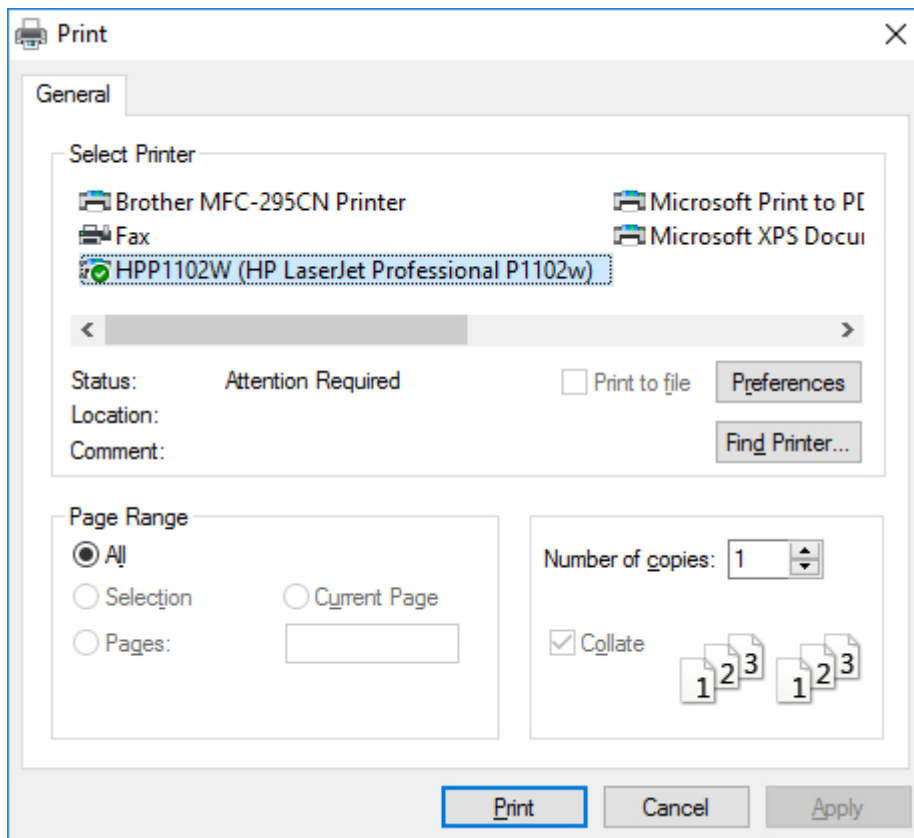
Any snapshot can be printed by any local or network printer added to the system. The export or printing process is executed by pressing the **PRINT** button.



To print the snapshot, press to **PRINT** button. If no printer is installed in the system, the application will display a warning message and printing will not continue. The preview of the final document is displayed in terms of the first phase. This preview includes information about cameras, servers, exact snapshot times and also additional descriptions entered by user.



After creating a preview, press the **CLOSE** button to go back. A print button is located in the top left corner of the print window, which opens the print dialog. This dialog is the standard Windows print dialog and includes printer selection, preferences and number of copies options. The printing process starts upon pressing the **PRINT** button.



7.1.4. Server camera preview

By clicking the **UPLOAD** button, a system administrator can upload the selected snapshot to the server where it will be used as a static camera video preview.

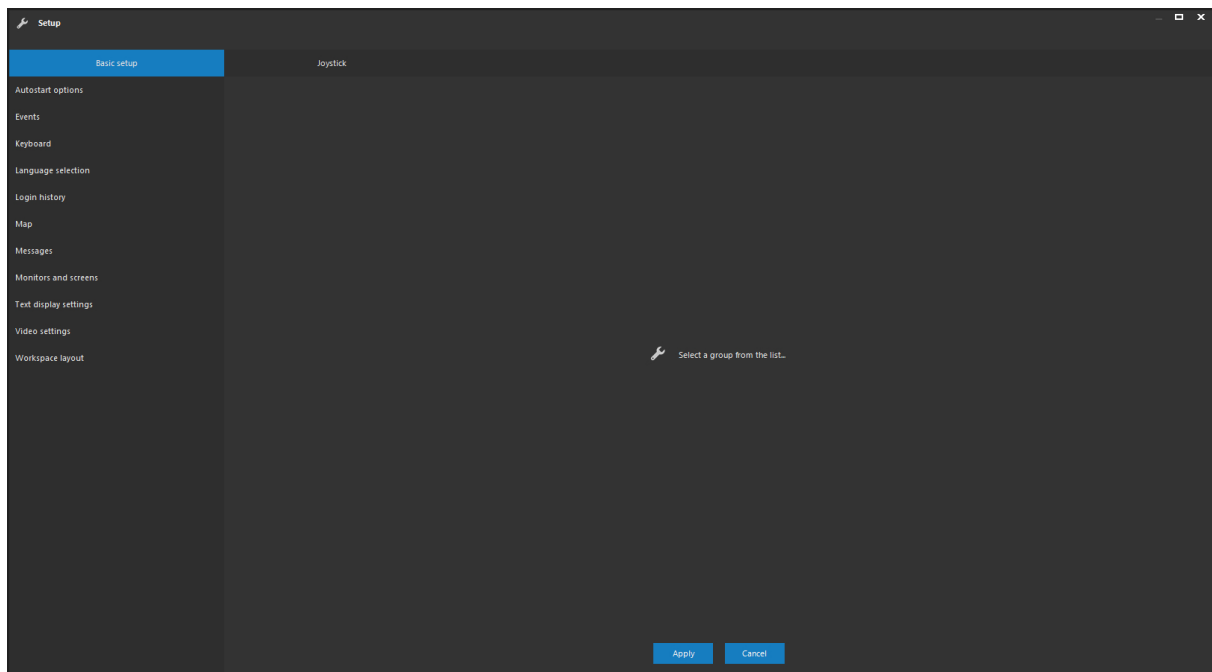
NOTE

These previews can be used, for example, by the ATEAS application for Android TV.

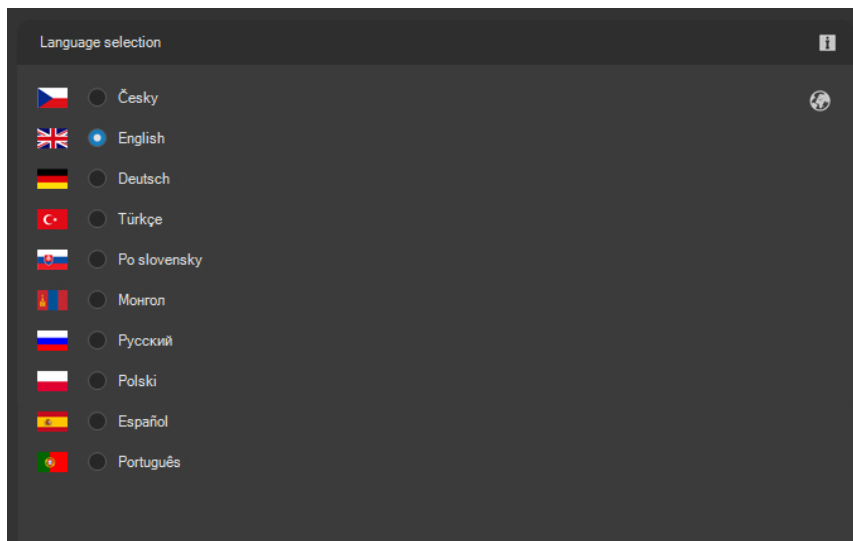
Chapter 8 - Local setup

8.1. Basic setup

The local station setup window can be accessed by selecting Setup from the main menu. You can configure application behavior from the **Basic setup** tab. Individual setup groups are displayed in the list on the left side of this tab in alphabetical order. After any options are selected, they are displayed on the left side of this tab. Settings performed on all tabs are saved upon pressing the **APPLY** button.



8.1.1. Language selection



Basic environment setup (including language setup) is executed by interactive dialogs which are displayed during the initial run of the application on a specific workstation.

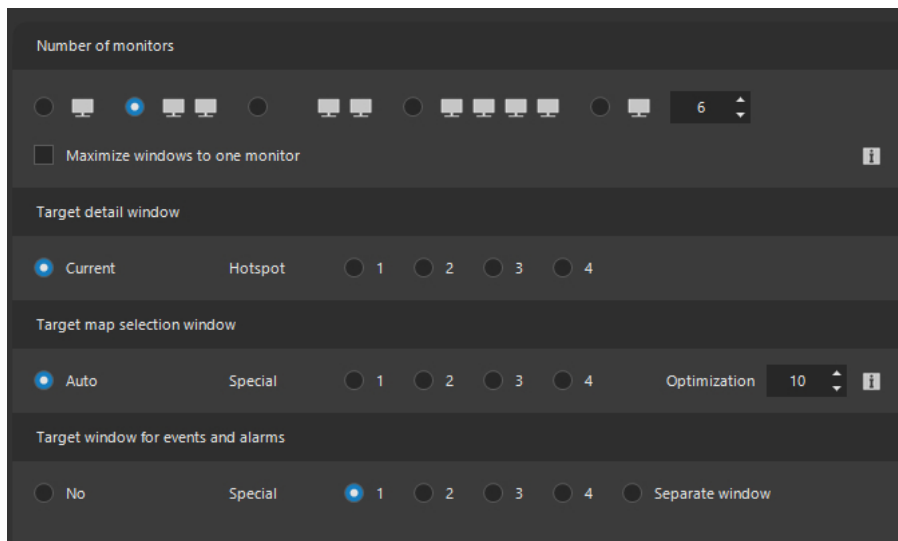
CAUTION

You must restart the application for the changes to take effect.

NOTE

The system administrator can activate a user policy for which the system will store the languages of all users and automatically switch them on any given station. These settings have a higher priority over the language setting in the local setup of the station.

8.1.2. Monitors and screens



On this tab, you can set the number of monitors currently connected to the computer (monitoring station). The maximum amount supported is 16 monitors. The application automatically detects a multi-monitor system (monitors in dependent mode with one desktop – horizontal span, monitors in independent mode with several desktops – dual or multi head) and will always work optimally for each specific configuration.

CAUTION

Considering performance factor we recommend using the configuration of a dependent mode (i.e. with one desktop – Windows desktop is expanded over all monitors).

If multiple monitors are merged to form a single desktop, the Maximize windows to one monitor option can be used to achieve an improved window behavior when maximizing them. Windows will be maximized to occupy the current monitor only instead of the entire desktop.

NOTE

Up to 16 monitors can be connected to the computer. However, a standard client can open up to 16 live windows. The monitors can also be used for displaying maps, replaying recordings, browsing snapshots etc. A video wall slave client can also display video on 16 monitors. For further information, see the chapter regarding the video wall.

The Target detail window option determines which live window will display the detail of a selected camera (after double-clicking on the camera header). The Current switch is checked by default, which means the current view in the live window will be replaced with the detail view. If you wish to display the detail view on another monitor, check the switch assigned to a particular live window.

The Target map selection window option has a similar function. Cameras can be selected directly within the map using map functions. The map selection is then displayed in either of the live windows. The target window can be designated using monitor symbols, numbered one to four. The Auto option is selected by default, which means the map selection will be placed on either the last active live window or the primary live window (if the primary window is not opened). Despite the fact that it is possible to select any number of cameras (elements) in the map window using selection tools, the target window will display 100 cameras at most, in a 10 x 10 layout.

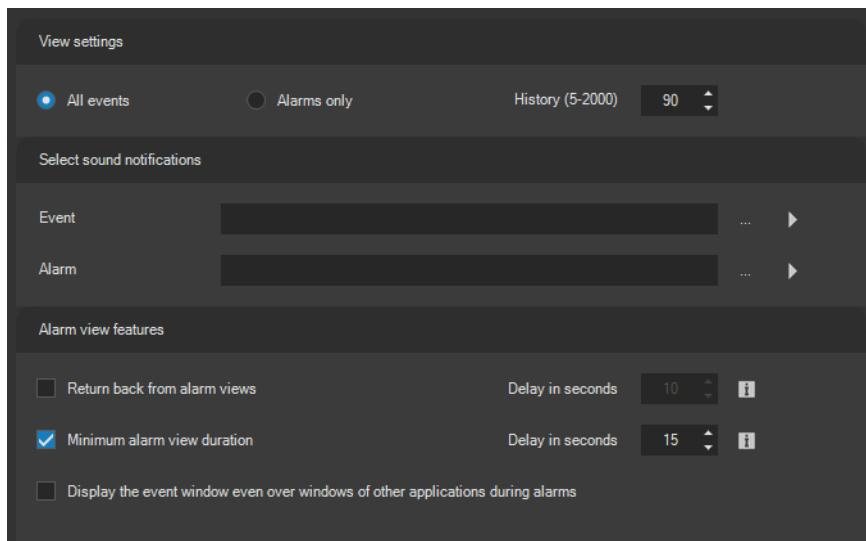
By setting the Optimization value, it is possible to determine the number of selected cameras in the map from which secondary camera streams will be used, if configured.

TIP

Thus you can decrease the load of the client after opening a map view.

The target live window for receiving events can be configured from the Target window for events and alarms. If reception is turned off (No option is checked), the application will not signal events and alarms received. The Separate window option makes a separate events window rather than a regular live window the target window for events.

8.1.3. Events



The following settings are available:

- Setting the filter for non-significant events. The user can filter non-significant events, so that only alarms will be displayed in the live window.
- Setting the maximum number of events and alarms stored in the event list within the live window. The history length is set to 20 events and alarms by default. This parameter, however, cannot limit the number of displayed alarms that have not been handled, but have their handling mode active.
- Setting sound notifications for receiving an event. In order to play a sound when an event or alarm is received, you need to fill in the path or find a valid audio file. The selection is initiated by pressing the folder browsing button. Audio files for events and events with alarm statuses can differ. To turn these notifications off, delete the content of the relevant text field.

A standard Windows dialog is used to select any audio file in a WAV file format. Several suitable audio files are included in the client application installation. The sound, whose path will appear in the text field, can be tested (played) by pressing the white arrow button.

The Alarm view features section still offer several features for configuring suitable ergonomics for accepting alarms.

If the option of returning from alarm views is activated, the original local or shared view, displayed before the alarm, will automatically return to the live window, which accepts the alarms, after the defined interval has expired. This significantly improves the work of the operator when he finds himself without a live window designated only for alarms, but displays other camera views on it as well.

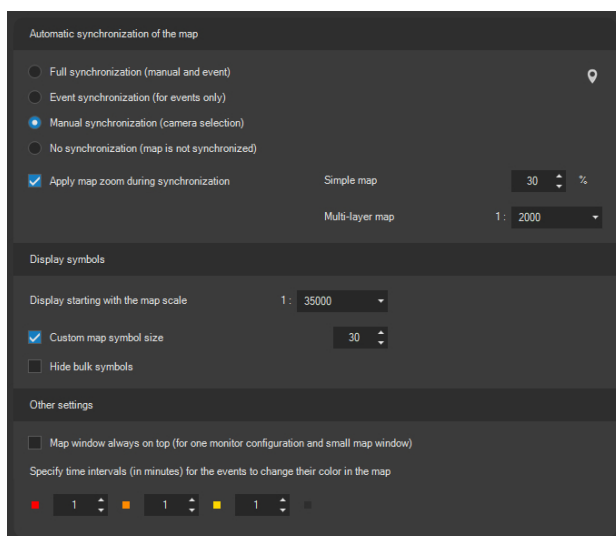
If the minimum alarm view duration feature is active, no other alarm view will be switched in the live window, unless the defined time interval has already expired since the last alarm view was switched. This feature is used to improve the operator's situation and his ability to respond to multiple alarms occurring within a short period of time.

NOTE

If the previous feature does not allow an alarm view to automatically appear, this will not, of course, have any effect on displaying this alarm in the event list in the bottom part of the live window.

When working simultaneously with multiple windows or applications, the event window is not automatically brought to the foreground in case of an alarm to ensure you can continue working in another window or application uninterrupted. You can be notified of an incoming alarm, for example, by a sound notification. However, if you wish the window with the event view to automatically appear in the foreground in front of other windows and applications, activate the corresponding option.

8.1.4. Map



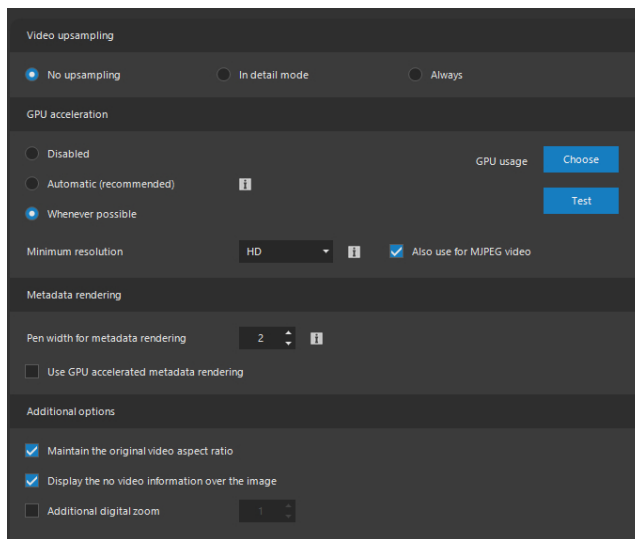
In this part of the setup, you can configure the behavior of a map window with local effect (for a specific station). The following settings are available:

- Automatic map synchronization. A map is an intelligent, locally integrated component, which can be synchronized during the course of all kinds of events (automatic localization of events,

cameras and objects including zoom adjustment). If the Full synchronization option is selected, the map will be synchronized every time possible, including events and manual selection of cameras located in a map. If the Event synchronization option is selected, the map will be synchronized only when an event related to a localized object occurs (but not during manual selections). By selecting the Manual synchronization option, the map will be synchronized only when cameras are selected manually, but not during system events. The automatic synchronization can also be turned off, by selecting the No synchronization option.

- Zoom adjustment. The map is automatically centered to a selected element or event during automatic synchronization. Additionally, it is possible to perform a map zoom operation. For simple maps, this value can be set as a percentage of the original map size, for multi-layer maps as an actual map scale.
- Displaying symbols in the map. Setting the maximum scale for a multi-layer map, for which symbols shall still be displayed in the map (cameras, custom buttons), can prevent cameras or buttons from being rendered with the map zoomed out too much, which could make orientation within the map difficult. To handle this case, the map is equipped with a smart grouping feature of map elements of the same type. These grouped elements stay visible, but they can be configured to be hidden - along with individual element symbols using the Hide bulk symbols option.
- Custom map symbol size. The size of all camera symbols in a map is 24 points by default. However, this size can be modified with regard to different monitor resolutions and subjective user perceptions.
- The Map window always on top option enables to switch the map window to a mode, under which it cannot be overlapped by another application window. This is useful for single monitor monitoring stations, where it is possible to scale the map window and let it always stay on top, providing better orientation and eliminating the need for switching between windows.
- Changing event colors in a map. When displaying events in a map, it is possible to change their appearance depending on their date. This feature makes it easy for the administrator to evaluate the current status of events and alarms. The event is always displayed by the bordered symbol, which invoked a particular event. The border turns red when an event occurs. After a while, it changes into orange and then into yellow before it is completely deleted from the map. Time delays between these changes can be defined using the controls available in this window. In case any events are refreshed, the whole process is repeated and the specific event is marked as active.

8.1.5. Video settings



In the Video upsampling section, you can choose if the pixel upsampling technique will be used when the resolution of a target place for displaying a camera on a monitor in a specific window is higher than the native resolution of the camera (upsampling). Upsampling (enlarged view) is turned off by default, however, it can be turned on for the detail mode (while there is only one camera in a view) or for all live views.

The use of the graphics card or dedicated graphics processing unit (GPU) can be activated under the GPU acceleration section. If this feature is activated, video decoding is accelerated via the GPU, therefore, the central processing unit (CPU) is not the sole bearer of the load.

NOTE

Using the GPU can be especially helpful for demanding applications, which make use of high frame rate video (60 FPS) or very high resolution videos (4K).

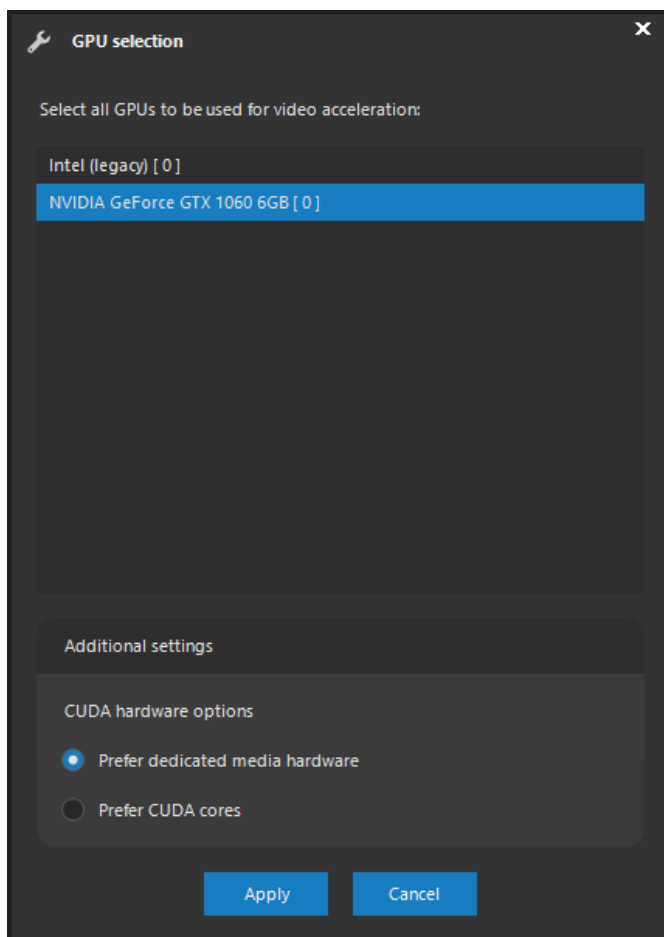
The radio buttons can be used to determine whether the graphics processor will be used only for displaying smooth video or also for limited frame rates. The recommended option shall suffice for the majority of installations, i.e. using the GPU for displaying smooth video. For H265 video, GPU acceleration is always used.

Under GPU acceleration settings, it is also possible to specify the minimum video resolution to activate GPU acceleration (if at least one of the video dimensions is equal to or exceeds the defined value). Disregarding the video resolution, MJPEG format can be excluded from GPU acceleration.

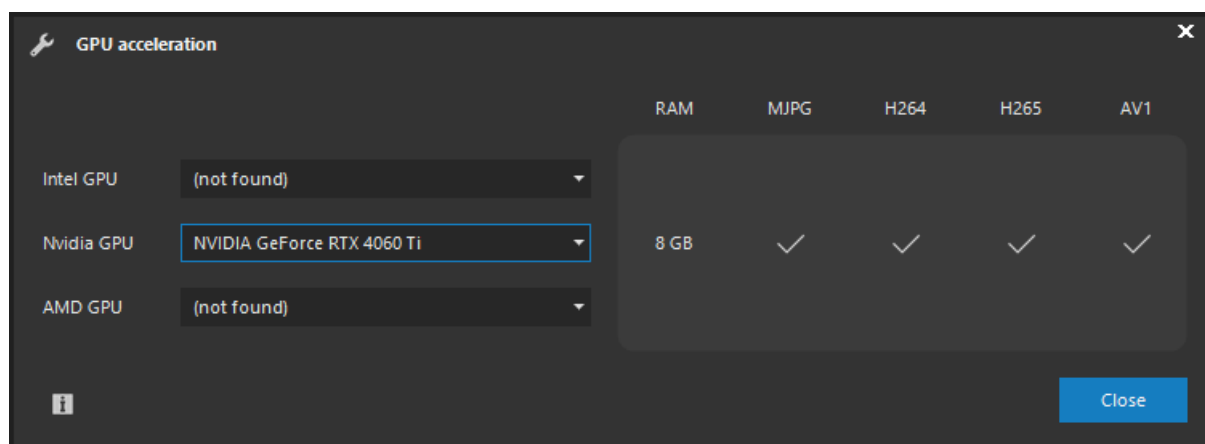
The **CHOOSE** button displays a dialog with the list of all graphic cards. One or more graphic cards to be used for video acceleration must be selected from the list. In order to achieve maximum performance, the client is capable of utilizing various GPU acceleration technologies, as well as multiple GPUs, even within a single application.

NOTE

With respect to CUDA, the user can also specify certain hardware preferences. In particular, it can be specified whether CUDA cores will be used for acceleration, or whether dedicated media decoding hardware will be used.



The **TEST** button can be used to verify whether accelerated video decoding can be used on the given computer. The following dialog displays the results of the graphic acceleration test for processing MJPEG, H264, H265 and AV1 video format. The acceleration interface of all major GPU manufacturers is supported.



NOTE

If the player is launched without logging into the system, GPU acceleration will be used by default.

In the Metadata rendering section the pen width option can be used to specify the pen width in points, which will be used for rendering metadata obtained from the neural network or from external sources of analytical data. The width can be set between 1 to 5 points with the default value being 2 points.

NOTE

This width remains the same, regardless of digital zoom level, which is significantly more comfortable for user perception of the rendered metadata.

When the number of detected objects is high, the video frame rate is also high and there are many cameras in the view, metadata rendering can become a CPU intensive task. When the rendered metadata do not appear properly synchronized with the video, it's time to activate the GPU accelerated metadata rendering, which will transfer the task directly to the GPU.

NOTE

GPU accelerated metadata rendering makes the metadata to be part of the video layer, thus, some CPU rendering features (pen width independent of digital zoom level or an optimized positioning of text boxes) will not be available.

GPU accelerated metadata rendering may especially be beneficial for video walls. For this to work, of course, GPU video acceleration with an Nvidia GPU must be activated as well as described above.

The additional options section contains the remaining options for this setup section, for example the option to keep the original aspect ratio. This option is selected by default. The effect it has is that it displays vertically or horizontally oriented dark stripes in the camera view. These stripes compensate for the difference between the side ratio of the video and the window. This feature can be turned off by unchecking this option. The maximum available window space will then be used for the video display, though the aspect ratio might be affected.

Further more, it is possible to enable displaying the video loss information directly in the image. This information is displayed as a No video label with a red font.

NOTE

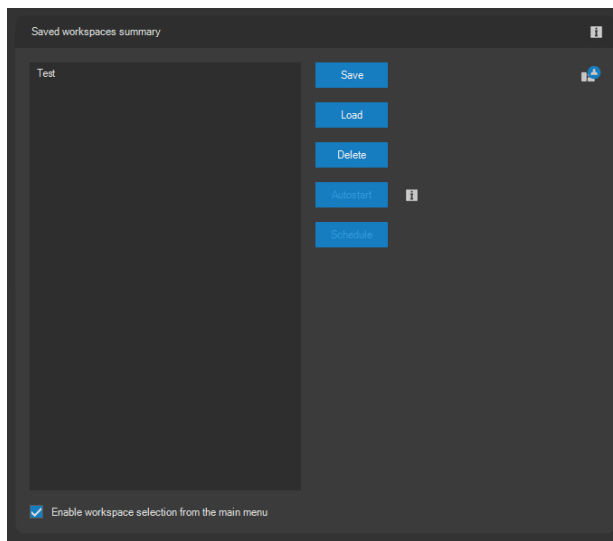
One of the synchronization indicators has the same functionality; nevertheless, this function can serve as a more distinctive means of notifying the operator that video from a camera is not available. This function is deactivated by default for live windows.

The digital zoom option above the native resolution of the video is deactivated by default. By checking the Additional digital zoom option, you will be able to digitally zoom in the selected camera to enlarge the picture to a size that is many times larger than the original. The value of the multiple can be configured from 1 to 10.

NOTE

The Video settings are related to local live windows only. There are some identical settings in the video wall administration section, concerning the video displayed on monitors that are a part of a virtual video wall. Therefore, this setup is not considered when using a slave station (logged in using a slave account to the video wall).

8.1.6. Workspace



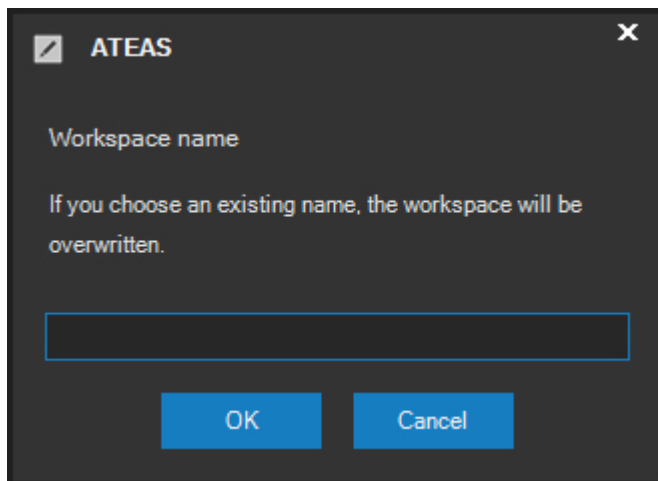
Most of the users who approach the camera system use a specific layout of live windows on their monitors, and a specific position and size of the map window. To refrain from adjusting these layouts every time the application is started, the client application saves user workspaces. The application will remember the following for a saved workspace:

- the number and position of all (i.e. 16 at most) live windows,
- the position and size of other windows (recordings, map scene, the main menu window),
- locally saved or shared views switched to the live windows,
- the live window status (F12 maximization),
- last selection view positions in the live windows,
- the event window (live or stand-alone) and visible columns with their order and size.

TIP

Saving the selected position makes it possible to automatically attach audio for the selected camera.

A workspace created this way can be saved by pressing the **SAVE** button. You will need to enter a name for your workspace before the actual saving process is executed.



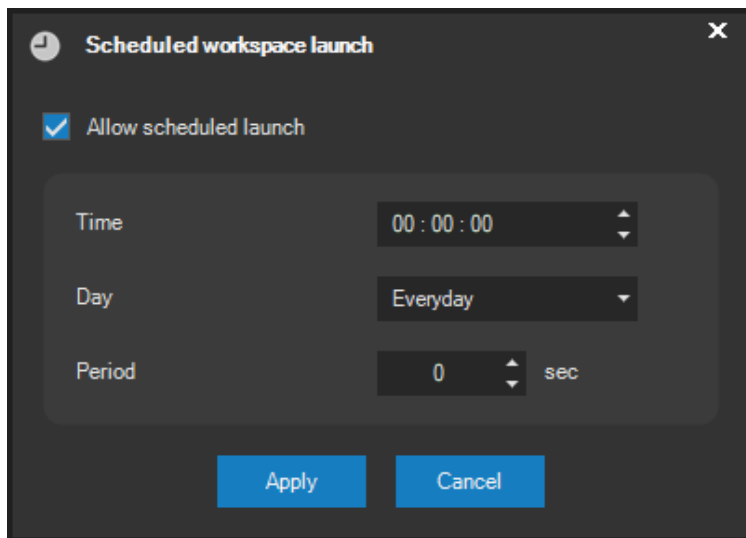
After the workplace is saved, it will appear in the list. You can create and save any number of workspaces. Any workspace can be loaded by pressing the **LOAD** button. Press the **DELETE** button to delete a workspace together including all information saved.

One workspace can be selected as automatic by pressing the **AUTOSTART** button. This means this workspace will be automatically loaded within a few seconds after a successful login. As a result, the application will automatically place all live windows on your monitors, open a map to a corresponding position and switch both local and shared views.

NOTE

To prevent the workspace to load automatically after startup, hold the SHIFT key.

Press the **PLAN** button to call the workspace on time instead of manually selecting it from the menu or from the workspace list by entering the time at which the workspace shall be automatically activated.

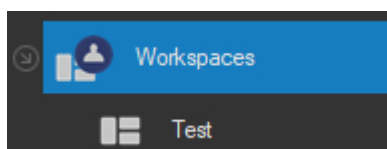


Enabling the Allow scheduled launch option and setting the time automatically activates the workspace at a specific time. You can also configure whether the activation will take place on a daily basis or only on certain days in the week and also the period. If a period is configured (value greater than zero), the workspace will always be activated at a specific time and then repeatedly when the period elapses.

NOTE

The workspace is automatically activated and period restarted at the specified time on the next day configured.

In order to simplify workspace loading, you can display the list of workspaces in the application main menu by checking the checkbox under the list of workspaces.



8.1.7. Auto start options



-  Hold SHIFT to override auto login during application launch.
-  To automatically open local or shared views after login go to workspaces settings.

In the Auto start options section, you can activate the automatic run option after Windows startup and also login as a specific user. Users can activate the automatic login for their own account only and not for other users. The automatic login feature can be abused. This is especially dangerous for a user with extensive rights. The best option is to use the automatic login only for universal users such as an Operator with low user rights.

If there are more user accounts created on a single computer, each user can activate the automatic login option. This will ensure the user currently logged into Windows will be automatically logged into the system.

NOTE

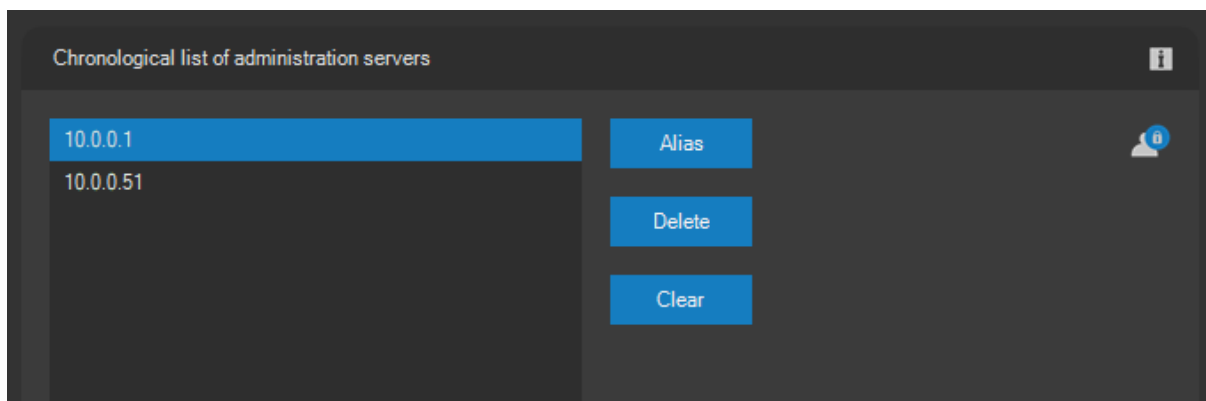
The automatic application startup can be successfully activated or deactivated only by a user who has the rights for editing the Windows registry. After doing so, the setup is valid for any operating system user account.

NOTE

If automatic user login is not successful due to the unavailability of the system administration core, the application will automatically repeat the login attempt in short intervals until the preconfigured amount of login attempts is reached. This process can be cancelled by a manual login attempt in between the automatic login attempts.

The start of the application can achieve complete automation upon integrating the automatic run option after Windows startup, automatic login and automatic workspace loading (see Workspace settings). The client application will be refreshed after all live windows or a map is opened.

8.1.8. Login history



The Login history section displays all camera systems (administration server addresses) to which the client has logged into successfully. The same chronologically sorted list is also displayed in the drop-down list located in the server field upon logging into the system.

If a list item is considered sensitive, i.e. you do not want the next user that logs in to see it, the list item can be deleted by pressing **DELETE**. The entire history can be deleted by pressing **CLEAR**.

Press the **ALIAS** button to define a custom name for an address or network server name for a selected list item. You can use this alias to login to the system in the same manner as you would using the actual address.

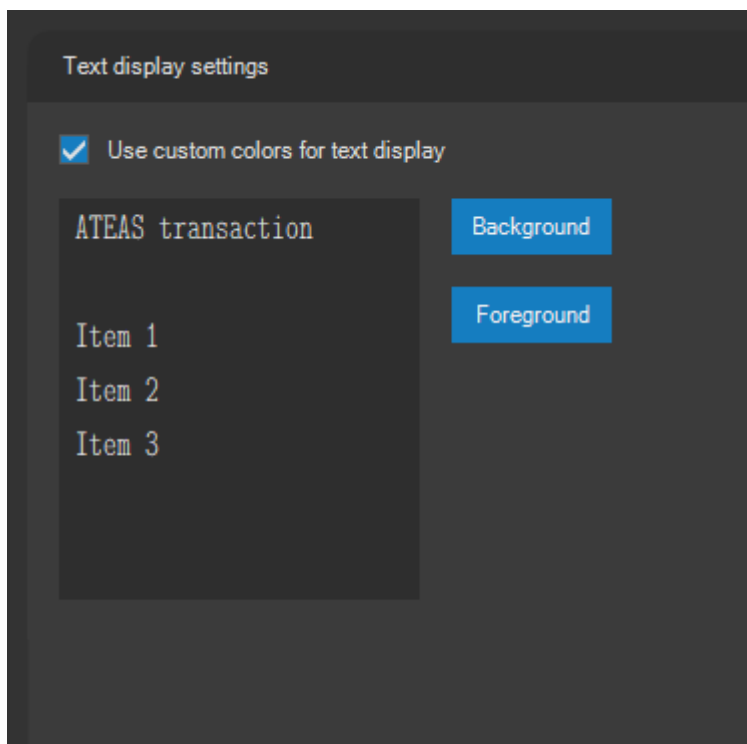
The custom server name (alias) can also automatically be entered during login, provided the alias is entered behind the server address in parentheses. This procedure is also described in the leading chapter about logging into the system.

CAUTION

If an alias is defined that can also be evaluated as a network name, the alias has priority for the evaluation.

8.1.9. Text display settings

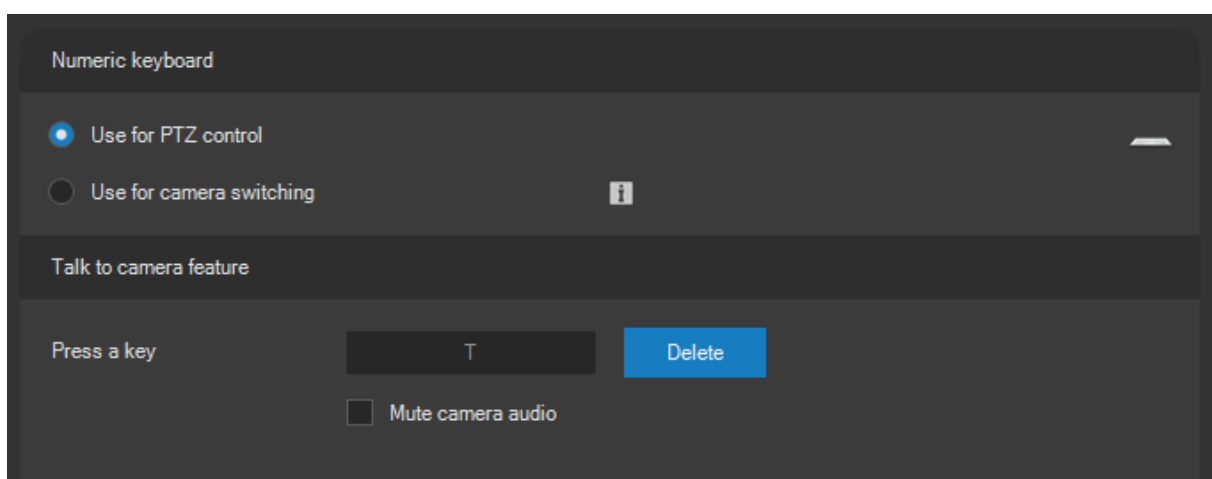
Under Text display settings, you can change the default color scheme for the text data displayed directly in live windows – e.g. transaction data or counters.



The **BACKGROUND** and **FOREGROUND** buttons are used to independently set a custom color for the text window background and the font (foreground).

8.1.10. Keyboard

By default, the numerical keyboard is used as PTZ camera control method. It can alternatively be used to select cameras (for more information, see the Selected camera functions chapter).



The live window contains a button for activating the talk to camera feature. Besides pressing and releasing the button to start or stop transmitting audio to the camera, you can assign this function to

any key under the Talk to camera feature section. When this key is pressed, audio is then sent to the camera, when the key is released, transmission is interrupted.

By enabling the Mute camera audio option, you can also mute incoming audio for the duration of the talking to prevent audio feedback.

NOTE

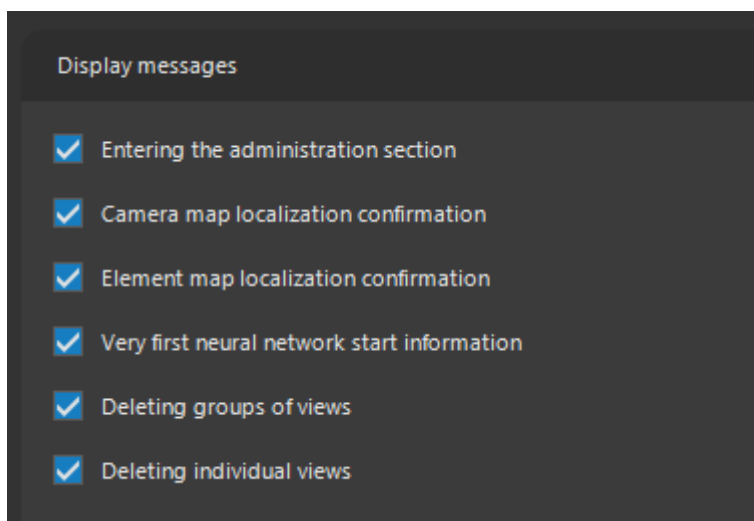
The same result is achieved by double-clicking the talk to camera button in the live window.

NOTE

The keyboard cannot be used for simultaneous transmission of audio to all cameras in the view. This can only be done by right-clicking the talk to camera button.

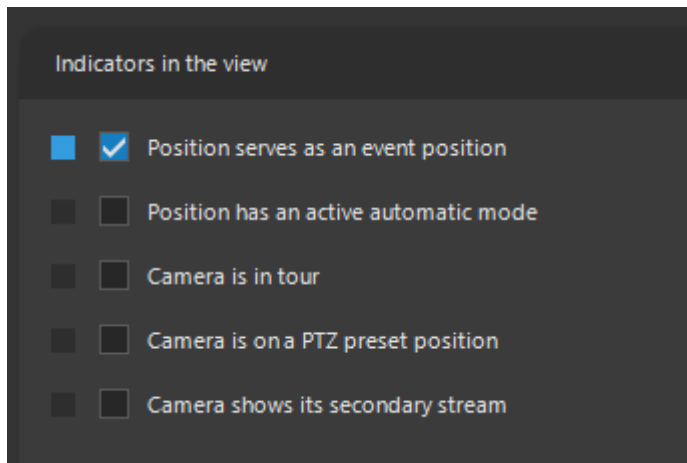
8.1.11. Messages

Some messages shown by the client application while using the system, can be disabled by selecting the Do not display again option. This part of the local settings shows the current display status for each message, as well as the option to enable them again.



8.1.12. Custom indicators

Whereas, in monitoring windows, the system indicators are displayed to the right, custom indicators are displayed at the end of the camera name. Custom indicators provide some smart visual feedback about camera states or view positions that may not be obvious at first glance.



For an active indicator, clicking on the color symbol allows changing its color.

TIP

Besides the color distinction, both the system and custom indicators offer a text description while hovering with the mouse over them.

NOTE

The event positions for receiving events in the view can be created using the view editor.

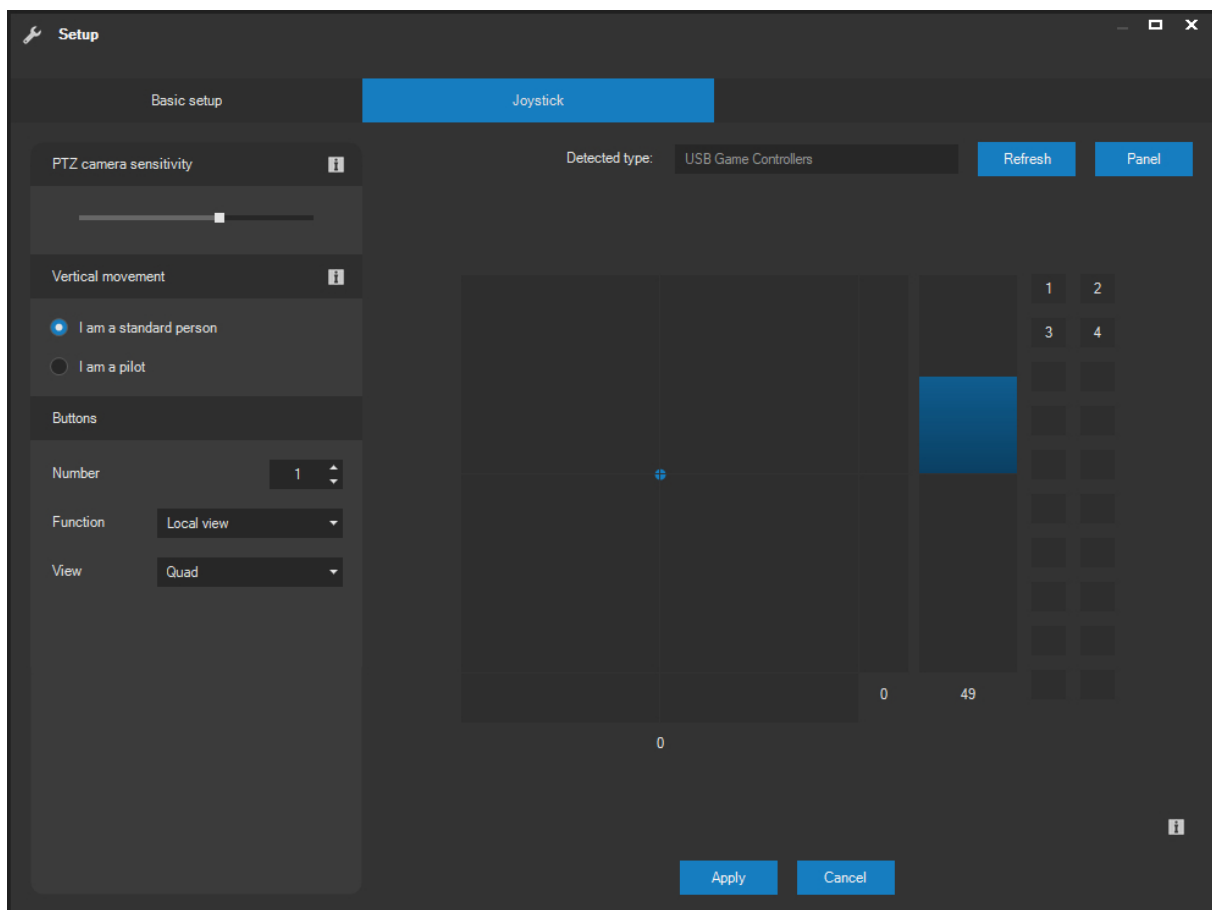
TIP

The PTZ preset indicator is especially helpful when using PTZ preset bound analysis.

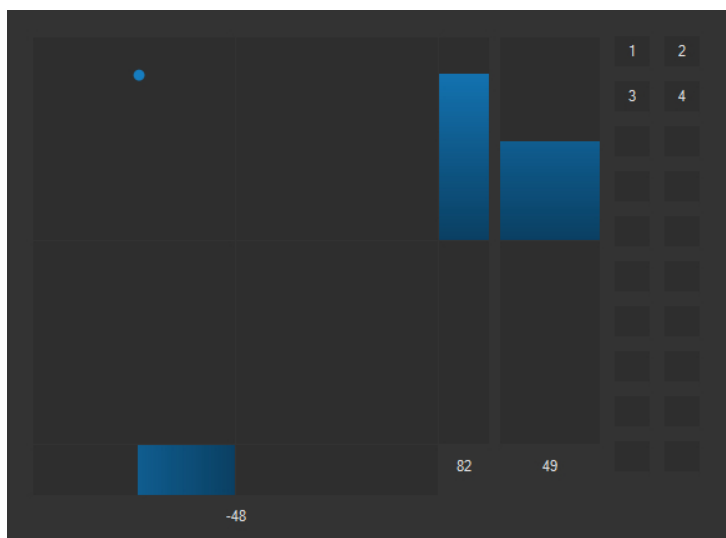
8.2. Joystick setup

8.2.1. Basic setup

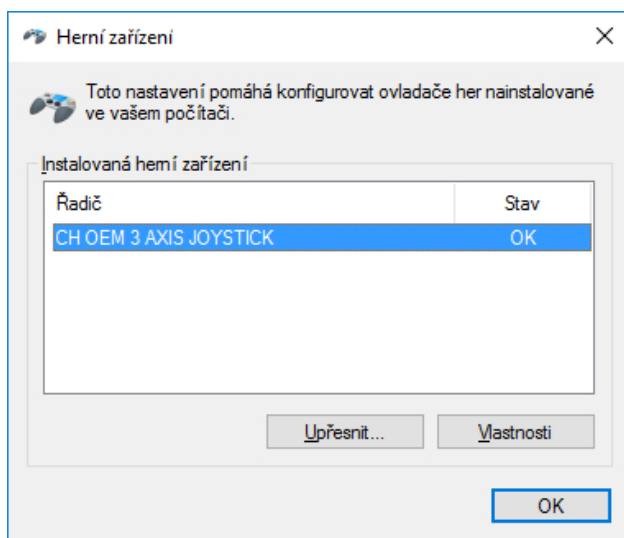
Settings related to joystick behavior can be configured on the **JOYSTICK** tab.



The movement of the joystick in all axes directions can be tested within the black big control area. The name of the joystick is displayed above this control. If the joystick is changed or a new one is added while the setup window is opened, you can obtain the name of the device (joystick) by pressing the **REFRESH** button. A preview for all buttons pressed is also available. These will be used for controlling the zoom of a PTZ device, if the joystick is not equipped with a third axis.



If the joystick can be moved smoothly around the whole perimeter of the square (the X and Y axes) or within the extent of the Z axis column, it will be necessary to calibrate the joystick. This is done in a standard manner, defined for the windows operating system. The list of all joystick devices will be displayed upon pressing the **PANEL** button.



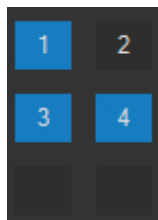
Upon pressing the **PROPERTIES** button, a new dialog will be opened with the **SETTINGS** tab, from which you can run the calibration process.

Joystick sensitivity, which grows by moving the scrollbar towards the right end, can be modified in the right part of the window. All sensitivity adjustments take effect immediately, without needing to save your changes in the setup window. The next available switch adjusts the behavior of the controlled camera while the joystick is moved along the Y axis. The ordinary human being setting makes the camera move up when the joystick is moved forward, the pilot setting makes it move down.

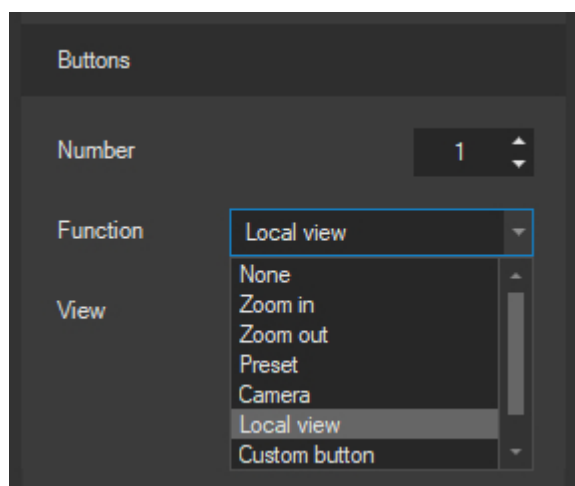
All adjustments made in this window can be saved by pressing the **APPLY** button.

8.2.2. Button functions

If a joystick is connected to a computer, the application will automatically recognize the number of buttons.



Each joystick button can be assigned a certain predefined function for controlling the active live window. As the following picture shows, you can select from several options.



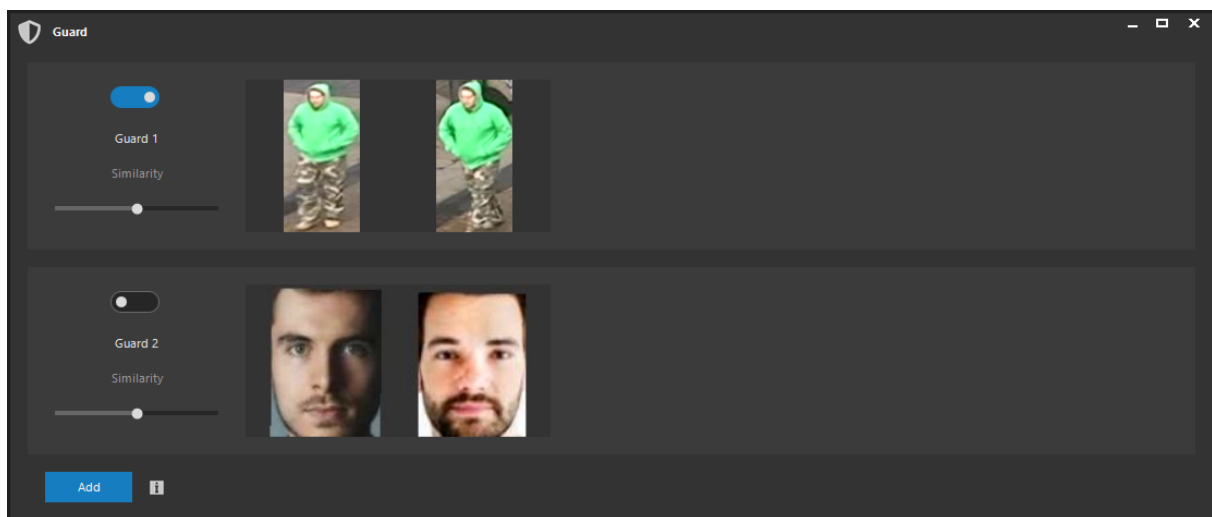
- If the None option is selected, the joystick will not have any function assigned.
- The Zoom in and Zoom out functions control the zoom of PTZ devices. Assigning these functions to the joystick buttons might be necessary especially if your joystick is not equipped with the third zoom control axis.
- By selecting the Preset option, the button will work as a fast selection of a PTZ device preset point. If this setting is active, the button number always corresponds with the preset number. The number 2 button will make the selected camera switch to preset point number 2 and so on.
- The Camera option will invoke a detail view for the selected camera in terms of the current live window. The camera has to be selected via the camera server and specific camera option.

- The Local camera option is similar to the Camera option. It enables performing a quick switch to the whole local view consisting of any number of cameras. The corresponding local view must be selected from the list.
- The Custom button option enables assigning a custom button to a selected joystick button. The joystick button will then have the same function as the paired custom button.
- The Switch zoom / focus option enables the user by pressing a joystick button to specify the third axis (Z) function, which will be used either for zoom or focus capability for the selected camera.

Chapter 9 - Additional tools

9.1. Live guard

The Live guard feature is a way for the user to create an alarm situation monitor creating real time notifications if alarms occur. This applies e.g. for visual similarity triggers for different kinds of objects like a face or a person based on the analysis of corresponding neural networks. This feature is available in Tools in the application's main menu.



You can use the **ADD** button to create new guards up to the maximum amount. Use the context menu and the Paste option on any particular position in a guard to insert an object to guard for. You can copy objects in the face bar in the live window or in the smart search tool.

You can activate a guard by activating the switch above the guard's name.

NOTE

In contrast to system events, any notifications created by the guard are only presented to the user, who created the guards.

The guard can be renamed by double-clicking its name and can be removed by using the cross symbol button that appears when hovering with the mouse over the guard.

Using the Similarity control, the required similarity level for any positive visual search matches can be decreased or increased. The lower the similarity, the more false notifications can be produced by the respective guard.

9.2. Custom buttons

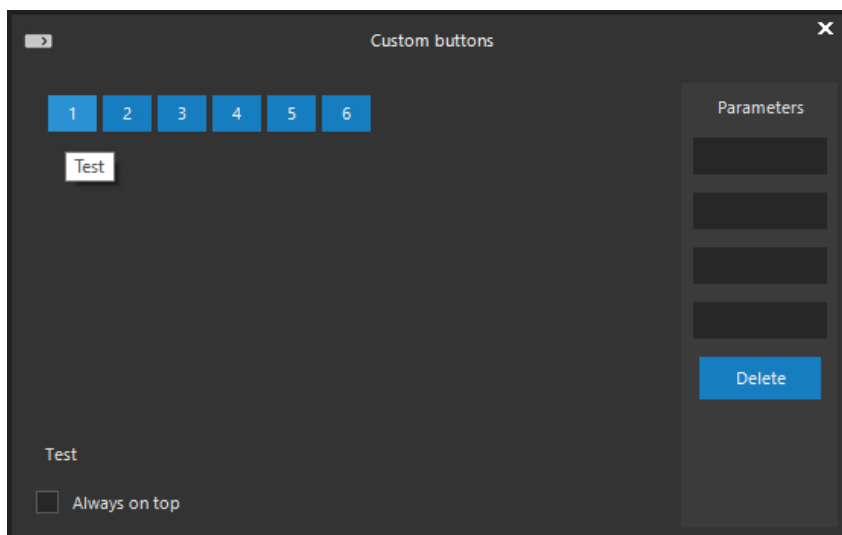
The administrator can create custom buttons within the system. Custom buttons can be used to execute custom actions or commands using the http or https protocol and can e.g. activate some extended device features or control a great variety of external devices. The window containing custom buttons can be opened directly from Tools in the application's main menu.

NOTE

If the administrator has not created any custom buttons in the system, the application will respond with a warning message and the user will not be able to continue.

NOTE

If you do not have the rights to use custom buttons in the system, the application will respond with a warning message and you will not be able to continue.



The buttons can either be configured to show their numbers with their text description shown in a tool tip or they can show the texts directly, in which case the size of the buttons is automatically increased.

Clicking on any random button will automatically start the pre-set action. Users do not have direct access to http commands linked to the given action nor to authentication data, which could be required to execute the given command. Hovering over individual buttons will display the description of the action, defined by the administrator, which should sufficiently characterize the action. The description is displayed in both the text row labeled Description and as a tooltip above the button.

NOTE

If the system administrator configures certain user buttons to act as switch buttons, these buttons will remain pressed after pressing them once and will become released after pressing them a second time. Various actions can be activated upon pressing or releasing the buttons.

NOTE

Some buttons configured as switch buttons may automatically be pressed when the custom buttons window is opened for the first time or when it is already open, because other users have activated these buttons.

If the administrator added special characters into the command to support parameters (see the system administration chapter for more information), the user can change the resulting command by entering concrete values into the text fields labeled Parameters.

Checking the Always on top checkbox will allow you to switch the window to the state in which it cannot be overlapped by any other windows in the system, and users will always have this window in their view.

NOTE

If the command created by the administrator does not contain any parameters, entering them on this window does not have any effect.

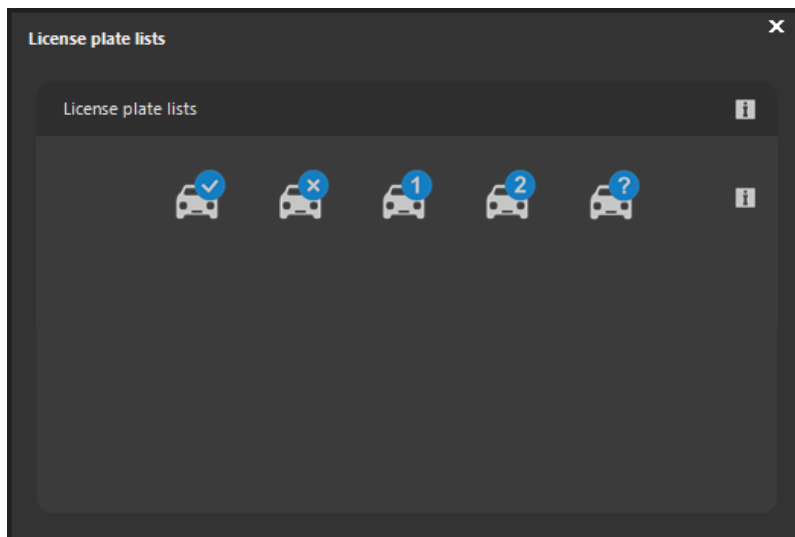
NOTE

The custom buttons window can be saved together with the workspace and opens to a specific point automatically when loaded.

9.3. Plate lists

Provided the user has been granted the Additional event features permission, he can use the Tools submenu of the application's main menu to open the window with vehicle license plate lists.

All LP lists can be edited using the respective buttons, plates can be added, removed or tested if they appear on a list already. Working with the window and the LP lists is the same if it is performed from the system administration section, where it is described in the Working with LP lists subchapter.



Chapter 10 - Web access

10.1. Running the web client and login

A web browser with full HTML 5 support can also be used to access your cameras. In order for the web client to work correctly, your browser should fully support even the latest HTML 5 extensions and other relevant standards including e.g. H265 video format support.

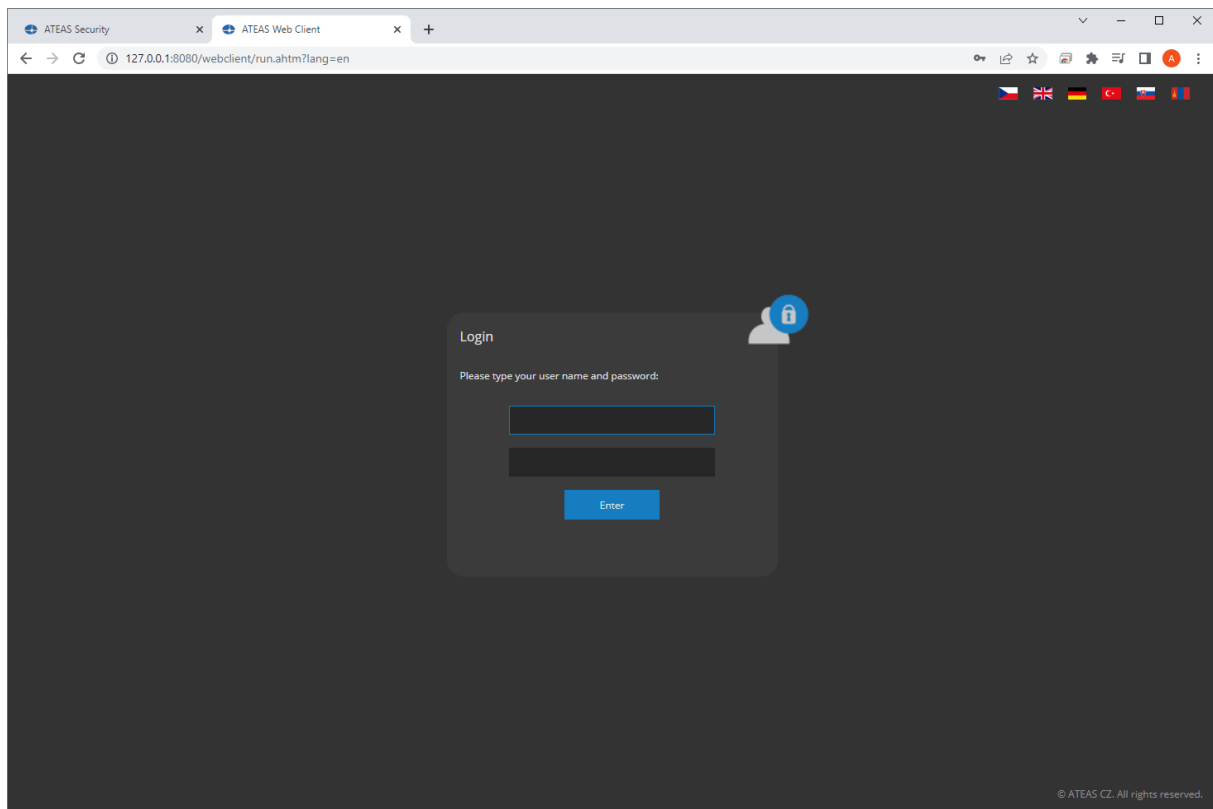
NOTE

ATEAS Security web client access is based on the HTML 5 standard, therefore installing any web content plug-in and technologies such as Flash, Silverlight or ActiveX is not required.

The web client can be launched directly via the link on your administration server webpage or by directly entering the address into your browser. This address contains your administration server address followed by /webclient/, e.g. <http://127.0.0.1/webclient/>.

NOTE

Based on the configuration performed by the system administrator, you can be automatically redirected to the secured http protocol version. The address will then begin with https://.



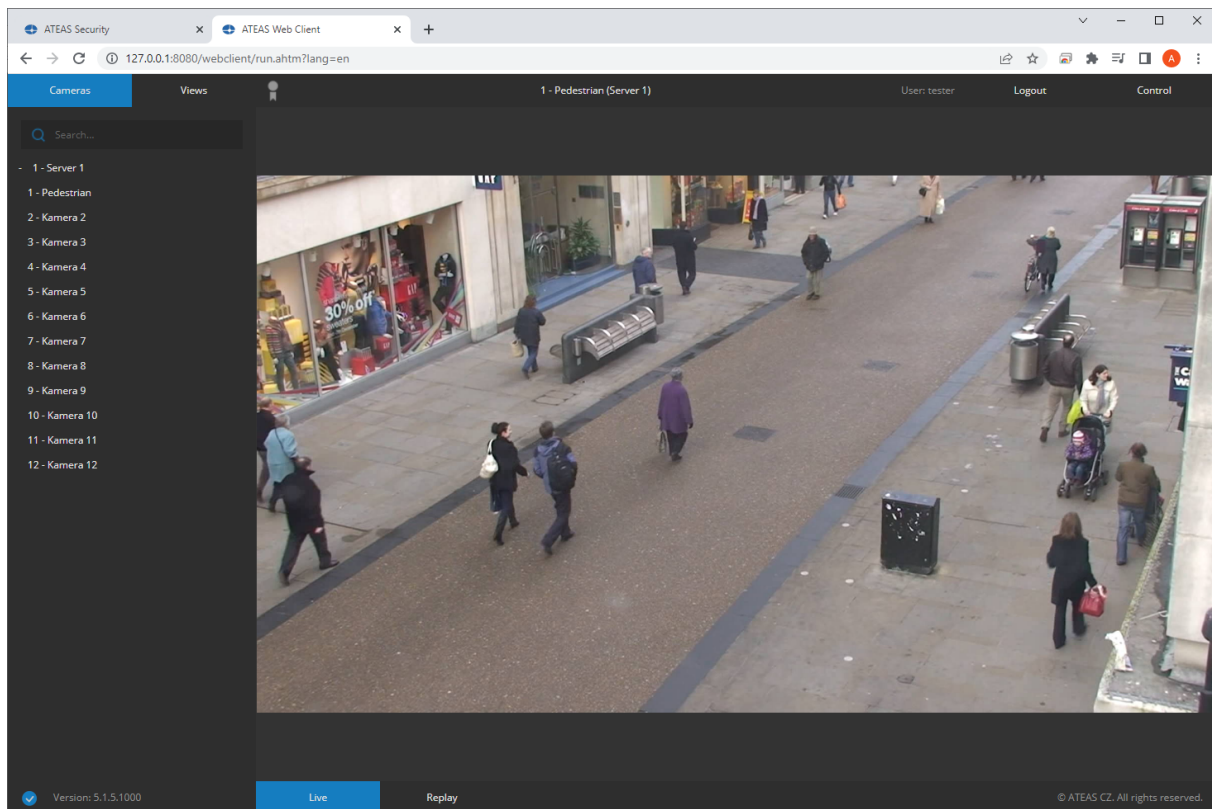
You can login to the system from the start page. The same rules apply for entering your username and password as when you login using the standard ATEAS client. The flag icons in the top right corner of the window can be used to change the preferred language.

NOTE

If your user account is being used for the first time or your password was reset or expired, you will be prompted to enter a new password exactly as it would be the case in the standard client. The system administrator determines the password length and strength for your password to be accepted.

10.2. Live view

After logging in to the system, you will automatically be connected to all camera servers to which you have been granted access, and all cameras (and camera views) will be available based on your camera system permissions.



The tree structure of camera servers and all cameras assigned to them is displayed on the left side of the window. You can switch between the tree structure of servers and views using the Cameras and Views tabs. Views can be organized in groups by the administrator and can consist of many cameras. By selecting any item from the tree structure you can display the live video stream from the selected camera or group of cameras in the view.

You can search for servers or cameras by using the search text field placed above the tree. It is possible to enter multiple words; phrases containing spaces can be entered surrounded by quotes.

NOTE

As in the standard client, secondary frame rate is used for all video streams in a multi-camera view and primary frame rate is used for a single camera stream. The system administrator can configure these frame rates for each camera individually.

NOTE

Despite staying at the address of your administration server while working with the web client (e.g. your headquarters), individual connections to camera servers are always established using the shortest route possible and video data will be transmitted directly from the camera server (e.g. directly from your local branch).

The top control panel contains the Menu link, which can hide or show the tree structure to enlarge the video area. The Control link works in a similar way and shows or hides the panel with additional functions on the right side of the window.

Besides these links, the top control panel also contains a grey or bold certificate icon. Clicking on this icon displays information about the end user and installation partner. In case of a certified installation partner, the icon is bold. This information is identical to the information displayed by the standard ATEAS client. More information can be found in the Certified installations chapter.

The top panel also contains the name of the camera or view currently displayed, the name of the user currently logged in, and a link to log out of the system.

The bottom control panel indicates the status of the administration server connection, displays the system version and contains links for switching between live view and recordings.

10.3. Selected camera functions

In single camera view, which we can achieve either by directly selecting the name of the camera from the tree structure of servers and cameras or by clicking into the video of any camera within a multi-camera view, you can perform additional functions for the camera that is currently selected.

NOTE

The primary frame rate is automatically applied when switching from multiple camera view. The resolution may also be automatically adjusted (depending on the configured camera detail offset value).

PTZ control and presets

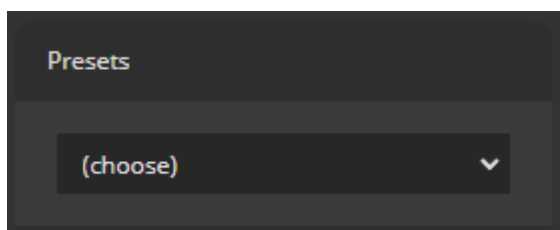
If you are working with a PTZ camera and have the necessary permissions to control this camera, you can touch or press and hold the mouse button to control the camera. The direction of the camera movement is defined by the direction of the mouse cursor position from the center of the video. The distance between these positions determines the speed.

You can easily control the camera zoom by scrolling the mouse wheel.

NOTE

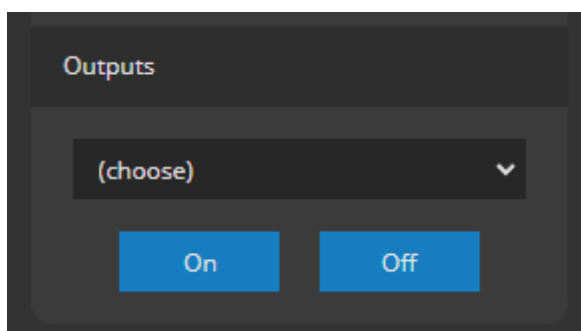
Whether you will be able to control a camera at a given time is also tied to your PTZ priority configured for the selected camera. Users with a higher PTZ priority can take over or lock the PTZ control of the camera.

Forcing the camera to a preset position is possible by selecting a preset from the drop-down list in the control panel located in the top right part of the window, which can be displayed or hidden using the Control link.



Output activation

If the selected camera has outputs connected to various external devices, it is possible to activate or deactivate these devices via the web client using the buttons in the control panel located on the right side of the window.



After selecting an output from the drop-down list, you can activate or deactivate the output by pressing **ON** and **OFF**.

Saving a snapshot

Pressing the Take shot icon located in the bottom part of the control panel on the right side of the window saves a snapshot of the currently displayed live or recorded video in JPEG format.

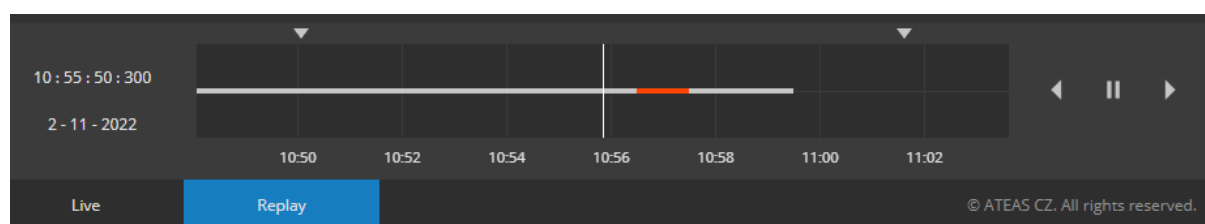
NOTE

Based on how this function is supported by your browser, the results of saving a snapshot may vary. For example, a new browser tab can appear displaying the saved snapshot, which you can then manually save, or the snapshot is automatically downloaded to a predefined browser folder.

10.4. Working with recordings

10.4.1. Replaying recordings

The Live and Browse links can be used to toggle between live and recorded video saved in media stores of the server. After switching to recordings, the timeline will appear under the video for the selected camera. The timeline shows the available time segments during which standard recording took place (white color), event recording took place (red color), or no recording took place (no color).



The timeline can be intuitively shifted by a touch movement or by dragging with the mouse. Video content is immediately and smoothly synchronized while the timeline is being moved. The current date and time of the recordings is displayed to the left of the timeline. Buttons for starting the replay backwards, forwards and for pausing the replay are displayed to the right.

The timeline resolution can be adjusted using the mouse wheel from displaying weeks down to displaying 30 second intervals.

10.4.2. Exporting recordings

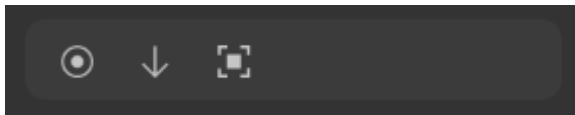
You can specify an export interval by moving the arrows displayed above the replay time axis. The selected time interval will be exported on the server and made ready for download followed by downloading the file in mp4 file format supporting both video and audio.

NOTE

The export interval must be in the range of five seconds and 30 minutes.

10.5. Client settings

The bottom part of the web client contains a configuration panel with some additional settings for live and recorded video with features as follows.



Besides the basic features, video upsampling can be activated. This refers to enlarging the video to a size larger than the native video resolution, provided the web client has enough space to enlarge the video.

NOTE

This setting can be beneficial on monitors with very fine resolutions (e.g. Retina displays), where a video with native resolution could appear small.

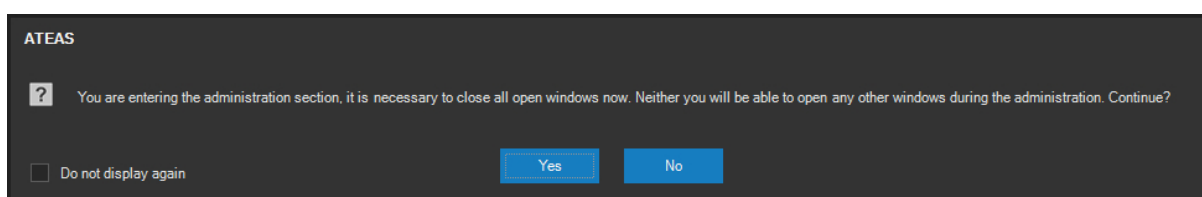
NOTE

A correct aspect ratio is always preserved even with video upsampling activated.

Chapter 11 - System administration

11.1. Entering the administration section

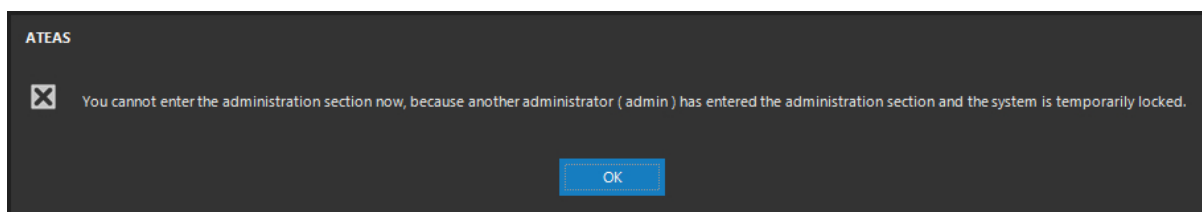
The system administration section of the application (i.e. all items of the Administration main menu) can be accessed by users defined under the administrator group only. Any user who is in the common user group cannot access the administration section. The following message must be confirmed prior to entering the administration section.



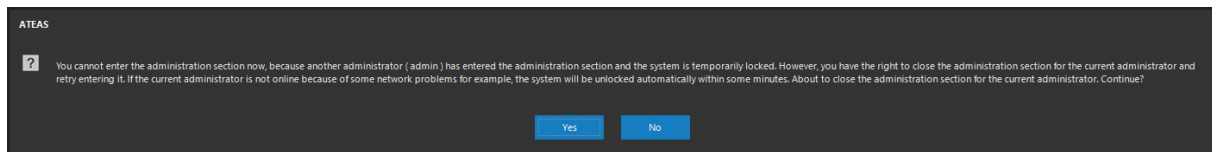
NOTE

If you do not want the client to display this message each time the administration section is entered, check the option in the bottom left corner of the window. Messages can be enabled again in the client's local settings.

When working with administration windows, no other windows can be opened except for the map window. Any number of users and administrators (according to the license number) can be logged into the system. However, only one administrator can access the administration section at a time. If another administrator attempts to enter the administration section, access will be denied and the following warning message will be displayed.



The only exception to this is the master administrator, i.e. the administrator account with number 1, the specifics of which are described in detail under the user administration subchapter. The master administrator is authorized to force access to the administration section despite the fact that another administrator is in the section at the given time.



Upon confirming the message dialog on the previous picture, the administration section of the other administrator will automatically close and access will be blocked for several seconds, making it possible for the master administrator to gain access to the administration section for himself.

In both cases mentioned above, the message contains the name of the administrator who has entered the system administration section.

Although the administration section can only be entered by one administrator at a time, privileged users with the corresponding permission are allowed to simultaneously configure certain system settings, e.g. camera preset points or do some more complex configuration like updating the motion detection or video analytics event source settings.

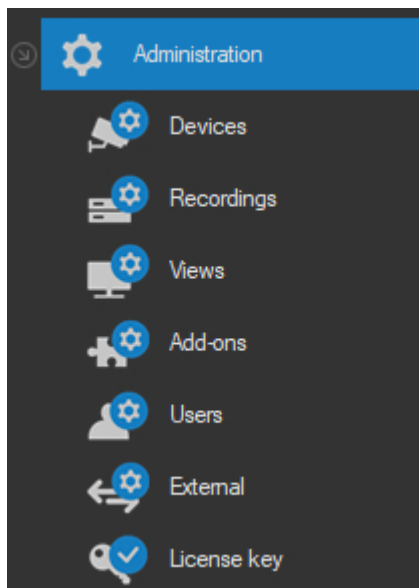
NOTE

During system administration, other clients can continue working without any restrictions. Certain changes, such as adding or removing cameras, are applied online.

CAUTION

The system enables remote management. If, for example, a network problem occurs during the system remote management and the application is disconnected, the administration section will not be reachable until the guard delay lapses (several minutes).

The administrator can switch between individual administration sections directly by selecting the application main menu items.



11.2. Camera management

11.2.1. Automatic camera discovery on the network

After selecting the Devices item, a window will be opened where the user can add and remove cameras or video servers to or from the system. All cameras are always connected to the system through a camera server (ATEAS Server), responsible for recording or evaluating events. Before the actual process of adding or removing cameras is executed, you must select the corresponding server from the Camera servers list for the given operation.

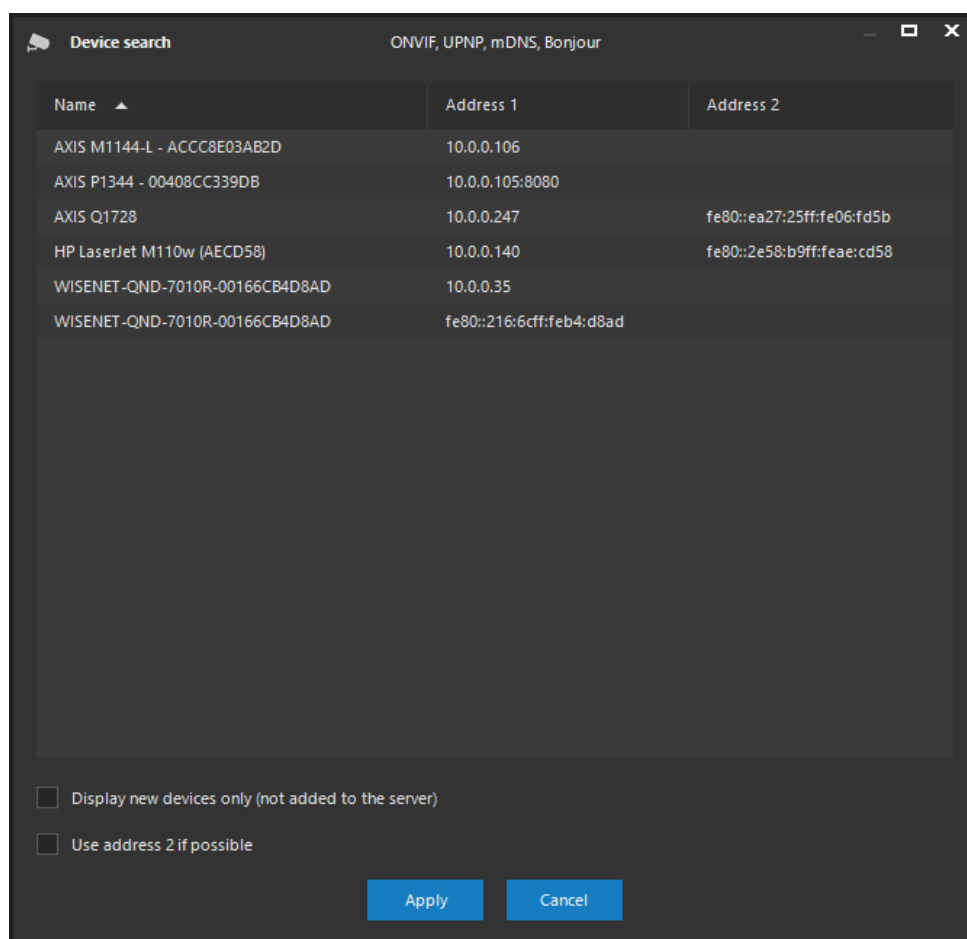
CAUTION

In all editions of ATEAS Security, you must add at least one camera server to the system for the given camera operations. Adding camera servers and assigning user profiles to them is done in the Users section, described further in this chapter.

Adding cameras to the system is very fast and simple, and it can also be performed as a batch operation and in automatic mode. Individual addresses or camera names can be entered manually or can be searched. The **SEARCH** button, located in the Add camera section, is used for searching devices. After the button is pressed a window is displayed containing the detected devices.

NOTE

The automatic discovery feature of cameras in the local network is available for all devices that support the following standards: ONVIF (WS Discovery), UPNP (Universal Plug and Play), or mDNS (multicast DNS, Bonjour).



The list of detected cameras contains the manufacturer code and model of the camera and its network address. The list is automatically and continuously updated with newly detected cameras. Some cameras may have two different addresses displayed by them (this can, for example, be an IP address obtained from the DHCP server and the APIPA address).

You can select multiple cameras that will be added to the camera server in the next step. Multiple selections can be made in standard fashion by repeating the mouse selection process while holding the CTRL or SHIFT key, as well as by dragging the mouse. By pressing the **APPLY** button, the addresses of all cameras selected, separated by a semicolon, are transferred to the Name field in the

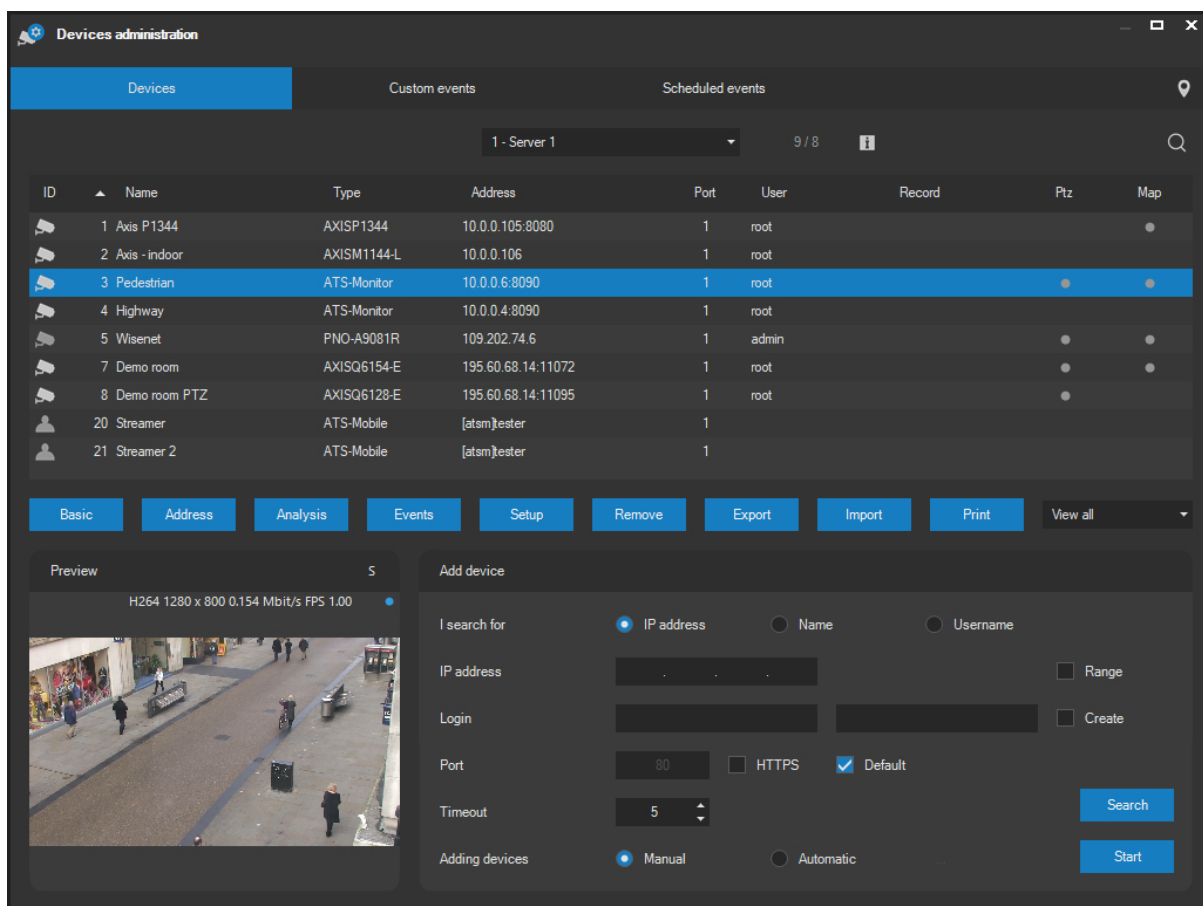
Add camera section within the basic administration window, where the cameras can be immediately added to the system via the **START** button.

By checking the Display new devices only option, the list of cameras can be effectively narrowed to only display cameras not yet added to the currently selected camera server. This can save time immensely when adding newly installed cameras to the system.

CAUTION

For the UPNP search to work correctly, the SSDP Discovery service must be enabled in the system while the ATEAS Server service is starting. For the Onvif search, however, the Function Discovery Resource Publication service should be disabled, as it may interfere with the Onvif search.

11.2.2. Adding and removing cameras in the system



The screenshot displays the 'Devices administration' window. The 'Devices' tab is active, showing a table of cameras. The table has columns for ID, Name, Type, Address, Port, User, Record, Ptz, and Map. The third row, '3 Pedestrian', is highlighted. Below the table, there are buttons for 'Basic', 'Address', 'Analysis', 'Events', 'Setup', 'Remove', 'Export', 'Import', 'Print', and a 'View all' dropdown. On the left, a 'Preview' section shows a live camera feed. On the right, the 'Add device' panel is open, showing search options (IP address, Name, Username) and fields for IP address, Login, Port, Timeout, and adding devices (Manual, Automatic). A 'Search' button and a 'Start' button are at the bottom right of the panel.

ID	Name	Type	Address	Port	User	Record	Ptz	Map
1	Axis P1344	AXISP1344	10.0.0.105:8080	1	root			
2	Axis - indoor	AXISM1144-L	10.0.0.106	1	root			
3	Pedestrian	ATS-Monitor	10.0.0.6:8090	1	root			
4	Highway	ATS-Monitor	10.0.0.4:8090	1	root			
5	Wisenet	PNO-A9081R	109.202.74.6	1	admin			
7	Demo room	AXISQ6154-E	195.60.68.14:11072	1	root			
8	Demo room PTZ	AXISQ6128-E	195.60.68.14:11095	1	root			
20	Streamer	ATS-Mobile	[atasm]ester	1				
21	Streamer 2	ATS-Mobile	[atasm]ester	1				

A list of cameras that are currently assigned to a selected camera server can be found under the drop-down list. You can add new cameras to the system via the Add device section. The following data is displayed for each device in the list:

- camera ID (unique for each specific server),
- device name,
- device type (or the video server type),
- IP address,
- port (1 by default, can be higher for multiport video servers),
- user name for camera login,
- currently assigned recording rule,
- information whether the device is a PTZ device,
- information whether the device is located in the map.

You can filter the list of cameras according to the connection type using the dropdown list to the right of the list of servers. Searching can be performed after pressing CTRL-F or the corresponding search button located above the list.

The number of cameras currently allocated to the selected camera server is displayed above the camera list. The number of cameras pertaining to the camera license is listed in brackets with the prefix "lic" These numbers can differ, providing a camera is added multiple times to the camera server. See further in the text for more information on this configuration.

ATEAS uses an IP endpoint based licensing model meaning that a device with one IP address will always consume just a single camera license (including the option of adding the device multiple times). This is also true for special cameras with multiple video sources or video encoders with multiple video ports.

NOTE

If multiple devices share one IP address (and therefore use more network ports) multiple camera licenses will be consumed.

A video preview is additionally displayed for the currently selected camera. All columns of the camera list can be used for quick camera classification. By clicking the column header, the camera list is shown in ascending order according to values contained in the column. By clicking again, the list is shown in descending order.

The video preview automatically displays statistical data about the codec, resolution, frame rate and bandwidth of the video stream. If configured, the secondary stream can be previewed by activating the S symbol in the preview window.

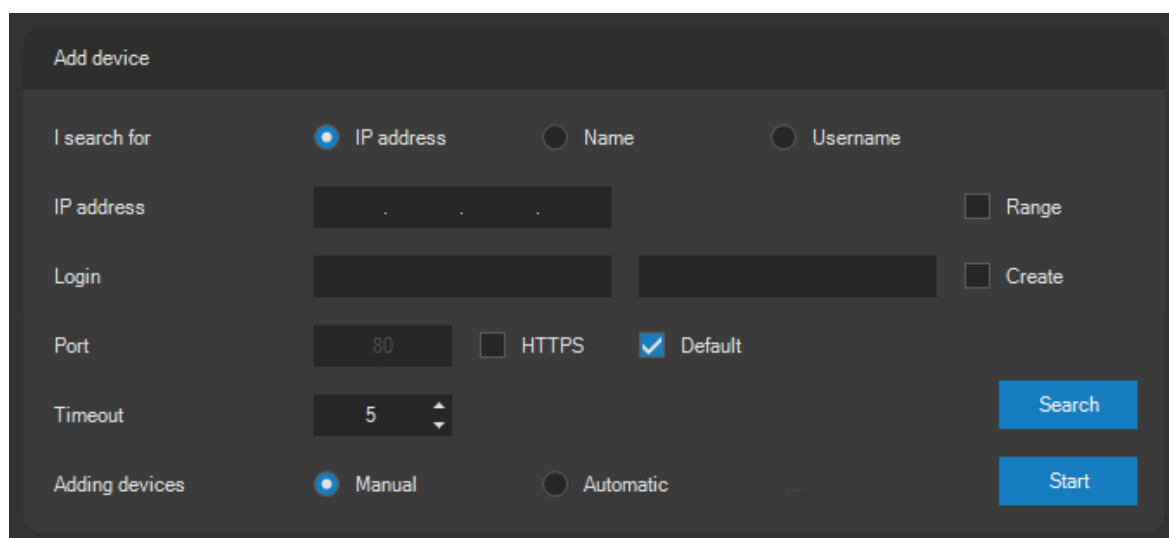
TIP

The same data can also be displayed for all cameras in the view using the SHIFT-S key combination.

The first column in the camera list with the camera ID also contains a camera symbol designating the connection type (proprietary camera interface, Onvif, RTSP only). Other video sources like mobile devices (e.g. smartphones with Android or iOS operating systems) or body worn cameras present a user symbol instead.

Adding a device to a selected camera server

The required data must be entered in the Add device section.

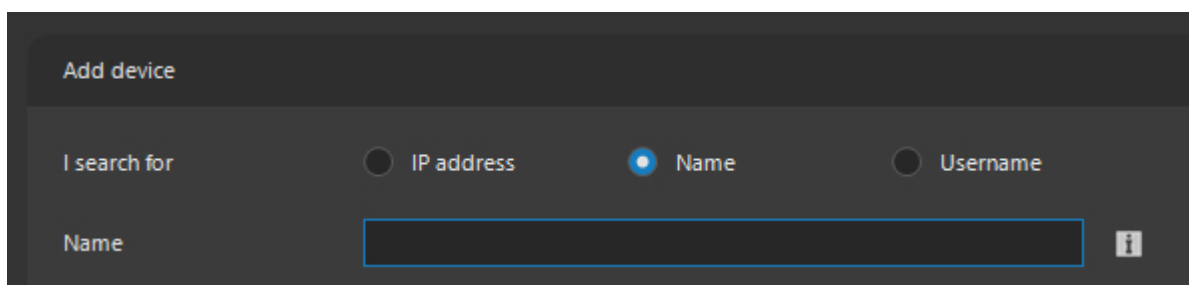


The IP address of the device being added must be entered in IP address field. If you wish to add more cameras, you can do so by checking the Use address range option. This way, an additional IP address field will appear. When adding cameras, the application will detect all IP addresses for the entered range from lower to higher addresses.

NOTE

If a specific range of IP addresses, defined by two addresses, is looked through, the addresses can only differ in the ending number, otherwise the adding process will not be started.

A camera can alternatively be assigned to a camera server by entering the camera name. If you check the Name option, the current IP address field will be replaced by a text field for entering the camera name.



The name entered must not include protocol specification (http). The camera server also supports DNS system (Domain Network System) name searches and translates them into IP addresses. However, the device name always stays in the server database. The system supports dynamic address assignment to end devices by using device names. If devices are added according to their IP address, you can add multiple cameras by specifying the address range. If the camera is added according to name, you can add multiple devices by entering a semicolon between their names or IP addresses.

When adding a camera by name, you can also enter the address beginning with the rtsp:// protocol. In this case, the RTSP video and audio stream will added directly using the given address, which does not require native or Onvif device support.

Another accepted protocol, when adding a camera by name, is the file protocol. With the file protocol a folder can be added that is accessible for the camera server (e.g. a folder on a local drive of the server). Any media content in ats or mp4 file format inside that folder will be streamed automatically emulating a real video and audio source. Files will be streamed in alphabetical order, after the last file has been reached, streaming will continue with the first file.

Each camera added with the file protocol is automatically assigned some outputs, especially to move backward or forward in the playlist or to pause or play the current file.

NOTE

Some ats or mp4 files cannot be streamed. This applies especially to multi-camera ats files or mp4 files with fragments or ctts atoms.

TIP

If a password protected ats file should be streamed, you can add the folder with the correct password or change it later.

It is necessary to enter a valid user name and password into the Username and password fields, in order to login to a camera or video server (if authentication is required). The camera server will use this data to access a camera, and it will not be visible for any user. Onvif devices also offer the option to create an administrator's user account for the camera upon adding the camera to the system for the first time.

NOTE

It is appropriate to use administrator level login credentials to ensure camera server access to all functions of a camera or video server.

If a camera is set accordingly, or if the camera server accesses the camera through a NAT-enabled router, you can enter a port number into the HTTP port field, different from the default number (80).

NOTE

If you add cameras according to name and the port is also part of the name, the port within the name will have priority over the port selected in the HTTP port field.

By activating https, the camera will be added directly using a secured connection. In this case, the camera must be capable of communicating via the https protocol.

NOTE

If the camera is added with https activated, the Use HTTPS option will be activated in camera configuration automatically. Moreover, the preferred RTSP scheme will be set to RTP (HTTP, TCP) because the https protocol automatically presumes the use of http.

The last option on the I search for row is the Username option. If we add a camera to the system via username, this user will be able to transmit video from his mobile device to the system, provided the device (phone, tablet) is equipped with a camera. This feature can be suitable for archiving video data from mobile devices used by security workers in the field and to support the decision-making process of the operator. More information about this feature can be found in the chapters covering individual mobile clients.

NOTE

When adding mobile cameras, entering credentials is not necessary, authentication is naturally performed by users logging in from the mobile app.

NOTE

Once the mobile camera is added, it can be used just as any other camera in the system. Thus, you can, for example, change the resolution, set a different video compression value from the default value or activate audio (in this case, audio from the mobile device's microphone will be transmitted along with video).

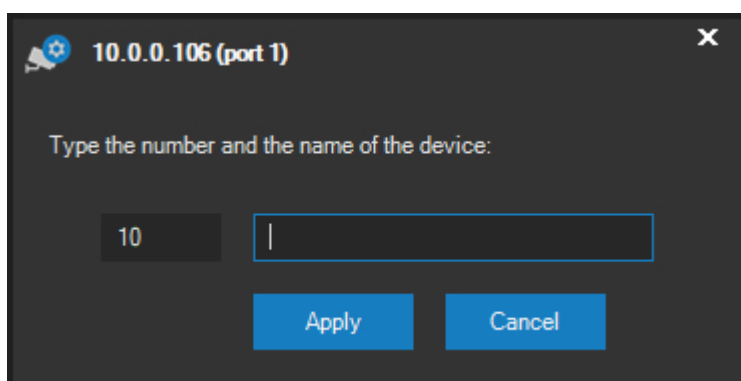
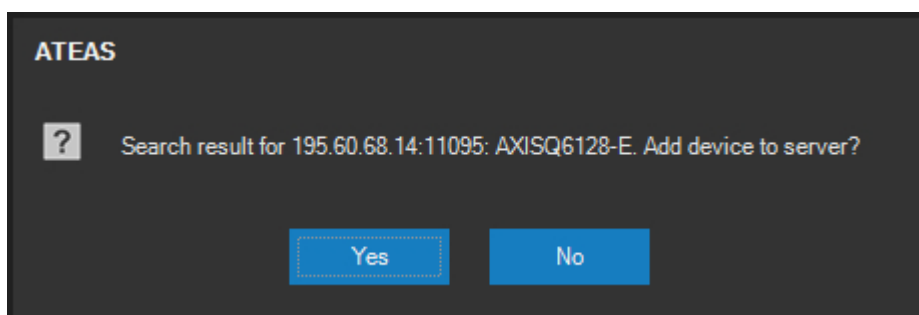
At the same time, the operator can monitor video from multiple mobile phone cameras. In a real-world situation, however, the important moment is when the mobile device user starts transmitting, for this could represent an important circumstance. The start of transmitting can be very easily linked to event management by creating a custom event named MOBILECAMERA on the respective camera server and activating the monitoring of this event for the given camera using the scheduler. Once transmitting starts, the configured event scenario is run as usual. In the easiest of cases, for example, the video from this camera is automatically displayed on the operator's monitor.

NOTE

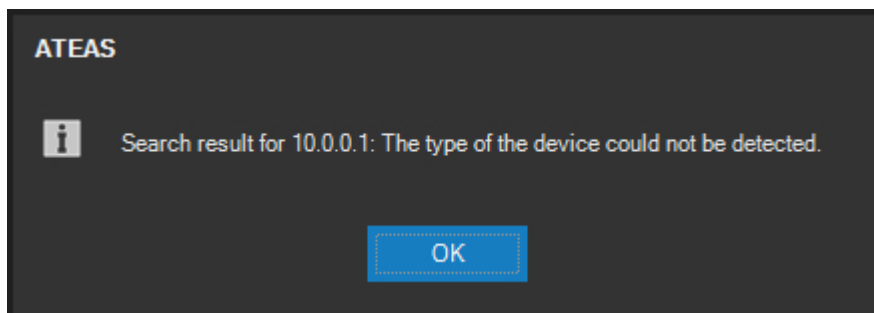
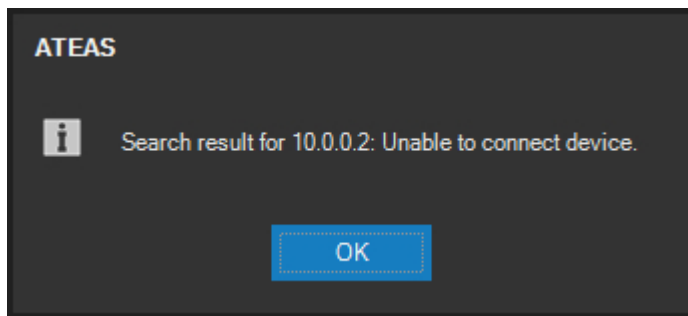
Using cameras from mobile devices is available starting with ATEAS Security PROFESSIONAL edition.

When adding manually, the detection result for each IP address will be displayed, as well as a confirmation for adding the camera, its number and name and a result message of the addition. When adding manually, a free camera number is suggested, equal or greater than 1 or the configured initial camera number in the adding options dialog.

The camera adding process has to be started by pressing the **START** button. All parameters can be set to default by pressing the **RESET** button. You can press the **STOP** button at anytime, when searching through a network segment and adding cameras found, to stop the search process.



A connection timeout (using the value from the Timeout field) or an unknown device type situation can occur while detecting an IP address. In this case, you need to verify device availability on the given address.



When adding a camera manually, verification is always executed to ensure that the entered camera number is not duplicate. The application does not accept a camera number that already exists in the system.

NOTE

Camera numbers can be assigned from the range 1 – 999 with the maximum number of 999 cameras per one server.

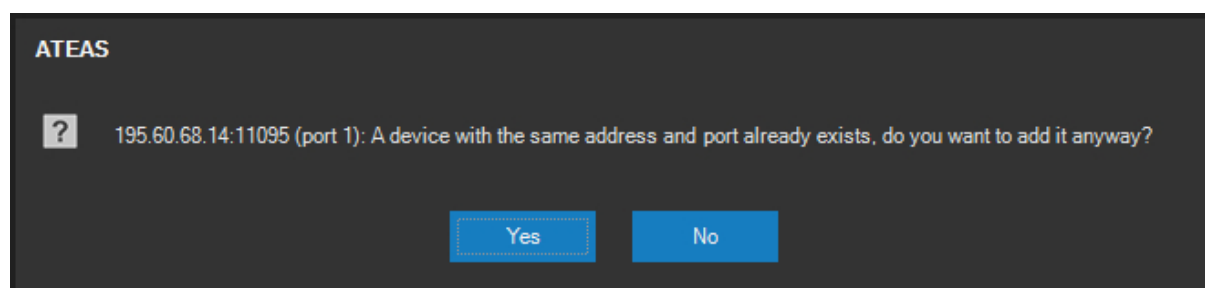
NOTE

Once the process of adding cameras is complete, all newly added cameras are automatically selected, allowing the user to immediately continue with their configuration.

ATEAS Security features such as flexible data flow adjustment to network conditions make it possible in most cases to cope with defining a single video format and its configuration for each camera, while ATEAS servers modify the distributed frame rate to clients (see primary and secondary frame rate concept) including multicast video redistribution. To further increase flexibility, cameras can be added multiple times to the server.

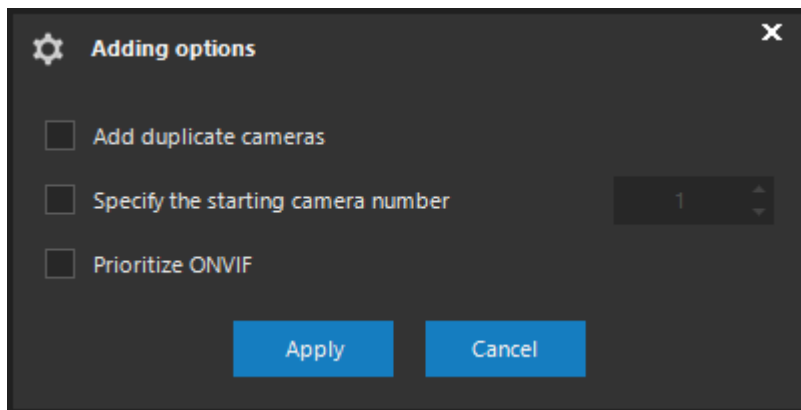
Additional camera licenses are not used for multiple additions of the same camera or video server to one camera server. Therefore, if a device with the same address or network name is added to the system more than once, only one camera license will be occupied.

The configuration mentioned above is achieved by adding selected cameras to the camera system more than once (the number of times is unlimited) and each camera is then configured differently. A warning message is displayed, when manually adding a camera that is already connected to the camera server, just to make sure the camera is not added unintentionally.



If a multi-port video server is detected on a specific IP address, the camera will be added interactively for a specific video server in the amount corresponding to all ports, i.e. up to four new cameras can be added to the system when using a quad-port device. However, this only concerns multiple port video servers, which work on one IP address.

No interactive communication with the administrator is in progress during the process of automatically adding a new camera. A specific IP address (or eventually the whole range) is scanned. After successful camera detection, the camera is automatically added to the system and assigned the first free camera number and default name. This name can be changed anytime later. When adding cameras automatically, cameras are not added multiple times by default, which makes searching for new cameras in large network segments easy. In many cases, however, we might want to also add the cameras multiple times even in the automatic search mode (e.g. to achieve camera pairing) and to specify the start for camera numbering. These options can be configured in the adding options dialog, which can be activated by pressing the three dot symbol button.



The Add duplicate cameras option determines whether duplicate cameras will be added in automatic search mode. In the same dialog, we can also specify the starting camera number for automatic numbering.

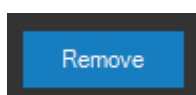
NOTE

Camera numbers already occupied are automatically replaced with the next higher free camera number. If this number were to exceed the largest permitted value of 999, the camera will not be added.

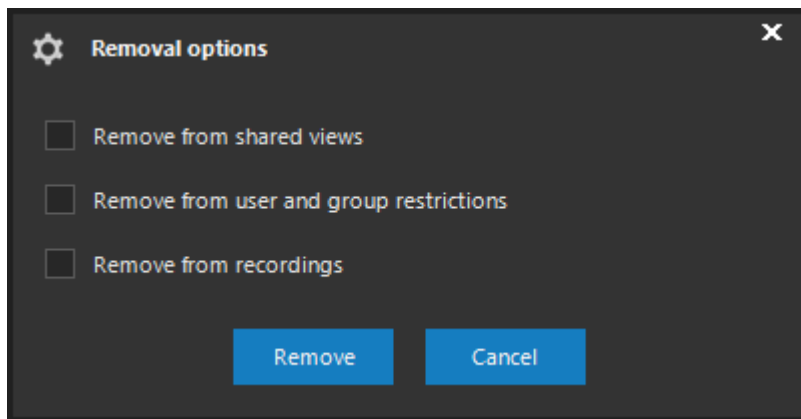
The dialog also contains the option to prioritize the ONVIF interface, should the device otherwise be added using its native interface by default.

Removing cameras

Any camera can be removed from the server by pressing the **REMOVE** button.

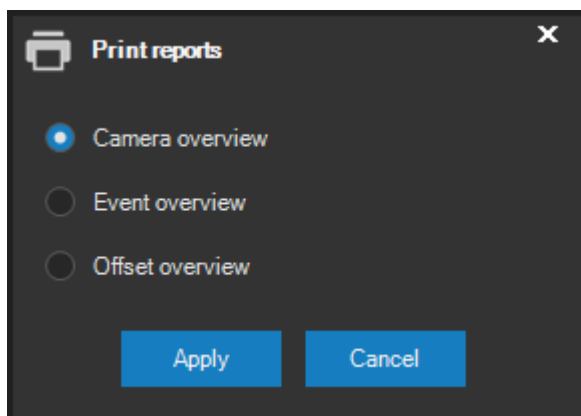


When removing cameras, a complete removal is performed including e.g. its actions in event scenarios. It is still possible, however, to specify the scope of removal.



Camera print reports

The current list of all cameras, including the basic parameters displayed in the list on the screen, can be printed for the selected camera server by pressing the **PRINT** button. Additional print reports are available.



The Camera overview print report prints the overview of all cameras mentioned above connected to the camera server currently selected.

Print cameras

Print Close

ATEAS

Camera overview

[1 - Server 1]

1	Kamera 1	AVISP1344	10.0.0.105:8080	1	root	
2	Kamera 2	AVISM1144-L	10.0.0.106	1	root	
3	Wissenet	XNB-6000	10.0.0.242	1	admin	PTZ
4	Kamera 4	RTSP	rtsp://10.0.0.106/Kamera...	1	root	
5	Kamera 5	RTSP	rtsp://10.0.0.106/Kamera...	1	root	
6	Kamera 6	RTSP	rtsp://test	1		
26	Kamera 7	IB9365-HT	192.168.222.182	1	root	

1 Printed: 04.11.2022 8:42 Printed by: admin

The Event overview report contains the list of all active event sources and event scenarios triggered during an event occurrence.

The Offset overview report contains information about the pairing of cameras added multiple times, i.e. information about camera offsets for displaying camera details and recordings. For recordings, the report shows the offsets for displaying the recordings, and for generating the video preview (e.g. in the live window). Incorrectly configured offsets are automatically highlighted with a different color.

NOTE

The Event overview and Offset overview reports are great tools for effectively reviewing the system configuration, in particular for larger systems.

11.2.3. Video capture card support

Using a special CAPT protocol scheme it is possible to also add some capture card inputs as cameras, which are installed in the computer running the camera server software. A reason for using

the capture cards might be minimizing the video delay when bringing some analog or HDMI video inputs to IP. A name scheme with the following syntax must be used when adding a capture card:

```
capt://device:port[:gpu]
```

where

device is the device number in the computer given by an ordinal number of by the manufacturer,
port is the port number on the card given by the ordinal number of the input,
gpu is the index of a GPU starting from zero which will be used for video encoding.

The GPU parameter is optional. When omitting it, a GPU will be assigned automatically.

NOTE

It is not possible to use the capture cards without also having a GPU in the computer which is used for video encoding. The GPU acceleration features will be used for encoding the video in H264 video format configured for minimal latency.

In the administration section, you can use some video setting parameters to fine-tune the generated video stream like frame rate or maximum bitrate, which also affects video quality during encoding.

11.2.4. Basic camera setup

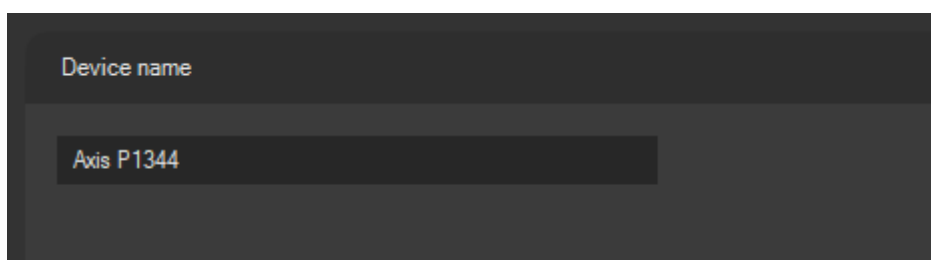
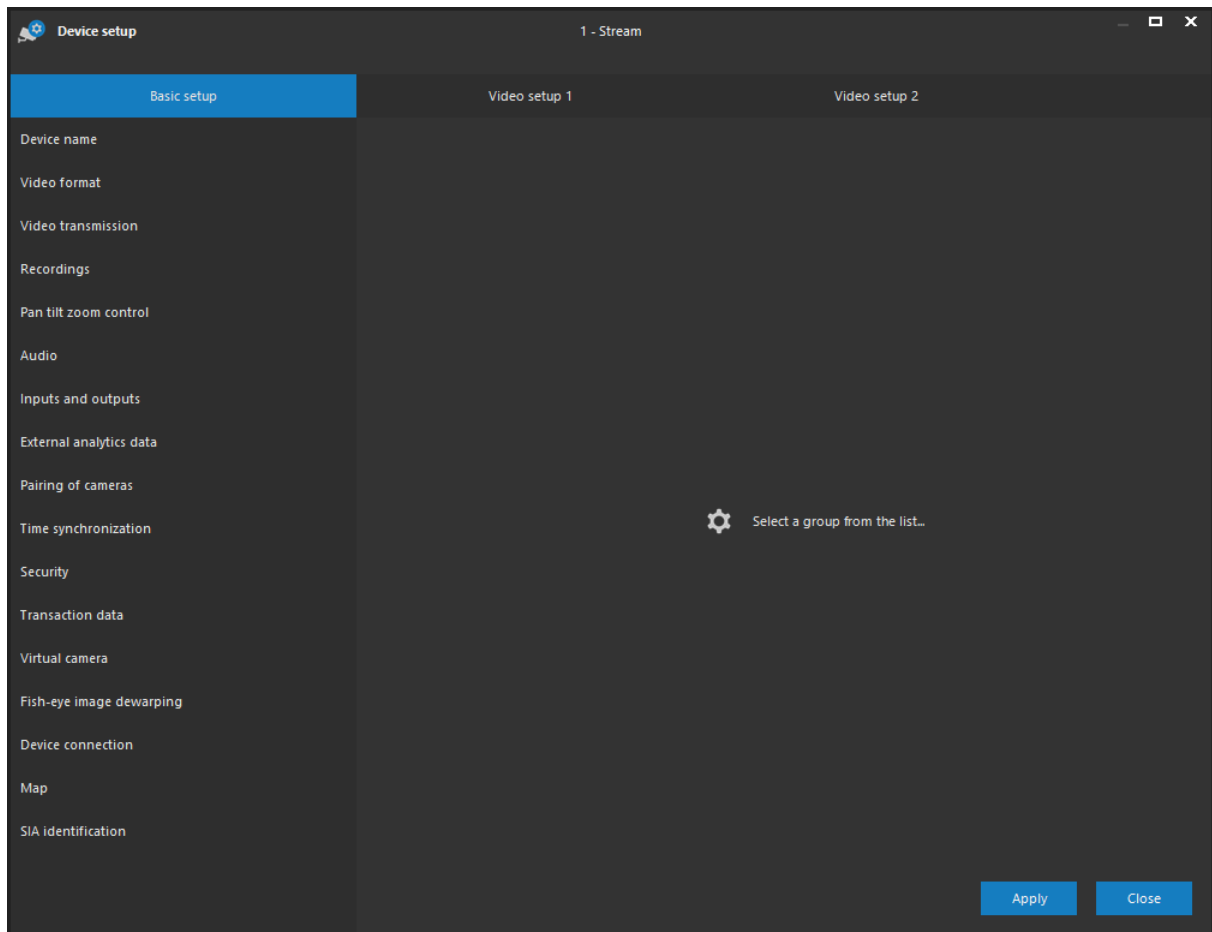
There are many settings available for a selected camera. Setup can be entered by pressing one of the buttons from the Setup group.



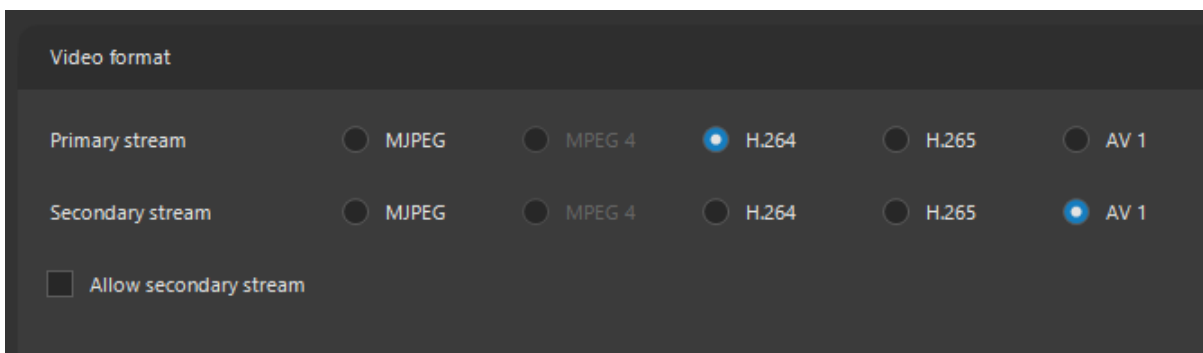
The basic setup is always saved on a current camera server, while the motion detection setup is saved either on a camera server or directly in the device. The event control setup is saved on both the camera server (event source settings) and the administration server (event scenario). The setup is always very simple and intuitive and the setup is saved automatically for the relevant system section. All settings are done in individual windows (see corresponding subchapters).

The basic setup section is entered by pressing the **BASIC** button. Next time you open this window, the configuration section used last will be entered automatically.

Basic



The camera name can be changed in the **Camera name** section by entering the name into the text field. There is a 60 character limit for the name; long names, however, may not be visible entirely in certain layouts of the view, as well as in other places of the application. The hidden part can be truncated and replaced by dots.

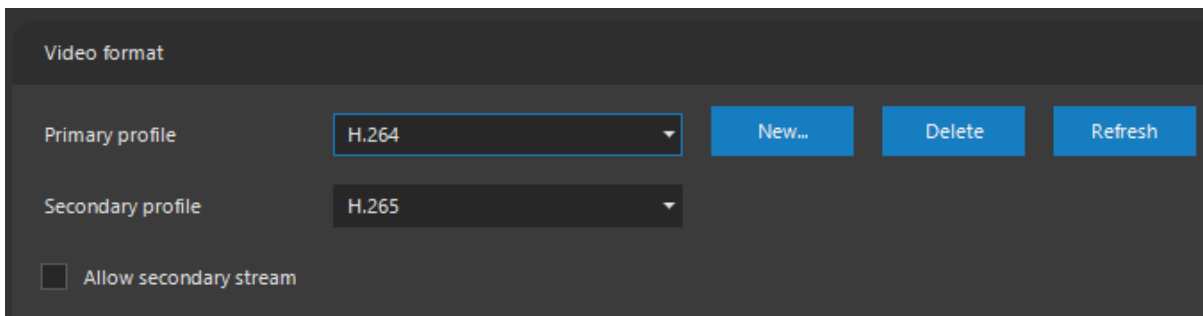


The **Video format** can be set, according to camera specifications, to MJPEG, MPEG4, H264, H265 or AV1 for both the primary and secondary streams. After adding a camera, its secondary stream will not be active unless the Allow secondary stream option is checked.

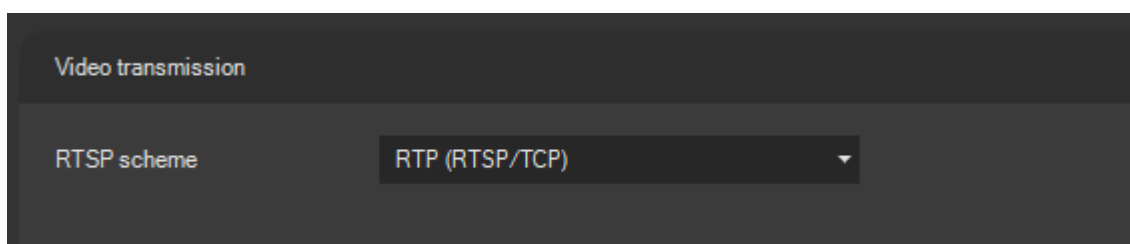
TIP

Secondary streams can be used e.g. for views with multiple cameras, recordings under no event or video analysis purposes.

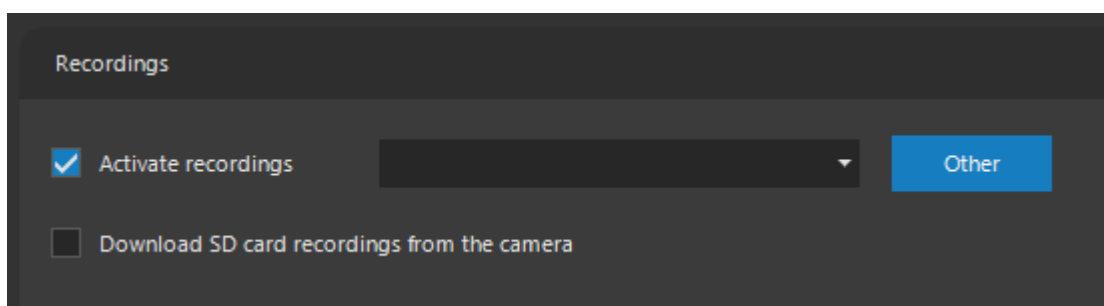
The video format settings are different for a camera (or selection of cameras) connected via Onvif instead of its proprietary interface.



There is a drop-down profile menu instead of the video format selection. These profiles are loaded directly from the device and contain all video and audio format settings. Devices according to Onvif specifications offer pre-set profiles ready for the most frequent situations and applications. The device profiles can be refreshed using the **REFRESH** button. Different profiles can be selected for primary and secondary streams. The **NEW** and **DELETE** buttons can be used to create new or delete existing device profiles. Profiles can be edited on the video setup tabs.

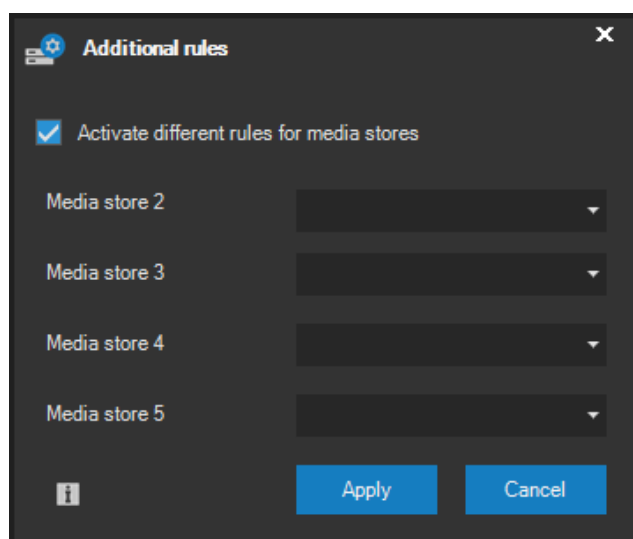


In the **Video transmission** section the preferred RTSP scheme can be set for media transmission using the RTSP and RTP protocols. In all cases, transmissions are unicast, because multicast transmission can be performed for all formats by the camera server on its own. For further information on this topic, see the chapter regarding user administration and assigning a user profile to a camera server, which can automatically initiate the utilization of multicast transmission.



In the **Recordings** section, you can assign a specific record profile to a camera. This profile contains information about the method of recording video or audio. Recording profiles are created in the recordings administration section (where they are also described) and represent a very simple way of setting the recording rules for a camera. Recording profiles can either be shared or each camera can have its own assigned.

If recording to multiple media stores simultaneously is activated for selected cameras, by pressing the button next to the list of recording rules, you can display a dialog in which you can choose a different recording rule for each media store. This way you can, for example, make recordings in higher quality that will be available for several days, and at the same time, make recordings in lower quality that will be available for a significantly longer period of time.

**NOTE**

If recording to multiple media stores simultaneously is activated for selected cameras, and there are no specific recording rules, the default rule selected in the Basic camera settings window will apply for recordings to all media stores.

NOTE

If a recording for the given time interval exists in multiple media stores, clients always receive the recording from the media store with a lower number. Thus, lower media store numbers have priority, meaning they should always contain recordings in higher quality than media stores with a higher number.

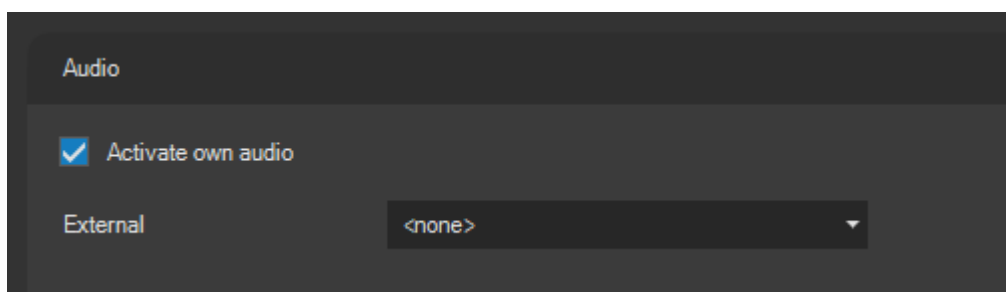
With the help of the Download SD card recordings from the camera option SD card recordings in the camera can be synchronized with the media stores of the camera server and any missing recordings after network failures or camera server restarts can be added to the media stores. Configuration of the recordings should always be done using the camera web interface. The recordings synchronization may be performed using a native interface or Onvif Profile G services.



In the **Pan tilt zoom control** section, you can activate or deactivate camera control by checking (or unchecking) the checkbox.

NOTE

The camera control is activated automatically when a PTZ device is added to the system. If there is a PTZ device connected to the video server, you must activate to device control manually.



Audio for a specific camera can be activated in the **Audio** section. The audio is not activated automatically together with adding a camera to the system, and the Own checkbox is available only when the camera supports audio. Without this checkbox being checked, listening to or recording live audio is not possible. The successful retrieval of camera audio for some device types can depend on the settings directly in the camera, where audio can be blocked by default. For multiple port devices with several video inputs, audio can be activated for a random combination of video inputs, even if the device with multiple video inputs is equipped with a single audio input.

The audio setup section also contains a drop-down list named External. The currently selected camera can be assigned an external audio source from this list. Audio obtained from an external source is handled in the same manner as its own audio source. Audio is automatically played upon selecting a camera from the live view and can be played upon viewing a record and exported along with the video. IP audio modules can serve as external audio sources. Devices, other than cameras or video servers (devices with no video sources), can however be equipped with additional functions such as inputs and outputs.

NOTE

Audio from a device with no video source, can be obtained independently; these audio modules can be added to the system similar to common cameras.

NOTE

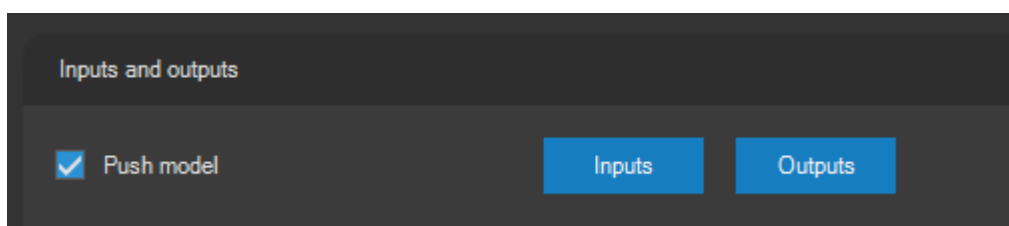
External audio can be assigned to a camera without its own audio source, but also to a camera, which does have its own audio source. If the camera audio source is active (Activate audio is selected), it has priority over the external source, providing external audio is also set.

NOTE

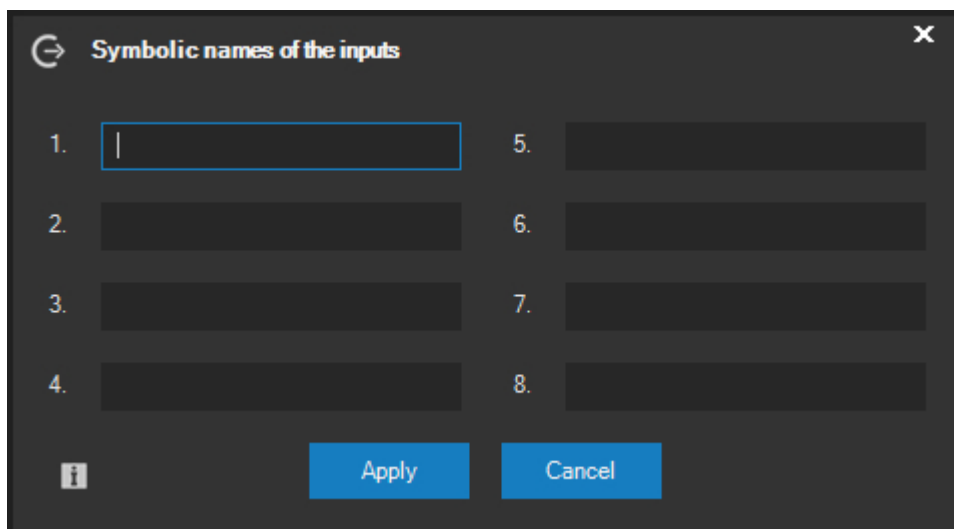
The feature of assigning a device as an external audio source also concerns the push-to-talk feature. Two-way audio transmission is therefore supported for external audio devices.

Following audio codecs are supported:

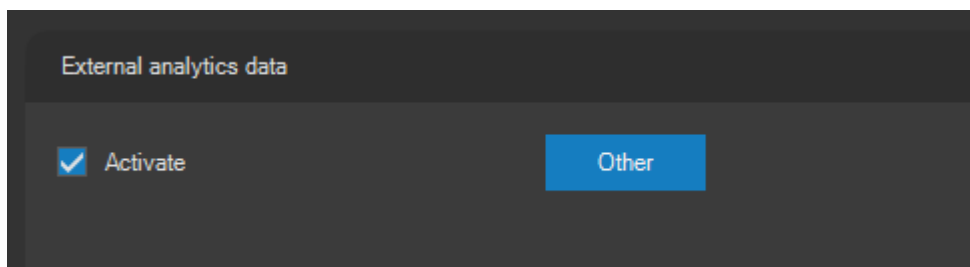
- G711 (64 kbit), u and A variants,
- G726 (24 – 32 kbit)
- AAC (8 – 48 kHz, 8 – 128 kbit)
- DVI 4 (IMA ADPCM)



In the **Inputs and outputs** section, you can define symbolic names for camera alarm inputs and outputs. The system inputs and outputs are normally named by the word Input or Output with a number assigned. The input and output names can be changed to provide better user orientation (during the manual activation of inputs and outputs and when receiving events). These buttons will not be available if there are no alarm inputs or outputs available.



A "push" communication model can also be activated in this part of the window. If the control is available and the latest firmware with support for this feature is installed in the camera, shorter response times to the state changes of alarm inputs can be achieved.



In the **External analytics data** section you can activate the reception of external analytical data from Onvif, natively supported or even some other external video sources.

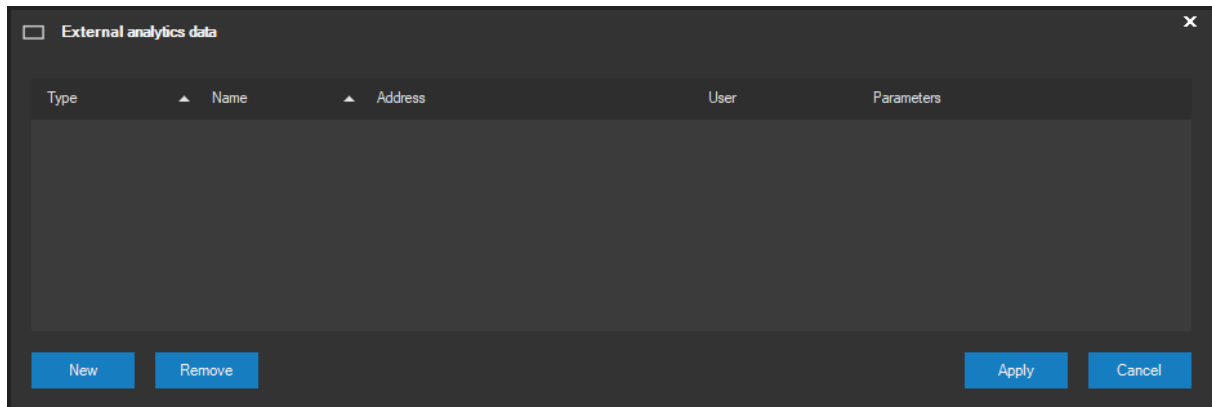
NOTE

The use of external analytical data is available starting with ATEAS Security PROFESSIONAL edition.

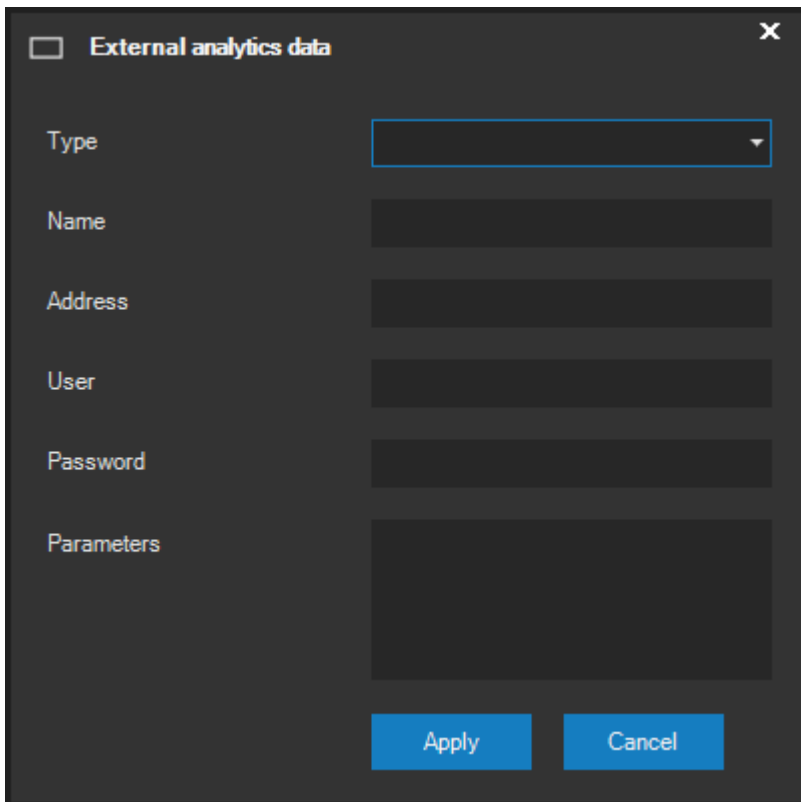
For Onvif analytical sources to work, the selected media profile must include configurations of type video analytics and metadata. Then, if the Activate data reception option is checked, the server may receive data about detected objects, their type, location or levels of detection reliability.

This metadata is displayed in the same way as data coming from ATEAS neural networks and can be used for event management or forensic search.

The list of additional external analytical data sources is displayed when the **OTHER** button is pressed.



To add a new external source, press **NEW**. Any external source can be removed at any time.



The screenshot shows the "External analytics data" dialog box with the "New" form. The form has the following fields: "Type" (a dropdown menu), "Name" (a text input field), "Address" (a text input field), "User" (a text input field), "Password" (a text input field), and "Parameters" (a text area). At the bottom of the dialog, there are two buttons: "Apply" and "Cancel".

In this dialog, you can select the type of the source, specify a name and enter its address (e.g. IP address). Adding a username and password for sources that require authentication is optional. The Parameters field can be used if a source requires further parameter configuration beyond the specification of address.

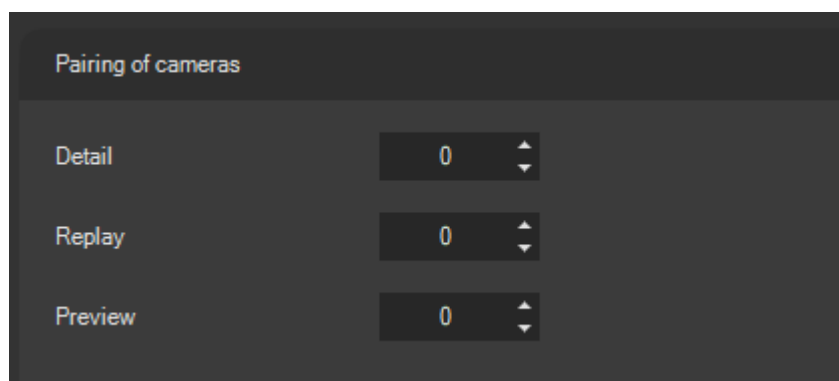
NOTE

Each integrated external analytics data source is documented separately within the External analytics data appendix.

After adding one or more external analytical data sources, authorized users will be able to monitor the results of external video analysis directly within the live window upon selecting the relevant source, which the users can switch between.

NOTE

External analytical data sources can often provide information regarding when an event occurs. These events can be handled in the same manner as custom camera events. In case of an event occurrence, ATEAS automatically selects the respective external analytical data source within the live window.



Under **Pairing of cameras** section it can be specified which camera should be displayed in the detail view after a camera has been double-clicked on its camera window header or which camera should be displayed when replaying the live view. These features are particularly useful when one single camera has been added multiple times to a server with different video stream settings and you want to display a different video stream (with a higher resolution) in the detail view or when replaying the camera directly in live view.

The Preview setting can determine which video stream will be used for the given camera when the video preview feature is activated in the live window during the recordings replay process. This accelerates the video preview loading because the video preview does not require high resolution video.

NOTE

For example, the same values can be often used for streams dedicated for displaying multiple cameras simultaneously in mobile clients and for recordings video preview, as in both cases a lower resolution may be preferred.

The values to be set denote a relative offset value that is added to (or subtracted from) the camera identification number. Therefore, if your cameras including their high and low resolution streams are ordered properly, setting this value can be performed for a large number of cameras at once. Then, each camera will use the offset value to display a different camera in the detail view or during the replay process of the live view.

These values default to zero, meaning that the camera will not change in the detail view or during the replay process of the live view. Although the video stream does not change, the frame rate in the detail view can be updated accordingly from the secondary to primary frame rate value.

NOTE

If the target camera computed by applying the offset value does not exist or the current user does not have access to the camera, there will be no camera change in the detail view or during the replay process.

NOTE

You can use both positive and negative values to set the offset.

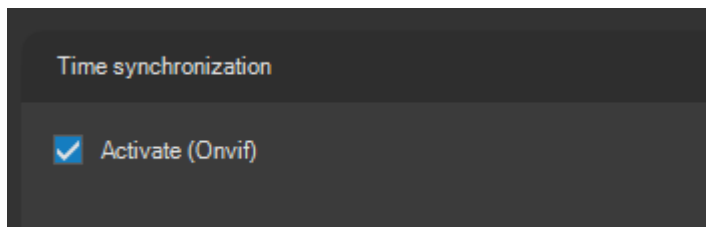
Provided cameras are paired with the Detail value, their PTZ control will also be automatically joined together. Cameras with a configured offset value are treated as PTZ subordinate cameras and cameras without a configured offset value are treated as PTZ superior cameras. The PTZ lock and information in the log will always be linked to the superior camera independently of whether the subordinate or superior camera is PTZ controlled. Cameras will also share their presets.

NOTE

Certain functions like tours or special PTZ functions are not available for subordinate cameras. These settings can be configured only after switching the camera to superior.

NOTE

Special permission to display the numbers of cameras added multiple times to the camera server in the camera number overview in the live window can be revoked from users, thus creating a better organized camera number overview.



Automatic time synchronization with the camera server can be activated for selected cameras under **Time synchronization**. Although the camera time is not decisive for the system (the decisive time is the time of the administration server, which automatically synchronizes connected cameras servers), it can be of significance in these cases:

- When communicating with the camera via Onvif, successful authentication, apart from entering the correct username and password, may also require the time to be synchronized, otherwise the authentication may fail.
- If you use the camera feature where the date and time are rendered directly into the video, then this time is obtained directly from the camera.
- If you store data on a memory card in the camera (e.g. SDHC card) and access the data via the ATEAS client, the data on the card is determined by the camera time.

NOTE

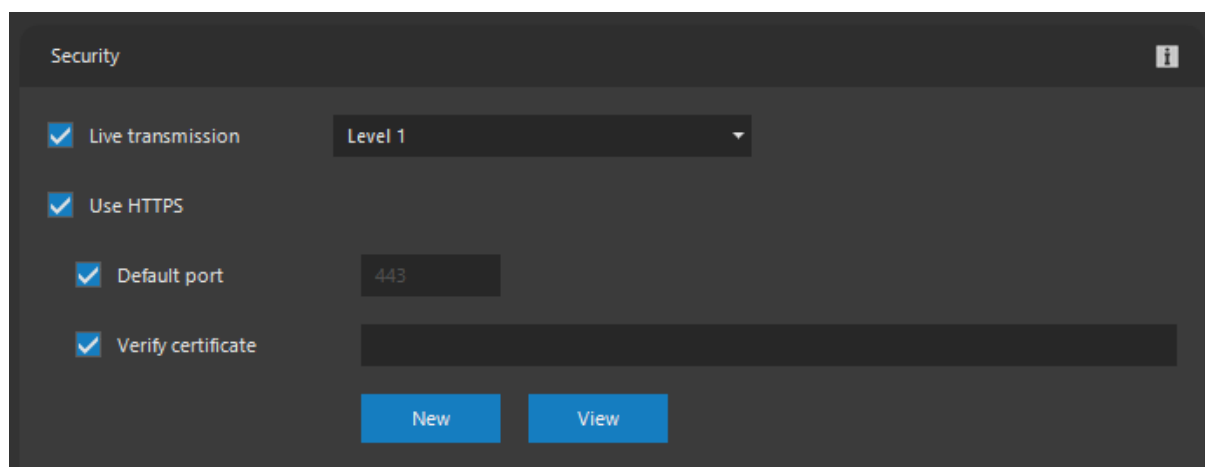
In compliance with the note above regarding time synchronization, which could be required for authorizing operations via Onvif, the camera may require time synchronization with the camera server computer, prior to adding it to the system for the first time, to ensure the authentication is successful.

NOTE

The time synchronization feature is only available for Onvif cameras.

NOTE

If the camera time synchronization is active and time synchronization via NTP server is also activated within the camera, the NTP server will have priority and the camera server will not synchronize the camera time.

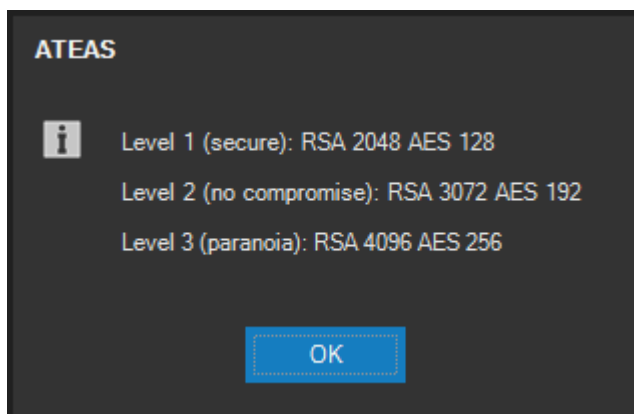


The **Security** section enables activating communication through a secured channel, both for the communication between server and clients and between server and cameras.

Advanced AES encryption can be activated to secure the live communication between server and clients (video and audio redistribution). This ensures that any network sniffing of transmitted packets cannot be used to convert data into a readable format and therefore a video cannot be viewed or audio played until it arrives to the ATEAS Security system client. Encryption will be applied to unicast

and multicast transmissions (providing users have the LOCAL profile set). For more information, see the user profile setup chapter.

The encryption level can be configured from 1 to 3. Although the first level already offers protection that cannot be attacked using the means available today, it is possible to trade a higher power consumption for increased security level, which specifically uses longer cryptographic keys. The parameters are shown in the following dialog.



NOTE

Communication between server and clients can be encrypted starting with ATEAS Security PROFESSIONAL edition.

If the camera supports TLS technology (Transport Layer Security), it will be used for securing communication. When securing the camera communication with TLS, the https protocol is used with the option to change the port.

CAUTION

The http protocol is a necessary precondition, so that the rtsp scheme of the cameras must use a tunnel over http protocol.

The Verify certificate option makes it possible to use a device certificate that must be successfully validated for the device to be able to enter the system.

NOTE

Using and validating device certificates is available starting with ATEAS Security PROFESSIONAL edition.

If, at the same time, a certificate validation on the server level is active, the device certificate and its validation will take precedence over any certificates installed on system level. While for system level certificates the whole certificate chain is inspected, the device certificate must match exactly. All major certificate file formats like cer, crt, pfx or p12 are supported.

NOTE

Some file formats may require a password to open the file.

Use the **VIEW** button to display a window with detailed information about the certificate. Of course, the certificate is not required to contain the private key but public key only to enable validation.



In the **Transaction data** section, you can activate the Data reception option that allows a seamless integration of any given external transaction data with your camera system.

NOTE

Receiving transaction data is available starting with ATEAS Security PROFESSIONAL edition.

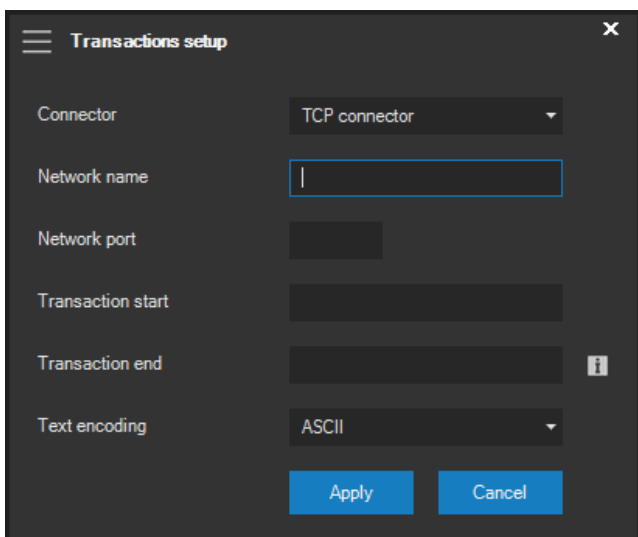
NOTE

Transaction data is considered any text data provided by a third-party system, which can be divided into transactions according to some control or repeated characters found in the data. The data is then associated with the camera and can be viewed live, replayed or searched for.

NOTE

A typical example for receiving transaction data are point of sales systems (POS).

After activating the reception option, data reception options must be configured using the **SETUP** button.



Data can be received over the UDP or TCP network protocol. The Network port field must be filled for both protocols. The TCP protocol additionally requires filling in the Network name.

NOTE

While for UDP protocol the network port denotes the local port for data reception, in case of TCP protocol it denotes the remote port belonging to the address or computer specified in the Network name field, to which ATEAS establishes a connection.

Strings that specify the start and end of a transaction can be entered into the Transaction start and Transaction end fields. Text information between the transaction start and end is considered to be the data of a single transaction. Individual transaction lines are then automatically parsed based on the presence of line endings in the transaction text.

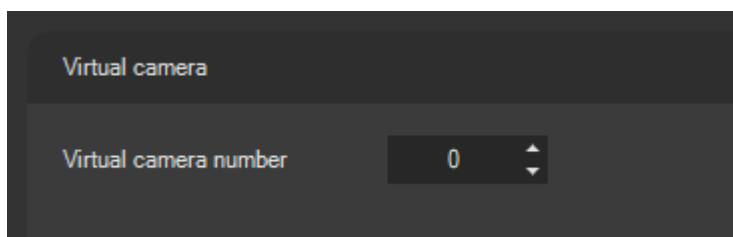
NOTE

You are not required to enter the transaction end. If the transaction end is not entered, the transaction automatically concludes when the start of the next transaction is detected.

CAUTION

Transaction data must be formatted to ensure the strings for transaction start and transaction end are unique and do not appear within the transaction. This would lead to incorrect transaction creation.

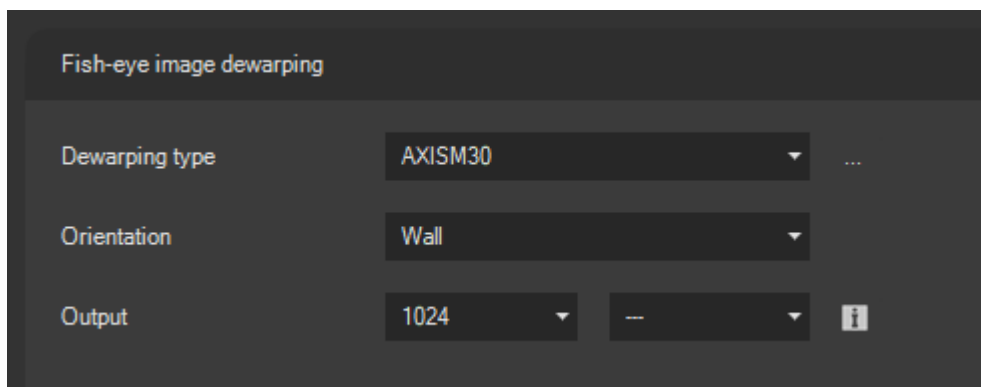
Always select the correct text encoding for transaction data from the Text encoding drop-down list. This will ensure the proper interpretation of, for example, diacritical marks or any special characters in various languages.



In the **Virtual camera** section you can configure some settings regarding virtual cameras. Virtual cameras introduce a technology used primarily by high resolution cameras which rests in the camera being capable of independently transmitting several different picture segments. Some camera types are capable of operating virtual cameras on an independent IP address or network ports. In this case, virtual cameras are supported natively, for they can be connected to the server using their own IP addresses or ports in the same manner as actual cameras. Some types of cameras, however, have virtual camera supported in terms of their own IP addresses and therefore a concrete virtual camera number shall be set in this part of settings.

NOTE

The user control for setting virtual camera numbers will only be available for cameras, which support the virtual camera option and at the same time, independent IP addresses or network ports are not created for them.



In the **Fish-eye image dewarping** section, you can configure selected cameras to allow users to use any of the fish-eye image dewarping modes in the view for the image from these cameras to compensate for deformed images due to the 360 degree scene. In order to perform dewarping operations in the live window, the dewarping type, camera orientation and target video dimensions shall be set for the selected cameras.

The dewarping type can be selected from predefined types or you can create a custom type. As the individual fish-eye lenses differ in their physical parameters (curvature function), you may be required to add your own lens type for the given manufacturer. The list of all types can be displayed with the button next to the drop-down list of types.

Fish-eye image dewarping types			
Name	Value 1	Value 2	Value 3
Axis M3007	-0,022618674	0,014994084	0,368175
Axis M3047	-0,0031351	-0,00599129	0,32334165
Axis M3048, M3068	-0,00076086	-0,00042091	0,30745344
Axis M305	0,038064737	-0,020348421	0,251166053
Axis M3057, M3067, M3077	-0,01601515	0,01786367	0,32169502
Axis M4308	0,02122631	0,01222815	0,23668515

New Remove Close

Press **NEW** to add a new dewarping type, where each of the three values express the polynomial coefficients used to calculate the distance between a point and the optical centre in the target image from the distance between a point and the optical centre in the source image.

Press **REMOVE** to remove the added dewarping type from the system.

NOTE

Predefined dewarping types, which are part of the installation and were not manually added, cannot be removed.

The camera mounting option shall be specified in the Orientation drop-down list, because the orientation of the camera is important input information for the dewarping algorithm, to ensure the result is properly oriented. Additionally, upon activating panoramic dewarping mode in the live window for wall mounted cameras, a single panoramic view is used instead of double panoramic view.

The target video width after recalculations shall be specified based on the input resolution of the fish-eye image and the required level of detail after applying the dewarping algorithms.

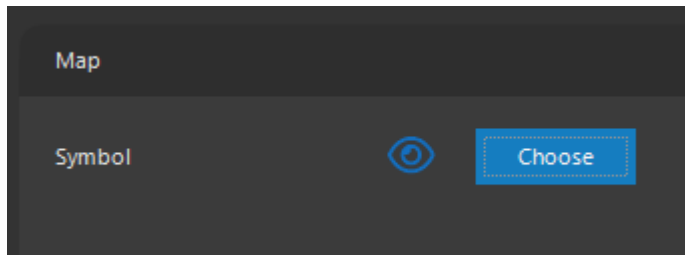
NOTE

The configured value applies to the dewarping into a single PTZ view, panoramic or quad dewarping modes will automatically generate video with a resolution twice as high.

The desired aspect ratio after correction can be selected from the Aspect ratio drop-down list. The default aspect ratio is derived from the original video aspect ratio, nevertheless, it might be appropriate to adjust the ratio for a non-adjusted video with a 1:1 aspect ratio (square).



The **Device connection** section contains a checkbox for maintaining a permanent connection with the device. This checkbox is checked by default. In some cases, it is very beneficial to uncheck this setting and monitor the alarm states without bandwidth consumption of the video stream.

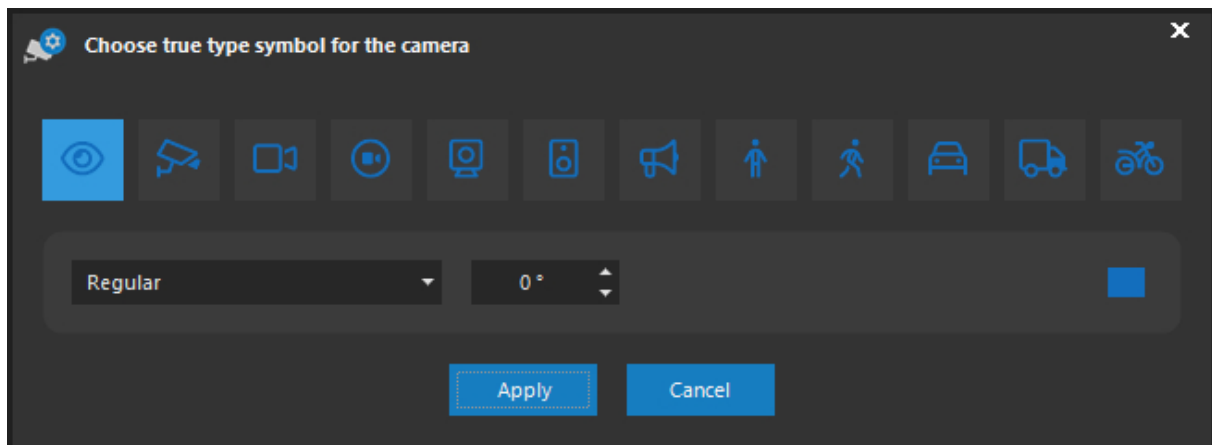


In the **Map** section, you can define the symbol appearance to be used when displaying the camera in a map.

NOTE

The symbol size, used for displaying, is not set by the administrator but by users according to their monitor, screen resolution and sensation of the local setup section.

Clicking the **CHOOSE** button opens a dialog allowing to select a different symbol (each camera has a default symbol and color after adding).

**TIP**

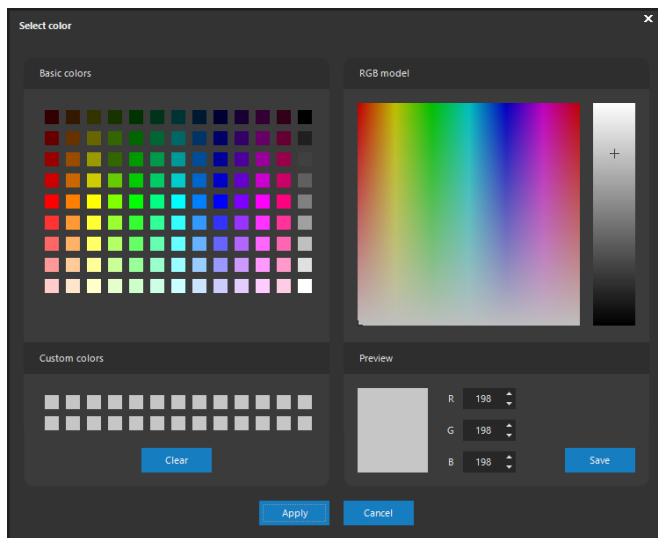
For cameras already localized in the map, the map symbol can be changed more easily using the context menu of the camera symbol in the map.

You can choose from different symbols and their weight. Symbols can be freely rotated, which makes it possible to adapt the real direction of fixed cameras in the map.

NOTE

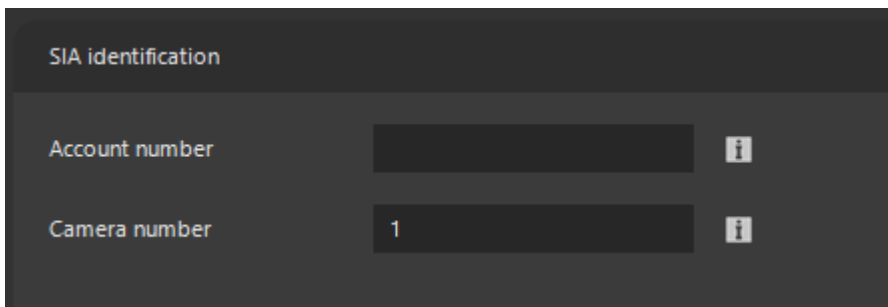
Mobile symbols such as the symbol of a man or vehicle can for example be used for mobile device cameras, which (provided their default location has been created in the map) are automatically displayed in the map while transmitting video based on their GPS location in real time or from recordings.

The colored button opens a dialog allowing the selection of a new color for displaying the symbol.

**TIP**

For dual-tone symbols, two colors can be configured. You can achieve the best look when selecting two colors with the same hue but different brightness, i.e. from the same column.

After pressing the **APPLY** button in the camera symbol selection window, the previous symbol in the preview will be replaced with the newly defined symbol. However, in order to use the symbol in the map, you must confirm all changes performed in the device setup window (see next).



In the SIA identification section, it is possible to configure the camera identification for the SIA protocol. The account (object) number has the same meaning as when opening the SIA channel and it might be necessary to change it for some cameras, if one ATEAS system includes cameras that belong to different SIA objects (accounts).

TIP

The account value can also be entered in hexadecimal form using the 0x prefix.

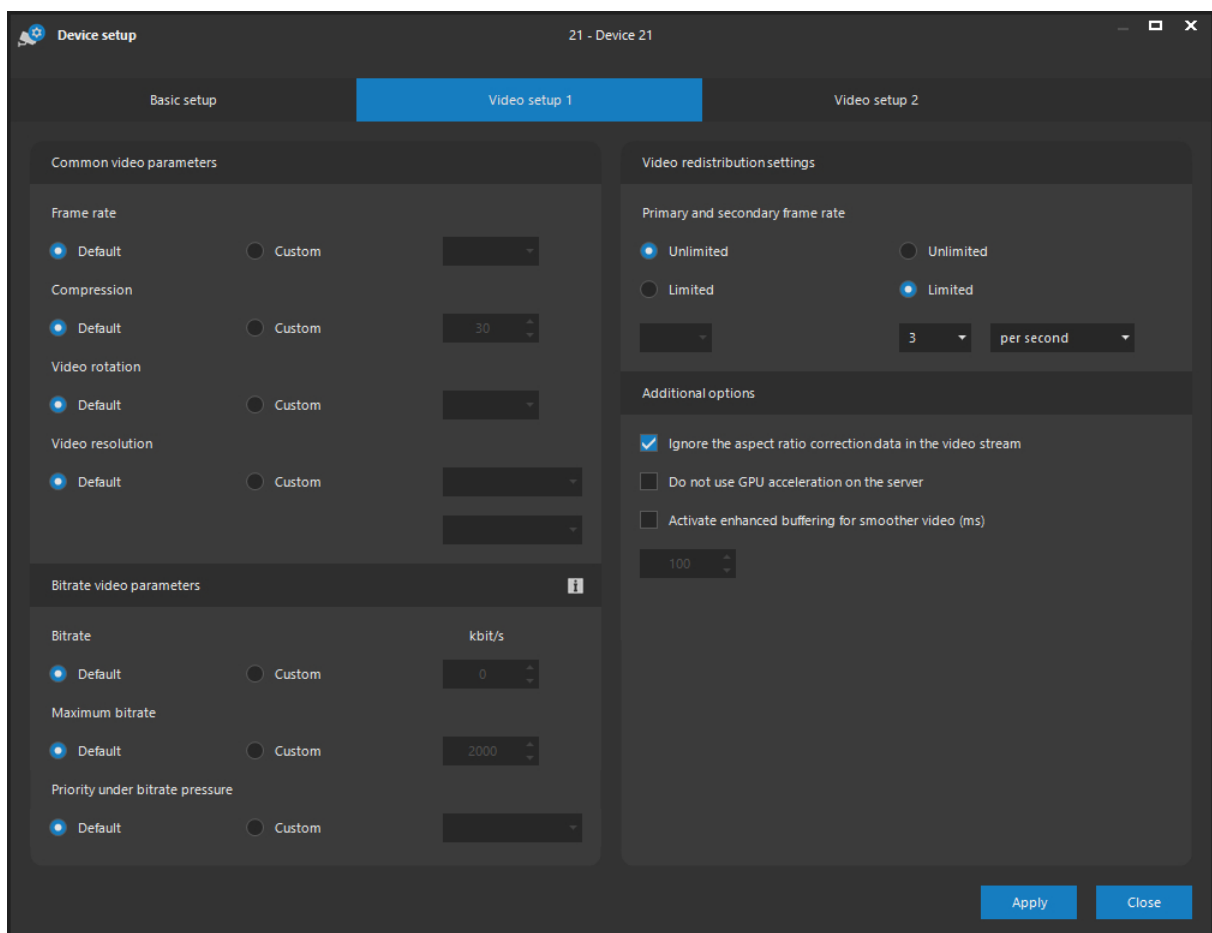
The camera number corresponds to the real camera number by default, but can be changed to a different value in 2-byte range.

11.2.5. Video settings

The Video settings tab contents differs depending on how the camera is connected to the server. In all cases, the primary and secondary streams can be configured separately on their respective tabs.

Video tab settings for native camera interface

The Video tab contains the basic video setup of camera(s) being adjusted.



In the Common video parameters (server input) section, you can adjust the frame rate, level of video compression and video resolution. When selecting the resolution, you must first of all choose the aspect ratio. When the Default option is selected, the currently set camera values will be used. The aspect ratio is not related to the final amount of pixels. Therefore, you can select several resolutions for a corresponding aspect ratio up to the maximum resolution of a particular camera (including the N megapixel resolution). The SCALE option is a special case, which does not select a particular resolution, but only a reduction factor for the maximum or default camera resolution (this concerns specific devices only).

In this segment, you can also set the video rotation parameter. If the default value is set, the rotation directly in the camera will be used, otherwise you can switch to any of the following video rotations: 0, 90, 180 and 270 degrees. Setting the video rotation can be important in connection with the motion detection configuration.

NOTE

Some types of cameras do not support video rotation or do not support all values.

In the Video redistribution settings (server output) section, you can select the primary and secondary video frame rate. The primary frame rate is used when the user has a camera displayed in detail view, whereas the secondary frame rate is used when the camera is displayed in a view with more than one camera. You can also set the secondary frame rate as frames per minute or second to enable the frame rate reduction less than 1 FPS, necessary especially when several views including tens of cameras are opened (up to $4 * 100$, i.e. 400 simultaneously displayed cameras on one workstation).

NOTE

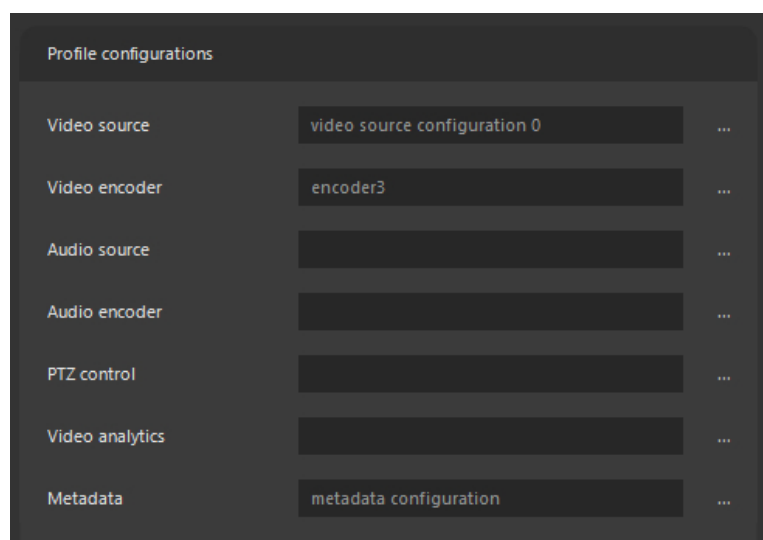
When a video codec other than MJPEG is used, the frame rate is reduced and counted from complete frames without any dependencies on others.

Bit rate video parameters can be adjusted in the bit rate video parameters section. When the Default option is selected, the values currently set in the camera will be used. The bit rate can be set to variable (VBR) or constant (CBR) in kilobytes per second. The maximum bit rate can also be reduced (suitable especially for VBR). In case a significantly greater than constant or greater than the maximum permitted bit rate is generated, in terms of the recorded scene, video quality or the frame rate must be limited. In this case you can set a priority while reducing the bit rate. If the Frame rate option is selected, the camera will maintain the frame rate at the expense of video quality. If the

Quality option is selected, the quality will be maintained at the expense of the frame rate. If the None option is selected, both the quality a frame rate will be reduced equally.

Video tab settings for Onvif camera interface

The Common video parameters (server input) section is different for a camera (or selection of cameras) connected via Onvif instead of its proprietary interface. These settings are displayed as follows for the devices with Onvif support.



Individual profiles according to the Onvif specification contain all settings divided into several groups (configuration entities) from which the resulting profile is built. The video setup sections contain the properties of the profiles selected in the basic settings.

Video source configuration: The video source can often be the whole view, as taken from the camera, the device however, can define multiple video sources, if it has virtual camera support or has multiple analog inputs for one IP address.

Video encoder configuration: Video compression combines all settings regarding video compression, such as the video format and its specific parameters, compression quality, resolution, frame rate etc.

Audio source configuration: The audio source can be an external or on-board microphone device.

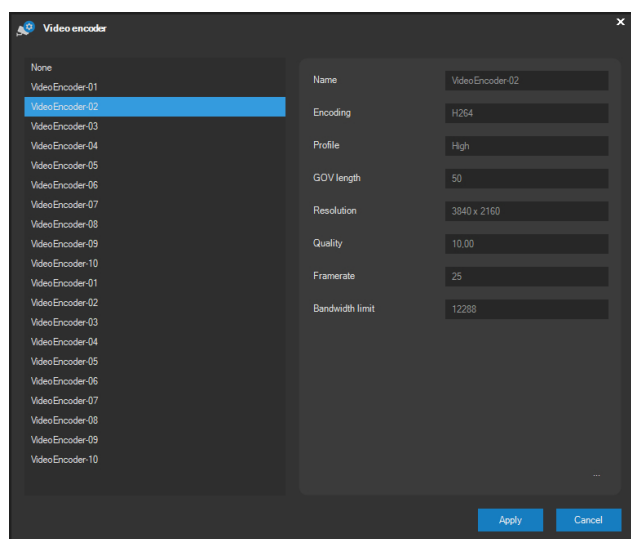
Audio encoder configuration: Audio compression combines all settings regarding audio compression, such as the audio format and its specific parameters, sampling rate or bit rate.

PTZ configuration: This configuration relates to the PTZ camera control method. True mechanical PTZ control can be a typical PTZ configuration in this context. However, PTZ configurations will also be available on (megapixel) cameras, which support digital zoom and digital control directly within the view.

Video analytics configuration: The configuration adds a video analytics component to the profile, which activates video analytics rules in the camera and determines the kind of metadata to be transmitted.

Metadata configuration: This configuration adds a metadata component to the profile, which activates scene description metadata transmission including e.g. object types, object bounding boxes, detection reliability levels etc.

By pressing the three-dot button located at the end of the configuration names, you can display the list of all available configurations for each configuration entity. The following image shows a list of configurations for video compression. The same procedure is used for other configuration entities.



In this dialog, containing the list of available configurations, you can mark the configuration you wish to use and press the **APPLY** button to assign the configuration to the given profile. If the profile already has a configuration set for the given configuration entity (e.g. video encoder configuration), the configuration will be replaced. The configuration can be removed from the profile by selecting the list item "None".

Individual configurations can be randomly grouped in random order within the profile, for Onvif specifications do not have any restrictions with exception to the following. Onvif recommends assigning video encoder configurations to profiles only after the video source configuration has been assigned (the same applies to audio configuration) and furthermore recommends removing video

source configurations only after the video encoder configuration has been removed (the same applies to audio configuration). These recommendations are implemented into the ATEAS client logic and the application automatically monitors these recommendations are observed.

CAUTION

If no PTZ configuration is assigned to a profile, the camera cannot be controlled with this profile active, not even if the control is permitted in the basic camera setup.

All details for the given configurations are displayed when the configuration is selected in the Configuration details section. The parameters for the selected configuration can be edited by pressing the button with three dots, located in the bottom right corner of the Configuration details section.

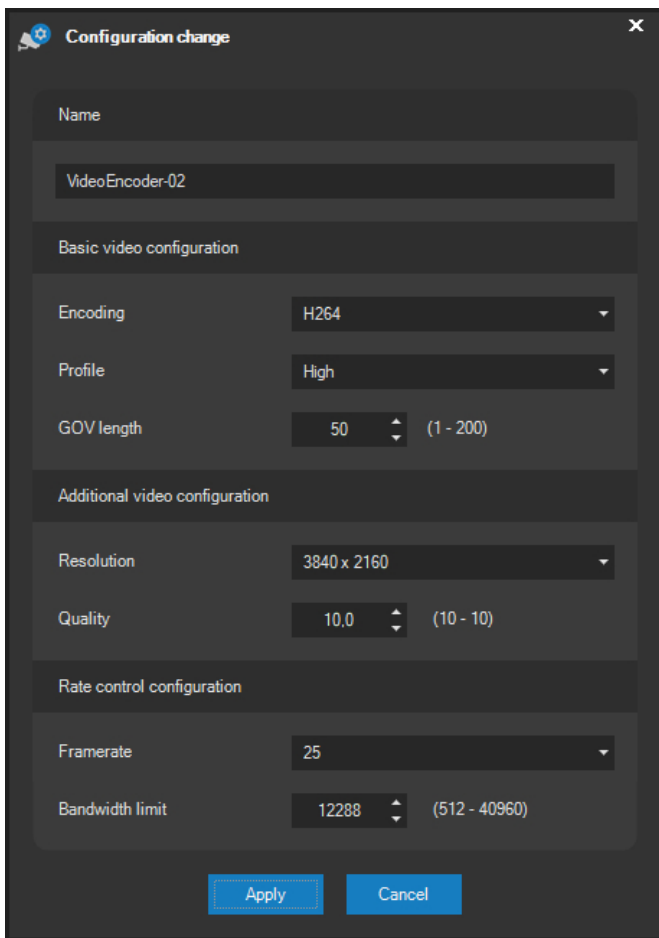
NOTE

While creating and deleting profiles within cameras is possible, the number of configurations is specified by the manufacturer and cannot be changed. However, configuration settings and parameters can be modified.

NOTE

For some configuration entities, the button for editing the configuration can be unavailable.

Pressing this button will display a dialog enabling the user to edit the given configuration. The following image shows the dialog for changing a video encoder configuration.



The image shows a 'Configuration change' dialog box with a dark theme. It has a title bar with a gear icon and a close button. The dialog is organized into sections: 'Name' with a text field containing 'VideoEncoder-02'; 'Basic video configuration' with 'Encoding' (H264), 'Profile' (High), and 'GOV length' (50, range 1-200); 'Additional video configuration' with 'Resolution' (3840 x 2160) and 'Quality' (10.0, range 10-10); and 'Rate control configuration' with 'Framerate' (25) and 'Bandwidth limit' (12288, range 512-40960). At the bottom are 'Apply' and 'Cancel' buttons.

In this dialog, you can change the name of the configuration, the video format; optionally also the profile and GOV length, which gives the number of frames from a complete frame (key frame) up to the following complete frame. Furthermore, you can change the video resolution, its quality and configure the rate control by changing the frame rate or bandwidth.

NOTE

The dialog can slightly vary for each camera depending for example on the version of certain Onvif services supported by the device.

NOTE

The range each parameter can assume is obtained for each parameter directly from the camera via Onvif. This means that in this dialog, you will see the list of all video formats or resolutions supported by the camera. For number expressions like the compression quality, the permissible range for the given device will always be obtained and enforced automatically.

Video tab settings for RTSP camera interface

If the video (also with audio) source is added directly using an RTSP address, no changes to the settings can be made under Common video parameters (server input). Certain video settings can, for example, be directly part of the RTSP address.

Additional options

Some additional video options can be activated under Additional options.

The Ignore the aspect ratio correction data option is turned on by default and enables to ignore any additional aspect ratio correction information that might be optionally included in the video stream. This technology might be used by some cameras with other than square pixels to subsequently update the aspect ratio

The Do not use GPU acceleration on server option allows you to exclude the decoding of the given camera from GPU acceleration on the server, even if it is enabled.

TIP

This way, the decoding load can be divided between the CPU and GPU on the server.

Additional cache memory buffer for smoother video can be activated by selecting Activate enhanced buffering for smoother video. This feature should only be activated if the live video smoothness is negatively affected by network transmissions. The negative consequence of the video smoothing process is, for example, impaired PTZ camera control quality due to higher video latency. If the option is activated, the value can be set for an interval between 50 to 500 milliseconds.

Changes performed in the device setup window have to be confirmed by pressing the **APPLY** button. The application will confirm the changes have been saved and applied. The window can then be closed by pressing the **CLOSE** button.

NOTE

The **APPLY** button will save all changes performed in all device setup tabs (providing there are at least two). Therefore, it is possible to perform changes in all tabs and then update by pressing this button.

11.2.6. Batch camera configuration and removal

The basic camera setup can be performed for any number of cameras at a time. It is also possible to remove any number of cameras with just a single action. However, it is necessary to select several cameras from their list. Multiple selections can be performed as follows:

- moving the mouse while holding the left button,
- repeated selection while holding the CTRL key,
- combination of the methods mentioned above,
- CTRL-A can be used to select all cameras in the list.

NOTE

While performing a multiple camera selection, buttons enabling independent camera settings will be disabled. Performing multiple settings, for example for motion detection is not possible (or pointless).

When entering the basic setup section with several devices selected (multiple selection), the window content will be adjusted so that the only settings valid for all cameras from the selection will be available. Only explicitly performed settings will be applied to selected cameras. This means that it is possible to change, for example, the recording profile for 10 selected devices at a time, without changing any other camera parameters that can remain different.

NOTE

For multiple camera selections, it is not possible to include cameras with different connection types (proprietary interface, Onvif, RTSP only).

For simpler multiple selections it is possible to apply a filter from the dropdown list above the list of cameras.

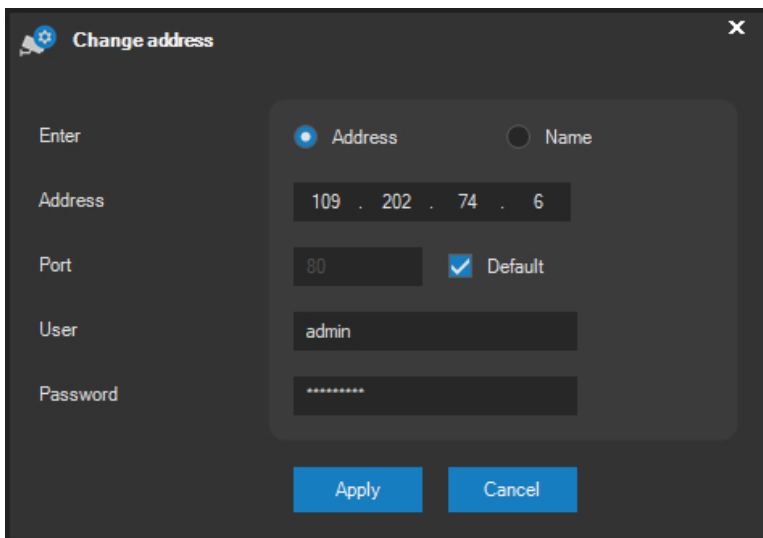
NOTE

Considering devices connected to the server via the Onvif interface are configured according to profiles stored directly within edge devices, batch editing of profiles and their configurations is not possible.

All cameras included in the multiple selection can be deleted from the system by pressing the **REMOVE** button.

11.2.7. Address and login change

The IP address and camera http port can be additionally changed by pressing the **ADDRESS** button. Camera credentials can also be changed in this dialog (username and password).

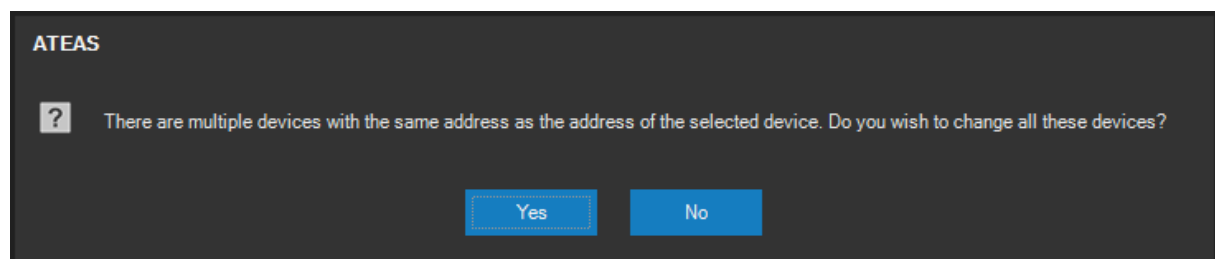


The basic principle of changing the address and port is the same as for adding cameras. Either the IP address or name of camera and http port can be entered.

NOTE

Changing the IP addresses and http ports of cameras can reduce or raise the number of licensed cameras assigned to the camera server, if you are changing the address of cameras added multiple times or you are changing the address to add one camera multiple times.

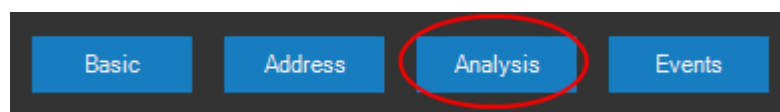
Therefore, the administrator is informed about the situation and can choose whether the address and other data will also be automatically updated for other duplicate devices added (devices with the same address or name).



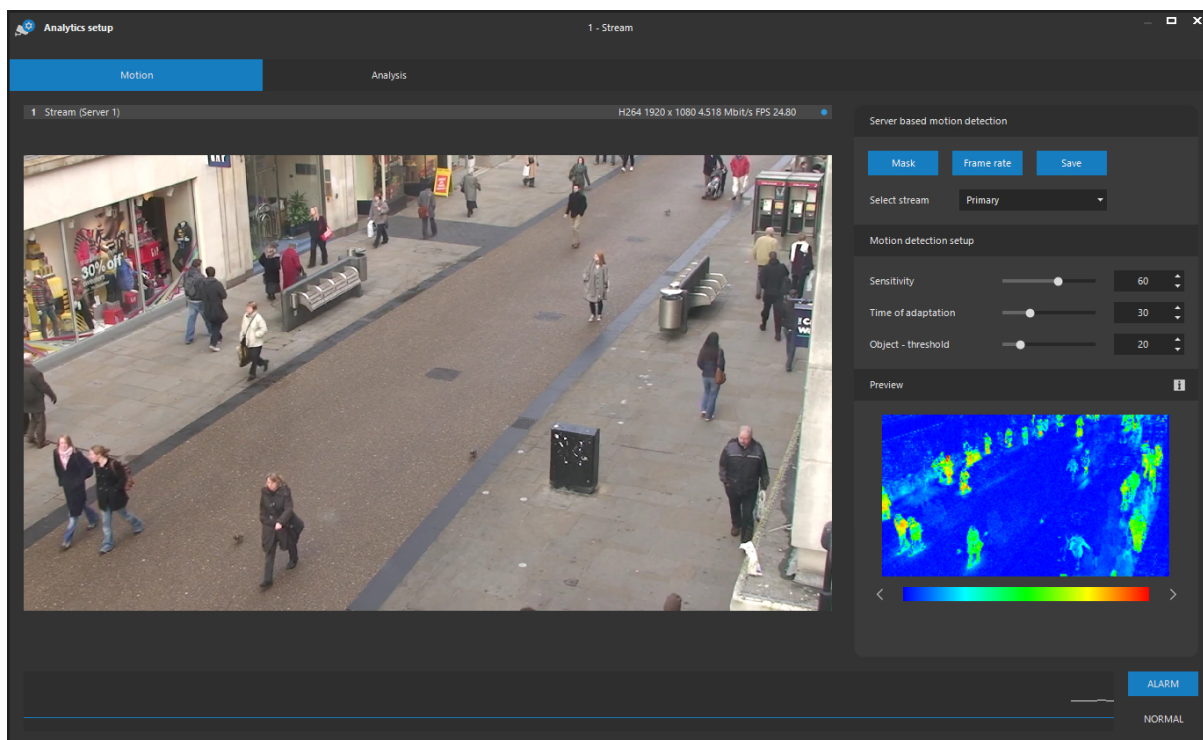
Under multiple camera selection, this feature can't be used to change the address or port, however, login details can be updated.

11.2.8. Motion detection on the server

Motion detection can be adjusted by pressing the **ANALYSIS** button and selecting the Motion tab.

**TIP**

The configuration can be performed even for multiple cameras selected.

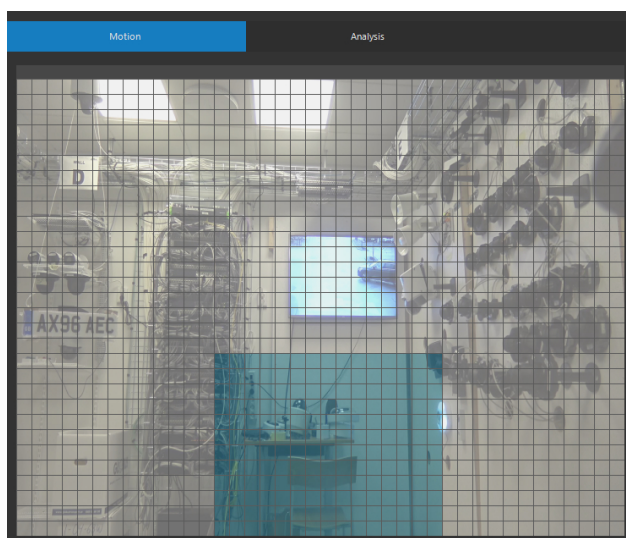


The current scene in front of the camera and a preview of the motion evaluation within the scene in real time can be monitored in the window. Motion and moving objects are distinguished by color, according to the intensity of the change within the scene, determined by the difference in color and brightness of the moving object. The color scale used for previewing motion within the scene, can be switched using the white arrow buttons, as shown in the following image.



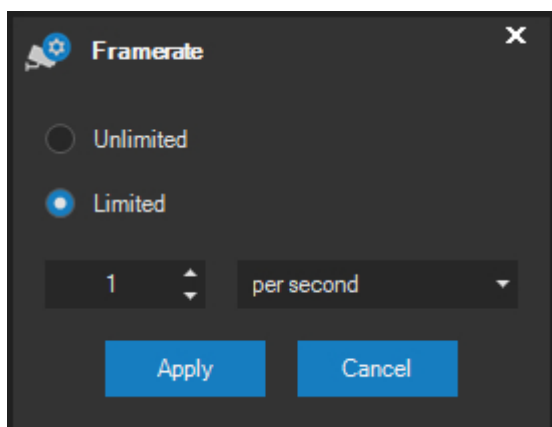
Basic setup

In the Server based motion detection section, you can perform the basic setup for the mask and frame rate for motion detection. The **MASK** button activates the mask mode that allows you to specify the areas of the scene in which the server performs motion detection. The mask can be defined at random, either including or excluding individual mask points from the monitored area. Creating a mask is completely intuitive, using drawing techniques you can add new parts of the image by left-clicking the mouse and deleting parts by right-clicking. To include the entire image into the mask, delete the entire mask or inverting the mask, use the **ALL**, **DELETE** and **INVERT** buttons available during mask setup.



Pressing the **MASK** button again that behaves like an option button, will immediately update the motion detection preview.

The **FREQUENCY** button opens the dialog for setting the frame rate for server based motion detection. The frame rate can be configured from 10 frames per minute (one frame per 6 seconds) up to an unlimited frame rate.



The frame rate value specifies how many frames per second should be analyzed. To keep object identities, the default value is 5. The decoding frame rate is inferred automatically. For video formats other than mjpeg, values above 2 (assuming a standard GOV length) result in the entire video stream being decoded due to inter-frame dependencies.

CAUTION

Setting high frame rates on many cameras simultaneously, particularly when using megapixel resolutions, can lead to an enormous performance consumption and computer processor overload situation. Therefore, the settings should comply with your hardware configuration.

In the Select stream drop-down combo, either the primary or secondary stream can be selected for detection.

TIP

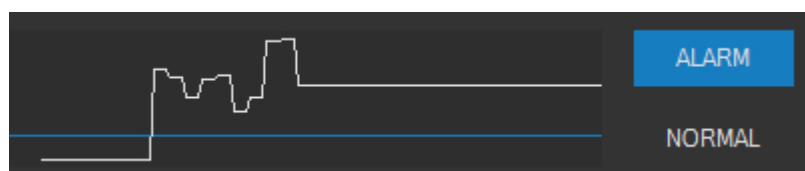
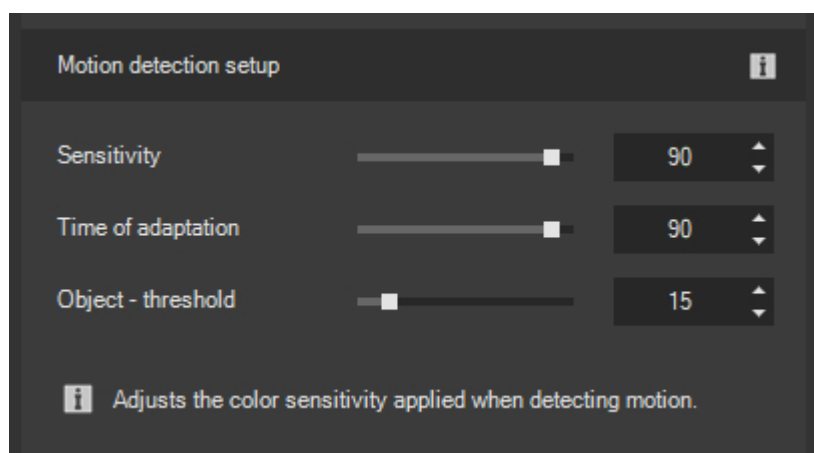
By using the secondary stream, performance requirements can be significantly decreased even when keeping higher frame rates.

Detailed setup

In order to efficiently use motion detection as one of the event sources, you should fine tune it using the available parameters. These parameters include:

- sensitivity – adjusts color or light sensitivity for motion detection,
- time of adaptation – adjusts the time till moving objects are merged with the background,
- object size (threshold) – adjusts the size of an object which invokes motion detection.

These parameters can be changed using the scrollbars provided with respective descriptions.



The control shown above indicates switches between ALARM and NORMAL and whether or not the currently detected motion level will lead to an event. It is important to realize camera servers use an intelligent method of generating events. This means that if the control changes the status to ALARM, then to NORMAL and shortly after to ALARM again, the system will keep the same event opened and will not generate a new one (or a new alarm). A new event will occur after the detected motion level drops under the threshold value and remains there for some time. These values can be set in the Events section.

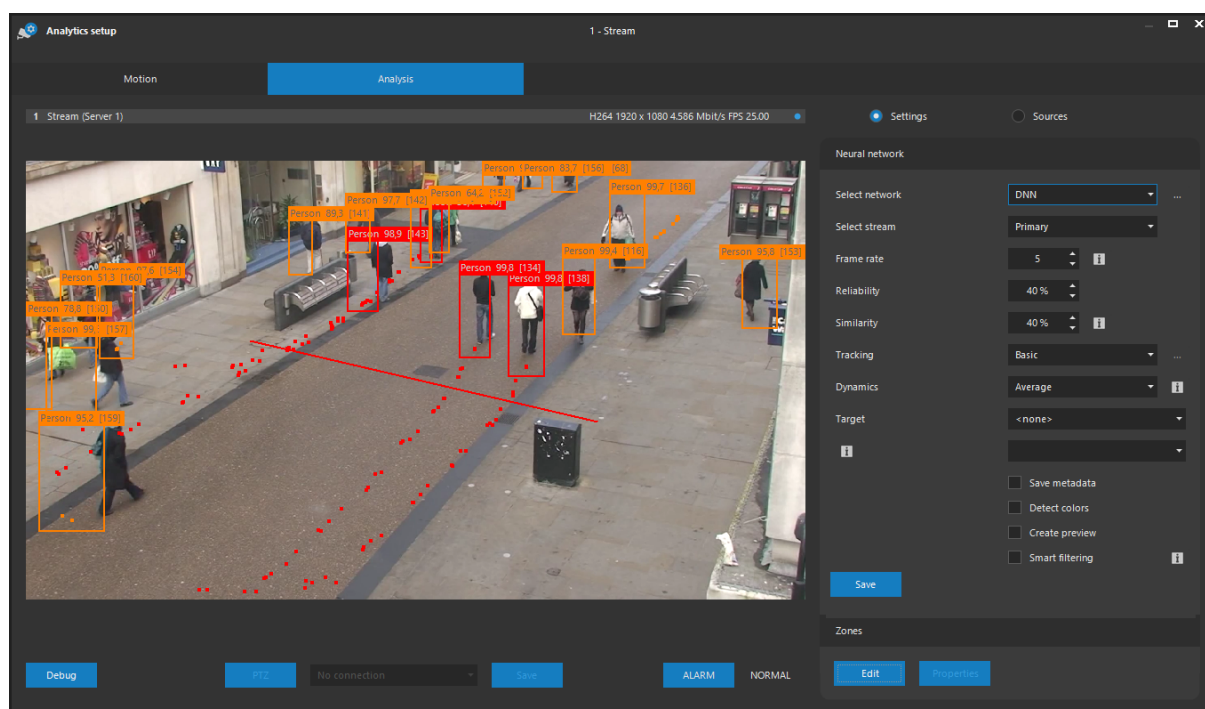
Changes to motion detection settings need to be confirmed by pressing the **SAVE** button. Only then the server will apply the updated settings. The need to save your settings is indicated by a warning exclamation symbol. If you forget to save the changes to the settings, the application will display a warning message.

11.2.9. Analytic sources

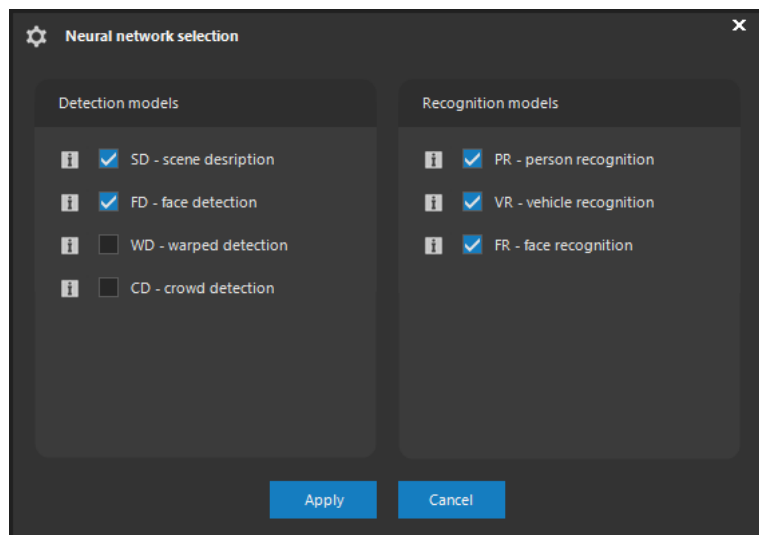
Analytic sources can be adjusted by pressing the **ANALYSIS** button and selecting the Analysis tab.

TIP

The configuration can be performed even for multiple cameras selected.



A name, as specified in the server administration section, can be selected from the Select network list. The name corresponds to a device (GPU) running one or more neural networks. If not set otherwise, the video from the camera will be analyzed by all network types launched on the selected device. This can, however, be changed in the network types selection dialog.



If a network type is selected that is not running on the GPU, no results will be available though.

NOTE

Some models on the first level like for example the SD and WD models cannot be combined.

In the Select stream drop-down combo, either the primary or secondary stream can be selected for detection.

TIP

By using the secondary stream, performance requirements can be significantly decreased even when keeping higher frame rates.

The frame rate value specifies how many frames per second should be analyzed. To keep object identities, the default value is 5. The decoding frame rate is inferred automatically. For video formats other than mjpeg, values above 2 (assuming a standard GOV length) result in the entire video stream being decoded due to inter-frame dependencies.

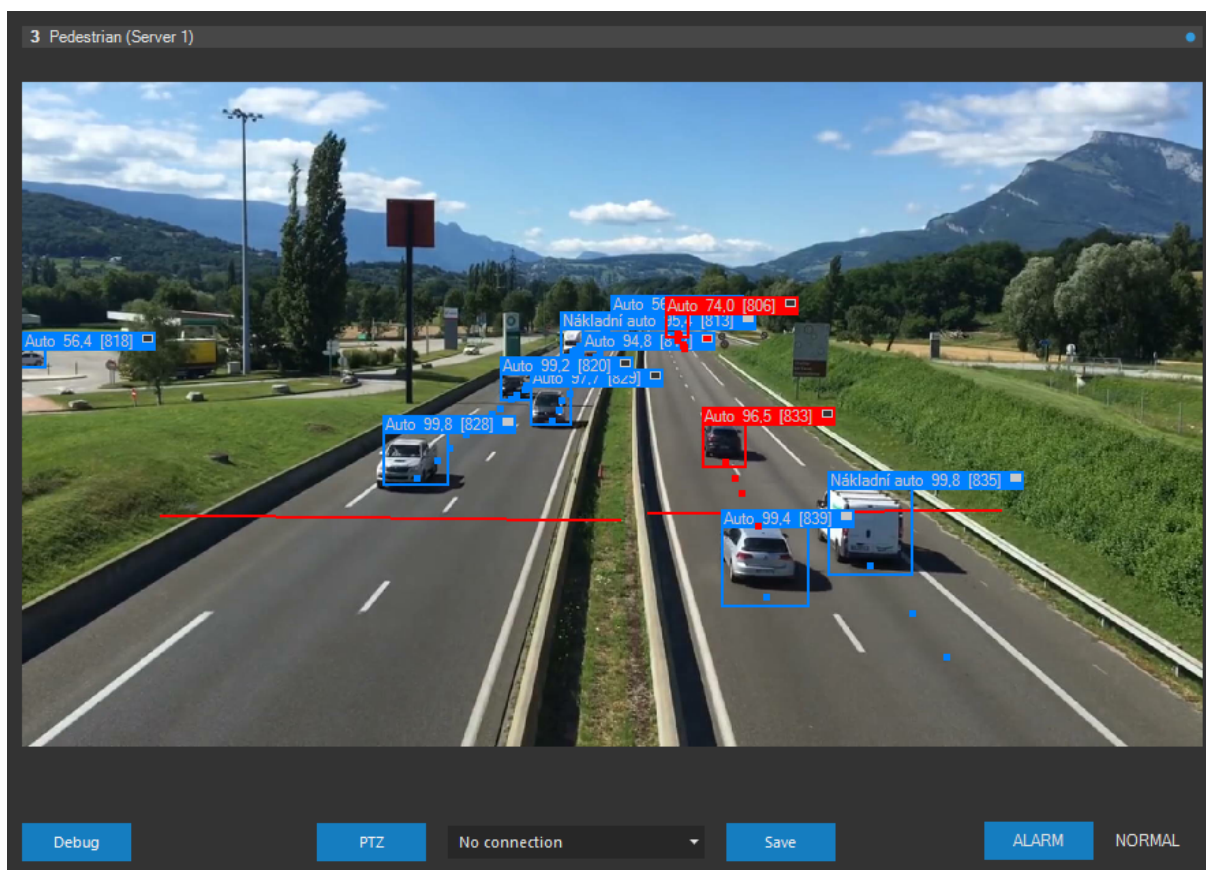
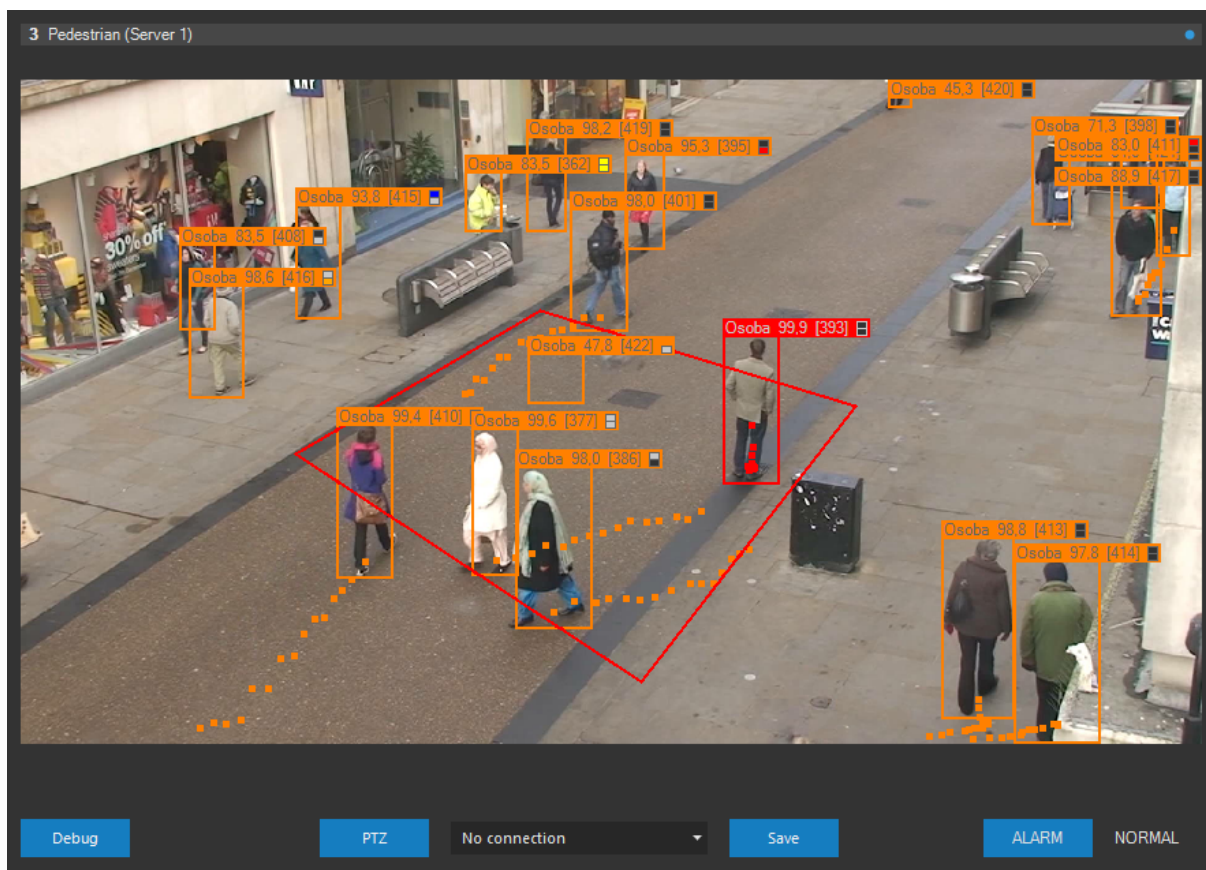
NOTE

Zero represents unlimited frame rate.

Reliability specifies the basic threshold value as a percentage. It specifies the extent at which the neural network is convinced that it detected a specific object type, and renders the classification into the scene.

Just like reliability, similarity is a metric in the range 0 to 100 but requires a different interpretation than reliability. It represents the value of the so called cosine similarity, in which context values around 0.5 already indicate a strong sign of similarity. Therefore, in practice, similarity values will be significantly lower. Similarity is used e.g. for the Face recognition type of neural network.

Object tracking maintains object identities and enables to determine their direction or scene dwell time. You can therefore use event sources such as loitering in the scene, wrong way detection for pedestrians, wrong way detection for cars or counting objects that cross a line.



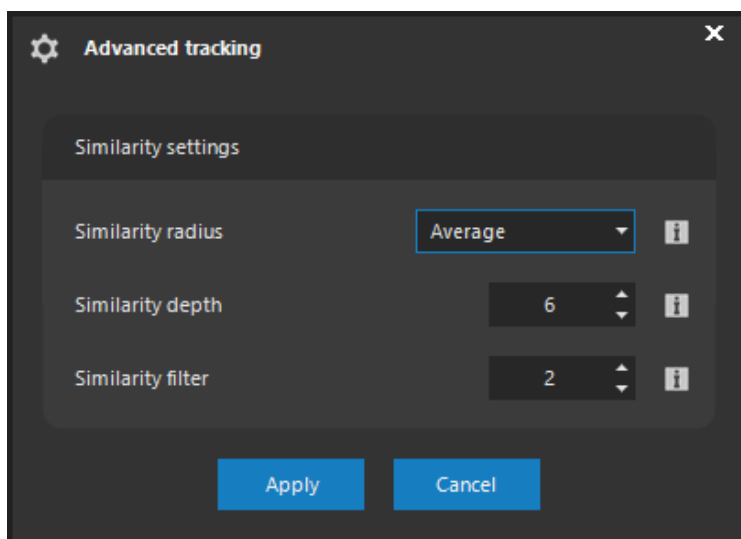
The following types of tracking are available:

- Basic: Complies with individual object tracking up to semi-crowded scenes, uses direction and size prediction metrics.
- Advanced: Complies even with crowded scenes, apart from the above metrics, AI similarity is used.

NOTE

Advanced tracking requires recognition networks to be run for the tracked object types.

If required, advanced tracking can be fine-tuned using some parameters in the dialog that can be opened using the button next to the tracking mode selection.



The similarity radius specifies the space discrepancy the algorithm can cope with if an object disappears from the scene. Not only the distance, but also the size of the objects is evaluated.

The Depth and Filter settings specify the effect of past recognitions. If configured like in the image above, 3 visual recognitions of each object (last 6 skipping every second) will affect the object identity evaluation.

The Dynamics setting determines the magnitude of changes in object speed and size that can be expected, and supports the tracking algorithm to optimize tracking results. There are five dynamics

levels that can be configured, from low to high, with respect to the nature of the scene. Dynamics is, in a certain sense, indirectly proportionate to the detection frame rate.

NOTE

The reduced detection frame rate can be compensated by using higher scene dynamics, nevertheless, this only applies to a certain extent and may reduce tracking reliability.

The quality of any identity based analytics, like counting or loitering, is greatly determined by the stability of object identities generated by tracking. You can use the **DEBUG** button to assign the objects different colors to better see the tracking results when configuring events.

Setting targets allows assigning neural analysis results to another device in the system. This configuration is suitable provided you have a neural network delegated to an independent computer (e.g. optimized station with GPU) and you intend to store analysis results on recording servers. When setting a target, the neural network metadata is automatically assigned to the target device, as if it were created directly on the computer with the target device.

NOTE

The target device can be connected to the same or different server within the system.

NOTE

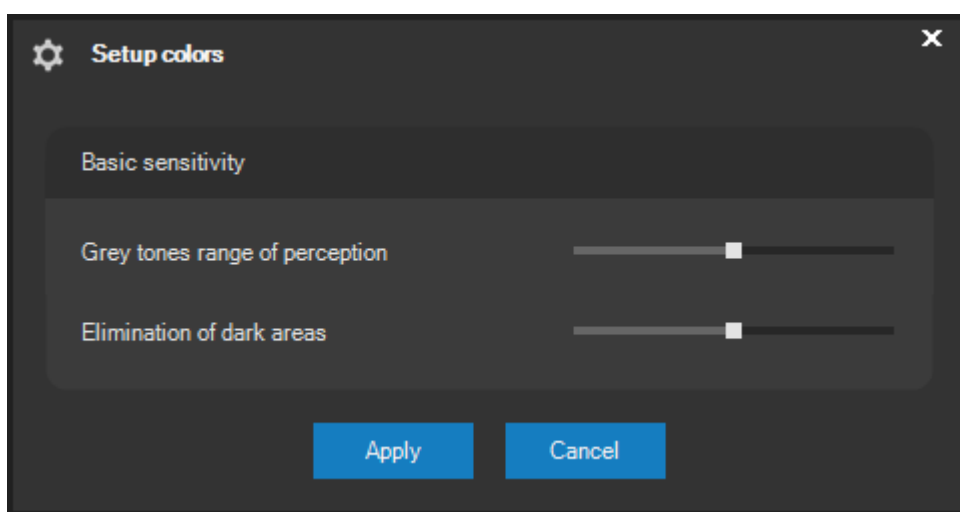
If a target is set, the neural network analysis is always executed, regardless of whether analytical event sources, scheduled statically or dynamically, are currently active or not.

The Save option allows you to permanently store the neural network output metadata and then replay and evaluate together with the camera video. Storing analytical outputs from a neural network is also necessary for using associated functions such as forensic search.

CAUTION

This metadata is stored in internal server databases within the installation folder and can be very demanding in terms of data quantity. Data is cleaned according to the metadata saving settings in the recordings administration section. System design shall therefore be adapted to the storage of metadata - installation drive size and performance.

The Detect colors option activates a GPU accelerated prevalent color scheme detection of the objects.



Depending on the scene, two parameters can be used to fine tune the color detection.

Grey tones range of perception determines the possible color deviation from a grey tone. Put simply, we can configure the color sensitivity in this way, i.e. whether a grey-blue will be detected as grey or blue.

Elimination of dark areas sets the level of favoring the deterministic color tones as opposed to dark parts of the object. Thus, for persons some dark clothing with only small colored parts can be detected (e.g. some protection suits).

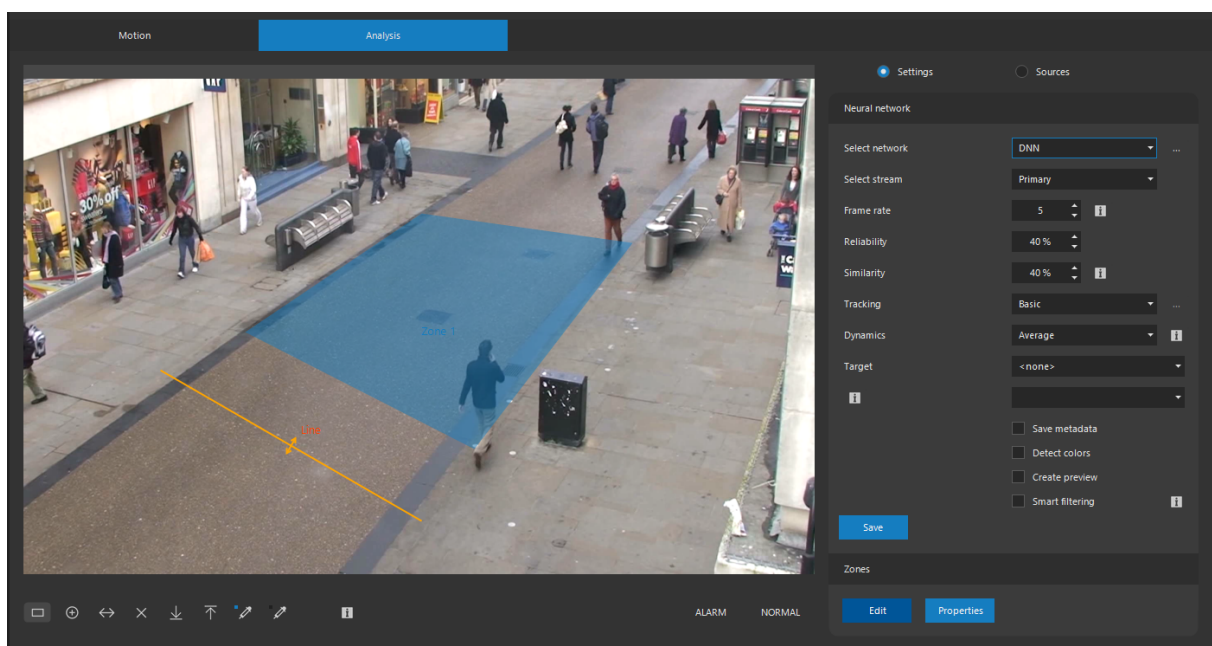
After activation, the detected colors are displayed together with the object directly in the scene. Whereas some objects may be assigned one color only (vehicles), some other types (persons) can be assigned two colors designating the upper and lower body prevalent colors.

By activating the Create preview option, apart from other neural metadata preview image data will be generated as well. This feature is not supported by all network types and can be used for example with

the Face recognition network to generate face images in canonical form that can later be inserted into the face database.

The Smart filtering option makes it possible to remove all object types from the scene that are not part of any existing event sources. The scene can be made clearer this way. If no sources exist, all types of objects will be displayed.

Under Zones, you can define areas, which, upon a defined object type enters this zone, will result in an event in the system. Areas can be defined as generic polygons.



A zone can be drawn after activating the zone edit mode by pressing **EDIT**. To start defining the zone, click anywhere in the image and continue by clicking each point of the polygon. Double-click to finish defining the zone and enter a name for the zone.

NOTE

When the zone definition is finished, the polygon is automatically closed. Therefore, it is not required to manually connect the points of the zone to form a closed shape.

The zone definition process can be cancelled at any time by right-clicking or cancelling the zone name dialog. A selected zone can be removed by pressing the Delete key or the Delete button. All changes like adding or removing a zone, or editing or changing its properties are saved automatically.

NOTE

If you hold the CTRL key when defining the first point of the zone, a so called negative zone will be created. Objects in this type of zone will be neglected.

If you finalize the zone already with the second point, this will create a shape defined by only two points, i.e. a line. Lines are activated when they are crossed by an object of the selected types, either in both directions or one of the possible directions. The direction can be selected by repeatedly pressing the Direction button. It is also possible to create polylines, i.e. lines consisting of multiple points. To prevent the zone to be closed after entering the last point, it is necessary to deactivate the Close zones button first (down on the left below the video).

If you wish to create a zone (including negative) that starts in another zone, you must hold the SHIFT key when starting creating the zone. Otherwise the zone would be activated and moved.

Editing an already existing zone or line

Any existing and selected zone can be moved arbitrarily within the visible video area. All its edge points are automatically highlighted at the same time. By moving any of these points you can change the shape of the zone or line. A selected point can be removed by pressing the Delete key or the Delete button.

NOTE

For a closed zone, the number of points cannot be reduced to less than three, for an open zone (line) to less than two.

If, on the other hand, a new point should be added to the zone, you have to select a point first and use the New point button under the video.



If the colors of the scene do not allow you to distinguish the created zones well, you can change their color by using the color indicator buttons below the video. You can change the color of regular zones and lines and negative zones and lines separately. Use the right button to restore the default color.

NOTE

The pen width for drawing the zone can be adjusted together with the drawing of other analytical outputs in the local client settings under Video settings.

Limiting the size of detected objects

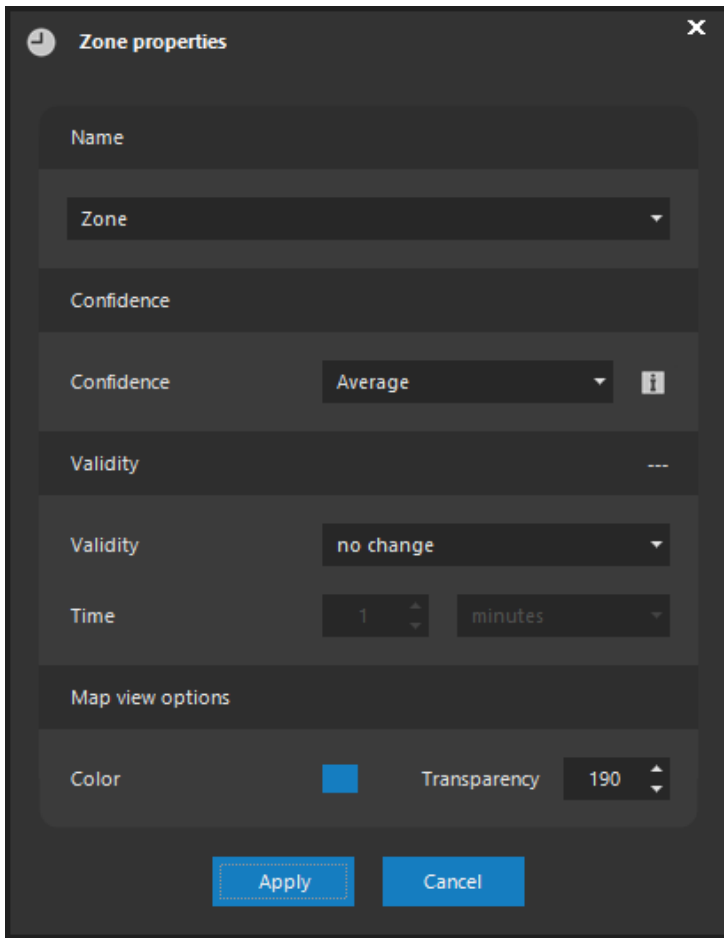
Using the limit object size buttons you can configure a minimum and/or maximum size of the objects for any zone or line. Setting the size is done by changing the object size rectangles – their height and width. When activating the minimum or maximum object size (or both) any object passes the size filter check provided it meets both the height and width criteria. E.g. when using a maximum size, the object is not allowed to exceed the configured height and width at the same time.

NOTE

Under active size filter, the objects not satisfying the size conditions are still detected and displayed in the scene, there are, however, excluded from any event handling – they cannot activate an event source and raise an event.

Zone properties

You can change the name and other properties of the zone at any time by using the **PROPERTIES** button. The system automatically checks for duplicate names.



The image shows a 'Zone properties' dialog box with a dark theme. It has a title bar with a clock icon and a close button. The dialog contains several sections: 'Name' with a text input field; 'Confidence' with a dropdown menu set to 'Average' and an information icon; 'Validity' with a dropdown menu set to 'no change' and a '---' indicator; 'Time' with a numeric input set to '1' and a unit dropdown set to 'minutes'; and 'Map view options' with a color selection (a blue square) and a transparency slider set to '190'. At the bottom are 'Apply' and 'Cancel' buttons.

A selected zone can be assigned a zone reliability level, which is set to average level by default. This parameter can be used to fine tune the alarm sensitivity of the selected zone. Besides the standard object detection percent reliability level (object score) this parameter describes the object identification reliability over time (i.e. whether the object is still the same). This parameter affects crossing line zones only, as filled zones can achieve a similar effect of increasing the reliability by moving the time spent in the zone parameter away from zero.

In this dialog, it is also possible to limit the validity of the zone only to a certain time, either by entering a predefined or custom validity. After the configured time has expired, the zone is automatically deactivated.

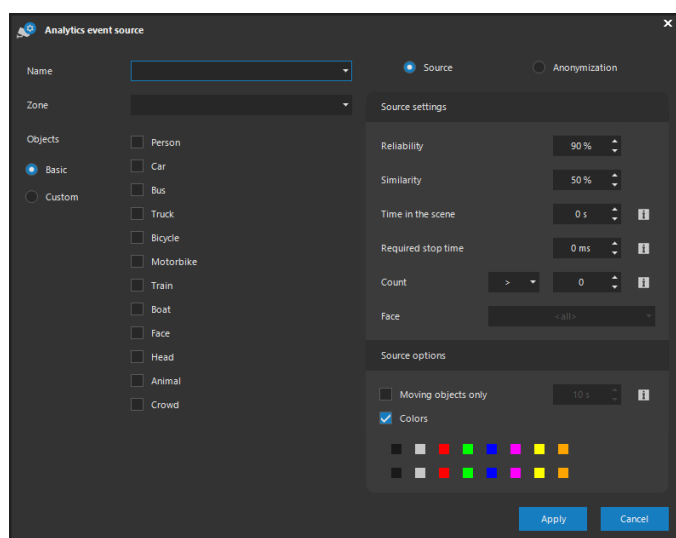
TIP

It might be beneficial to use the limited zone validity for negative zones.

In **Map view options**, zone color and transparency can be specified, which will be used for displaying the zone in the map.

On the **Sources** tab under Event sources, for each camera, you can define its event sources that will be handled further as any other event source in the system (scheduling, event scenario).

If a neural network is assigned to the camera, you can use the **NEW** or **EDIT** buttons to display the dialog for creating event sources. The **DELETE** button removes the selected event source.



When creating a new or editing an existing event source, you must enter the name, specify the zone in which you would like the neural network to respond to selected object types and choose one or more object types from the list. Objects are divided into two groups, it is possible to select from both at the same time. The basic group contains objects that are supported by freely available ATEAS neural networks, the custom group displays object types that you can create by yourself. For more information, see the chapter on custom object types.

NOTE

The animal object type only supports a few common animal species such as dog, cat, cow, sheep or horse and requires sufficient resolution for successful detection; detection is not suitable for objects in the background.

TIP

For source names, names of existing sources are suggested as you type. Using identical source names automatically consolidates metadata searches and generated charts.

The reliability and similarity settings allow us to configure thresholds to which the network is convinced it has detected an object of a specific type.

Similarity is a different type of metric than reliability and is used for some network types like face recognition. It is described above in the analytics configuration section.

NOTE

When creating an event source, reliability and similarity can be set to higher values than for object detection for the selected camera. This enables displaying objects with a lower reliability without the system producing an event.

Whether the given configuration has the potential to induce a system event is clear upon storing the zones and event sources directly in the analysis window based on the ALARM and NORMAL states. The zone, in which an event occurred, is automatically highlighted.

For cross line events, advanced tracking may lead to better results especially for crowded scenes, because, in contrast to basic tracking, the alarm reliability is not required to be achieved directly on the line, but also later.

By increasing the Time in the scene value from the default zero value, the event will be created only after the object remains in the given zone for the specified number of seconds. An event can therefore be generated, for example, if a person remains in the scene for a suspiciously long period of time, if a car drives too slow on the highway, a car stops in a tunnel or similar.

NOTE

This time parameter is only effective if tracking is active and for area type of zones.

The Required stop time setting helps to respond to situations, when an object refuses to stop for the specified time interval. For this feature to be used, at least two zones must be created with one of

them being a closed (detection) zone and the second one being a closed or open (alarm) zone. An event occurs in the alarm zone, if an object doesn't stop in the detection zone for the required interval.

For this feature to work reliably, it is, of course, necessary to use a detection FPS compatible with the required stop time. E.g. using a FPS of 5, stop times shorter than 200 ms cannot be detected.

TIP

This feature can be used as an automated Stop sign violation detection system.

The Count setting allows the user to specify the number of objects that will trigger an event. This way (maybe also in combination with the time parameter) the system can automatically respond to a group of loitering people or to traffic congestion. The parameter can be configured as an exact value or a value greater or less than specified. If the value equals zero, an event will arise if the zone doesn't contain any objects (an alternative solution would be a negation operator in a complex event source).

If multiple object types are selected, the count refers to all types. If we needed to trigger an event for a specific number of multiple object types (while making difference in the object types), we would have to create multiple neural event sources based on the same zone and combine them within one complex event source.

If the event source contains an object of type face and face recognition is running, the event can be restricted to faces from a specific group only as specified in the Face section. Restricting to a single person can be easily achieved by adding just one person of interest to a separate group.

The Moving objects only option only takes moving objects into consideration when evaluating events. The time value specifies the amount of time an object must be at rest to not be considered a moving object.

TIP

This can be helpful for eliminating some false alarms even without making use of negative alarm zones.

Using the Colors option a list of colors can be displayed, which might be used as a part of event evaluation. If some colors are selected, only objects colored with one of the selected colors will

activate an event source. For person object type colors in two rows can be selected relating to the upper and bottom parts of the body.

After one or more event sources are created, we can configure or use these further as part of the server based event sources.

NOTE

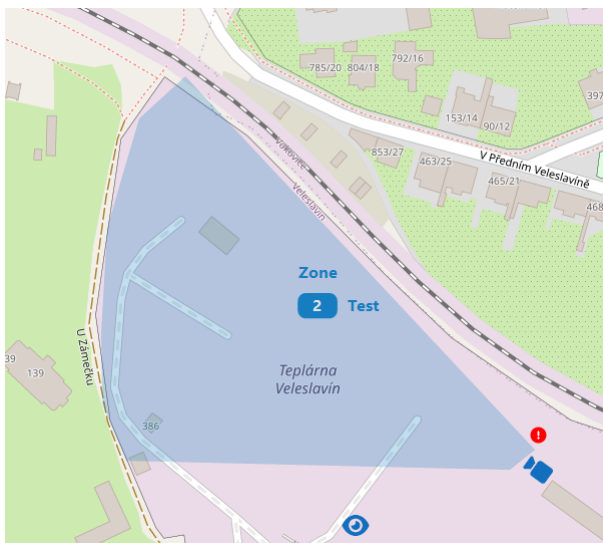
All these parameters with exact same meaning can also be used when searching in recordings using stored neural metadata.

NOTE

All analytical event sources in the list also display auto generated numbers which are used for publishing the events over the ATEAS API integration channel.

11.2.10. Zone map localization

A quite similar approach to localizing cameras, external elements or user buttons can be used to localize zones. After selecting a zone and pressing the location button in the map, in contrast to a single point, you need to create a polygon by multiple clicks followed by a double-click.

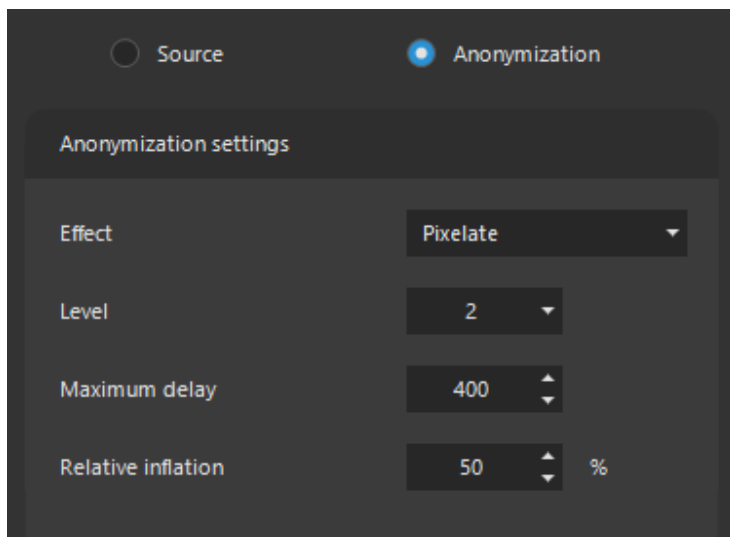


Once zones are localized in the map, apart from better awareness, video can be displayed when hovering over the zones. In addition, the camera can be sent to a bound zone preset. Moreover, automatic zone counters will be displayed in the map, which are described in a separate subchapter.

The zones are also integrated in the map window search.

11.2.11. Video anonymization

Camera systems must handle visual personal data in accordance with the requirements of the applicable legislation regarding the protection of personal data. Using the options in the Anonymization section, such requests can be easily fulfilled.



All object types configured in the event source settings will be anonymized. Anonymization applies to both live and recorded video. Special deanonymization permission is required to display original live or recorded video without the anonymization.

The Effect drop-down offers some visual implementations of the anonymization ranging from completely blackening the objects to pixelization. For pixelization, a level can be selected. The higher the level, the stronger the anonymization effect will be.

NOTE

An equal anonymization level is applied to close and remote objects for a given effect strength. The size of the pixelization squares differs and adapts to the size of the objects.

The Maximum delay value is in milliseconds and determines the time validity of the detected objects for anonymization purposes. As soon as data for detected objects is not available for a given zone within the specified interval, the entire zone would be anonymized to prevent any possible unauthorized display of sensitive data in the video.

The Maximum delay also determines the additional latency of the anonymized video introduced to prevent partial displays of objects with incomplete anonymization due to the slight delay of neural network computations.

The Relative inflation value determines the percentage by which the anonymization area will be enlarged compared to the actual size of the objects.

TIP

The object anonymization rules and settings can be different in each created zone.

11.2.12. Server based static masking

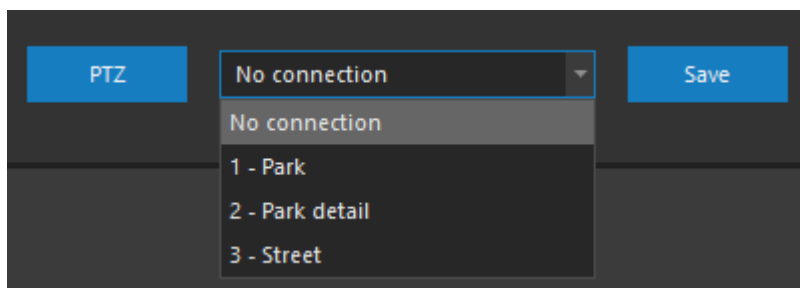
If no objects but a zone are selected when creating an analytics event source, static masks will be created automatically. In these cases, the whole zone will always be anonymized using the configured anonymization effect.

NOTE

Compared to masks created in cameras, major benefits apply. For example, unmasking is only a question of permissions and does not require connecting and storing a second stream.

11.2.13. Connecting analytical sources to presets

Using PTZ cameras makes the concept of zones and any subsequent analysis more complicated because the camera can be turned around. That's why you are given the option to connect zones (closed zones or even lines) to camera presets. Connecting zones to a preset is done by selecting a preset from the dropdown list under the video preview.



After selecting a preset, camera is automatically sent to that preset and zones already connected to this preset are displayed, which you can now edit or create some new.

Any active events based on zones bound to a preset can only be activated once a camera is sent to that preset, which can be done manually by the user, automatically using a tour or as a result of an event. Once the camera is moved away from such preset, the event can no longer be raised.

This feature also takes effect during smart search, where only relevant results will be presented according to the selected preset.

CAUTION

When adding a ptz camera to server multiple times and connecting them with detail offset values, subordinate PTZ is automatically activated for cameras with offset values set to keep the ptz priorities working. Therefore, preset bound analysis must be configured on the target device only.

If presets need to be adjusted, it is possible to do it directly from the analysis window. The **PTZ** button activates full PTZ control and the **SAVE** button allows to overwrite the current position.

TIP

This method saves time, if slight adjustments of the presets according to the already created zones must be performed.

11.2.14. Detailed setup

The detailed parameters for individual cameras are adjusted through interfaces that come directly with each camera (mostly web interfaces accessible through the http protocol).

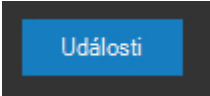
The **SETUP** button automatically opens the default web browser, which is redirected to the camera web. The fundamental difference between direct access to the camera web is the fact that web access is granted directly by the camera server through its address and designated port 8506. Provided the web browser has this address open and another camera is selected from the list of cameras in the administration section, upon refreshing the page in the browser, you will be redirected to the newly selected camera.

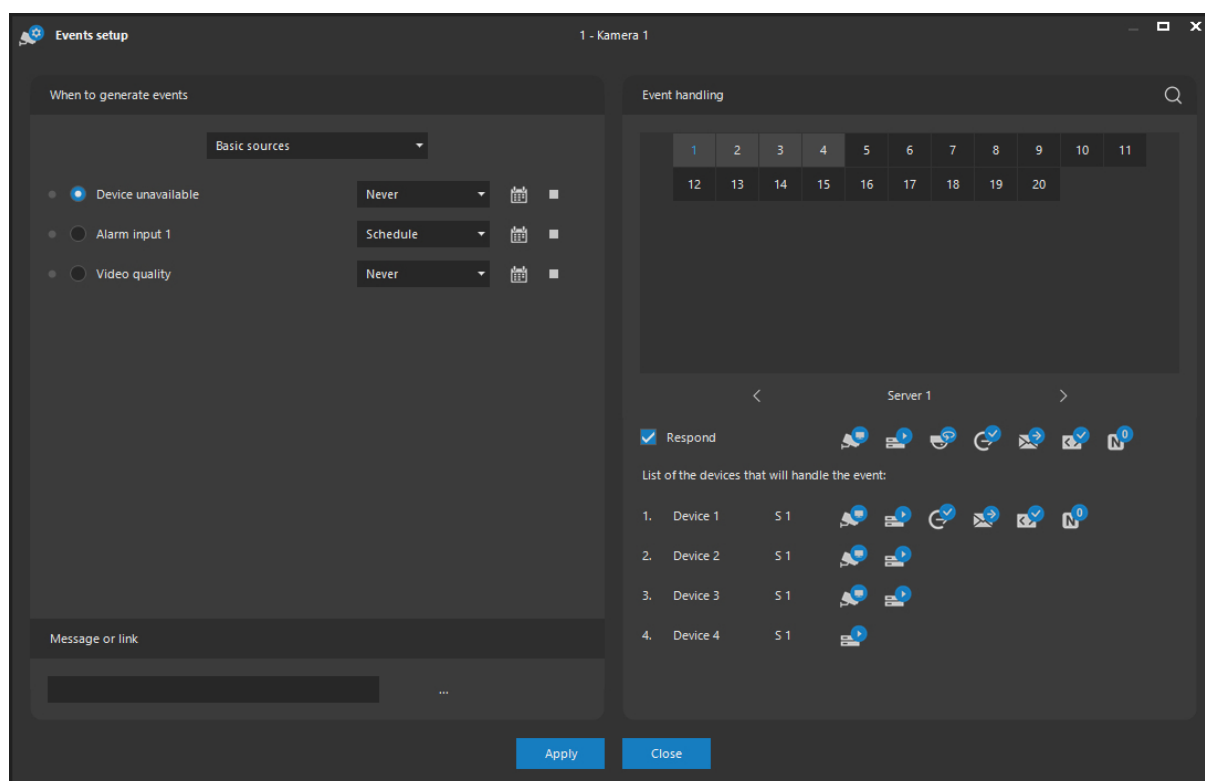
NOTE

With this function, you can access the camera web on the local network or remotely at any time without having to redirect their ports, for example, using NAT. The only port that must be available is the 8506 port of the camera server.

11.2.15. Events and their management

The Events section (mapping and setting event sources and creating event scenarios) can be accessed by pressing the **EVENTS** button. All event management related actions are performed in this window. The basic principle is to create an event scenario for a specific event source (event input). An event scenario for a selected event input can include any actions performed on other cameras or servers.





Event sources

In the When to generate events section, a list of all event sources is available for the selected (and currently configured) camera. Individual sources are divided into logical groups according to their nature (basic sources, server sources, custom sources, license plates, analytics). A color indicator is presented to the left of each event source depicting the current event status.

Commonly used Basic sources include:

- **Device unavailable:** Continuous testing is performed for cameras connected to the camera server to determine their presence in the network. A detected failure could lead to an event (this does not concern the loss of video signal for devices with analog video input, see below).
- **Alarm input activation:** Depending on configuration, the event can be invoked by a state change on the relevant camera alarm input.
- **Video quality control by monitoring the frame rate.**

Commonly used Server sources include:

- **Motion detection:** Based on the analysis of the images from the camera directly on the server, data for detected motion is constantly evaluated, according to the configuration of detection mask, sensitivity, object size etc.

Commonly used Custom sources include:

- Audio detection: This function can be invoked by detecting audio using cameras supporting the function (exceeding the volume threshold or on the contrary, reaching the quiet threshold).
- Tamper detection: The event can be invoked upon detecting camera tamper on cameras supporting this function (rapid rotation, covering the view, loss of light, spray on lens).

NOTE

More information on custom events is provided under chapter Custom camera events.

Commonly used events from the License plates group include:

- Unregistered LP: The event will be invoked if a LP, not registered in any list, is detected.
- White listed LP: The event will be invoked if a LP, registered on the LP white list, is detected.
- Black listed LP: The event will be invoked if a LP, registered on the LP black list, is detected.
- User defined LP: The event will be invoked if a LP, registered on any of the LP user defined lists, is detected.

NOTE

More information on vehicle LP detection is provided under chapter Add-ons management – LPR engine.

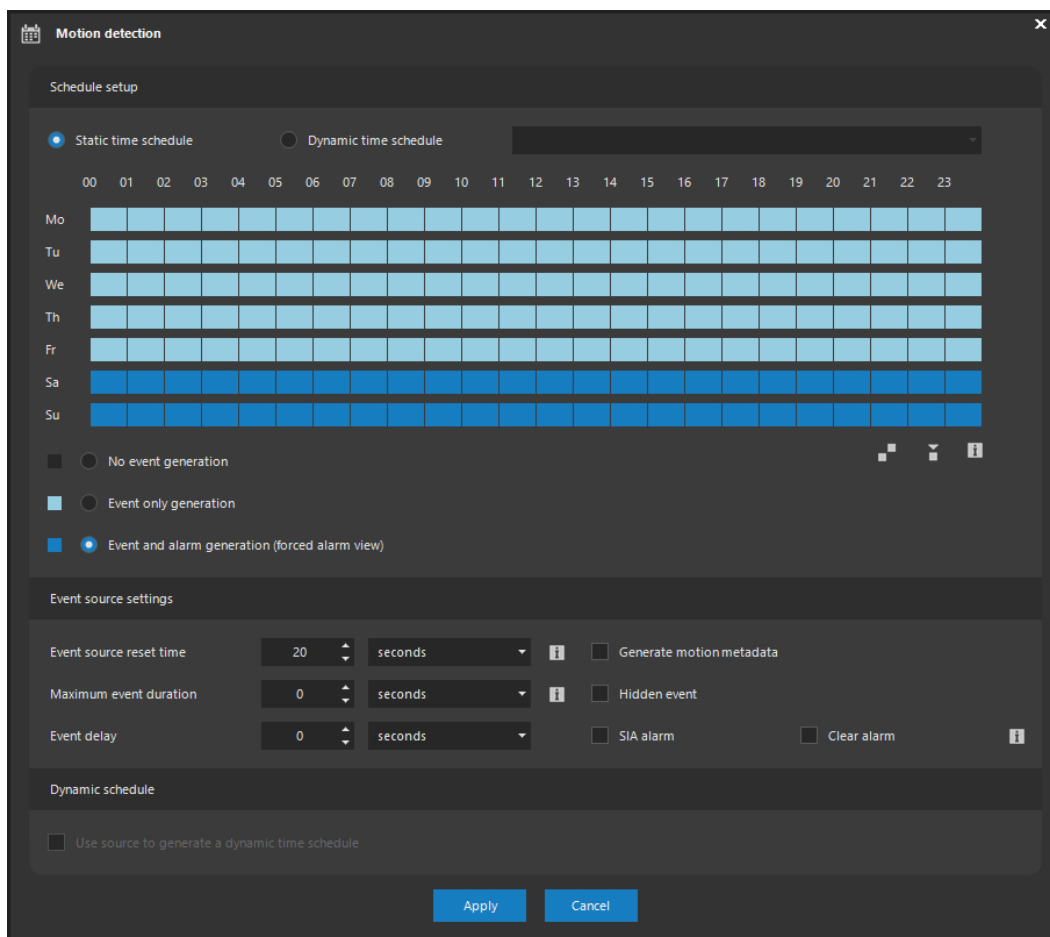
The Onvif option is also available in the list of Event sources for cameras connected via Onvif. This option is used to create events from sources provided using Onvif. The following subchapter describes the utilization of these sources.

At the end of each event source line, the currently assigned color is displayed. The color can be changed by clicking on the color symbol and selecting any user-defined color. The color is then used for events displayed on the replay timeline when replaying recordings.

TIP

You can quickly restore the original default color by using the right mouse button.

You can select the time when an event source generates an event or alarm in the drop-down list next to each event source. The first option is Never (the event source will not be monitored), the second option is Schedule. After selecting the Schedule option or pressing the calendar button, a window will be opened where it will be possible to graphically mark the time, for which the event source will be monitored.



In the Schedule setup section, the event input can get assigned a created static time schedule. Another option is to use the dynamic time schedule. Dynamic scheduling is described in a separate subchapter. If a dynamic schedule is selected, the static schedule design control becomes unavailable, for whether or not the event input is active (for example if a motion detection is in progress) is determined dynamically depending on another event input.

When using static scheduling, a control for graphical schedule setup, for monitoring a certain event source (event input), is available. Individual rows include days of the week. A day divided into 24 hours is available in the vertical direction. The minimum resolution is 15 minutes. Individual segments 15 minute segments can be selected by moving the mouse while holding either the left or right mouse button. If you use the left mouse button, the switch setting under the control will always be used. Use the right mouse button to delete the content, i.e. the content will be rewritten to default values (refers to the left button when the No event generation switch is checked).

TIP

To quickly select a day or entire week, double or triple-click the area.

To quickly apply a static schedule to a different event source, you can use the copy and paste buttons placed under the scheduler.

TIP

To quickly schedule working hours in multiple days, use the ALT key.

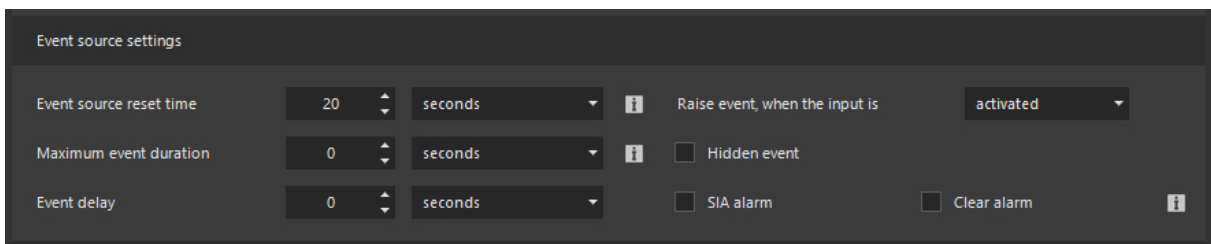
The difference between the Event only generation and Event and alarm generation switches rests in the significance of the generated event. The event scenario remains the same for both cases. Considering the fact that common events do not force clients to automatically switch to the event view and can also be filtered by clients completely, you can achieve very efficient scenarios. If a person strolls down the hallway during the day, the application starts recording. If the same happens during the night, the hallway will automatically be displayed on the monitor.

The Hidden event option can be enabled for each event source (identical option is available also for scheduled system events). If the option is enabled, users will not be informed about the event, as it will be hidden from system clients at the time of occurrence. The event scenario, all reactions to the event as well saving to system metadata runs as usual. A hidden event, however, is not saved among the events triggering the recording, so it is not included in the list of events in the Recordings window and it does not interfere with the timeline when replaying recordings.

NOTE

Hidden events can be used, for example, with complex events where you do not wish to promote every single event towards system clients. Using hidden events is more suitable than alternative solutions such as restricting user rights to receive events from all or specific cameras or switching off receiving standard events under local settings.

Additional event source parameters can be adjusted in the Event source settings section.



The screenshot shows the 'Event source settings' window. It contains three rows of settings. The first row has 'Event source reset time' set to 20 seconds, an information icon, and 'Raise event, when the input is' set to 'activated'. The second row has 'Maximum event duration' set to 0 seconds, an information icon, and a 'Hidden event' checkbox. The third row has 'Event delay' set to 0 seconds, a 'SIA alarm' checkbox, a 'Clear alarm' button, and an information icon.

Parameter	Value	Unit	Info	Option
Event source reset time	20	seconds		Raise event, when the input is: activated
Maximum event duration	0	seconds		☐ Hidden event
Event delay	0	seconds		☐ SIA alarm Clear alarm

You can determine whether or not an event will occur while activating or deactivating the input for binary input event sources (not related for example to motion detection). This is important, for example, for certain motion detectors that are activated while there is no motion, and deactivated when motion is detected.

The Event source reset time parameter indicates the minimum duration an event input must remain inactive, ensuring its following activation leads to a new event being created. If this configured period does not lapse between two input activations, the system combines both occurrences to a single event.

The maximum event duration limits the duration of a single event. This way, you can e.g. protect your media store from exhaustion if cameras are configured to use high recording frame rate during events or ensure the return of a dome camera from an event tour after the maximum duration elapses.

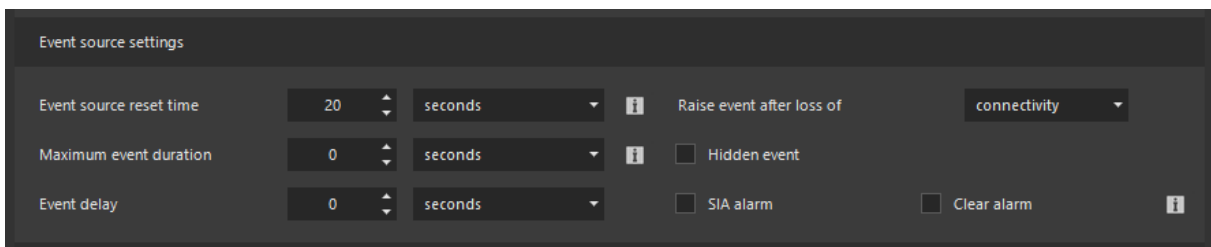
NOTE

If the maximum event duration is set to the reserved value of zero, there maximum event duration will not be specified for the event.

The reset time mentioned above can be configured individually for each input.

Event delay can be activated for all event sources. If the event delay is set to a value greater than zero, the camera server will wait, after the event source has been activated, for the duration of the configured event delay and generate the event later. If the event source is deactivated again during this period, the event is not generated. This feature can be used in many practical situations, e.g. if we intend to monitor a door that was left open, but at the same time wish to exclude common passages through the door, when the door closes after several seconds.

Advanced settings are available for a Device unavailable event source in which the user can define how device unavailability will be evaluated. By default, camera unavailability is evaluated as the camera being unavailable at the defined address and port via regular TCPIP messages (connectivity option).



This evaluation method automatically informs the user about various failures such as camera failure on the network, disconnection, power failure etc. There are situations, however, when a camera (or rather video) may experience failure without losing IP connectivity (e.g. a camera firmware issue). In this case, system clients can be informed by a warning message directly in the camera window (provided the camera is currently being monitored), however, generating a system event would not be possible. If the user were to configure the unavailability evaluation based on the loss of video feed, the system will be capable of generating an automatic event even in these cases.

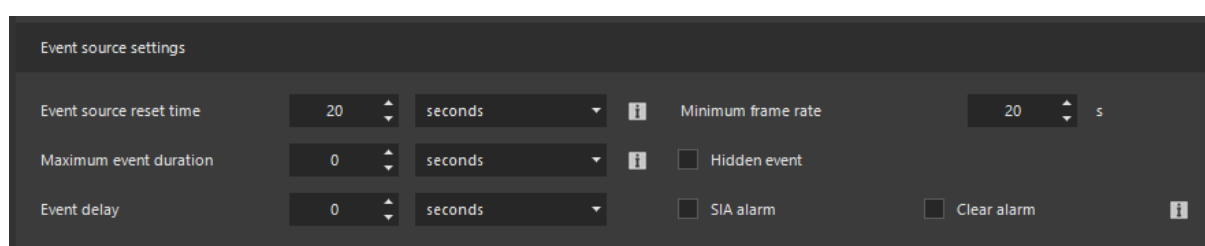
NOTE

The evaluation of camera unavailability based on the loss of video feed does cover a larger set of various failures, on the other hand however, false alarms may be generated for short-term network congestion (video break up) etc.

CAUTION

The evaluation of camera unavailability based on the loss of video feed cannot be used when turning off the permanent connection with the camera (cameras are connected based on video on demand policy).

A threshold value for the frame rate can be defined under advanced settings for a Video quality event source. If the current frame rate drops below this value, an event will occur.



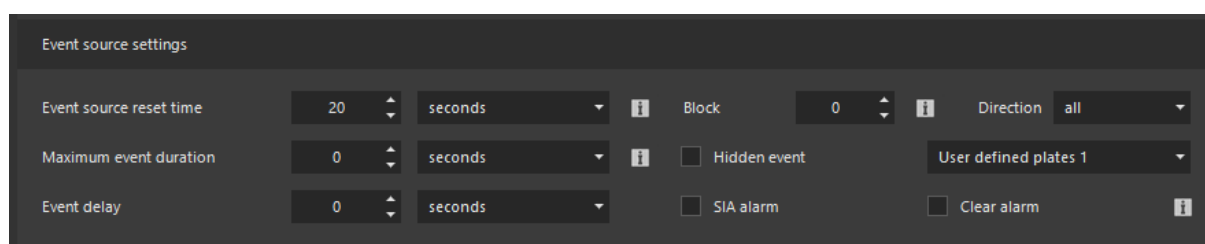
The screenshot shows the 'Event source settings' window for a Video quality event source. It includes the following controls:

- Event source reset time:** 20 seconds (with an info icon).
- Maximum event duration:** 0 seconds (with an info icon).
- Event delay:** 0 seconds.
- Minimum frame rate:** 20 s.
- Hidden event:** ☐
- SIA alarm:** ☐
- Clear alarm:** ☐ (with an info icon).

NOTE

As is the case with other event sources, monitoring video quality can also be combined with the delayed event tool. For example, if we decide to tolerate a temporary drop in video quality for a duration of 5 seconds, the event can be delayed for this given duration.

Advanced settings for LP detection and recognition event sources also enable specifying the number of seconds during which the detected LP is blocked on other cameras of the camera server.



The screenshot shows the 'Event source settings' window for an LP detection and recognition event source. It includes the following controls:

- Event source reset time:** 20 seconds (with an info icon).
- Maximum event duration:** 0 seconds (with an info icon).
- Event delay:** 0 seconds.
- Block:** 0 seconds (with an info icon).
- Direction:** all (dropdown menu).
- Hidden event:** ☐
- SIA alarm:** ☐
- Clear alarm:** ☐ (with an info icon).
- User defined plates:** User defined plates 1 (dropdown menu).

It is beneficial to use blocking, for example, for two-way entrances with one lane and two cameras - for vehicle entrance and exit. In this case, we would like other camera to ignore the respective LP for a given period of time.

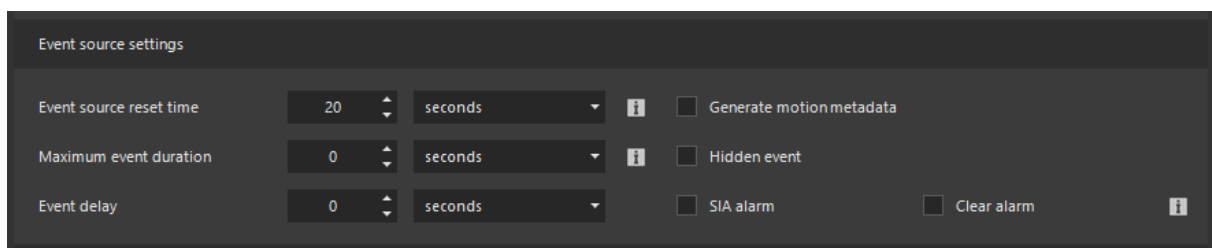
Using the Direction option, you can limit the event to occur for the specified direction only.

NOTE

For the direction determination to be reliable, it is necessary to correctly configure the frame rate and recognition threshold to cover the entire focused range of the camera, where the size of the LP lies between the minimum and maximum width.

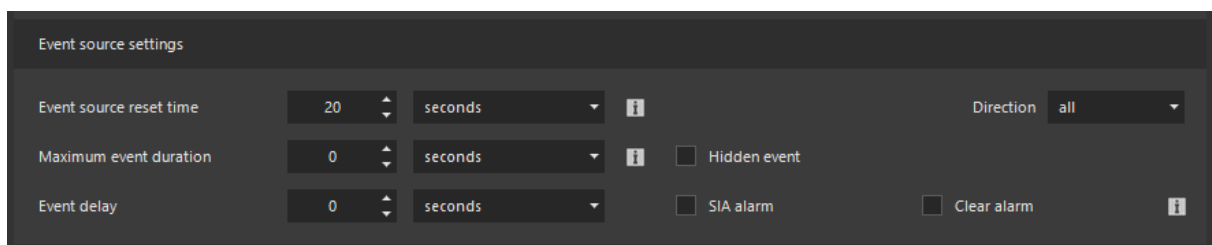
For user defined LP event sources in particular, a non-default LP list can be selected. Therefore, it is possible that different cameras (e.g. connected to different servers) evaluate this very event source based on different lists of license plates.

The server based advanced motion detection enables to activate the generation and storing of metadata for subsequent searches for changes in the image using the smart search feature.



Storing this metadata is similar to storing the neural network metadata, the same maximum storage duration applies. When activated, the smart search feature will allow searching for general objects as well, instead of just the objects of neural networks.

Using the Direction option, custom events with the UIC code can be bound to a specific detected wagon direction.

**NOTE**

In contrast to LP, where approaching or leaving can be detected, UIC detects a left or right movement.

If open, the SIA alarm option adds this alarm to the SIA integration channel.

Checking the Clear alarm option activates the extended alarm handling mode for the given event source. See also the separate Alarm handling mode subchapter for more information.

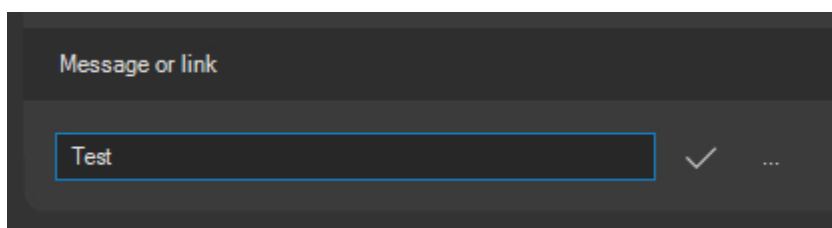
NOTE

The SIA alarm and Clear alarm options apply to alarms only, i.e. in situations, when a static time schedule is designated with the darker color.

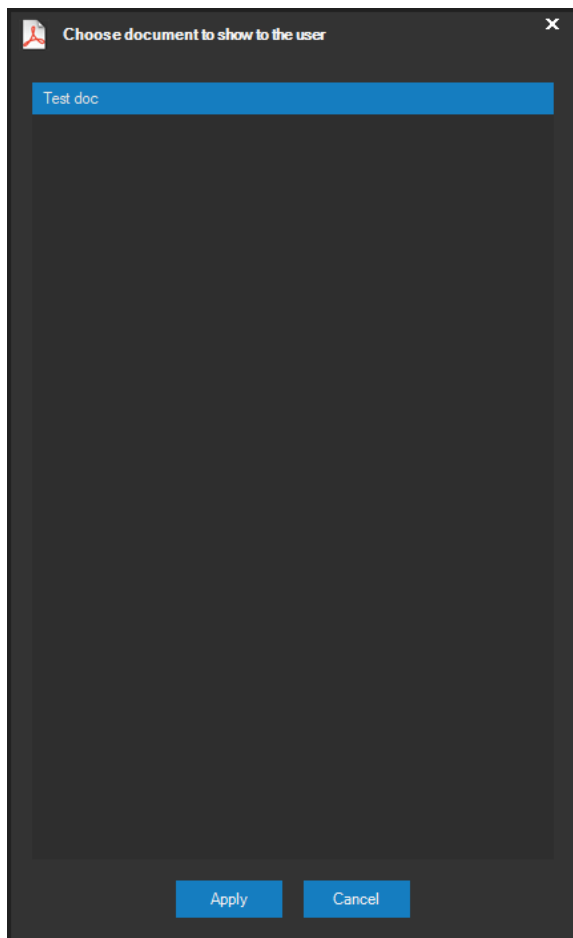
In the Dynamic schedule section, you can make certain event inputs use their statuses to generate a dynamic schedule to can control the switching of other system event inputs. For further information, see the corresponding subchapter.

The adjusted time schedule is preliminarily saved by pressing the **APPLY** button. Its transfer to the server is a part of saving process and camera setup, performed by pressing the **APPLY** button in the main events window.

In the bottom part of the window, you can set a text message for a selected event input (with the switch checked). When an event from this event input occurs, this message will be displayed to the user, together with other information about the event. The message is preliminarily saved by pressing the button next to the text field.



If a simple text message is not sufficient enough for the given event source, a document previously uploaded to the system can be added to the event. A document is submitted by pressing the three dot symbol button.



Once the document is submitted, the Message text field will display a special syntax indicating a document has been assigned. The syntax consists of the doc: prefix followed by the document title enclosed in square brackets.

NOTE

The syntax can, of course, also be entered manually, although selecting a document directly from the list is much easier.

The last option is to use a hypertext link that can be activated after receiving the event and opened in a web browser. Any text starting with the http or https protocol prefix will be considered to form a hyperlink.

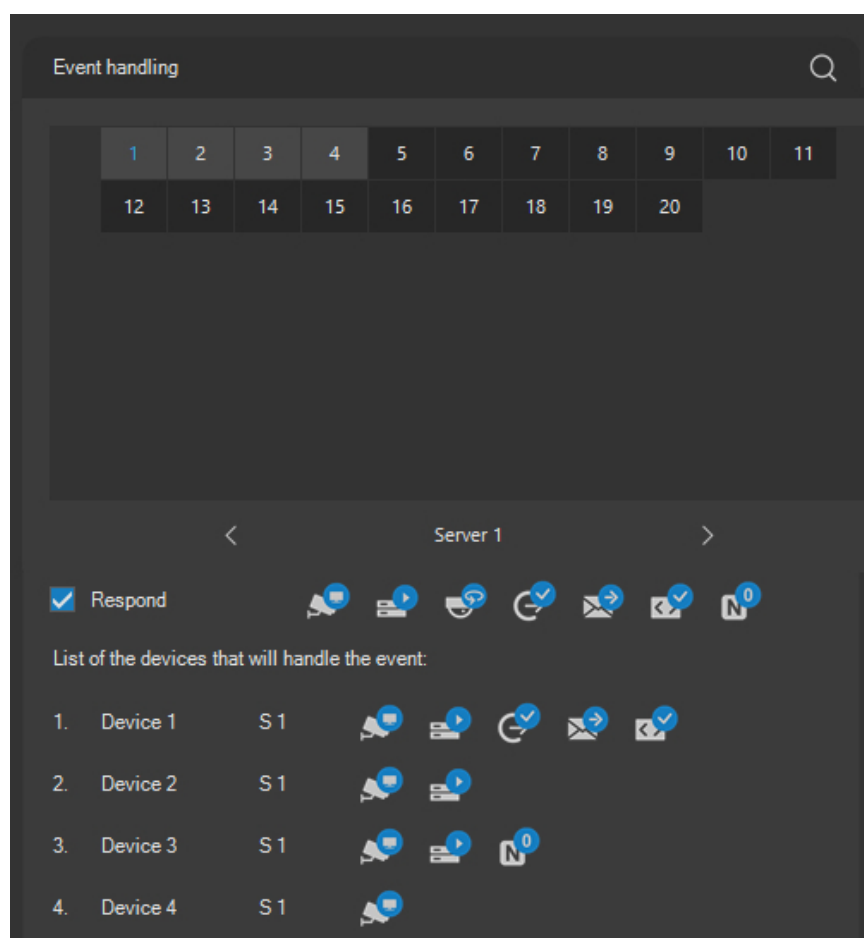
Event scenario

The event scenario is configured in the Event handling section. Each event scenario is set for a specific event input, whose switch has to be marked.

An event scenario can include any cameras from any servers. In order to assign a camera to an event scenario, select a server (in the bottom right corner of the control panel displaying camera numbers), then select a camera, and finally check the Handle the event checkbox. In order to remove a camera from an event scenario, uncheck the previously checked checkbox. Cameras already included in the event scenario are always highlighted for a selected server. A list of all cameras (from all servers) included in the event scenario is continuously updated along with icons symbolizing actions. This list is found under the camera summary of the selected server.

You can display a search field by pressing the search symbol and search for cameras by their names.

In order to display cameras from another server, you can use the arrow buttons near the server name or click on the name and select a server from the list.



You can define actions the camera will perform during an event and which will be included in the scenario for a camera included in the event scenario and selected from a camera selection control panel (indicated by a blue text). The event source camera is selected automatically.

In case there is a greater number of cameras in the system, you can display a list of all available servers, from which you can make a direct selection with no need for listing. You can also select a server which is currently offline, since the event scenario setup of individual camera server connections does not require the servers to be online.

CAUTION

Individual cameras can be included in several event scenarios. When several events occur simultaneously, actions for all corresponding event scenarios will be initiated for the specific camera. If an event recording is configured, it will stop after all events that invoked the recording stop.



If cameras are gradually added to the event scenario, they are always added to the end of the list. A total limit of 64 cameras applies for the cameras that can simultaneously respond to one event source.



This button works as a switch. Its status can be switched between pressed and not pressed by using a mouse. When this button is pressed, a selected camera will be included in the event scenario, i.e. it will belong to a group of cameras, automatically displayed to the user when an alarm occurs on a certain event input.

NOTE

If there is no camera included in the event scenario or no camera has been included in the event view, the event view will implicitly consist of a camera which invoked the event. This camera will also be displayed if an alarm occurs, or if you select a certain event from your list in the live window.

NOTE

The resulting event view will consist of all cameras with this option activated in the event scenario. The event view is always selected from the predefined square or wide-screen views to ensure the given number of cameras are displayed with the least amount of empty camera windows (ideally zero).

NOTE

Camera positions in the event view are implicitly determined by the order of the cameras in the event scenario. These are displayed in the view in rows, left to right and top to bottom.



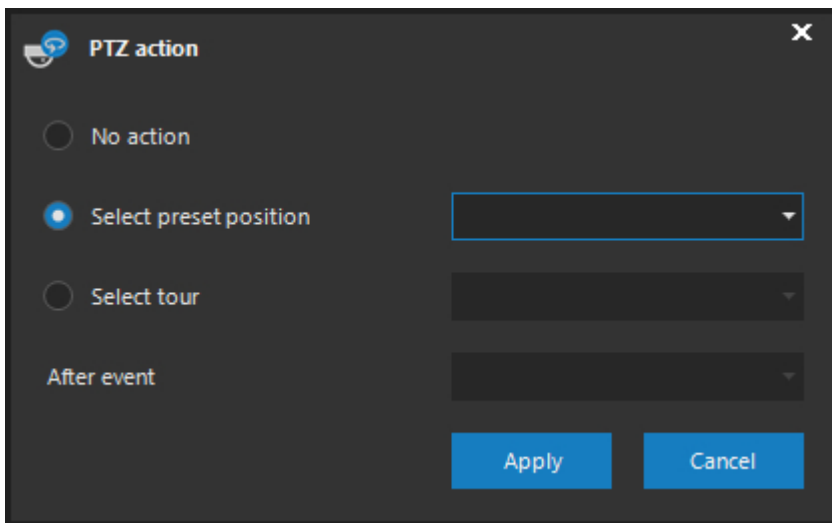
This button works as a switch and can be used for determining if the camera will start recording when an event occurs. A special function can be activated clicking the right mouse button – see below.

NOTE

In order to make a camera start recording, when an event occurs, it has to have a recording rule (profile) assigned. A recording rule enables recording at a specific time (either specific time recording is activated during an alarm or the frame rate is enhanced during an event). Otherwise, the event might not be recorded or the record parameters might not be configured.



This button is available for PTZ devices only, and enables to automatic camera positioning to a selected preset point during an event. Alternatively, you can specify an alarm tour, which the camera will be switched to during an event. The third possibility is to turn off all control actions related to the selected camera for a specific event scenario. In order to be able to select presets or tours, they must be created by an authorized user first.



If you use the third possibility (i.e. the camera will be switched to an alarm tour), you can optionally enter a preset point which the camera will be positioned to when the event ends. This can be used especially when a camera is positioned to a specific default position, it is then switched to an alarm tour during an event and it is necessary to ensure that it returns to the previous (default) position after the event ends.

NOTE

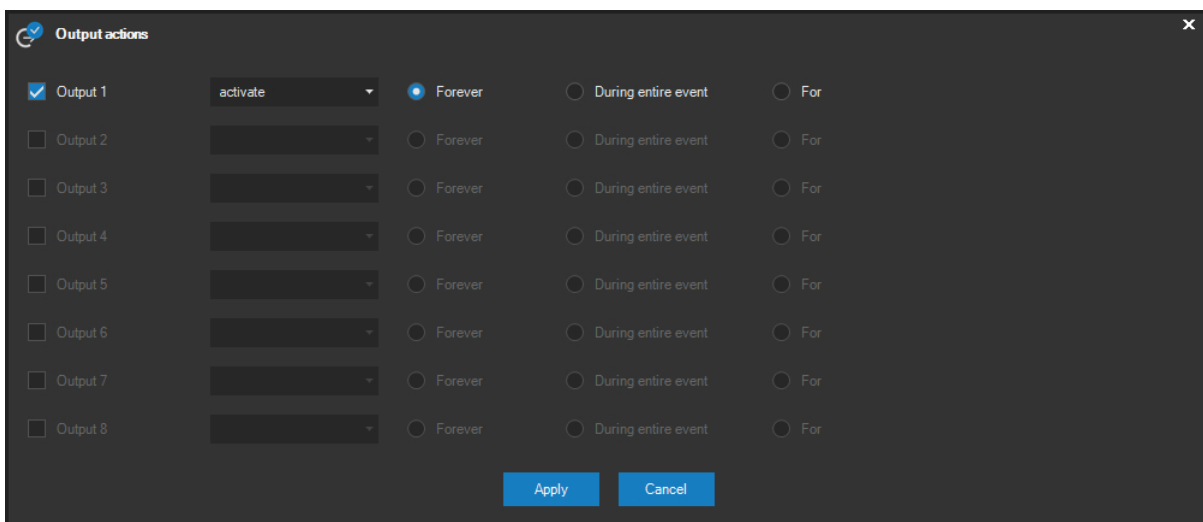
If a camera is switched to any tour even before an event, an alarm tour (selected in the previous window) will be applied during the event. The previous tour will be reactivated as soon as the event ends. Therefore, there is no need for setting a final preset.

NOTE

Even when an alarm tour is in effect, it is possible to pause it with a manual intervention into the camera control. The event tour, however, is only paused for several seconds, regardless of the resume time interval of the tour.



If you are using a camera or a video server equipped with outputs, you can automatically activate or deactivate these outputs for a specific time, forever or for the duration of the event by pressing this button. A dialog will be opened where the user can set this time or completely turn output activation or deactivation off.



Output actions

Output	Action	Forever	During entire event	For
☒ Output 1	activate	☒	☐	☐
☐ Output 2		☐	☐	☐
☐ Output 3		☐	☐	☐
☐ Output 4		☐	☐	☐
☐ Output 5		☐	☐	☐
☐ Output 6		☐	☐	☐
☐ Output 7		☐	☐	☐
☐ Output 8		☐	☐	☐

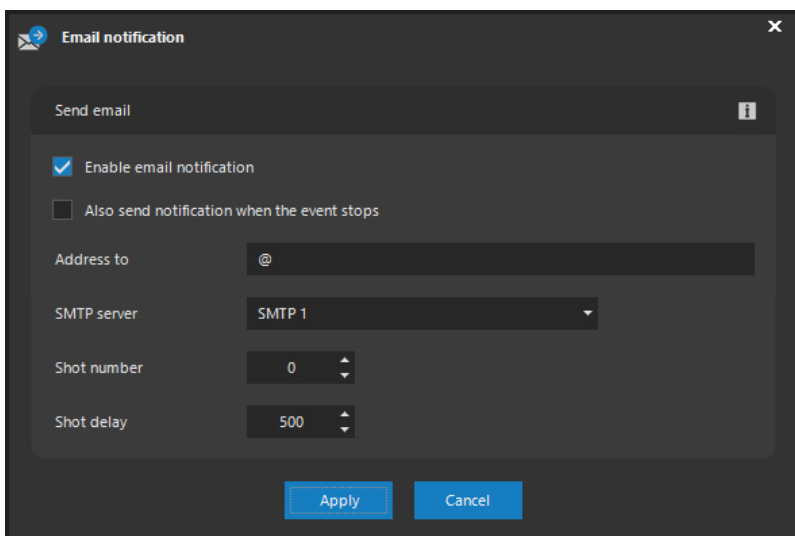
Apply Cancel

CAUTION

One set of inputs and outputs is normally available on the device when using multi-port video servers. To ensure no contradictory settings are available, which refer to both inputs and outputs for various cameras of the same video server, the settings are always available for a camera which is assigned to the first port of a multi-port video server.



This button activates email notifications when an event occurs. If this feature is activated, administrators can receive emails in the event of a camera failure, for example. In case of an invasion, these emails can also include attachments containing snapshots from cameras etc. A window enabling e-mail communication setup will be opened after pressing this button.



Email notification

Send email ⓘ

☒ Enable email notification

☐ Also send notification when the event stops

Address to: @

SMTP server: SMTP 1

Shot number: 0

Shot delay: 500

Apply Cancel

In the sending email section, you can either activate or deactivate sending e-mails for the selected event source using the Enable email notification option. If the Also send notification when the event stops option is enabled, an e-mail notification will also be sent when the event ends.

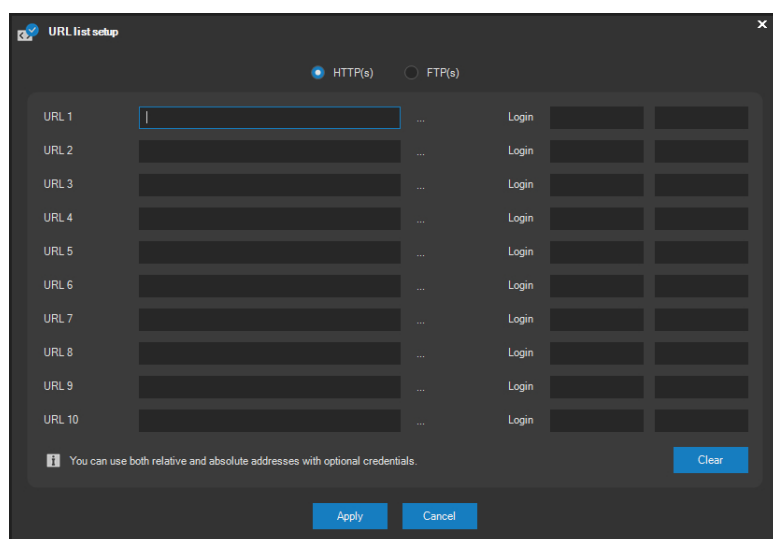
An e-mail address, to which the email will be automatically sent, is entered in the Address to field. You can also adjust the number of images and the delay when taking them that will be attached to the e-mail. If it is not possible to obtain images from the camera (e.g. camera failure e-mail), at least the email body will be sent. It is also mandatory to choose an SMTP server.

NOTE

The Address to field may also include several e-mail addresses separated by a comma or semicolon. Upon an event, e-mails will be sent to all addresses entered in this field.



This button activates various camera functions and other external devices directly through http commands.



Commands available over the camera http or https protocol can be entered into individual text fields labeled URL1 through URL10. Login data, which will be used for authentication, can also be entered optionally for each command.

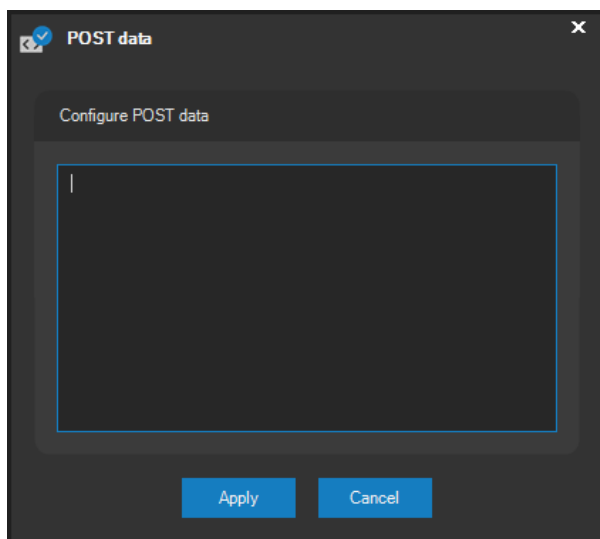
NOTE

Both absolute and relative http command addresses can be used. If a relative address is used, the command will be executed within the context of the camera on which the reaction to the event is currently being set.

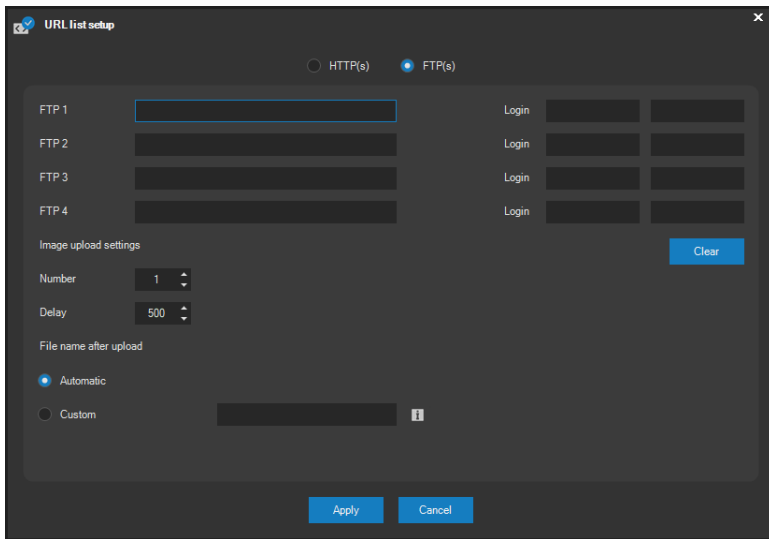
NOTE

If no login data is entered for a relative address, the login data for the camera used in the system will be used. If you enter login data for a relative address, they will have priority over the system login data.

Even though you can pass complex URLs with CGI command parameters etc., some devices may require a different HTTP method than GET to invoke an action. Using the button behind the URL text box an additional dialog can be opened to insert data to be sent using the HTTP POST method.



By choosing the FTP option, the event scenario can also include uploading snapshots to any given FTP server.



Up to 4 different FTP addresses and login credentials can be entered into the address list. The number of snapshots to be uploaded to the FTP servers during an event and the delay between them shall be selected under the address list.

NOTE

The secured version of the FTP protocol will be used automatically if the address begins with `ftps://`.

NOTE

The names of the snapshots that are to be uploaded to the target folder, which can be included in the FTP address, will contain the server number, timestamp, device number and index by default to ensure the names are unique. The first part that consists of the server identification and timestamp together make up the "snapshot identifier", which is published in the XML event notification and allows you to unambiguously link the XML notification to exported snapshots.

CAUTION

ATEAS uses the more recent, and currently most widely used, passive version of the FTP protocol. Active FTP is not supported.

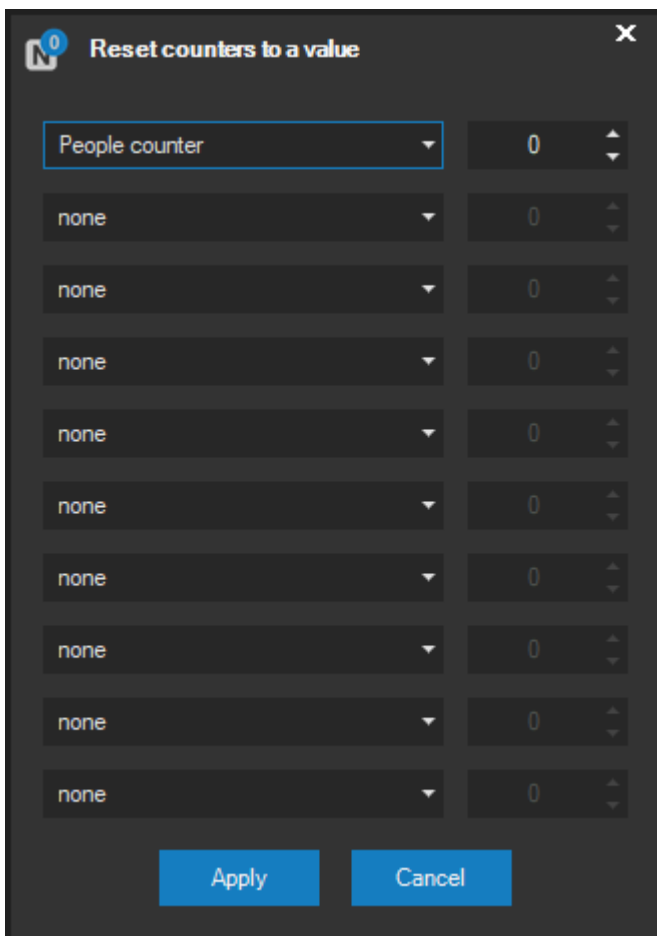
Under File name after upload, you can specify the naming mode for the file after it has been uploaded to the remote FTP server. If you do not want to accept the default file name, you can enter a custom name of a file that will continuously be overwritten.

NOTE

Using the same file name is suitable especially for some simple web applications, which might, for example, be using JavaScript to refresh an image on the web page. The file is always uploaded to the server with a temporary name and then renamed to ensure the web application does not try to load an incompletely saved image.



This button gives you the possibility to respond to an event with a counter reset action resetting the value of the counter to zero or another value as shown in the following picture.



Counter Name	Value
People counter	0
none	0
none	0
none	0
none	0
none	0
none	0
none	0
none	0
none	0

Apply Cancel

In order to create an event scenario for all demanded event inputs of the selected camera, you need to press the **APPLY** button. Changes will be applied to all servers immediately. Saving the scenario and updating the setup are confirmed.

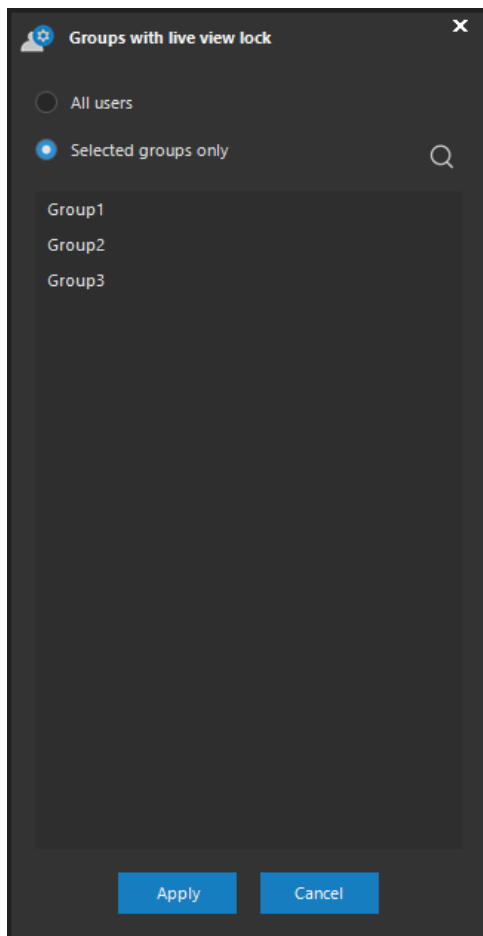
Special options

In the frame where an event scenario is created, you can also activate certain special options. These are activated by right-clicking on the proper button.

The first special option disables live video and audio broadcast from selected cameras during an event. This option will be activated after right-clicking the button to add to the event view. The button symbol will change its design according to the following picture. If the distribution of live video and audio is restricted as a result of an event, the user is informed not only by the event itself, but also explicitly by the information in the camera windows, containing text informing of the current viewing restrictions applied on the given camera.



The live view lock can be performed for all users or for selected groups only, which can be marked in the following dialog window.



The next special option is disabling the recording process during an event (can be used in special cases). This option is included to the event scenario by right-clicking on the record button, which will then change into a recording restriction symbol.



CAUTION

When using these options, keep in mind the maximum event duration to prevent a premature stopping of the event.

11.2.16. Dynamic sources and Onvif event sources

Cameras connected natively or with the Onvif interface can have their own event sources that can be used in ATEAS Security. Selecting Dynamic sources or Onvif sources from the Event sources list will display the list of sources.

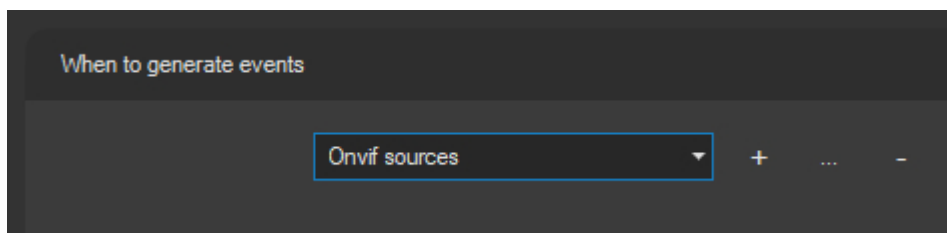
NOTE

Unlike other event sources, dynamic and Onvif event sources must first be created, therefore the list may be initially empty.

The fundamental benefit of using dynamic or Onvif event sources is that any given event source can be used, including analytical application or other specific event sources for which the application does not have any information beforehand.

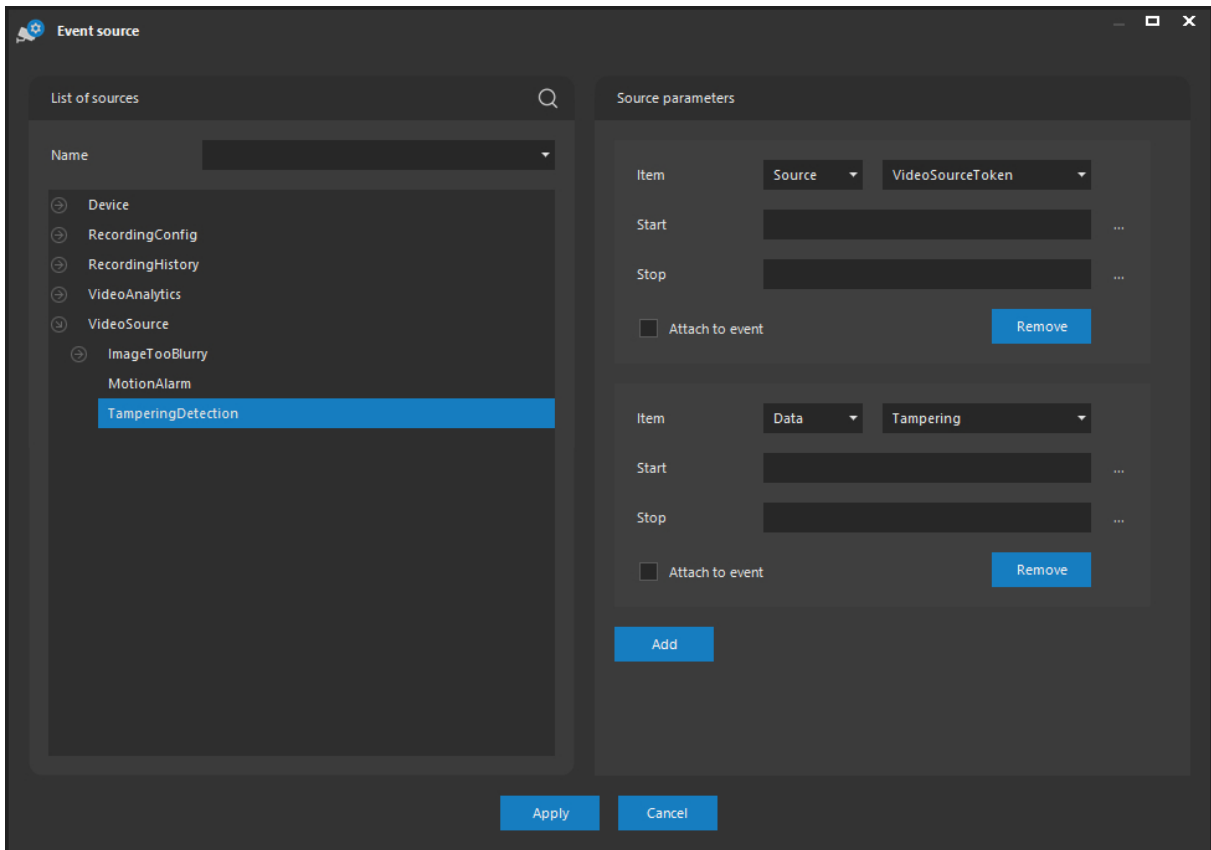
NOTE

Despite the fact that, from an implementation perspective, the dynamic and Onvif event sources can differ, e.g. in the network protocols used, their logic and use is identical and therefore a unified description can be given for their system integration.



There are three buttons next to the drop-down list with the selected Onvif sources item. The button with the plus symbol creates a new event source, the button with the dotted symbol is used to edit an existing event source and the button with the minus symbol removes an event source.

The list of all available sources is automatically retrieved directly from the camera when creating an event source.



Creating a new event source requires entering its name and selecting a source from the provided list. Event source parameters are displayed in the right part of the dialog after selecting an item from the provided list. The camera can offer additional event values for each event source. By creating conditions we can cause the event to only be raised when these conditions are met.

TIP

For source names, names of existing sources are suggested as you type. Using identical source names automatically consolidates metadata searches and generated charts.

In the Source parameters section, you can specify the data items that will be assigned to the event, as well as the conditions that must be met for the event to start and stop. The items can be of two different types (source and data).

NOTE

Some event sources can only have one or even no additional parameter.

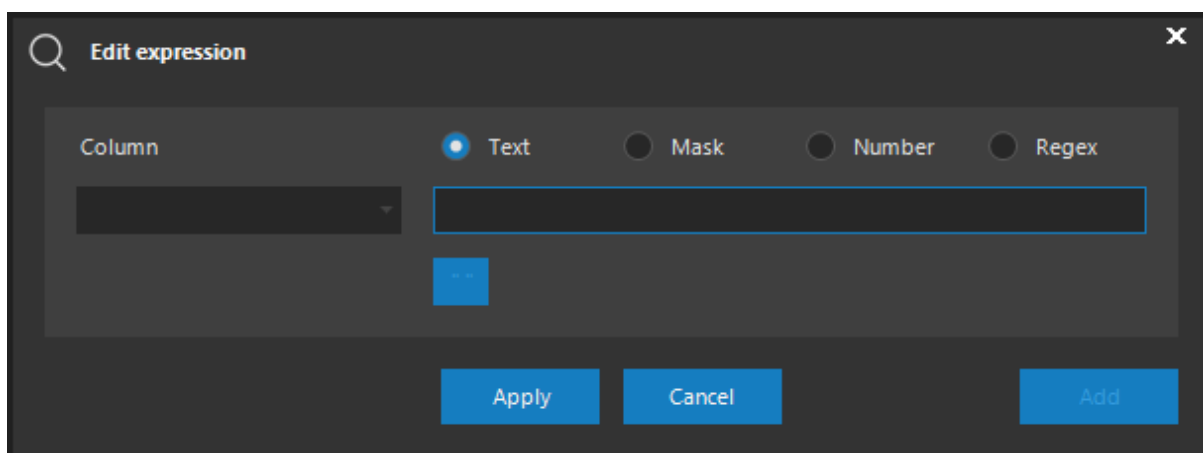
We can use the Attach to event checkboxes to decide whether these additional parameters will be attached to the event. If parameters are attached, they will be shown to the user during an event and it will also be possible to perform meta searches based on there parameters. Attached parameters will be automatically formatted for optimal searchability. The parameter name will be followed by a colon and its value.

TIP

This automatic metadata formatting is ideal for advanced metadata searches.

Since there is a large amount of Onvif compatible cameras, it is not clear beforehand what the values of additional parameters for event sources will look like. Therefore, it is good to observe the following procedure when creating event sources for Onvif cameras: Assign all parameters of interest to the event source, limit the maximum event duration and, based on new events, inspect the values the cameras are sending. Use this observation to define conditions for events to be started or stopped.

You can set the conditions for the start and end of the event for individual items by entering text directly or using a helper dialog by pressing the three-dot button behind the text field.



The same dialog is used for metadata searches, where we document its functions and the ways of defining a text condition, condition based on evaluating a mask, a numeric or regular expression. However, compared to the metadata searches, there are some differences as follows.

- You cannot enter a Column value because it is determined by the data item.
- You cannot use the **ADD** button because you create a condition for the selected data item.

- In the context of dynamic event sources, the text condition requires an exact match; therefore, the quotes button is disabled.

CAUTION

In the context of dynamic event sources, the text expression requires an exact match with the data item with the exception of character case.

If conditions for multiple data items are set, all of them must be met for the event to start or stop. If no conditions are specified, they are considered met if the data item appears in the dynamic event source with any content, namely for the start of the event.

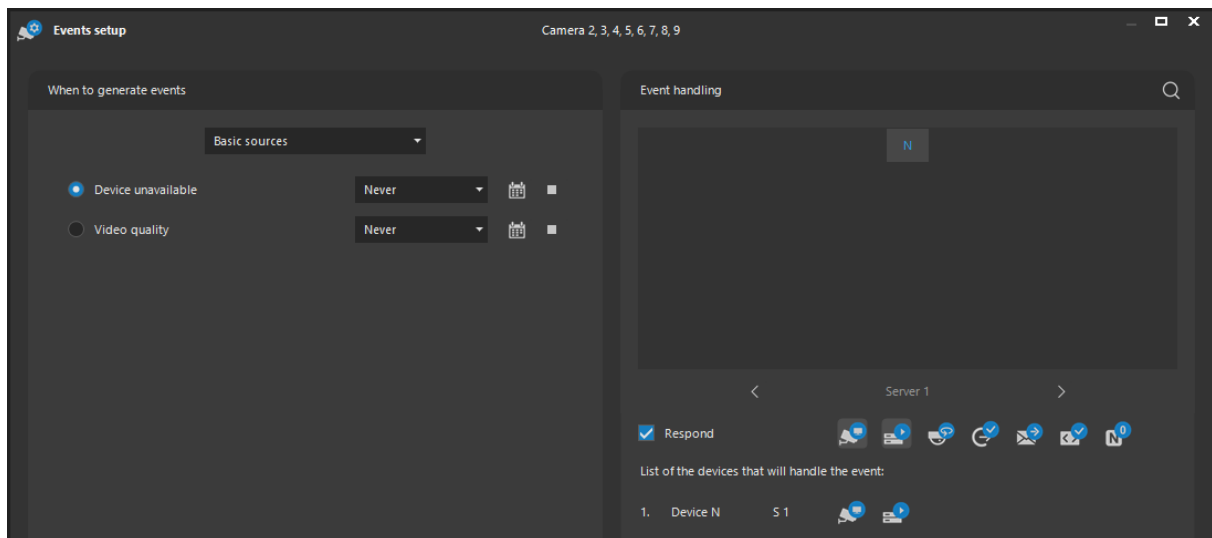
NOTE

Within one item, you can also specify a condition for either the start or end of the event. In such a case, the condition is evaluated and if the result is negative, the blank part of the condition is considered to be true (start or stop).

11.2.17. Batch event configuration

Events can also be configured for multiple selected cameras simultaneously, i.e. even for all cameras of the given camera server. The principle of batch configuration lies in the ability to simultaneously configure common event sources for all cameras in the selection, as well as the event reaction. In general, an event reaction (event scenario) can include actions on one or more cameras on one or more camera servers.

Given that cameras are represented by numbers, the batch configuration process needs to come with a way to configure the event reaction for all selected cameras identically. This is done under the event handling configuration by using the relative (substitutive) camera number N, which represents all cameras in the selection.



NOTE

Batch event configuration can, therefore, be used to configure only such event scenarios that consist of actions on the camera that generated the event. If the event scenario needs to be extended to include other cameras or servers, the configuration shall be carried out individually.

NOTE

Specific names for dynamic, complex, or Onvif event sources, configured in multiple camera mode, can only be displayed if the name is identical for all cameras. Otherwise, a generic name will be displayed.

11.2.18. Dynamic event scheduling

You can create static time scenarios, making it possible to schedule, for example, the motion detection or alarm input monitoring activation. The time schedule can also be performed in two priority levels - regular event or alarm. In both cases, the complete event reaction scenario applies, in case of an alarm, an alarm view is automatically switched onto the operator's monitor.

In terms of the dynamic schedule, the evaluation of alarm events (motion detection, alarm inputs, PIR camera sensors, black listed vehicle LPs) is activated dynamically depending on other event inputs such as:

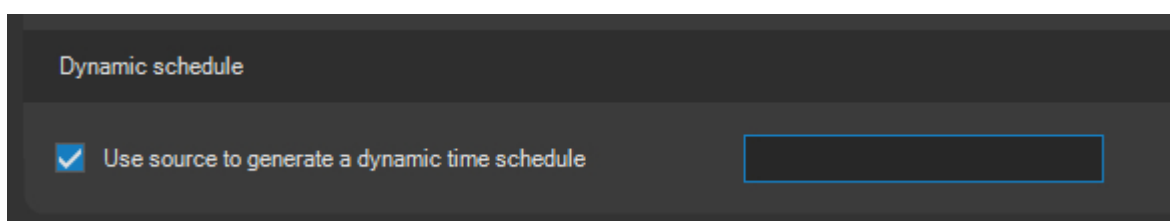
- native input - camera alarm input,

- external input – input of an external device or a message from the ARC panel (activation through the use of either SNMP protocol or ATEAS API).

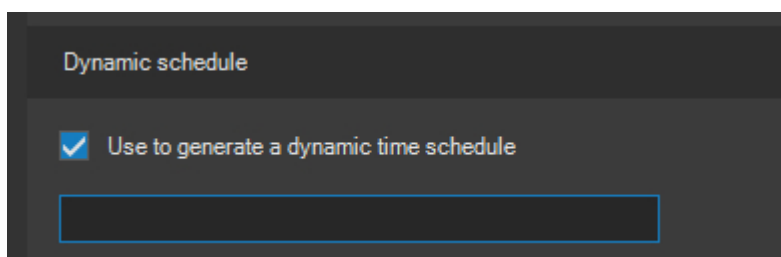
Creating a dynamic schedule

A dynamic schedule can be added to the system in two ways.

A dynamic plan generated on the basis of a native camera input can be created by checking the Use source to generate a dynamic time schedule control, found in the Dynamic schedule section of the Event source settings window (for a selected camera input). The dynamic plan will automatically be created, updated and ready for use, upon saving the camera event setup.

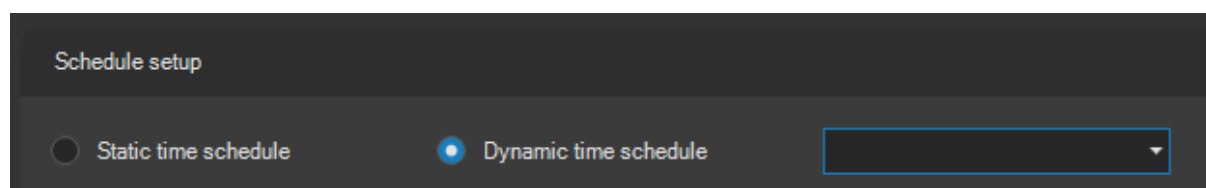


A dynamic plan generated on the basis of either an external input or an ARC message can be created by checking the Use to generate a dynamic time schedule control, which is found in the Object element window. This can be done while creating or adjusting the object in the External section of the administration.



Using a dynamic schedule in the system

Using a dynamic plan for any number of events is simple. You can select between the static and dynamic time schedule in the upper part of the Event source settings window. All time schedules created are sorted in alphabetical order in the dynamic schedules drop-down list.



See the notes below specifying the function of dynamic schedules.

NOTE

It is very simple to activate an alarm by moving the camera (i.e. turning on motion detection), for example, depending on the input status of the same or other camera. You can also simply monitor properties using external inputs or ARC messages.

NOTE

The dynamic schedule is generated and recognized throughout the whole system. Therefore, a selected camera input or an external input for generating dynamic schedules can be applied to any number of cameras connected to completely different camera servers.

NOTE

The camera input used for generating a dynamic schedule can still generate insignificant events or alarms, namely based on both static and dynamic schedules! A specific input will not logically generate events if it is dependent on a dynamic schedule which is generated by this input.

11.2.19. Complex event sources

If we plan to have the system react only in situations when there is more than one event source active, we will need to create a complex event source. Complex event sources can consist of several elementary event sources, joined not only by a logical AND condition, but also a logical OR condition, or XOR condition (exclusive OR, where exactly one condition must be met). A complex event source will help, for example, in resolving the request to create an event only after motion is registered simultaneously on multiple cameras or when motion detection is also linked to the PIR motion detector activation, or when external element 1 or external element 2 are active and at the same time camera 1 detects motion, or when the selected analytical event is active.

Besides these binary logical operators, we can also use the unary negation operator (**NEG** button). This operator can be used when we intend to induce an event without an active event source (e.g. stopping a production line and terminating the detection of movement).

Complex events are treated as counters automatically by the system. For any complex event, the system maintains the number of activations of all its base event sources. Sources without a logical negation are added to, sources with logical negation are subtracted from the result value. The result value can then be monitored in the live window. You can find more information about counters in the Working with counters subchapter among the live window features.

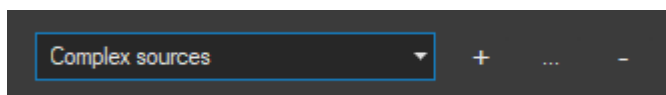
Operators are classified based on their priority of evaluation as follows (from highest priority to lowest):

- NEG (unary negation operator)
- AND (binary AND operator)
- OR (binary OR operator)
- XOR (binary exclusive OR operator)

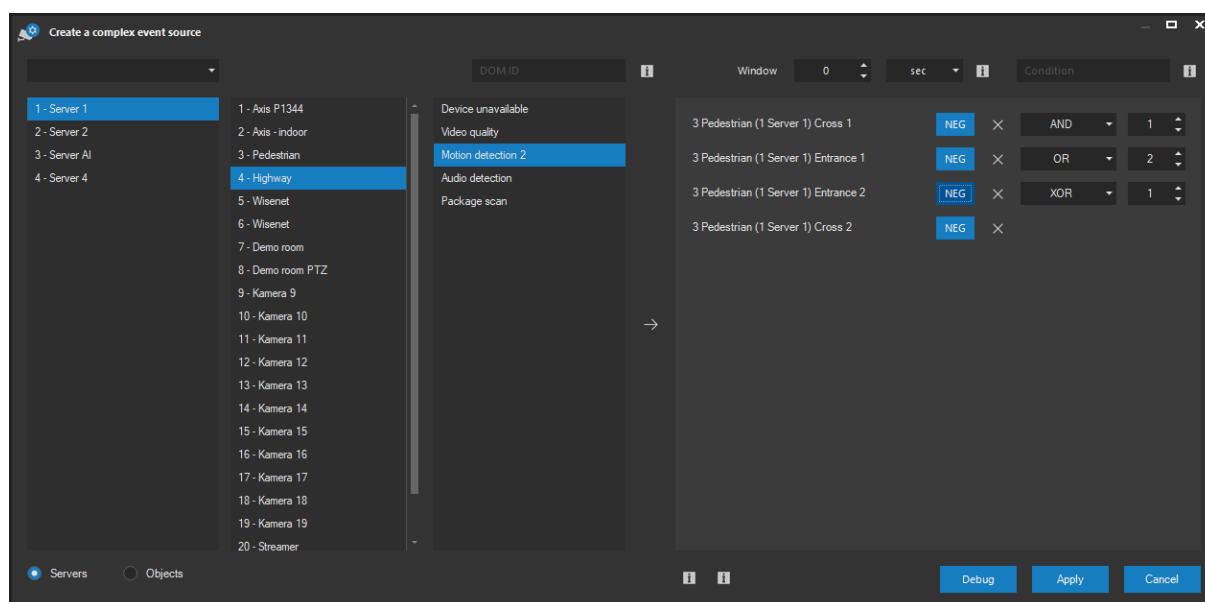
NOTE

Complex event sources are an ideal tool for your system to resolve demanding security requirements and also a tool used to significantly reduce the amount of false alarms and handle an operator overload situation.

A complex event source for a specific camera is created by selecting the Complex sources option from the list.



The buttons to the right of the list are used to create a new, edit an existing and delete a selected complex event source. Pressing the button with the plus symbol opens a dialog which can be used to create a complex event source.



The left side of the window displays all event sources available in the system from which we can choose, including basic sources such as motion detection or input activation, analytical sources, vehicle LP detection, custom event sources or Onvif sources. The radio buttons below the list allows you to choose between camera system sources and external sources. The selected source can be added to the complex event using the central arrow button. Sources already included can be easily moved around to new positions by dragging with the mouse.

NOTE

We are not limited by the camera or server when creating a complex source. A complex event source can therefore depend on sources from one or more cameras connected to one or more camera servers and even on external events.

A name shall be given to the complex event source being created. This name will be used for this camera throughout the entire system.

TIP

For source names, names of existing sources are suggested as you type. Using identical source names automatically consolidates metadata searches and generated charts.

A special DOM ID text field is located to the right of the event source name, which can be used to inject the counter value into a web page displayed directly in a live window or on the video wall. To inject the counter value, the source html document must contain any particular html tag with an ID parameter corresponding to the value in the text field, e.g. `<div id="xxx"></div>`.

The counter values can also be injected into websites not viewed by ATEAS standard or video wall clients. For this purpose, it is obviously not sufficient to mark the insertion place with the corresponding html element. Instead, a more complex integration logic must be used. The ATEAS administration server contains an api subfolder in its httproot folder that includes full integration examples with all necessary comments for web creators or web administrators.

Apart from complex counters, automatic zone counters exist in the system that correspond to all analytical event sources bound to closed zones. The integration of these counters into web pages is, therefore, also based on automatically identifying elements in the page. The ID format consists of a fixed reserved part and a server, camera and source number (in this order). The source ID is displayed in the analytics settings. Example:

auto-zone-1-10-201

The individual event sources, which are part of the complex source, can be removed from the right side of the list at any time by pressing the cross button. The negation operator can be enabled for each source, along with connecting to the subsequent event source using an operator selected from the drop-down list. Default operator priorities described above are applied when evaluating complex sources. The evaluation priority can be changed by updating the priority of individual logical combinations in the Priority column.

NOTE

Increasing the priority in the Priority column is the user's way of establishing a logical statement including parentheses for changing the order of evaluation.

A complex event source generates an event when the condition for its generation has been met according to the defined logical links between elementary event sources. A complex event source concludes when this condition is no longer met.

CAUTION

In order for a complex event source to create an event, which the complex event source depends on, shall be created and active in the system.

NOTE

Bear in mind that a complex event source has its own event source reset time and scheduling meaning that if the conditions for generating a complex event source are no longer met, the complex event will not conclude until its event source reset time has expired. Should the conditions be met once again, prior to expiration of this time interval, the original complex event will continue.

When the prevalent usage of a complex event source is a counter, the actual event start or stop times based on the logical dependencies between the elementary sources are often insignificant so that it might be suitable to configure this event as hidden. It is much more common, however, to raise such event when a certain numeric condition is met. This condition can be entered into the corresponding text field at the bottom of the window. Any numeric value, optionally with a > or < operator, or even an interval like (50, 100) are supported.

If a positive value is set for Window, the complex event – counter is changed to a dynamic counter. This means, that any increment or decrement of the counter invoked by a basic source activation will be followed by an inverse operation (decrement or increment) of the counter after the time window has elapsed. This way you can e.g. display or respond to the number of people who crossed a line within the last hour.

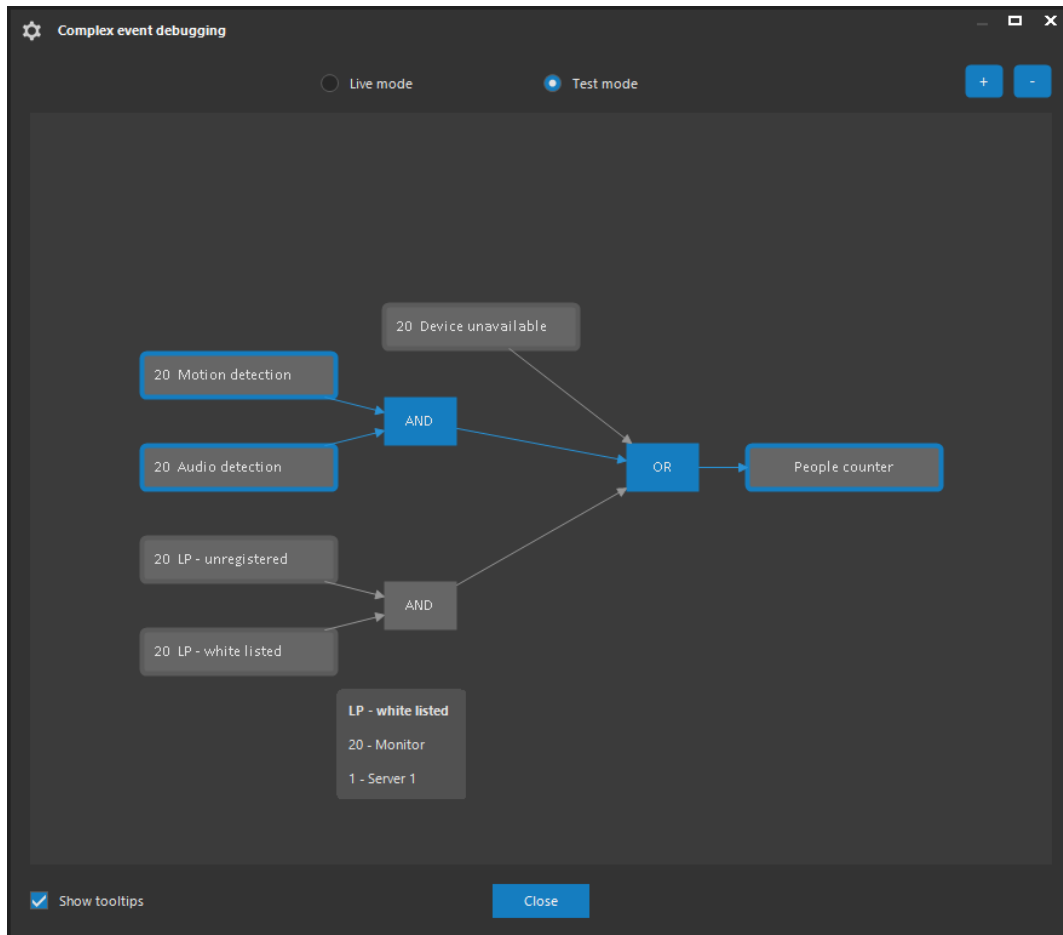
NOTE

When resetting dynamic counters (manually or by events), all pending inverse operations of the counter are also reset. Values of dynamic counters are not saved and restored when the camera server is restarted.

Debugging complex events

Complex events can comprise many elementary sources and can use different operators and evaluation priorities. Therefore, it might not be easy to follow, when an event is supposed to occur

and, when it doesn't, what the actual reason was. The **DEBUG** button opens a debugging tool to understand the event using a visual tree.



The event preview can be put in a live or testing mode. Whereas in live mode the elementary event sources reflect the actual system status, in testing mode, individual sources can be activated or deactivated manually. In both cases you can see how the complex logical result is propagated through the visual tree of the event. You can easily see the effect of operators and priorities.

You can zoom in or zoom out the visualization using the zoom buttons or the mouse wheel. Parts of the tree can also be moved to different positions.

You can deactivate displaying additional information about a hovered event source using the Show tooltips option.

Complex event data

The data of complex events automatically includes the data of all basic events that make up the complex event.

NOTE

This feature can be used in metadata searches, where complex events can be searched based on additional data.

11.2.20. Locating cameras in the map

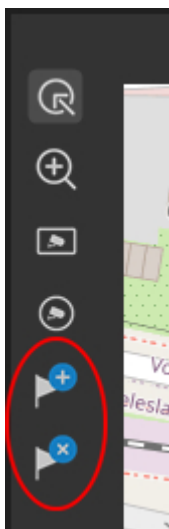
An administrator with access to a certain camera server can specify and further adjust camera coordinates (map position). Other operations related to the map window are listed in a separate chapter. Here we will only explain how to specify a camera position in the map.

If there is no map displayed while working in the system administration section, use the Tools menu to open it. When the map window opens, select a camera from the list to automatically synchronize the map (centre and optionally zoom). The synchronization will be performed even if it is turned off or turned on only during events. This simplifies the procedure of assigning new coordinates to cameras.

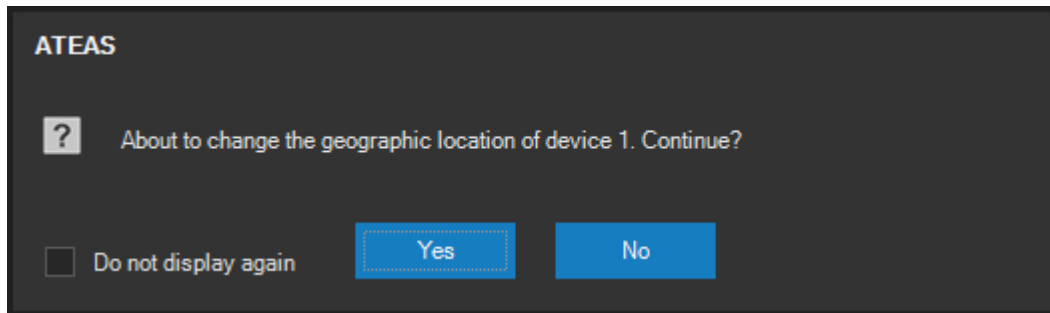
NOTE

The camera symbol in the map will flash for a couple of seconds for better orientation.

The system administrator can use the following functions for camera localization.



After selecting a camera (from the camera list) and you wish to change the map position (or to change its location), activate element placement map function and then click on the new destination where you wish to place the camera. Upon doing so, confirm the following message by pressing the **YES** button.

**TIP**

Cameras already localized in the map can be relocated or removed from the map more easily by using the context menu of the camera symbol in the map.

After the dialog is confirmed, the camera will be positioned to new map coordinates and all views of all users currently displaying the map scene will be updated. Positioning and repositioning to new coordinates is always confirmed by a message. A camera can be removed from the map in the same way. The only difference is that you use the Remove element button.

The cameras on your mobile phones or other devices with iOS or Android operating systems, i.e. cameras added to the system under a user name, can be located in the map. If video (and audio) streaming is activated from this type of mobile camera, this device can be automatically located in the map via GPS. The map window always displays the current position of all devices, which the operator has displayed in any of the live windows.

NOTE

The precondition for using this function is the mobile device being equipped with a GPS receiver.

NOTE

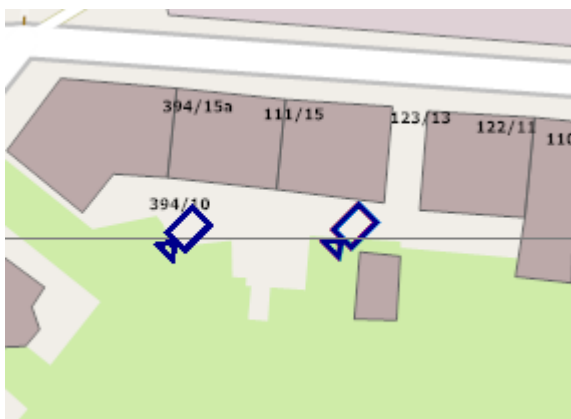
If the mobile camera does not have a default position specified in the map, the streamed video will not include GPS metadata and the device cannot be located. If the mobile camera is not located or map data is not available, the device will not waste energy trying to determine its GPS position.

NOTE

The route for individual devices can also be displayed when replaying recordings. When multiple live windows are opened, the map is always being used by the last active window, to be able to determine whether the actual or historical GPS coordinates shall be displayed.

Snap mode

As the label for the Place element button suggests, cameras can be positioned in snap mode by simultaneously pressing and holding the CTRL key. In this mode, the target position of the camera (horizontal and vertical) is set to the same value as the camera that is located closest, either horizontally or vertically (or both), i.e. it is snapped. The following image depicts the snapping.



Snapping allows easy positioning of the cameras so that they form a line, even at longer distances, thus improving the overall visual impression of the map scene. A thin guide line is always shown between the camera currently being positioned and the camera to which we are snapped. If snapping occurs in both horizontal and vertical direction (usually to two different cameras), there will be two guide lines displayed.

NOTE

The snapping tool is activated only once you are close enough to the target camera.

11.2.21. Exporting and importing cameras

Using the **EXPORT** and **IMPORT** buttons it is possible to save the configuration of selected cameras to be imported later to the same or a different server, or even to a different system with the same version. This feature is available using the following two buttons.



This, it is easily possible to quickly transfer cameras to a different server e.g. when we want to relocate the cameras within an UNLIMITED system edition. When importing to the same server, it is possible to quickly create a configuration with duplicate cameras for mobile monitoring purposes or to record video in different quality of video format. Importing to a different system altogether, we can prepare camera configurations in a lab environment and only import it at customer premises.

NOTE

The fundamental difference to making a full configuration backup and restore from XML files is that this tool exports the selected devices only, which is extremely beneficial in the cases mentioned above.

Cameras cannot be exported and imported in systems with different versions. Therefore, the application suggests a filename containing both the export date and the system version.

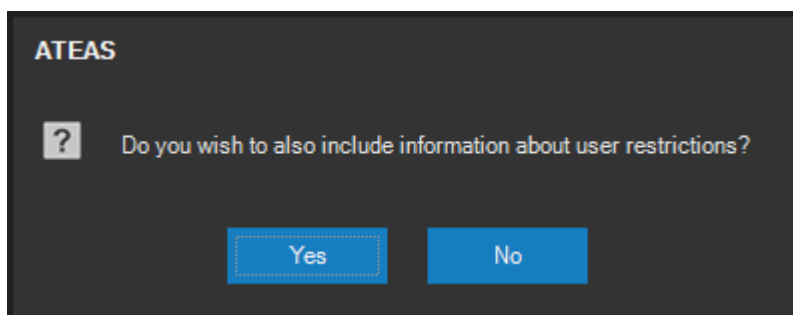
When importing cameras, the same dialog is presented to the user as when adding cameras automatically, where an initial camera number can be chosen (when duplicate numbers are found, the next higher number is used) and it can also be determined whether duplicate cameras will be imported.

All settings related to the cameras are part of the export including all event source settings, zones for neural network analysis, symbolic names, presets, tours etc.

NOTE

The event scenario is also part of the export, however, only the part bound to the camera being exported. For a wider scenario including other cameras from the same or a different server, these parts of the scenario cannot be exported for the system wouldn't be able to set the import logic later.

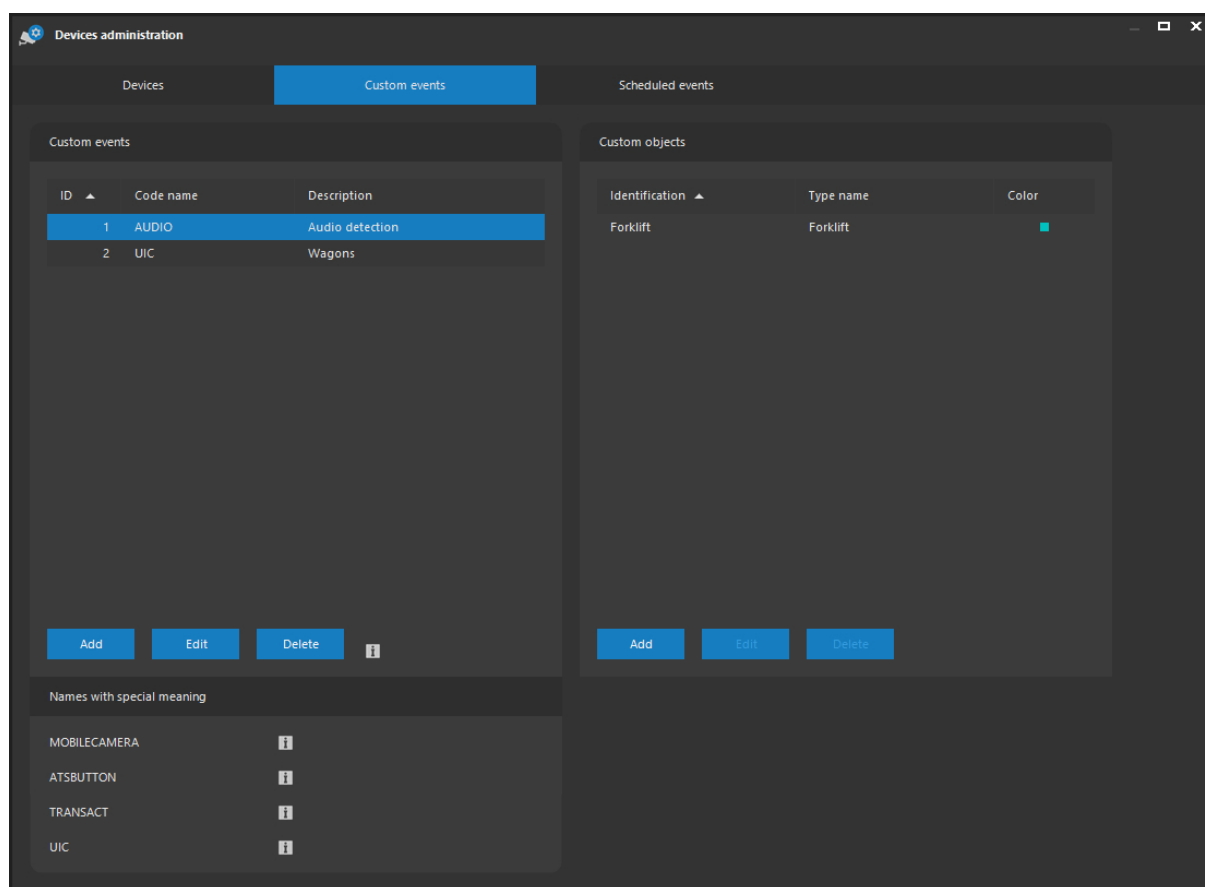
User and user group restrictions linked to the exported cameras can also be part of the exported data. This data only makes sense when importing the cameras still in the same camera system (including other servers). Therefore, it is possible to refuse this data to become part of the export.



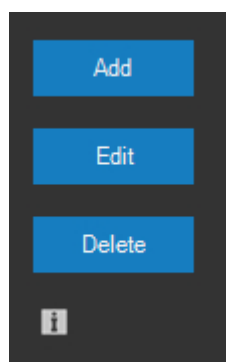
11.3. Custom events and object types

11.3.1. Custom events

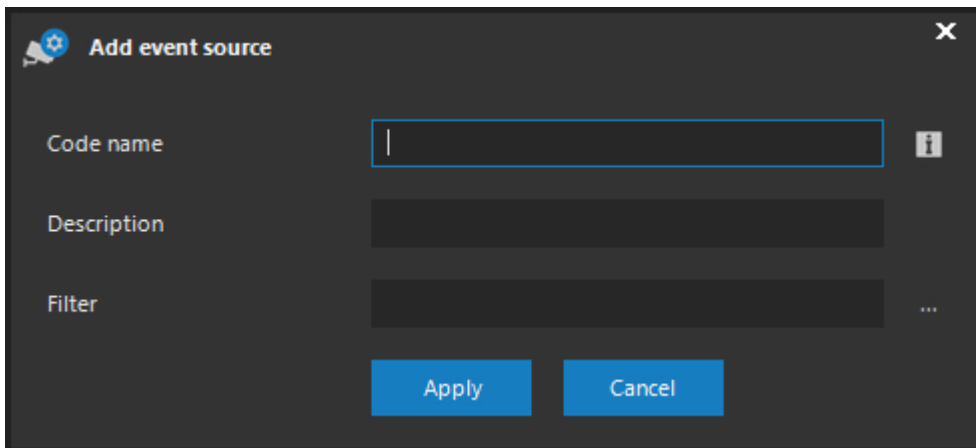
Besides event sources implicitly available for individual cameras in the system, you can add other additional user-defined event sources. These can be both added and removed in the Custom events tab in the Devices administration section and can refer to any device event sources.



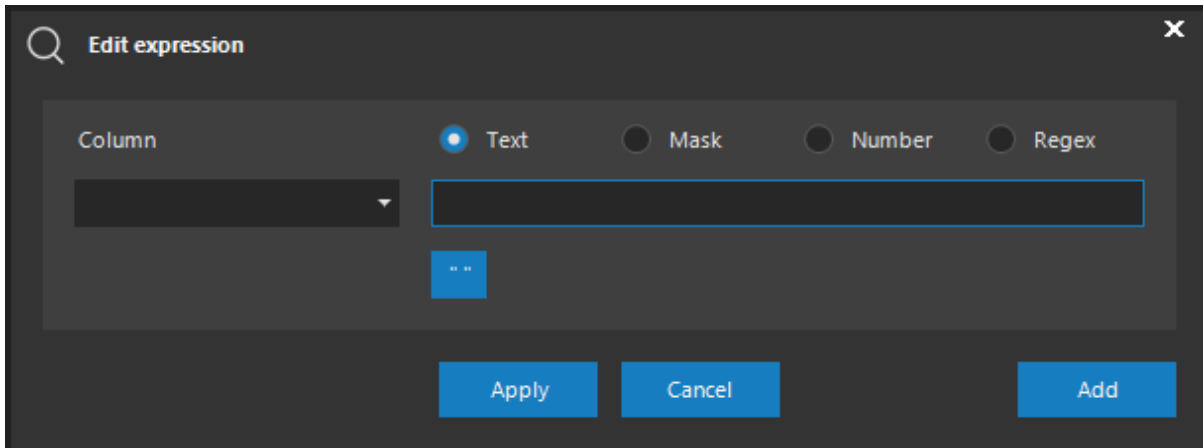
The system receives user-defined camera events using the ATEAS API – application interface for receiving external events. This part of the ATEAS API, its principle and examples of use are described in terms of a separate document, available on the ATEAS Security homepage (at the address of your ATEAS Security administration server).



Using the **ADD**, **EDIT** and **DELETE** buttons, you can register or update (or cancel) user-defined camera events. These operations are central and are related to all camera servers within the system. A simple dialog requesting information about the new event source will appear after pressing the **ADD** button.

A dark-themed dialog box titled "Add event source" with a close button (X) in the top right corner. It contains three input fields: "Code name" with a text cursor, "Description", and "Filter". An information icon (i) is to the right of the "Code name" field, and a three-dot menu icon (...) is to the right of the "Filter" field. At the bottom are "Apply" and "Cancel" buttons.

The code name is a symbolic and unique name for an event source, which is also part of an external notification for this event type in the ATEAS API. The description applies to a user description of this event source, used when this event occurs and also on event panels for individual cameras. Optionally you enter a filter value. Here you can specify a condition that must be met for the event to start. You can enter the condition directly or by using a helper dialog after pressing the three-dot button behind the text field.

A dark-themed dialog box titled "Edit expression" with a search icon and a close button (X) in the top right corner. It features a "Column" dropdown menu, four radio buttons for "Text" (selected), "Mask", "Number", and "Regex", and a large text input field. A small blue button with three dots is below the text field. At the bottom are "Apply", "Cancel", and "Add" buttons.

The same dialog is used for metadata searches, where we document its functions and the ways of defining a text condition, condition based on evaluating a mask, a numeric or regular expression. Likewise, the column syntax can be used here.

NOTE

The previous filter functionality can be used, for example, when receiving point of sales transaction data and we might wish an event should only occur when a particular item is registered by the cash desk or when an item is cancelled.

The new event source will be registered on the administration server upon pressing the **APPLY** button.

11.3.2. System names for custom events

Some custom event names are predefined in the system and automatically linked to a certain type of event. The list of these names is shown directly in the bottom part of the window. The system names for custom events available in the current version are:

MOBILECAMERA – A custom event with this name is generated for cameras on your phones or other mobile devices added to the system under the name of the user logged on. The event is created once video streaming from the mobile device starts and allows activating an event scenario as a response to this action (displaying the event on the monitor, notifying operators, recording, other actions). See also the corresponding chapter dealing with adding cameras to the system for more information.

ATSBUTTON<n> – A custom event with this name (where <n> is a number ranging from 1 to the largest user button number in the system) is generated for pressing the user button with the respective number. The event is created after the button is pressed. If the button is configured as a switch button, the event will end when the button is released.

TRANSACT – A custom event with this name is generated for each transaction line. It is therefore very appropriate to configure a filter for this custom event to ensure the event only occurs in specific situations – e.g. when cancelling an item on the cash desk, as well as other actions.

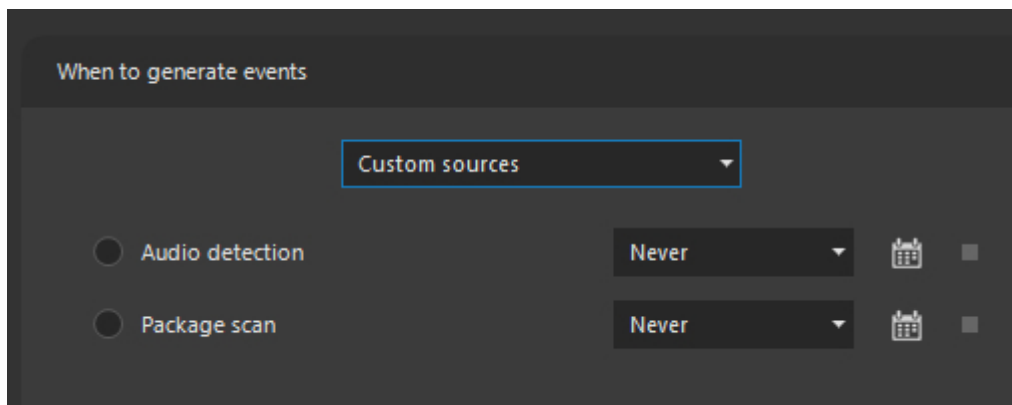
UIC – A custom event with this name refers to wagon detections with UIC numbers on them.

NOTE

If these custom event sources with predefined names are not created, no such events will be generated.

11.3.3. Event management

User-defined custom event sources are used exactly the same way as existing system event sources. The only difference being that custom events are started (or ended) through ATEAS API. Custom sources are available in the events window in a separate group called Custom sources.



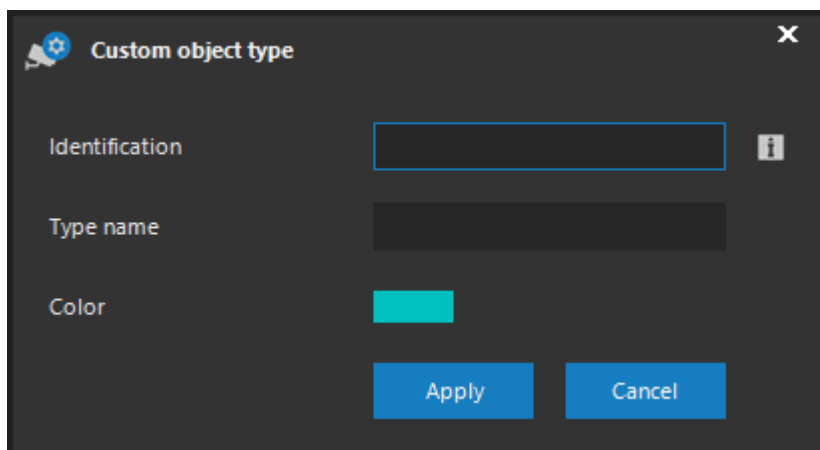
Specifying time schedules (the beginning of an event or alarm) and creating event scenarios that can include several cameras and contain various actions is completely identical to methods related to predefined event sources.

11.3.4. Custom object types

In the Custom objects section, new object types can be created using the **ADD** button that are otherwise not supported by the freely available ATEAS neural networks.

NOTE

Adding new object types might be necessary for custom neural networks or for analysis running in the cameras.



In the Identification field, it is necessary to enter a unique identifier for the given object type at the point of its origin (in a neural network or in the camera), in the Type name field, you can use the name to be displayed to users.

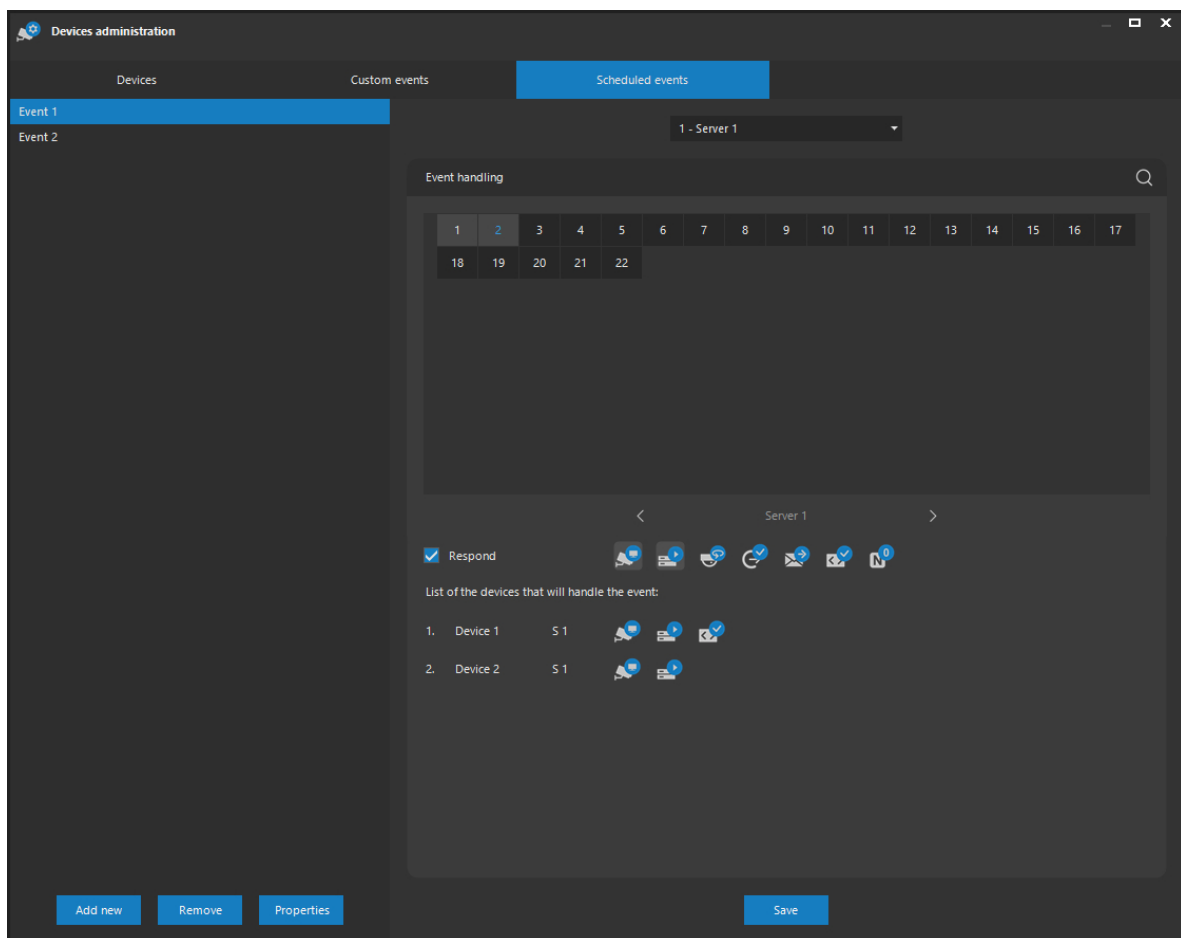
By clicking on the color area, you can choose any color for this object type. The color will be used when rendering metadata, including rendering on mobile clients or in the SDK. When created, custom object types work pretty much in the same way as system object types, e.g. when creating event sources or performing forensic searches.

An already existing custom object type can be edited or even deleted using the **EDIT** or **DELETE** buttons.

11.4. Scheduled events

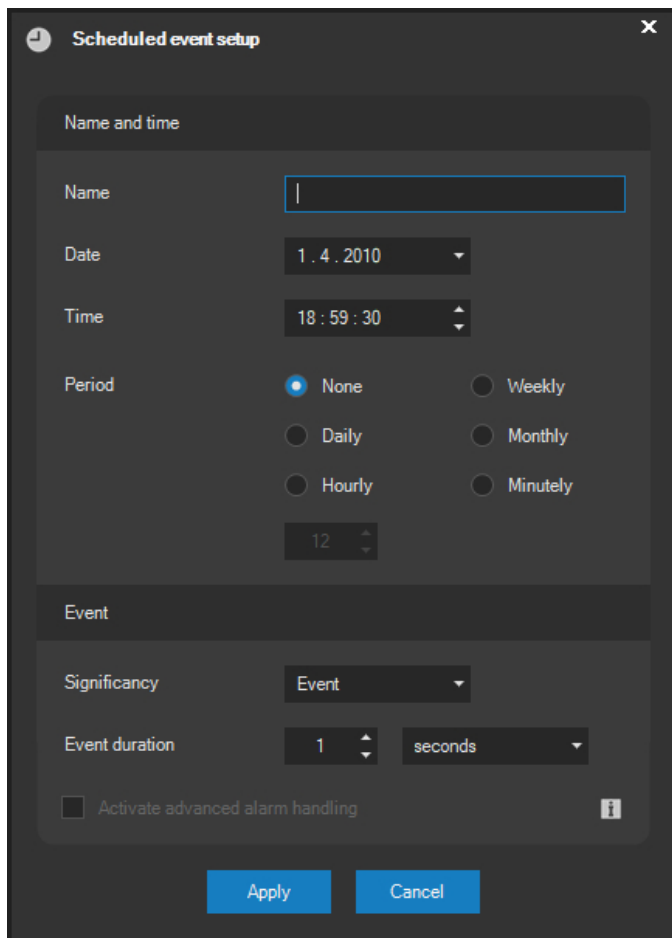
11.4.1. Basic setup

The ATEAS Security platform also enables planning events at precise times. If, for example, we need certain PTZ devices to be directed to a preconfigured position at a specific time, once or repeatedly, or to monitor certain places in tour for a specific duration, we can plan these events in the system. Apart from these cases of planned movement to preset or temporarily switching to a tour, it is also possible to plan other camera reactions such as camera switching on the operator's monitor, output activations, starting the recording process or sending e-mails. Scheduled events can be created in the device administration section.



The scheduled event administration window is divided into two parts. The left part of the window contains a drop down list for selecting the camera server. The current list of scheduled events will be displayed under the selected camera server. Using the buttons under this list you can create a new scheduled event, delete or edit an entry. The right part of the window contains an event scenario for the selected scheduled event.

A user dialog appears upon creating a new scheduled event via the Add event button. The basic parameters for creating a scheduled event must be entered into this dialog.



The name of the new event and the precise date and time, when the event shall take place, are required.

The created event can have an assigned time period or can be created without a period. This setting is performed by selecting any of the options from the Period group. If no period is selected, the event will only occur once at the configured time. Selecting a different option can lead to an event occurring periodically every day, week, month or after a given number of hours or minutes lapses.

In the Event section, it is possible to assign a significance level (common event or alarm) for each scheduled event and determine the event duration.

The Significancy drop-down list contains the Hidden option, which indicates the configured event scenario of an event will be carried out in its full extent, however, the event will not appear in the user's live view. Another way would be to revoke the user's rights to receive events or change application's behavior upon receiving events in local settings, nevertheless, setting the event to hidden is the easier way.

NOTE

For example, this can be helpful if we use scheduled recurring events to upload snapshots to an FTP server, when it is not necessary for this type of event to create a separate row in the event window.

Checking the Activate advanced alarm handling option activates the extended alarm handling mode for the given event source. See also the separate Alarm handling mode subchapter for more information.

NOTE

Scheduled events are searchable within the system, just as other types of events from individual camera recordings.

NOTE

If a scheduled event is configured for a longer duration than its period, the new event in the given time will only occur if the previous event has finished. The camera server prevents the multiple occurrence of one scheduled event. Various scheduled events can, of course, overlap each other.

CAUTION

By deleting a scheduled event, however, you cannot stop or prematurely conclude the event if already initialized on the camera server.

The Properties button displays the same user dialog as for creating a new scheduled event. The configured event parameters are automatically pre-entered and can be edited in this dialog.

11.4.2. Event management

Creating event scenarios for scheduled events is exactly the same as creating scenarios for native camera events or for external events. The user control for creating a scheduled scenario always displays the event scenario for the selected scheduled event. The event scenario can also include all

available actions such as the camera view on the operator's monitor, the event driven recording, camera output activation, sending e-mails, controlling PTZ devices, external device activation etc. Multiple cameras can also be part of the event scenario for one scheduled event.

NOTE

Unlike event scenarios for native camera events or external events, cameras, other than those currently assigned to the camera server, for which the scheduled event is created, cannot be part of the event scenario for scheduled events. To create a reaction on a different camera server, you will need to create a scheduled event on this server directly. The buttons for switching servers are not available in this context.

The created event scenario must always be saved via the **SAVE** button.

NOTE

There are no special rights in the system, which would permit or restrict the reception of scheduled events from the system client (unlike external events). If a non-empty event scenario is created for an event, the client will only receive the event if it has access to at least one of the cameras belonging to the event. This way, scheduled events can be intelligently distributed throughout a system with a greater number of servers, cameras and clients.

11.5. Alarm handling mode

11.5.1. Mode basics and activation

Advanced alarm handling mode can be activated for all event sources within the ATEAS system (camera events including custom camera events, scheduled events or external events). All you have to do is to check the Activate advanced alarm handling option in the respective dialog when updating the event source settings. If a system alarm is fired with advanced alarm handling mode active, the system's behavior changes compared to standard events and alarms as follows:

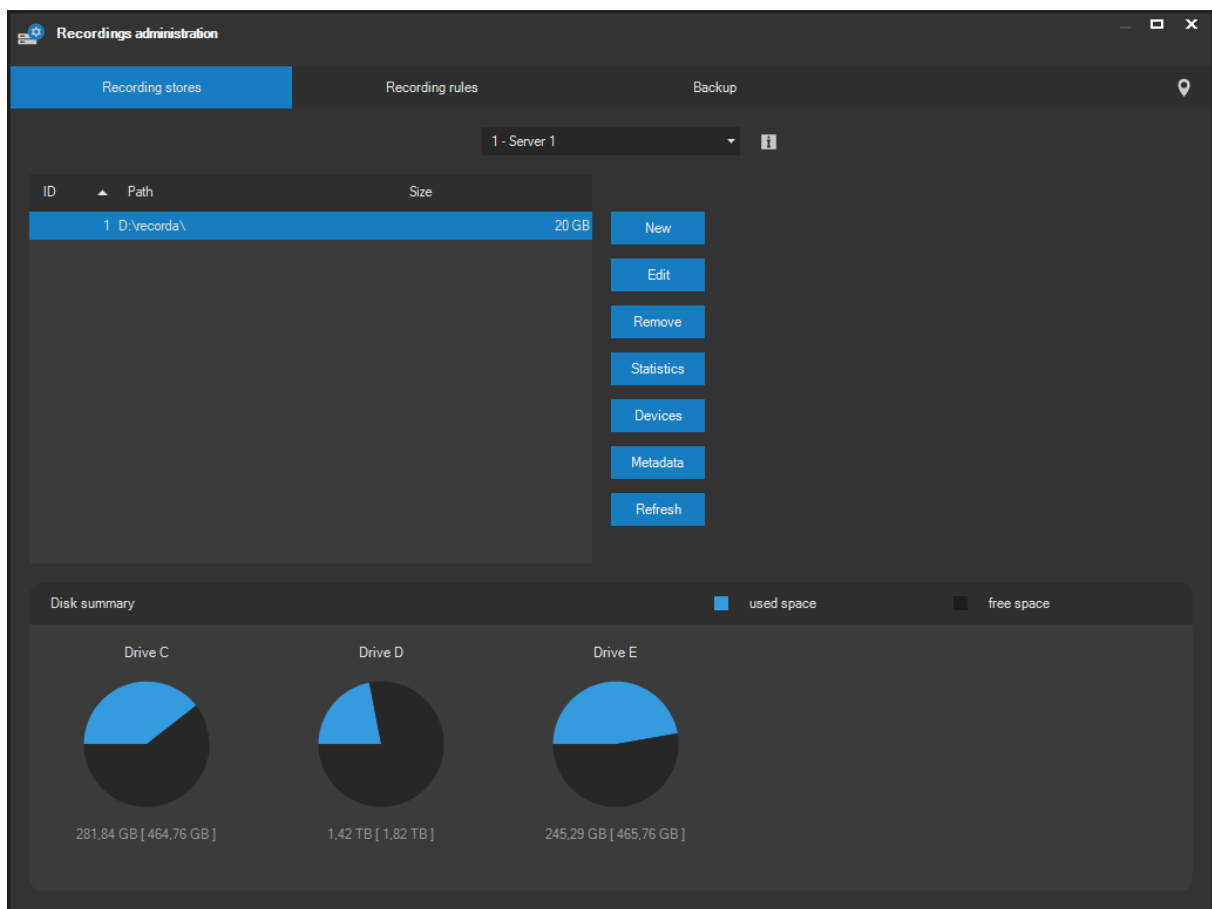
- Alarms with advanced handling active have a darker red exclamation mark compared to standard alarms (events have a grey exclamation mark).
- Alarms with advanced handling active will be displayed in the alarm receiving live window, until an authorized user actively handles the alarm. Alarm handling from the system operator's point of view is described in Monitoring chapter.

- Until these alarms are handled, they are not subject to the local settings for maximum events and alarms displayed in the live window.
- These alarms are automatically stored in the alarm log, which is available in the Recordings window. The alarm log feature is described in chapter Working with recordings - Alarm database.
- These alarms cannot expire in the system even if no client authorized to accept or handle the given alarm is connected. Late delivery is activated for these alarms, for example, immediately after a client authorized to handle the alarm logs in.
- Unhandled alarms cannot expire in the system, even after server connection drop-out or server restart.
- In order to handle an alarm, the user must not only be authorized to accept alarms from the given resource (camera, external system), but must also be authorized to handle the alarm.

11.6. Recordings management

11.6.1. Media stores

Specifying a media store on a camera server is the first step for configuring recordings. The camera server can place its record database to specified hard drive sections, limited by size. To start managing records, you must select the Recordings item from the administration menu and then select a corresponding server from the Camera servers list on the **Recording stores** tab. The server must be connected, otherwise configuration will not be possible and the application will display the respective warning message.



This tab displays all media stores that have already been created. An overview of camera server hard drives, showing free space remaining (detailed information is displayed under the hard drive graph), is available in the disk summary section. Hard drive information can be refreshed by pressing the **REFRESH** button.

Creating media stores

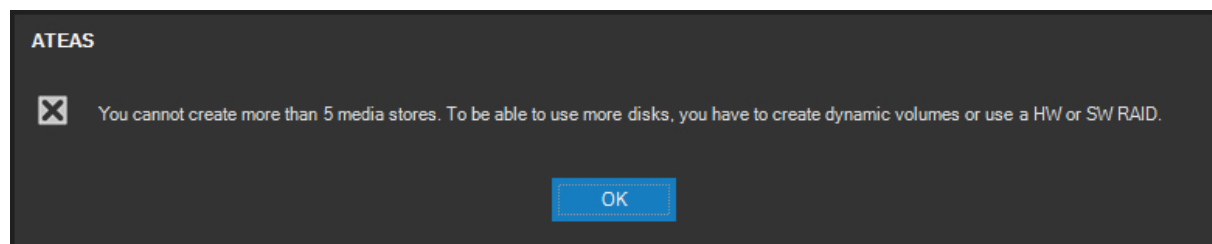
A new media store can be created by pressing the **NEW** button. With ATEAS Security version 3.9.4 the option of creating 5 independent media stores is made available. The reasons for creating more than one media store include for example:

- the need for more independent disk spaces, which cannot or are not suitable to be linked into a single logical unit,
- the need to define different periods for preserving records for various camera groups using different limiter configurations for each media store.

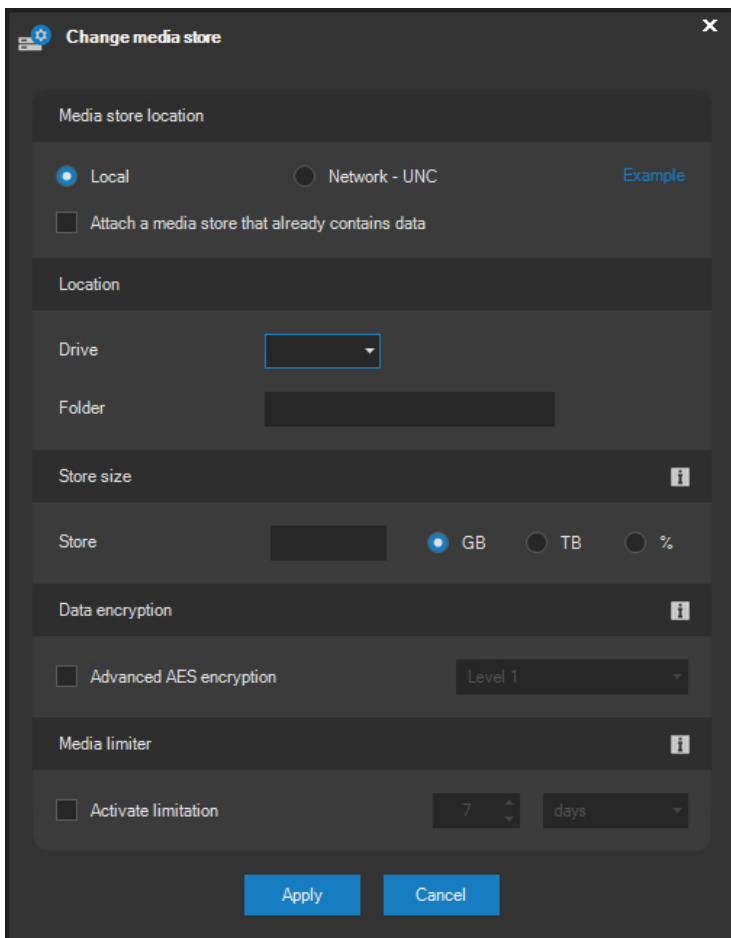
CAUTION

The option of creating multiple media stores should not, although possible, serve as a primary tool for increasing the total size of the recording space. You must remember that no redundancy rules apply between individual media stores (see chapter on clusters for entire server backups). If your only goal for multiple media stores is to increase the overall capacity of the record space, you should always consider the use of performance tools for linking stores or entire disks into a single logical unit, which can also secure certain redundancy, for example, during a disk failure. This particularly applies to RAID technology on a software or hardware basis (the hardware solution is significantly more powerful).

If you attempt to create more than five media stores on one camera server, the application will react with a warning message and will not permit the creation of another store.

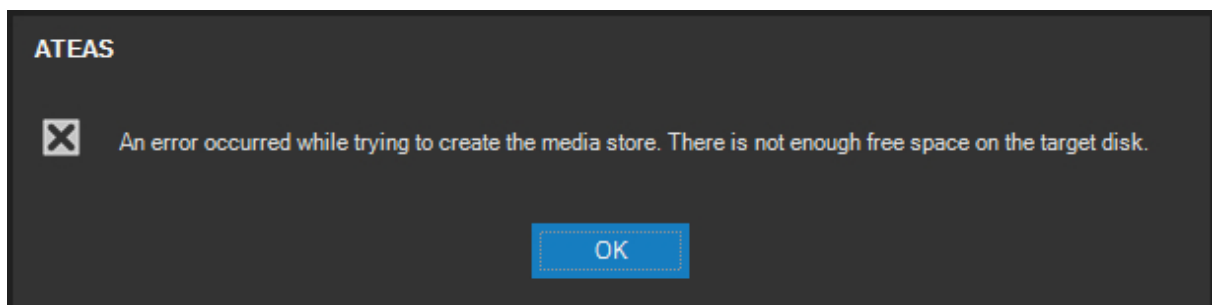


Upon pressing the **NEW** button, a dialog will appear where you will be required to add basic parameters for the created media store.

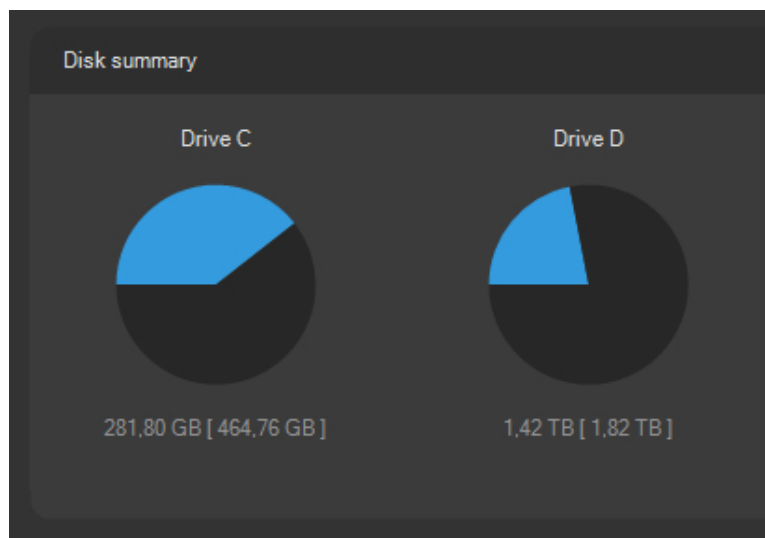


The 'Change media store' dialog box is shown with a dark theme. It has a title bar with a gear icon and a close button. The main content is organized into sections: 'Media store location' with radio buttons for 'Local' (selected) and 'Network - UNC', and a checkbox for 'Attach a media store that already contains data'; 'Location' with a 'Drive' dropdown menu and a 'Folder' text input; 'Store size' with a 'Store' text input, radio buttons for 'GB' (selected), 'TB', and '%', and an information icon; 'Data encryption' with a checkbox for 'Advanced AES encryption' and a 'Level 1' dropdown; and 'Media limiter' with a checkbox for 'Activate limitation', a numeric input set to '7', and a unit dropdown set to 'days'. At the bottom are 'Apply' and 'Cancel' buttons.

If the media store is saved locally, you must select a drive from the drop-down list, enter the name of the folder to be created on the specified drive and adjust the maximum database size. The maximum size can be set in Gigabytes, Terabytes or the percentage of drive size assumed. The minimum database size is 1 GB. The maximum database size is the capacity of the entire drive. If the maximum size is exceeded, the application will display the respective warning message.



Creating a media store with a size greater than the free space on the destination drive is not possible.



The limiter function, described further, can also be activated optionally directly at the start of the media store creation.

The media store can be created anywhere in the network. You must select the Network – UNC switch and instead of selecting a hard drive, enter the UNC path which must start with the \\ symbols. Finally, specify a folder which will be created by the server in the destination location.

CAUTION

After the installation, the ATEAS Server service is run under the Local System account. This account cannot access network devices. Therefore, if you wish to create the media store in the network by entering the UNC path, you must change the account under which the application will be run. This action is performed via the Service Control Manager application. You must use an administrator account that has access to the specified network location.

NOTE

The record server will always keep a certain reserve of free disk space, even if the media store has not reached its maximum size specified. This also applies if the size of the media store is set to full disk capacity. Therefore, disk space will not be completely used up.

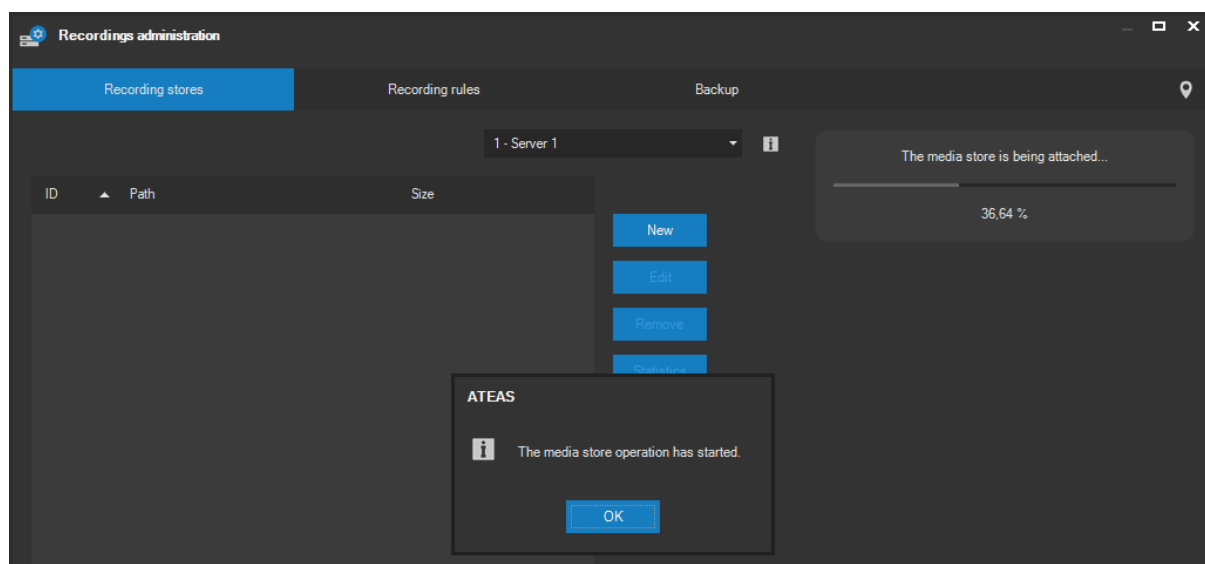
NOTE

The ATEAS Security platform does not limit the maximum size of a media store. The only limitation rests in the capacity of destination disk or disk array. The overall media store conception and performance ensures usability and zero seek times, even when using high disk capacities up to 100 TB.

The application will display a message after the media store is successfully created on the server. However, creating a media store may result in an error. This can occur, for example, when it is not possible to write to selected hard drive or when it is not possible to create a folder with a name already entered (the folder already exists or the name is not valid).

Attaching an existing media store

As often is the case, we create an empty media store to which camera servers save recordings according to defined recording rules. Nevertheless, it is also possible to attach a media store to a camera server that already contains data. This feature will be required, for example, when a hard drive on which the camera server is installed crashes and we want to attach the original (existing) media store after a clean installation of the hard drive. Enable the Attach a media store that already contains data option when creating a media store to attach this media store. The progress of attaching the media store is shown directly in the administration window.



NOTE

The media store operation runs in the background, the client and camera server can continue operating normally.

Once the media store is attached, the new media store will be filled with data. The user can immediately work with this data, as he normally would, via replay, export and other tools.

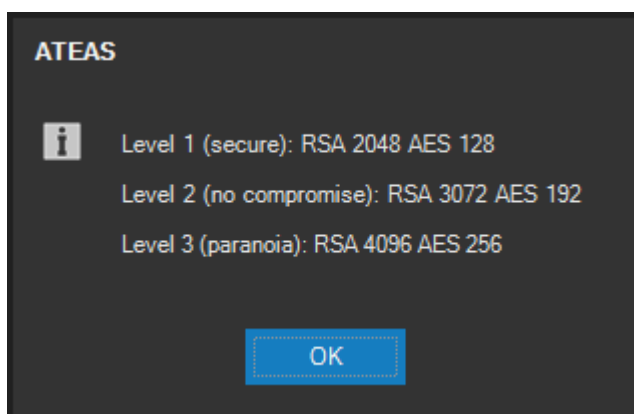
NOTE

If we attach a media store already containing data, the inspection of free space on the target hard drive is skipped.

Media store encryption

When creating or making future changes to a media store, you can choose to activate the advanced AES encryption option to activate the data encryption for the media store using advanced AES encryption (Advanced Encryption Standard).

The encryption level can be configured from 1 to 3. Although the first level already offers protection that cannot be broken using the means available today, it is possible to opt-in for an even more secure level with longer cryptographic keys.



The following attacks can be prevented by activating the advanced AES data encryption for media stores:

- Direct access to media store data: If the encrypted data from the unsecured data storage is loaded using different software (via direct access to the media store disk), its content cannot be converted to readable format.
- Hijacking the server including the installed ATEAS Security software. It is possible to restrict access to data of the servers within a distributed system, even if the hacker gets his hands on the entire server. If this server already left the original ATEAS Security system installation, the camera system will under no circumstances obtain a key to decrypt the media store data.

NOTE

Media store encryption is available starting with ATEAS Security PROFESSIONAL edition.

Modifying a media store

You can additionally modify a created media store by pressing the **EDIT** button. The same dialog is activated when modifying the media store as during the creation of the media store with the only difference being that the media store location cannot be changed (local or network) as well as the directory name. You can, however, change the size of the media store, limiter settings, encryption settings etc.

CAUTION

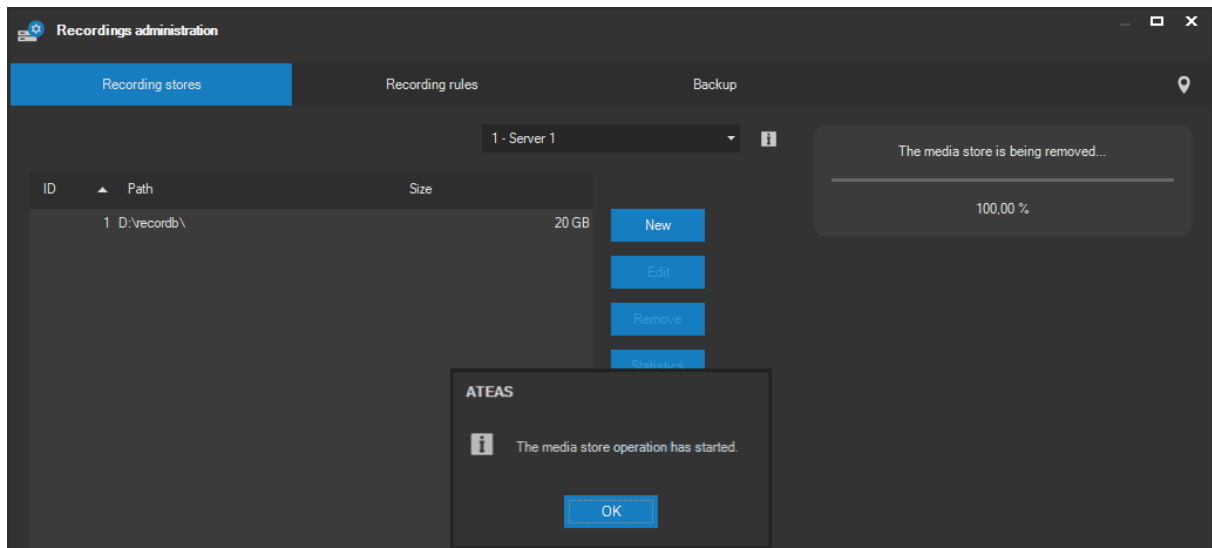
In order to maintain recording database consistency, the size adjustment is not performed immediately, but afterwards during the two following write cycles when the media store size is intelligently modified (i.e. the oldest data are deleted when the size is reduced).

Considering the fact that the camera server uses advanced methods for managing data and free disk space including for example automatic non-fragmented space allocation, frequent and significant media store size adjustments may lead to increased fragmentation. Therefore to enhance record database performance, you should perform a hard drive defragmentation after a greater number of size adjustments (from tens to hundreds). Pure cyclic database rewriting does not increase the level of fragmentation.

Removing media stores

A media store can be deleted by pressing the **REMOVE** button. Removing the media store can cause data loss in the media store directly, as well as its physical removal from the hard drive. You must

confirm two warnings before the unrecoverable deletion process begins. Depending on its size, removing the media store can be a time-consuming operation (it may take several minutes), and so this operation is accompanied with a progress bar with the progress shown as a percent value.



NOTE

The media store operation runs in the background, the client and camera server can continue operating normally.

Limiter configuration

When creating or modifying the media store you can assign a media limiter function to the media store. This function can automatically limit the age of data in the media store in order to not exceed the maximum limit, which can automatically meet legal requirements on the camera recording in relation to the protection of personal data. Various limiter settings can be defined for each media store; therefore you can maintain different camera groups in recording for various periods of time.



The Activate limitation checkbox activates (or deactivates) the video and audio data limiter. You can set the number of days (or hours) for which the data should be recorded. Hour units can be used in

case you need to limit the media store data age to a period less than a day, or to specify the period more accurately.

NOTE

Modifications to limiter settings are applied immediately after they are made or after media store parameters are changed using the **APPLY** button.

NOTE

Limiting the age of data within the media store does not lead to a lowered media store size. In order to delete part of the media store to free up disk space back to the operation system, you need to change the size of the media store by pressing the **EDIT** button.

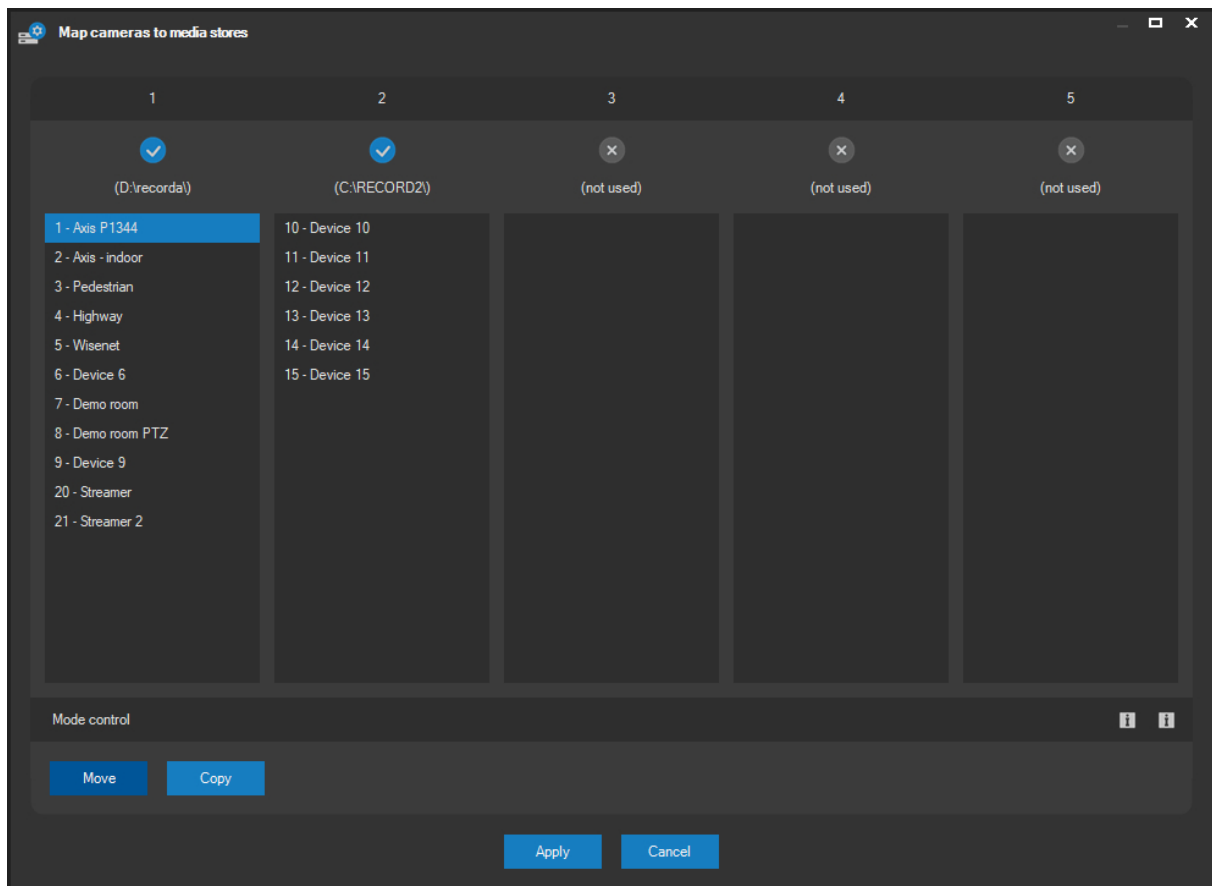
Assigning cameras to media stores

If multiple media stores are created on the camera server, you can determine which cameras will be used for a specific media store. For some cameras, you can define an extensive media store, where for another group of cameras, you can define a smaller media store, providing our demands on the duration of maintaining data are not so high. Various limiter settings can also be defined for media stores.

NOTE

By adding a new camera to the system, the camera will be automatically assigned to media store number one.

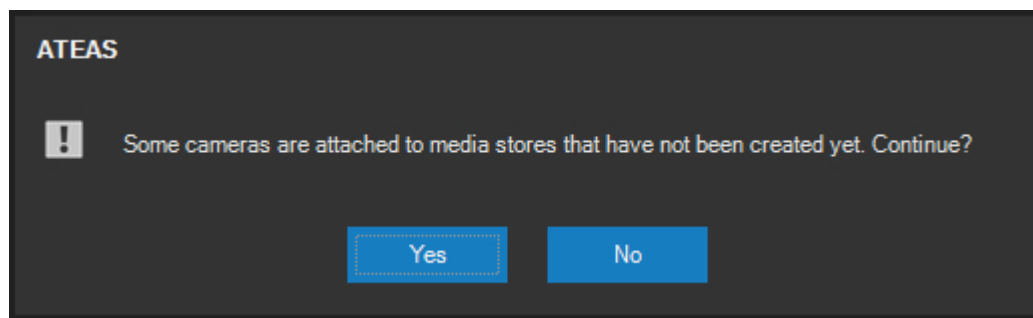
Use the **DEVICES** button to assign individual cameras to various media stores. A camera mapping window will then open to the media stores.



The picture shows the maximum number of five media stores. You can also immediately recognize how many stores have already been created and how many the camera server is using. Lists under the media store labels contain the numbers and names of cameras, which are currently assigned to the respective media store. Cameras can be easily moved between individual lists by dragging the mouse. You can also move a number of cameras at the same time by making multiple list selections (e.g. using the CTRL key or by using a mouse drag operation). To start moving or copying selected items to another list, click the mouse button again on one of the already selected items.

NOTE

Cameras can also be moved to media stores, which have not yet been created. Upon saving these settings, these cameras are of course not capable of recording. Recording, however, begins automatically after the media store is created. If the application detects this state, you will be given notice by a relevant message dialog.



By default, dragging and dropping cameras within this dialog moves them to another list under a target media store. However, if we activate the **COPY** button, instead of the **MOVE** button, the items will be copied. This means that the respective cameras will record in multiple media stores at the same time. This feature can be used, for example, for ensuring a longer archiving period for camera video and audio in lower quality in a different media store.

NOTE

Cameras can use various recording rules for recording to various media stores. This configuration is carried out in the Basic camera settings window next to the list of recording rules.

NOTE

If you wish to remove a camera from the list, you can move it to another list. If the camera already exists in the target group, it will only be removed from the original list.

When moving or copying list items, you can force an operation change via the CTRL (force copy) or SHIFT (force move) key, independent of the button pressed in the bottom part of the window.

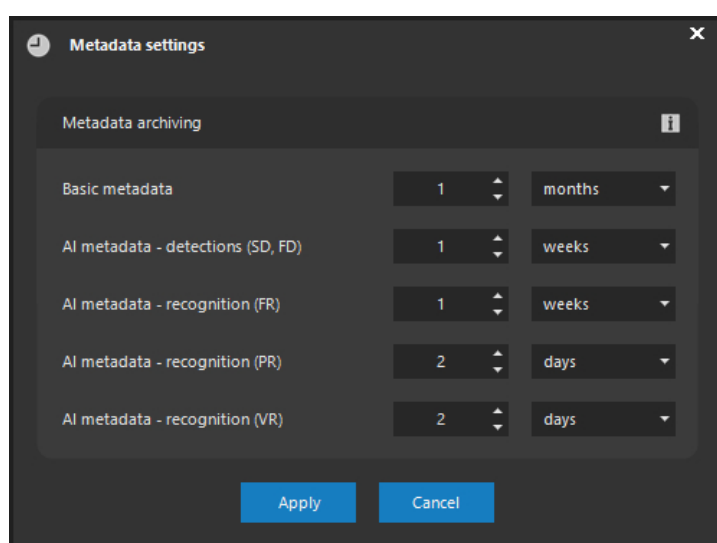
Metadata archiving

Metadata archiving time can be configured for each camera server. Basic metadata include e.g. motion detection or alarm input triggers. Neural network metadata enable the advanced forensic video search feature (zone intrusion, line crossing etc.) as well as a similarity search based on a selected visual sample.

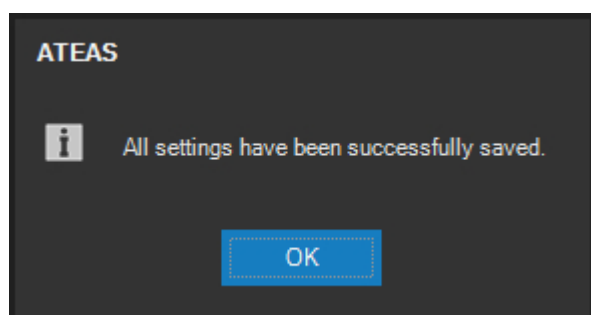
CAUTION

Especially the metadata generated by a neural network can take up a significant amount of disk space, a good system design is advisable when increasing the interval.

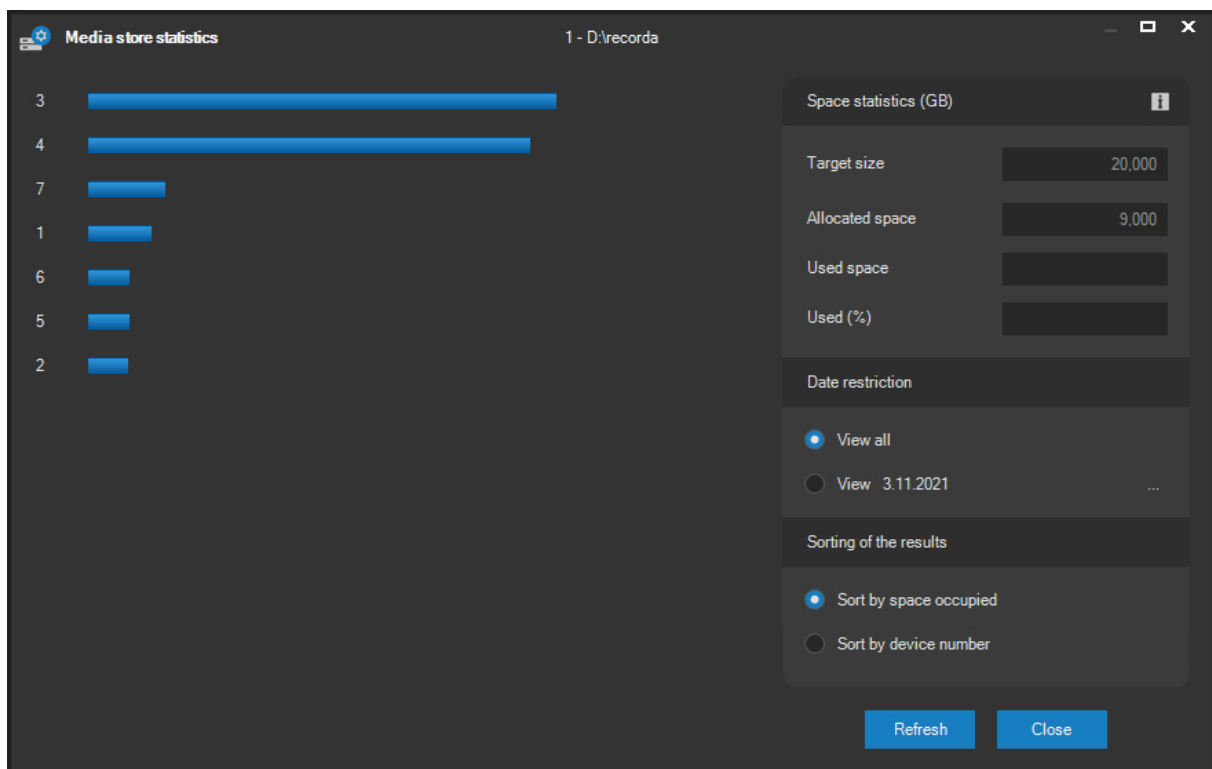
The archiving period for metadata can be modified by pressing the **METADATA** button. This configuration can be executed at any time and completely independently of the creation of media stores.



A confirmation message will be displayed after the change is successful.

Media store statistics

Pressing the **STATISTICS** button displays the statistics of occupied space for the selected media store of the camera server. This information can be essential when the recording rules (profiles) should be redesigned.



The window contains a bar graph showing the amount of space occupied by each camera in the recording database. The graph is relative, whereby the maximum value (100 percent) is set as the value of the camera with the maximum amount of occupied space. Next to every row, the occupied space is also written in absolute value in GB with an accuracy of 3 decimal places.

The window also contains an overall information overview of the media store:

Target size: Media store size set by an administrator.

Allocated space: Current actual allocated space.

Used space: Currently used space for video, audio and metadata.

All information is displayed in GB with an accuracy of 3 decimal places or relatively in percentages.

NOTE

The allocated space can be temporarily higher or lower than the target size, until the database is filled up during the initial recording cycle or upon changing the target size by the administrator. In this case, the media store adopts the new size within one or two recording cycles.

NOTE

The used space can actually be lower than the allocated space, if the database creates a reserve in the area due to the automatic age limiter in the database. Recordings created by versions of ATEAS Security older than 4.0.0 will also be considered as unused space until they have been overwritten.

The relative graphical statistics can be displayed either for the entire media store or also for a day of your choice, which can provide further valuable information for the evaluation of changes to video stream settings, recording rules or evaluation of event frequency for example.

The graph is automatically sorted from the camera with the highest demands for space within the database to the camera with the lowest demands. Using the option buttons in the Sorting of the results group, you can also sort the graph according to camera numbers.

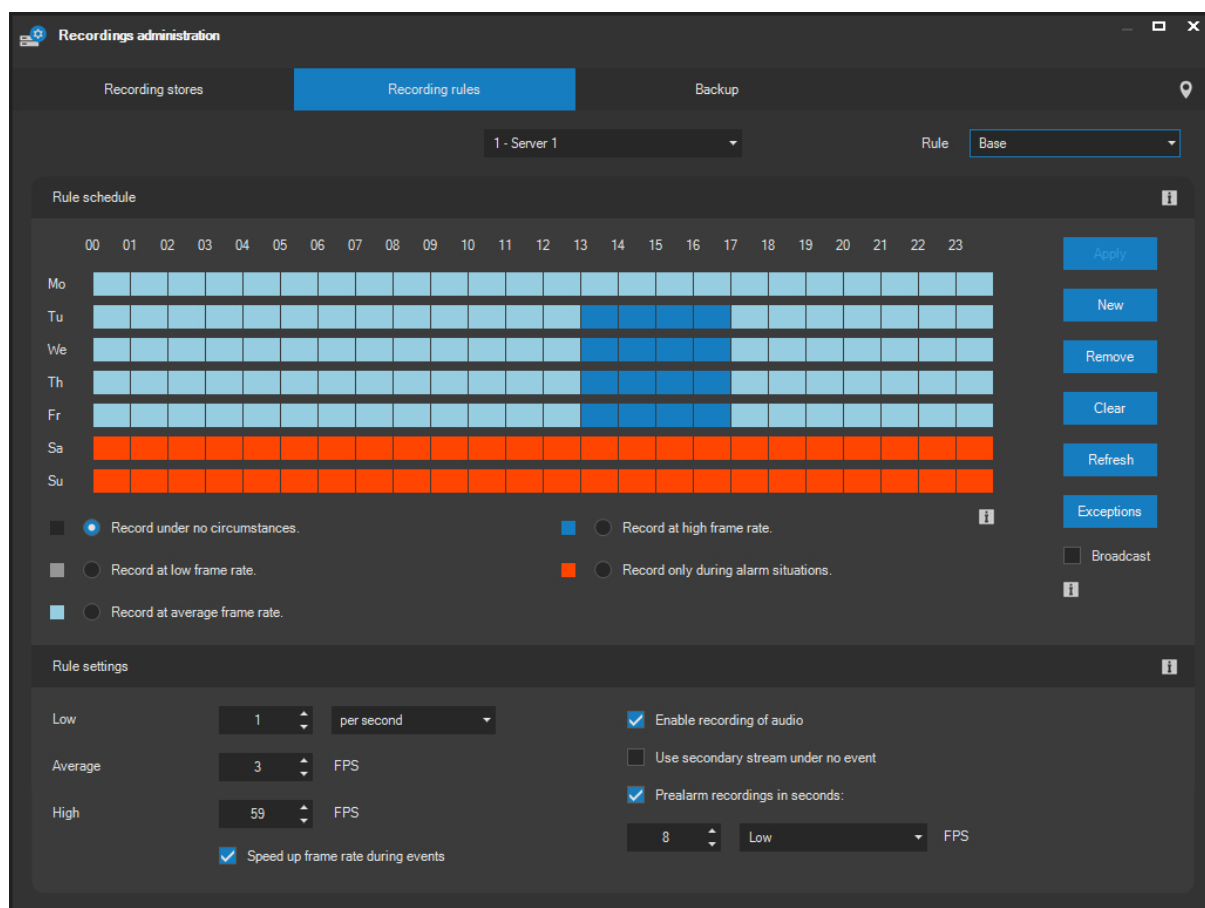
11.6.2. Recording rules

A recording rule is a group of rules for recording from a camera. This rule is always created on a relevant camera server and can be used for one or several cameras from the specific server. To access recording rules, you must display the **Recording rules** tab in the recordings administration section.

NOTE

Profiles created may be assigned to cameras in the devices administration section, basic camera setup.

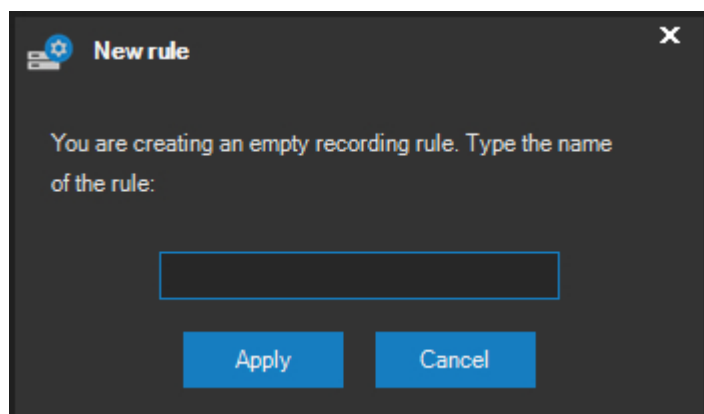
When working with profiles on a specific server, you must select this server from the drop-down list of camera servers. After doing so, all recording rules saved on the selected server will be displayed in the Select rule drop-down list. A rule itself is displayed after selecting it from this list.



The screenshot shows the 'Recordings administration' window with the 'Recording rules' tab selected. At the top, there are tabs for 'Recording stores', 'Recording rules', and 'Backup'. Below these, a dropdown menu shows '1 - Server 1' and a 'Rule' dropdown shows 'Base'. The main area is titled 'Rule schedule' and features a calendar grid for days of the week (Mo to Su) and hours (00 to 23). The grid cells are colored: light blue for 'Record under no circumstances', dark blue for 'Record at high frame rate', light grey for 'Record at low frame rate', orange for 'Record only during alarm situations', and medium blue for 'Record at average frame rate'. To the right of the grid are buttons: 'Apply', 'New', 'Remove', 'Clear', 'Refresh', and 'Exceptions'. Below the grid are radio button options for recording under no circumstances, high frame rate, low frame rate, average frame rate, and only during alarm situations. There is also a 'Broadcast' checkbox. The bottom section, 'Rule settings', includes frame rate settings (Low: 1 per second, Average: 3 FPS, High: 59 FPS) with a 'Speed up frame rate during events' checkbox. It also has checkboxes for 'Enable recording of audio' and 'Use secondary stream under no event', and a 'Prealarm recordings in seconds' setting (8 seconds, Low FPS).

Creating and removing recording rules

A new record rule (profile) can be created on the selected server by pressing the **NEW** button. Next, you must enter the name of the rule. This name must not already be used.



The screenshot shows a 'New rule' dialog box with a close button (X) in the top right corner. The text inside says: 'You are creating an empty recording rule. Type the name of the rule:'. Below this text is a text input field. At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.

An empty recording rule is created after pressing the **APPLY** button and is confirmed by a message dialog. The newly created rule is also automatically selected for further configuration.

The selected rule can be deleted by pressing the **REMOVE** button and confirming the message by pressing the **YES** button.

Adjusting recording rules (profiles)

The selected rule can be configured using the recording rule adjustment control. Individual rows represent days of the week. The vertical direction includes a day divided into 24 hours. The minimum resolution is 15 minutes. Individual fifteen-minute segments can be selected by moving the mouse while holding either the left or right mouse button. If you use the left mouse button, the settings under this control will take effect. If you use the right mouse button, the current content will be deleted, i.e. re-written to default values (corresponds to the left mouse button while the Record under no circumstances option is checked). There are several possibilities available for writing into this control when using the left mouse button:



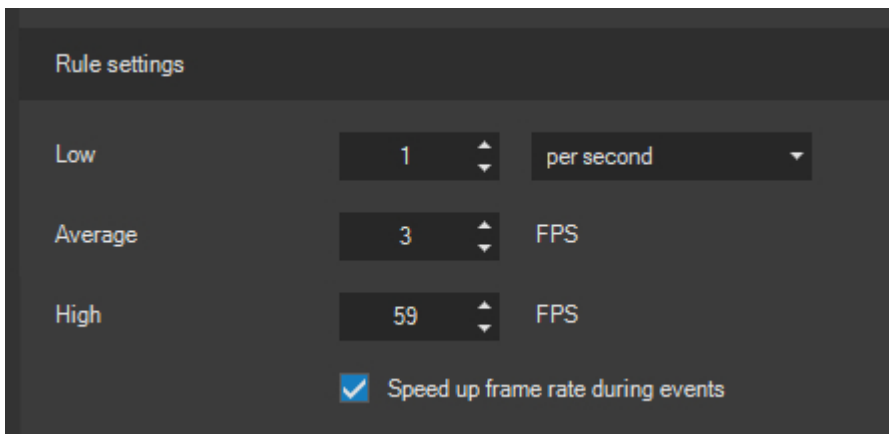
TIP

To quickly select a day or entire week, double or triple-click the area.

TIP

To quickly schedule working hours in multiple days, use the ALT key.

The frame rate can be adjusted using the relevant controls, namely low frame rate, average frame and high frame rate. Low frame rate can also be adjusted by setting the number of frames per minute (besides the standard FPS option – frames per second).



Rule settings		
Low	1	per second
Average	3	FPS
High	59	FPS
☒ Speed up frame rate during events		

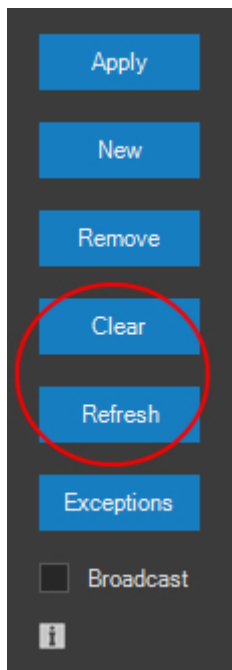
CAUTION

Streams with other video codecs than MJPEG may not precisely observe these frame rates, since precise control is not possible due to compression dependencies between frames. Both the low and medium frame rates are derived from key frames only. A high frame rate always means recording all frames.

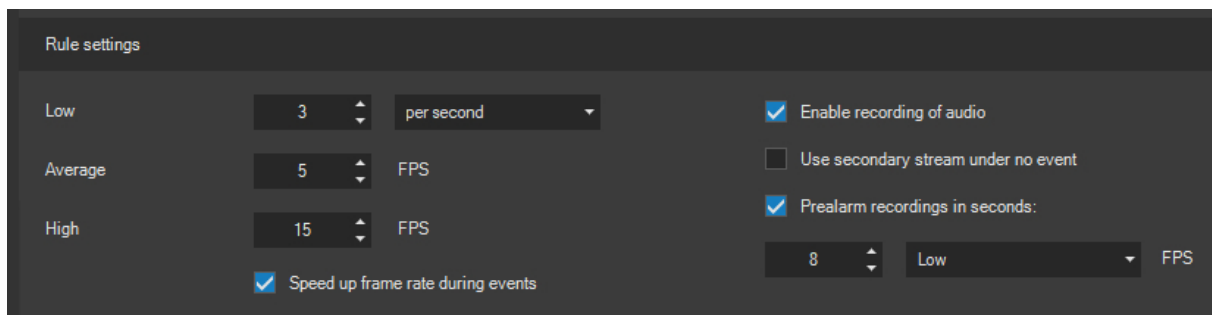
For special purpose high FPS cameras delivering the MJPEG video format, this value can be increased up to 500, when the very same effect is activated as for other video formats, i.e. all video samples from the video stream will be stored.

Two additional buttons with the following functions are available for recording rule configuration:

The **CLEAR** button clears the rule to the extent that the Record under no circumstances option is applied throughout the entire time schedule. The **REFRESH** button will apply the rule as it is saved to the server (i.e. last saved changes).



You can perform additional settings by checking the available checkboxes within the frame of adjusting recording rules.



If the Speed up frame rate during events checkbox is checked while either a low or medium frame rate is applied, the recording frame rate will be raised to high during event or alarm situations.

The audio will be recorded together with the video if the Enable recording of audio checkbox is checked.

CAUTION

The audio will be recorded only if it is activated in the corresponding camera setup and at least a low frame rate video must be recorded at the same time.

A recording rule can be used to lower the recordings frame rate when no event is currently taking place. The Use secondary stream under no event option can be used to save recordings capacity not only by lowering the frame rate, but also by reducing the video resolution or changing the video format.

NOTE

For this switch to work, a secondary video stream must be activated in camera settings.

If the Pre-alarm recordings in seconds checkbox is checked and an event occurs, you can add a certain period of time to the record (pre-alarm buffer) before the event beginning. The time parameter defines the duration of the recording, saved before the occurrence of an event, in seconds. The frame rate used for creating the pre-alarm buffer can also be defined.

TIP

The pre-alarm buffer can replace the given recordings section even when continuous recording with a lower frame rate or different resolution is already taking place.

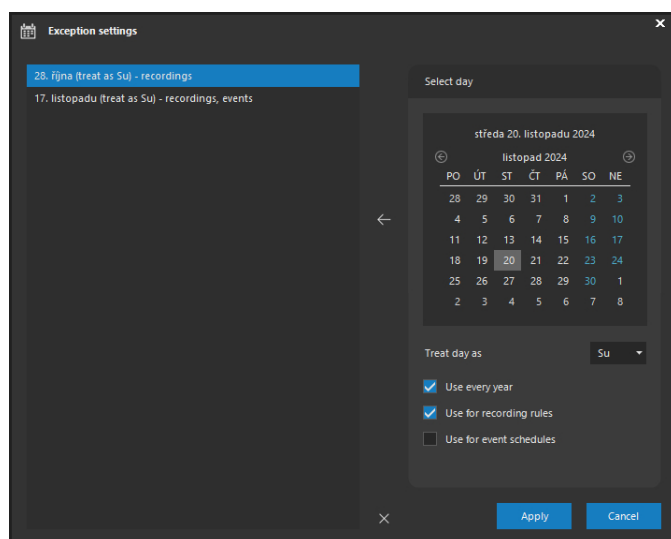
CAUTION

If a recording rule with the pre-alarm buffer activated is applied to the camera, the Keep permanent connection to the device option will not be effective in the camera setup, since this demands a permanent connection.

Recording rule configuration is saved by pressing the **APPLY** button. The application will confirm the configuration is changed by showing a message dialog. The new recording rule configuration will immediately take effect for all cameras that have this rule assigned.

If the Broadcast option is enabled, when creating a new or editing an existing rule, the changes in the recording rule will be applied to all camera servers the administrator has access to.

The **EXCEPTIONS** button enables creating a database of special dates, on the given camera server, which will be perceived differently than specified by the recording rule. Exceptions can be used, for example, on national holidays, where in terms of recording, these dates can be perceived as Sundays instead of workdays. Setting exceptions is valid for all recording rules, not just for one rule that might be selected in the list.



The calendar user control is displayed in the dialog after the **EXCEPTIONS** button is pressed. Here, it is possible to select an arbitrary calendar day for an arbitrary year, we would like to mark as being special, and therefore remove it from the recording profile settings. We can select how the date selected in the calendar will be perceived in terms of recording. Therefore, holidays can, for example, be perceived as a Sunday, weekend days with scheduled work activity as a Monday. For each day we can also decide whether this exception will only be valid for the specific year selected or whether it will be repeated each year.

Upon selecting the date and additional settings, you can add the exception to the list via the button with a white arrow, which can be found between the calendar control and the list of exceptions. Removing an exception can be performed via the cross button. Exceptions without a yearly recurrence are listed without the year, non-recurring exceptions include the year information.

To apply the exception to recording rules, the Use for recording rules option must be activated when adding the exception. The Use for event schedules option allows applying the exception also to static (not dynamic) event schedules.

Changes to exception settings need to be confirmed by pressing the **APPLY** button.

NOTE

The application will not permit entering a duplicate exception to the list (same date and same period). However, it is possible to enter the same special date with or without an annual period. In this case, the day without an annual period is perceived as an exception to an exception and will be given priority, in terms of recording, over the date with an annual period set.

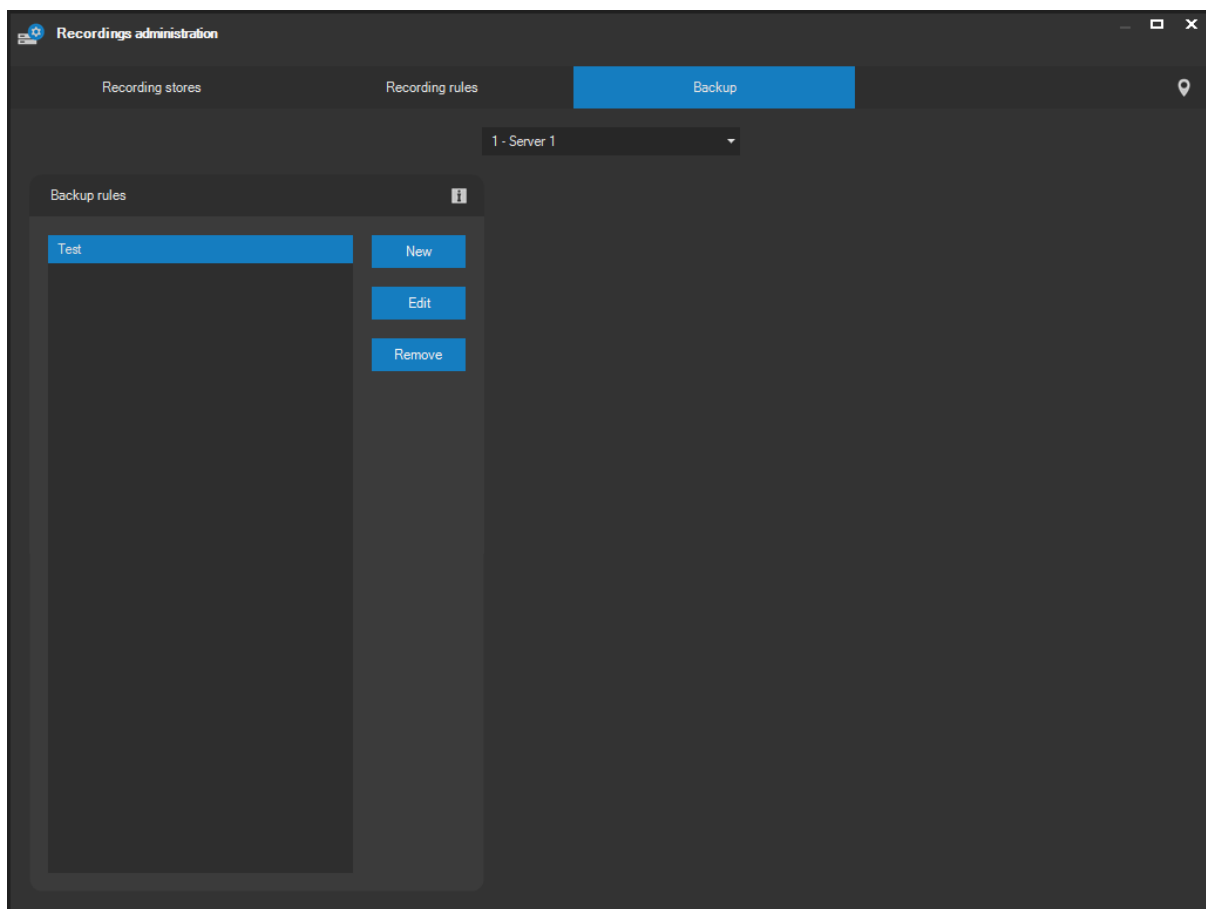
11.6.3. Backup

Media stores and their very large sizes, basically limited only by hardware, allow storing data for a long period of time, which of course is affected by additional settings, namely the recording rule for the respective camera. However, should there be a request to create permanent backups stored outside of the media store, and should these backups be made on a regular basis, and therefore using the Download manager client tool would not be optimal, the Backup server tool can be used.

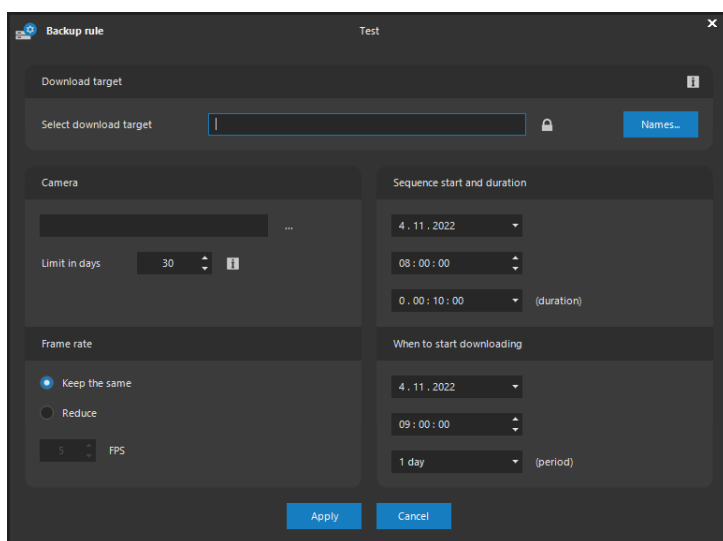
NOTE

The backup tool is available starting with ATEAS Security PROFESSIONAL edition.

The Backup tool allow defining backup rules, which the server will automatically and regularly apply and make data backups of the media store to another storage. Data backed up is in ATS format and therefore provides maximum security via advanced AES encryption. Backed up data is automatically organized at the identified target location according to server, camera and data. Individual files are then given a suitable name according to the recording time. The file naming structure and convention is identical as for downloading data via the Download manager client tool.



When creating backup rules via the **NEW** button, after entering the name you must also enter several basic parameters, as shown in the following picture.



First of all, the download target shall be filled out, which is the local or network location for the backup. The location can therefore be entered as a local path, for example `e:\backup` or as a UNC path, for example `\\ext1\backup`.

NOTE

Although this location is specified from the ATEAS client environment, it must be a path that is valid for the given camera server, for which you are creating the backup rule. This makes sense because it will be the camera server creating the backup.

NOTE

The exact same principle applies for using UNC paths as for creating media stores defined by a UNC path. In this case, the camera server service cannot be started under the Local System account, but requires an administrator account with access to the given location.

Using the button next to the text field for entering the target location, you can activate advanced AES encryption for ATS file backups.

The cameras that will be part of the rule can be selected in the Backup settings – Camera section. In addition to this, you can also specify the limit to the number of days. This limit determines that backups older than the specified number of days will be automatically deleted to make space for new backups being created.

CAUTION

If there are no files older than the defined number of days and there is not enough space, new backups cannot be created.

NOTE

If Limit in days is set to zero, no files will be deleted. This can be used when backups are permanently stored and, for example, backup medium is replaced (connecting a different external drive etc.).

Under Sequence start and duration and When to start downloading sections, we define the period for which the data backup should be made and also when the backup should start. This makes it possible, for example, to plan backups overnight, when lower network loads are expected etc. The period value determines how often a backup is made. When set to 1 day, the respective backup will start at the default time periodically and the time interval backed up will also be shifted 1 day forward.

Under Frame rate, we can define whether we would like to create the backup with the same frame rate originally used for the recordings or with a reduced frame rate. With a reduced frame rate, we can backup the given interval of the media store with a lower demand on free space.

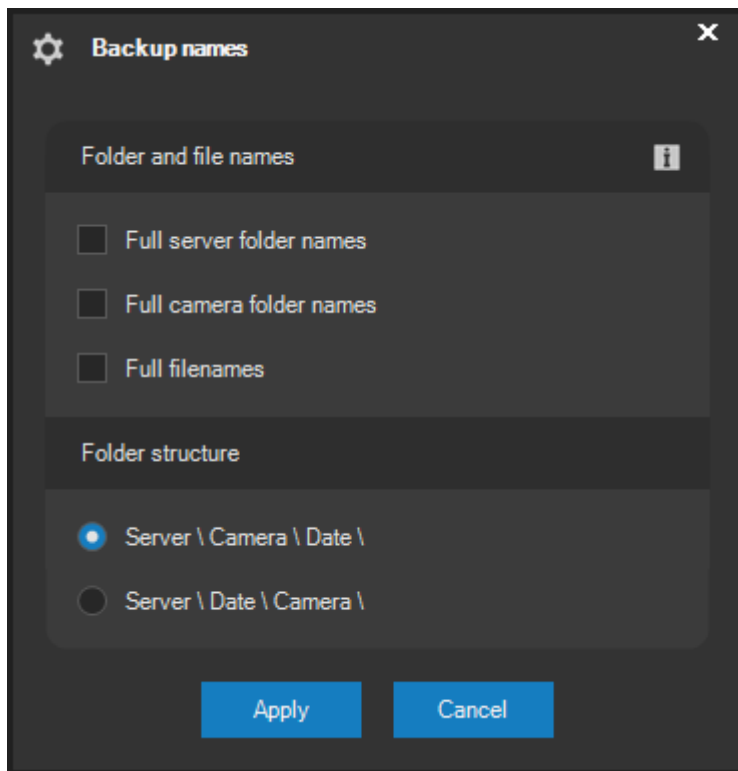
NOTE

The frame rate of a video other than MJPEG can be left unchanged or reduced to at least the rate of key frames (or lower), because leaving out only certain dependant frames (P frames) would result in the video being unreadable.

The created backup rules can be updated or removed via the **EDIT** or **REMOVE** buttons. Updating or removing rules does not have any impact on completing the backup process for the respective rules, provided the backup process has already started.

Target structure of folders and files

Data backups are stored in folders according to servers. These can then be classified based on camera and subsequently based on date. The second option is to classify them according to date first and according to cameras second. The method of classifying the backups into folders, and the potential enabling of long names for folders and files (i.e. including server and camera names) can be performed within the dialog after pressing the **NAMES** button.



11.7. Views management

11.7.1. Sharing views

Administrators can easily share views or entire groups of views by dragging them into the Shared views location in the main menu. Menu editing, creating or deleting groups or moving and copying views within the shared views is identical to editing the local views structure, where these techniques are described.

Changes to shared views take immediate effect for all users. Shared views can be removed using the very same button in the monitoring window that is used for removing local views.

NOTE

Views or entire groups will be automatically hidden from the users if they lack permissions to any of the cameras contained in them. Therefore, it is not necessary to configure user permissions to access the views. The views menu generation is fully automatic.

11.7.2. System shared view groups

Some names of shared view groups created on the first tree level can have system defined meaning and can therefore satisfy other enhancements and special functions. The system supports these reserved names for shared view groups:

- **Mobile:** If you create a shared group of views with this name, clients on mobile platforms will offer these views for display. This way you can smartly distinguish between views for mobile monitoring and standard views. Only views consisting of 4, 9 or 16 cameras are currently supported. No other types of views can be shared in this group.

11.7.3. Video wall

NOTE

Video walls are available starting with ATEAS Security PROFESSIONAL edition.

ATEAS enables remote controlling monitors connected to other client workstations. Using this option, you can easily configure and use a video wall. This requires setting and installing client applications to workstations which have up to eight monitors connected. These monitors are either a part of the video wall or controlled remotely.

NOTE

Controlled monitors do not have to be included in the video wall. A video wall can also be virtual enabling the control of various monitors from different workplaces.

Establishing and setting a video wall (physical or virtual) is executed as follows: First of all, create special user accounts, subordinate to the video wall. Then login as these users on individual slave workstations and set the number of monitors. After completing this step, configure the video wall (see following text) and open the video wall control window from the application main menu. Operations related to controlling a video wall are listed in the Monitoring chapter.

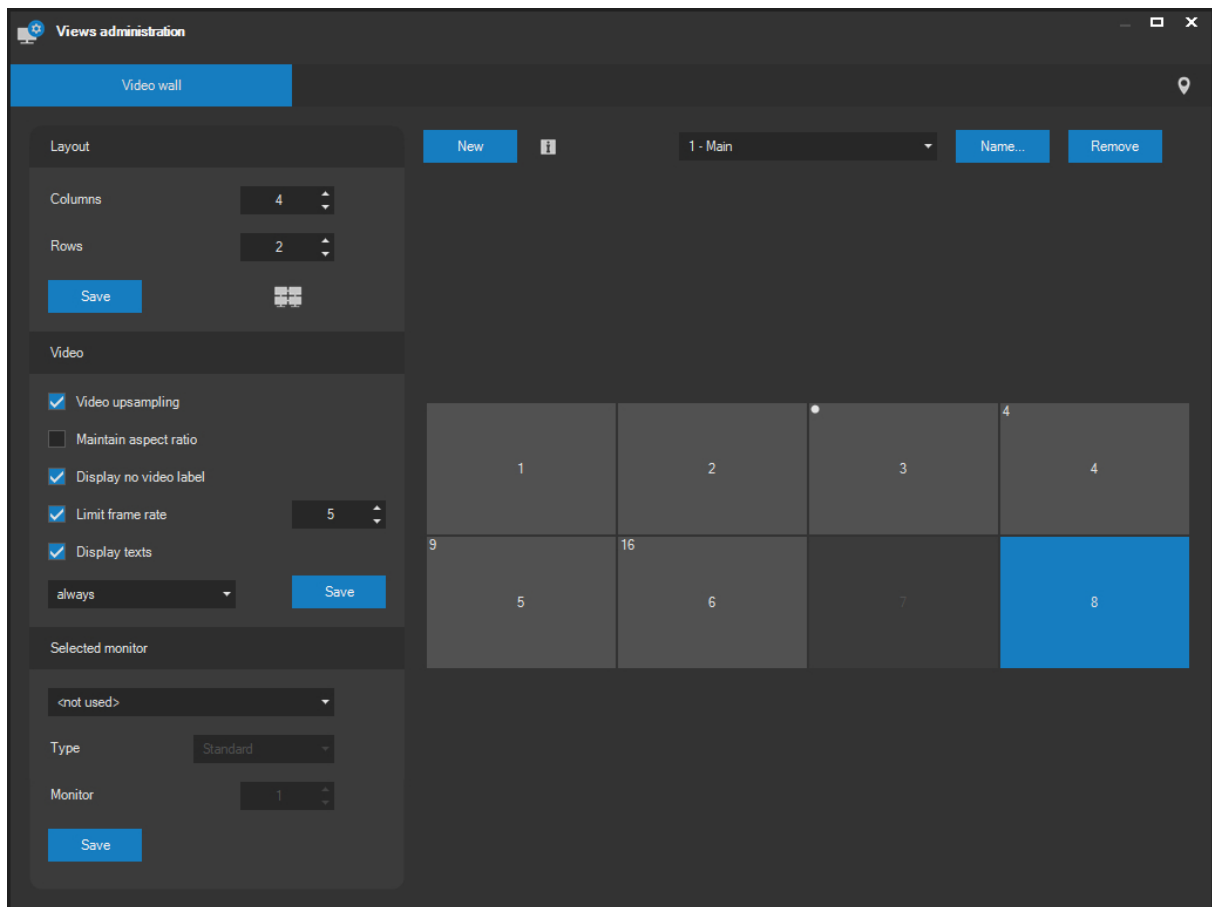
CAUTION

To ensure the correct layout interpretation for monitors connected to subordinate video stations, using all available configurations in dependent and independent mode (span, multi-view), you must adjust the slave video station to the N:1 monitor layout. So if there are four monitors used, the monitor layout on the station must be 4:1 and not 2:2 for example. This does not apply to the final monitor layout of the video wall. This layout can be random. The N:1 layout condition is only used to make the ATEAS client correctly recognize all monitors.

Slave stations or monitors can include any computer with a pre-installed full ATEAS client, or a television or display equipped with the Android operating system, on which the ATEAS client for Android is launched. There is no difference in controlling both types of external monitors for video wall users.

Special slave accounts used in standard ATEAS client application have some specifics which need to be considered.

- Live windows are opened on a corresponding number of monitors several seconds after the login process (when using standard clients, a workspace with an automatic start activated works in a similar way).
- The application main menu is shortlisted to two items, namely Exit and Setup. The setup item can be used for deactivating application automatic startup (together with the operating system) and for disabling the automatic login of a slave account. That is the only way of logging in as a standard user.
- After logging in with a slave account, the local settings of the ATEAS Observer application will be automatically adjusted in the auto start section. After the login, the application auto start is automatically activated together with automatic user account login. This ensures independent operation at all stations and automatic refreshing after system restarts.
- A video wall slave account is, of course, capable of reconnecting and repeating the login process to the server when the connection to system administration server fails. This also enhances the automatic video wall refresh during various failures (server, network).
- A video wall client automatically hides the mouse cursor when mouse is not used.



One video wall identified as number one is created in the system by default. The **NEW** and **REMOVE** buttons are used to add another video wall to the system or remove it. Existing video walls can be renamed at any time by pressing **RENAME**.

NOTE

The video wall identified as number one cannot be removed.

When configuring a video wall, it is reasonable to set its layout first. Controls for setting the number of columns and rows are found in the upper left part of the window. All changes can be sent to the server by pressing the **SAVE** button and will take effect immediately. The application main menu will also be updated for all authenticated clients, so that the Video wall item will be either displayed or removed. Its use is bound to a permission that must be granted to the user for him to be able to access the video wall.

The maximum amount of monitors (slave monitors) included in the video wall is 192 for the virtual layout of 16 by 12 monitors with up to 1000 video walls in total. Therefore, up to 16 live windows

connected to a computer, and up to 192 thousand slave monitors can be controlled from one client workplace.

NOTE

We would like to remind you again that the layout you have set can correspond exactly with the physical layout of monitors, though it is not a condition. In practice, a video wall with a 4 x 2 monitor layout can correspond to two separated slave workplaces containing four monitors. You may also be required not to fill some of the monitors during the configuration, if your video wall consists of monitors of various sizes.

The Video section for adjusting video options is found in the left part of the window. The following video wall properties can be set using these controls:

- Video upsampling – specifies if the video resolution will be automatically increased if the screen resolution is higher. This option is turned on by default.
- Maintain aspect ratio – specifies if the original aspect ratio will be maintained when the video resolution is adjusted (increased or decreased). This option is turned on by default. If the aspect ratio is maintained, either vertical or horizontal dark stripes compensating for the difference between aspect ratios of the video and monitor can be displayed on video wall monitors.
- Display no video label – specifies whether the loss of video will be indicated with visible No video text. This feature is enabled by default for the video wall.
- Limit frame rate – declares the frame rate used for the video wall display. The frame rate is not limited by default.
- Display texts – declares the number of seconds during which the texts in the video will be displayed. These texts include camera labeling (camera name and ID, server name and ID) and eventually an additional text that identifies the event source in case the camera has been switched to the monitor because of an event. The number of seconds can be selected from the drop-down list (including permanent display). Displaying texts can be forbidden by unchecking this option. The value is set to five seconds by default.

A key part to the video wall configuration is the Selected monitor section, found in the bottom left part of the window. In this section, each monitor used within the video wall frame must have a slave user account assigned and a monitor sequence number related to the slave client station (not the sequence number for a monitor included in the video wall):

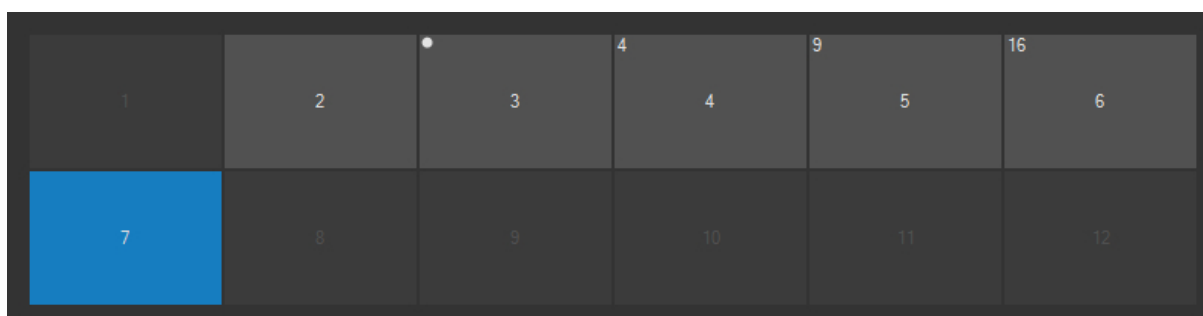
- Standard – ordinary monitor, only one camera at a time can be switched to this monitor type,

- Alarm – see Standard, the monitor will additionally be included in a group of monitors which automatically display system alarm events,
- Quad – the monitor will be divided into 4 partial monitors, making it possible to display up to 4 cameras.
- Triple – the monitor will be divided into 9 partial monitors, making it possible to display up to 9 cameras.
- Sixteen – the monitor will be divided into 16 partial monitors, making it possible to display up to 16 cameras.

NOTE

When an event is received on a video wall, the system will try to display all cameras included in the event scenario with the Include in alarm view option activated. When an event is received, the monitors from the group of event monitors are filled always from the lowest monitor number. The cameras are automatically shifted. During an event, cameras of newly occupied monitors are switched to monitors with higher numbers. The last cameras from the event monitors group will logically disappear.

A video wall monitor can be either inactive or active (assigned to a slave station) and can be used by authorized users. Active monitors can be additionally included in the event monitors group and or they can Quad type. The group of event monitors can be used the same way as other active monitors, the only difference being the inclusion of alarm events. All statuses are indicated by monitor symbols displayed on the video wall. Select a monitor to modify its configuration (selection is indicated by a blue background). The following picture these types of monitors (from the left): inactive monitor, standard monitor, event monitor, Quad monitor, Triple monitor and a monitor of type Sixteen.



NOTE

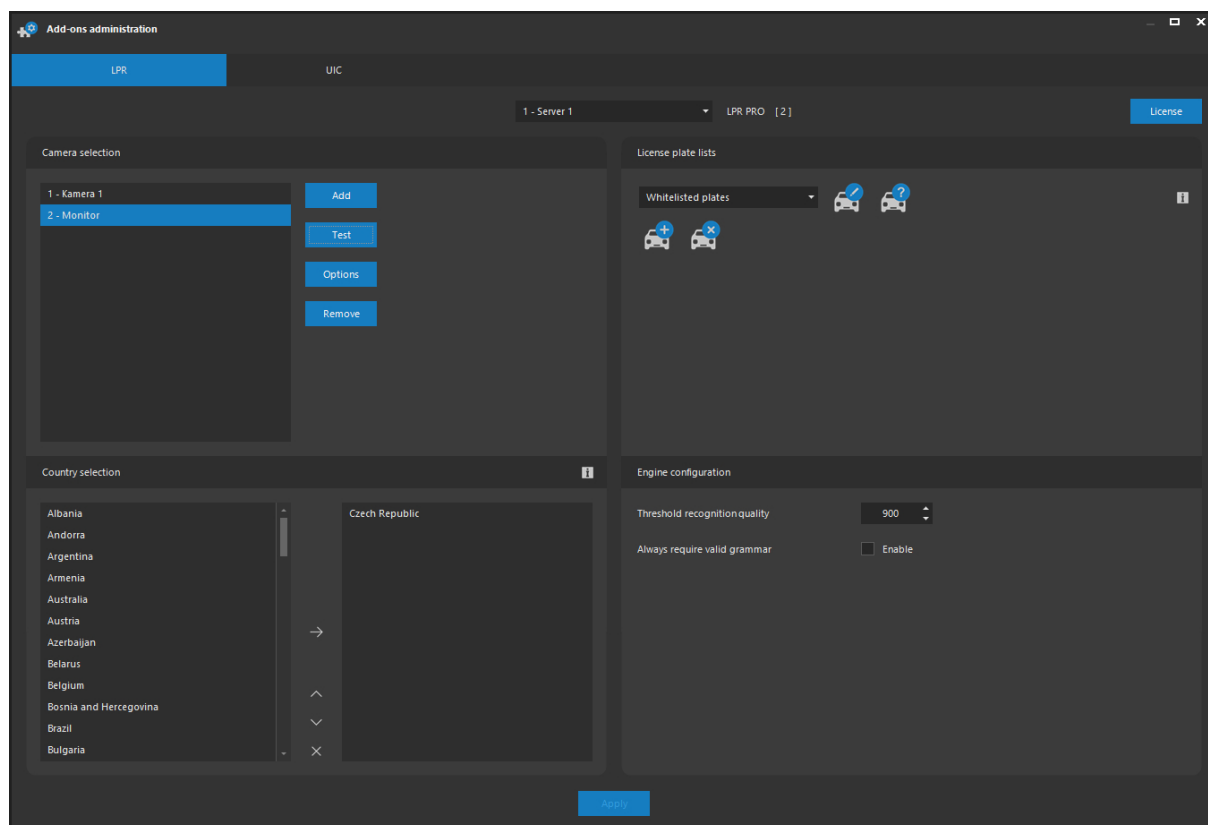
Video wall setup in the Video section automatically changes the behavior of the entire video wall, including all slave view stations without the need to manipulate or configure them in any way.

The video wall is equipped with an auto-restore mechanism after the restart or replacement of any video wall client, as well as after the restart of any system server component.

11.8. LPR engine administration

11.8.1. Selecting cameras for detection

The LPR engine administration is available in the add-ons administration section under the LPR tab. After selecting this tab, you must select a camera server from the drop-down list, where the LPR module has been installed. If the selected server does not contain this module, or it is has not been activated as an evaluation version, or if the hardware key is missing, a warning message will be displayed and it will not be possible to perform any settings.

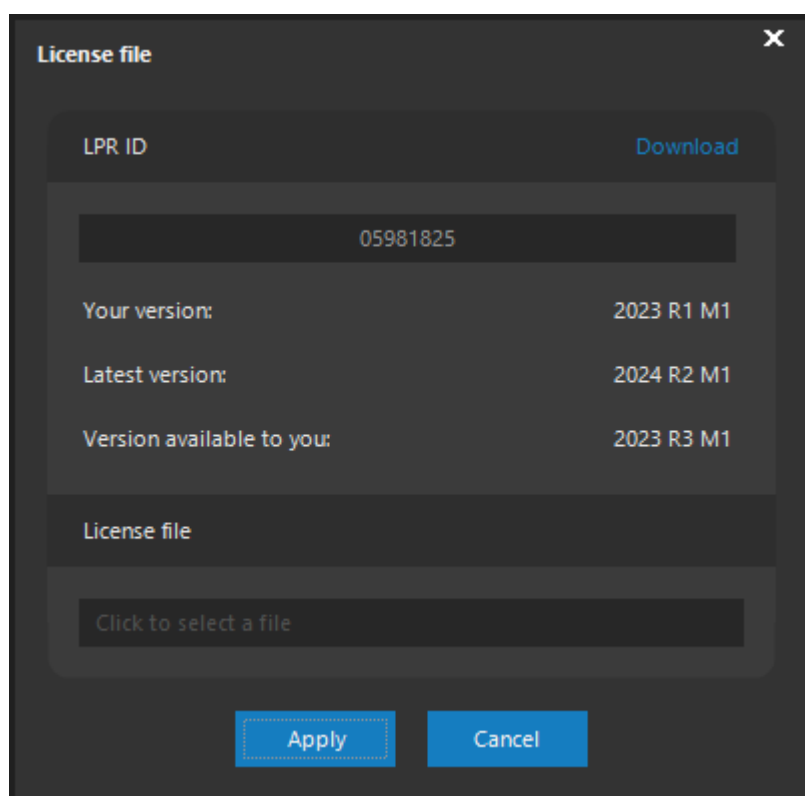


Using the **ADD** button, you can display a list of all available cameras on the camera server. Any camera from the list can be selected and added to the list of devices used for LP recognition by pressing the **APPLY** button. A single camera server can run the detection for up to 64 cameras simultaneously. To delete a camera from this list, press the **REMOVE** button.

NOTE

The current device license for LP detection and recognition is displayed next to the currently selected camera server.

When extending the LPR engine license (upgrade to a higher edition or increasing the number of cameras) use the **LICENSE** button to display a dialog where you can upload a new license to the selected camera server.



The image shows a 'License file' dialog box with a dark background. At the top left is the title 'License file' and a close button 'X'. Below the title is a section with 'LPR ID' and a 'Download' link. The LPR ID is displayed in a text field as '05981825'. Below this is a table with three rows: 'Your version:' with value '2023 R1 M1', 'Latest version:' with value '2024 R2 M1', and 'Version available to you:' with value '2023 R3 M1'. Below the table is a section titled 'License file' with a text field containing 'Click to select a file'. At the bottom are two buttons: 'Apply' (dashed border) and 'Cancel' (solid blue).

LPR ID	Download
05981825	
Your version:	2023 R1 M1
Latest version:	2024 R2 M1
Version available to you:	2023 R3 M1

License file

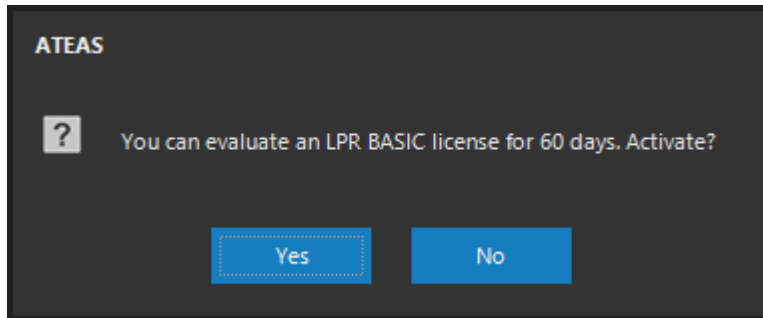
Click to select a file

Apply Cancel

In the upper text field, the ID of your hardware key is displayed, which you are going to need when extending your license. In the License file section, a single or double click opens a dialog for selecting a new license file.

The dialog shows some important version information including the highest version that can be used with this LPR ID without ordering upgrade.

If there is no hardware key in your system, you can activate the vehicle LP detection and recognition module for one camera for 60 days as BASIC version and start the evaluation period.

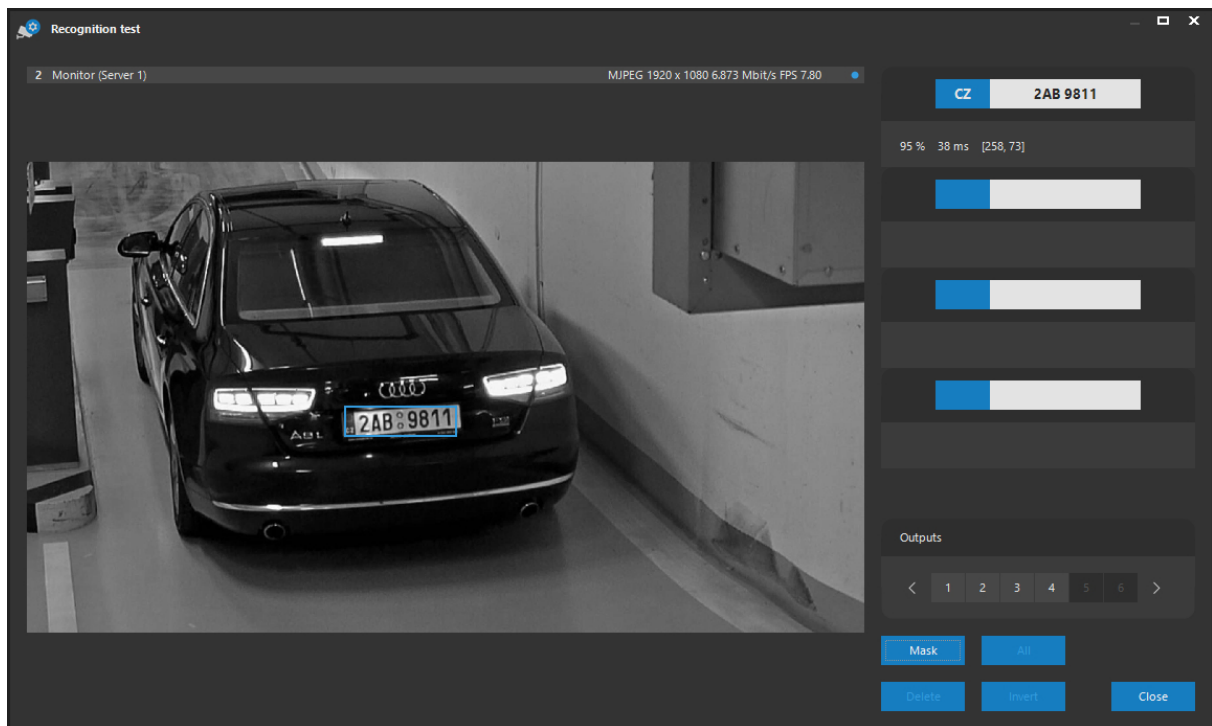


After the activation as a trial version, the expiration date will be displayed along with the license information. After the evaluation period expires, it will no longer be possible to reactivate the trial version on the given camera server.

NOTE

To activate the evaluation version of the module, it is necessary for the camera system client (not the server where the module is installed) to have a temporary internet connection

The **TEST** button opens the detection test window.



CAUTION

Results for the given camera are not sent to the server for further processing if the LP detection and recognition testing window is open. Events previously configured will not be generated for LP detections for the given camera while testing and fine-tuning the system.

For a single video stream, up to four LP can be published simultaneously including other attributes like direction etc. Apart from the recognized LP additional information is displayed as follows:

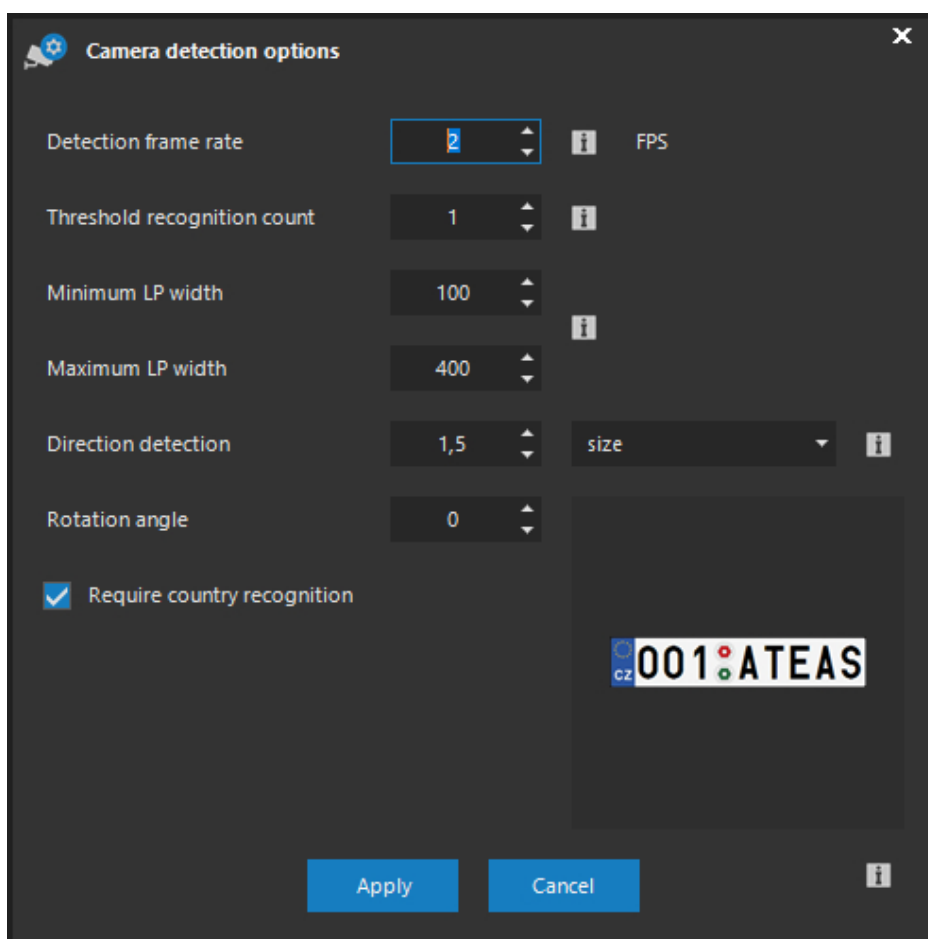
- Detection quality indicating the reliability of recognized LP with the maximum value of 1. Values below 0,9 may be evaluated as insufficiently reliable.
- Detected LP system (a state or another group).
- Detection time of a last LP in milliseconds.
- Direction of the LP (also indicated by an arrow nearby the LP), provided a higher recognition threshold count is used so that the direction can be calculated.
- The exact border of the rectangle highlighting recognized LP.

In this dialog, outputs can be activated in the same way as in the live window.

NOTE

You might find this useful for skipping files if this is a camera created from a folder containing video files.

Using the **OPTIONS** button, you can adjust the frame rate of LP recognition. Increasing the FPS leads to faster detection and recognition of the license plate (must be applied if the vehicle is in the view for only a short period of time). However, it also calls for higher server performance (especially when the LP is detected on several cameras simultaneously). The LPR frame rate can be adjusted for each camera individually.

**NOTE**

If the frame rate is set to zero, unlimited frame rate will be used.

NOTE

For other video formats than MJPEG, starting with a detection frame rate of 2 it will be necessary to decode the entire video stream. You can offload this work to supported GPUs by activating GPU usage on the server.

The threshold recognition count indicates the minimum number of recognizing the same license plate before creating an event in the system. By default, the count is set to one meaning an event will be created in the system after the first license plate recognition with the required reliability rate. If you increase this parameter, for example, to two, the server will create an event only after the license plate is successfully recognized, with the required level of reliability, in two different images.

TIP

The threshold parameter is crucial for achieving the maximum detection reliability and a good direction detection.

It is recommended to set a range for the LP in the image by setting the minimum and maximum LP width. In this way, useless background detections can be eliminated and the detection time is reduced. Recommended values are 30 percent below and above the expected LP width.

Depending on the scene, direction can be determined based either on the LP size or position.

If size is used, the Direction detection value indicates the minimum required relative change of the LP area for a successful direction detection (approaching or leaving). For the direction detection to be reliable, the detection frame rate, threshold and direction detection parameters must be configured properly so that successful detections are available throughout the entire focus range of the camera.

If position is used, the Direction detection value indicates the minimum shift expressed in pixels that must be detected in order for the plate to be assigned a direction.

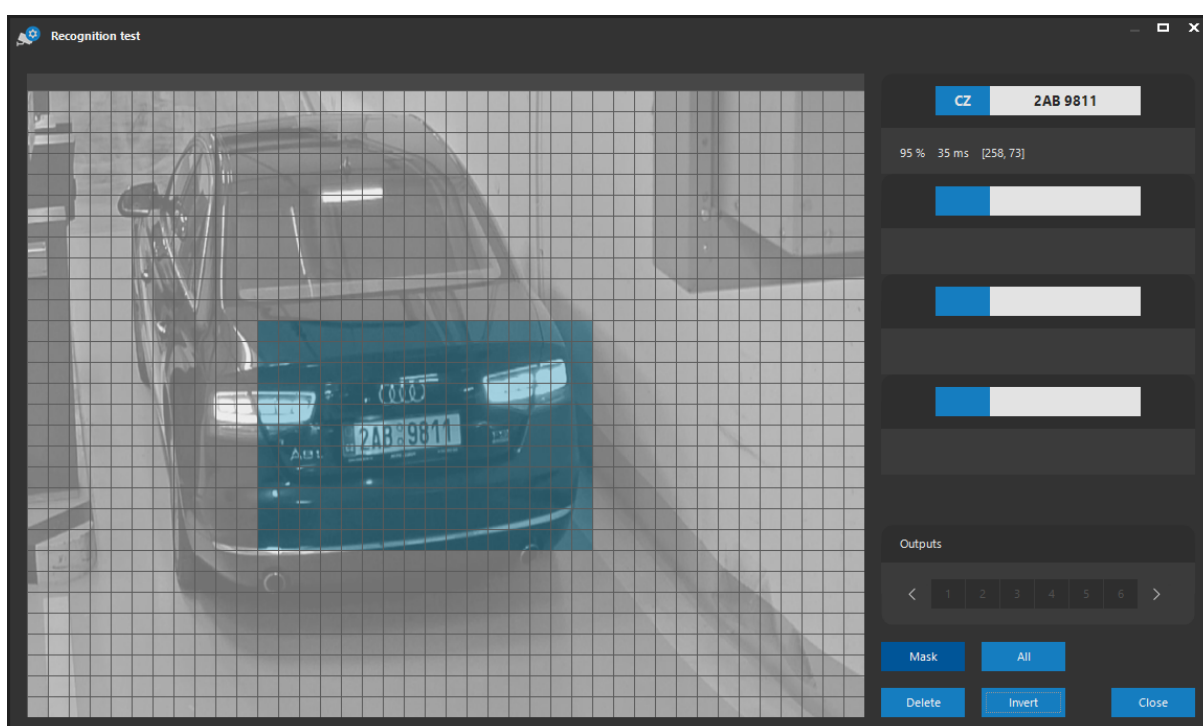
The rotation angle should correspond to the real rotation of the LP in the image so that the deviation does not exceed 15 degrees.

The Require country recognition option, if active, will prevent publishing a LP that could not be assigned to one of the selected countries.

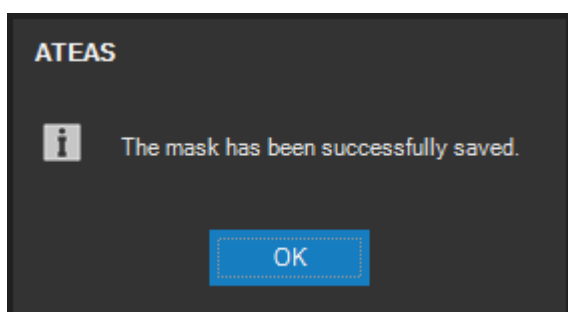
11.8.2. Mask configuration

The LP detection and recognition test window contains the **MASK** button, which can be used to identify the parts of the image that will be ignored or included in the detection of LP presence in the image.

When the button is pressed, the image will freeze and the mask currently configured will appear. Parts of the image that will be included in the detection or ignored can be added or removed using the mouse. The right mouse button is used to remove areas from the mask.



Any random mask can be created. A mask can consist of any given number of discontinuous areas of various shapes. A mask can be further edited using the **ALL**, **DELETE** and **INVERT** buttons, which will expand the mask to include the entire image, remove the entire mask, or invert the mask. The mask is saved by releasing the **MASK** button, saving and applying the mask is confirmed with a message.



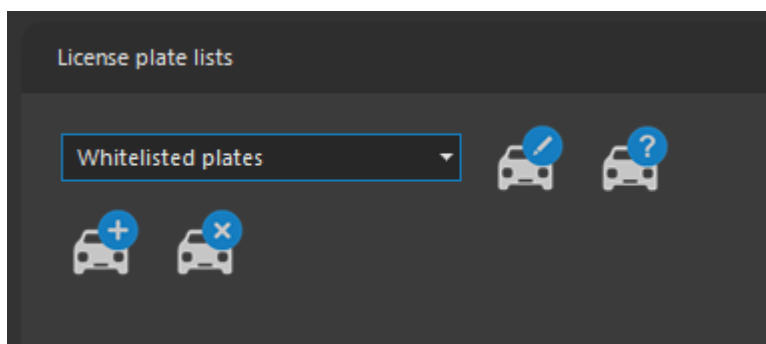
In real world installations, we can flexibly respond to traffic changes at the point of installation, to vehicles appearing in parts of the image where detection shall be ignored, or to new objects in the image interfering with the detection or leading to performance degradation.

NOTE

Configuring the mask at the detection level can be a better solution than configuring the mask at camera level, for the masked areas remain part of the camera recordings.

11.8.3. Working with LP lists

In order to extend event control possibilities, you can file LP lists in the system. These lists allow the system to react to LPs included only in a certain list accordingly. You can, for example, invoke an alarm only when a recognized LP is on a list of black listed LPs, or automatically release the gate for vehicles whose LPs are registered in the LP white list. Other responses can be assigned to LPs listed in user-defined lists.

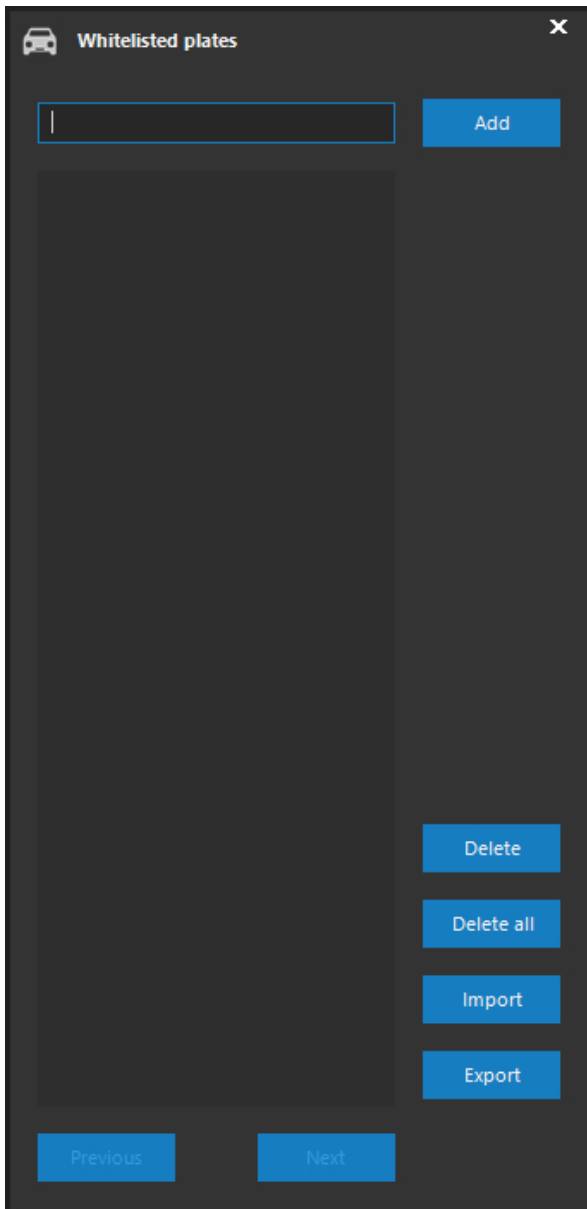


Using the Add and Remove list buttons, new lists can be added or deleted. There is no real limit to the number of lists. System lists like Whitelisted plates and others cannot be removed.

TIP

User defined LP event sources come with the option to select any arbitrary new list.

You can open the selected list with the Edit list button located next to the selected list. The list can be edited in the following window.

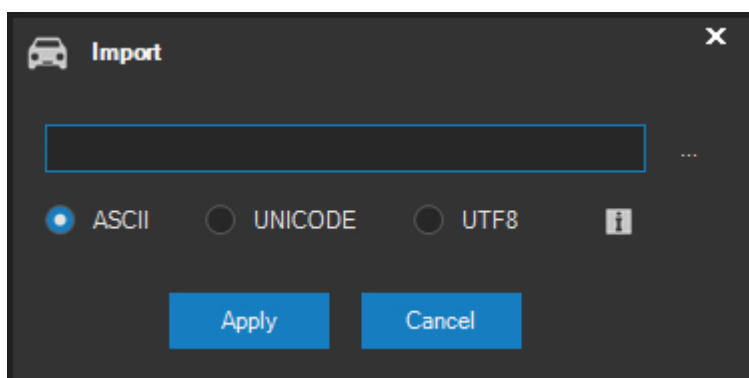


A new LP is added by entering its number to the text field under the list and pressing the ENTER key. The same function is assigned to the **ADD** button. The list is automatically updated after saving. Any selected LP can be deleted from the list by pressing the **DELETE** button. A whole list can be deleted by pressing the **DELETE ALL** button (requires confirmation).

NOTE

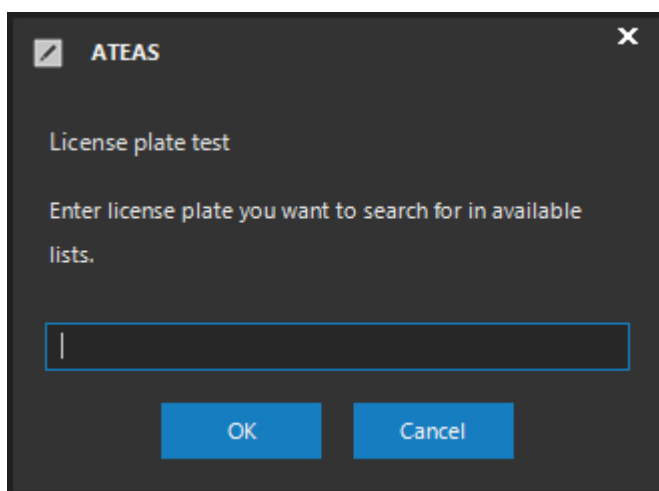
LPs can be entered in both the decorative and normalized form, i.e. with spaces or dashes but also without them.

If a greater amount of LPs is required, you can use the **IMPORT** button instead of adding LPs manually. You can search a file containing the list of LPs and set the text encoding used within the document. The file must be organized so that each row contains a single LP. The line separator can assume the style of either Windows OS (CR + LF) or Linux OS (LF). Therefore, you can transmit large lists of LPs from various database systems using the text plain format.



The **EXPORT** button creates a text file which will contain a list of LPs, currently being modified.

The **TEST** button verifies a particular LP and checks if it is already included in any of the LP lists.



11.8.4. LP recognition settings

LPR setup is performed in the bottom part of the window. LP systems used for the LP recognition are configured using the two lists. Any selected LP system can be added to the list of currently used LP systems using the arrow button between lists. In the list of selected LP systems (states), you can also change the order or delete selected items.

NOTE

National LP systems can contain other subsystems such as various forms of LP types in a particular state etc.



The following rules and recommendations apply for creating a list:

- A list has to include at least one item.
- Adding a particular LP system (a particular state) is not a requirement for proper detection and recognition, however, it is better to specify the state to ensure higher reliability thanks to the ATEAS LPR Engine capability of checking grammar.
- To achieve the highest performance, try to sort the list from most frequently registered LPs.
- Adding more items to the list can increase the probability of correctly recognizing license plates with a rare appearance, however, this comes at the cost of possibly more frequent confusion errors for countries with similar plates.
- Activating systems, for which the share of the total reaching at least half of a percent cannot be expected, is not recommended.

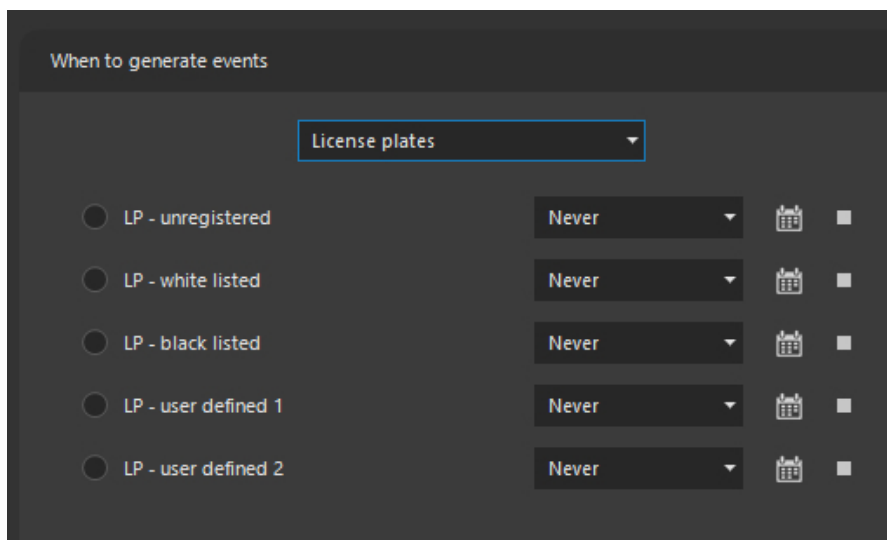
Besides specifying an LP system, you can also adjust other parameters with the following purpose:

Threshold recognition quality: Specifies the minimum level of detection quality (reliability) that must be achieved in order to make the LPR engine send the LP to the system (for an event, alarm or a direct forwarding to the client). The level of quality can be set from 700 – 999. The higher the recognition quality threshold is, the lower the error rate. At the same time, however, the ratio of recognized LP decreases because some of the correctly recognized LP will not be published because the quality threshold is not achieved. The default value is 900.

11.8.5. Event management

Monitoring detected vehicle LPs (described above) together with other parameters makes it possible for administrators to verify LP recognition reliability under particular circumstances. However, you must configure the events administration section if individual LPs are expected to lead to events and alarms.

As soon as a specific camera is added to the list of cameras used for LP recognition, new event sources become available in the events administration section under the following group: License plates – LP – unregistered, LP white listed, LP black listed, LP user defined 1, LP user defined 2. Managing these event sources (time mapping, creating event scenarios) is absolutely consistent with other sources (motion detection, alarm inputs etc.).



When to generate events

License plates

☐ LP - unregistered	Never		☐
☐ LP - white listed	Never		☐
☐ LP - black listed	Never		☐
☐ LP - user defined 1	Never		☐
☐ LP - user defined 2	Never		☐

By using this division, you can define different event scenarios for situations when the recognized LP is either white listed, black listed or not registered in any of the lists. Therefore, it is very easy to configure the following example behavior:

- A tollgate blocking the entrance to the property will be automatically opened for white listed LPs (input activation).
- A camera will invoke an alarm if a black listed vehicle is detected (for example stolen).
- Users can monitor vehicles and verify their LPs through the use of a PTZ device. In the events row (or by different sound notifications used for events and alarms), you can, for example, check stolen vehicles online.

TIP

Events can be bound to a specific LP direction, if detected.

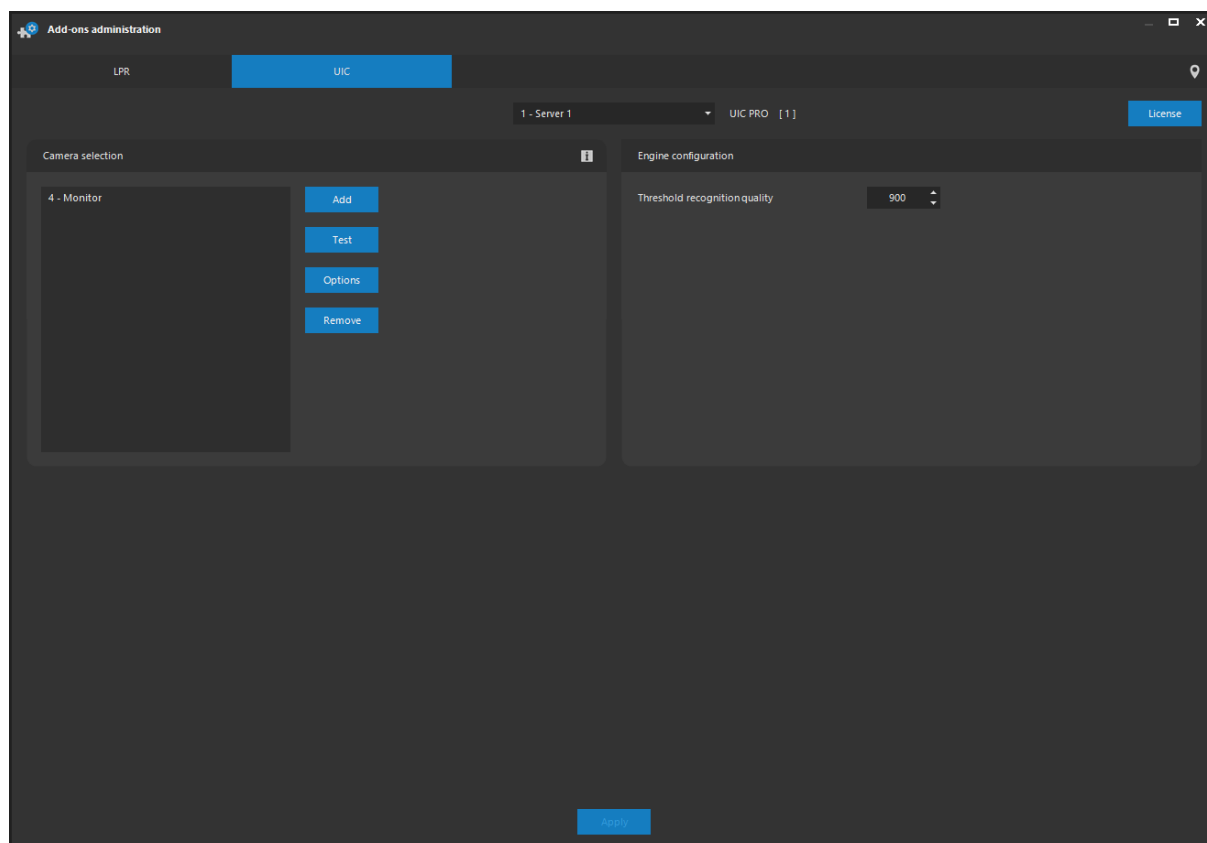
Recognized LPs are stored in the metadata database and the user can search for a particular LP. When browsing records displayed in the Media search section, all events and alarms including events and alarms invoked by LPR are displayed for individual video segments. These events and alarms can be searched online and the specific sequence can be downloaded. However, if you wish to search the

record for a particular LP, this event and time oriented search is not the considered the most efficient method. A meta search tab is available in the window. On this tab, you can perform searches for the selected metadata group (not according to time as is the case for Media search), i.e. for example accordingly to LPs. For further information related to this topic, see the chapter on searching for a record.

11.9. UIC engine administration

11.9.1. Selecting cameras for detection

The UIC engine administration is available in the add-ons administration section under the UIC tab. Prior to that, the UIC engine must be installed and active using a corresponding hardware key. Some principles are similar to the LPR engine.

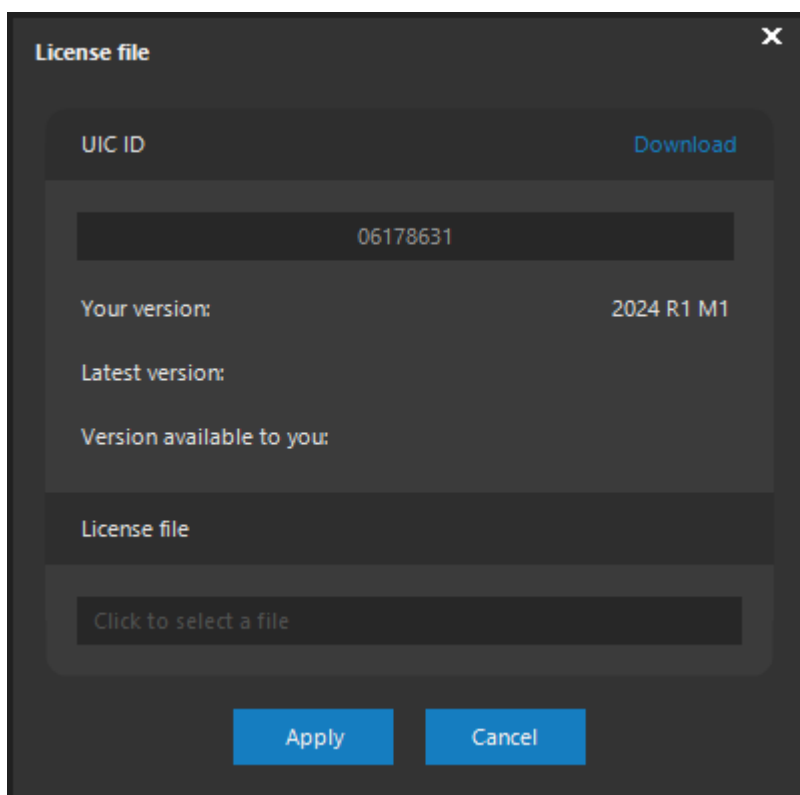


Using the **ADD** button, you can display a list of all available cameras on the camera server. Any camera from the list can be selected and added to the list of devices used for LP recognition by pressing the **APPLY** button. A single camera server can run the detection for up to 64 cameras simultaneously. To delete a camera from this list, press the **REMOVE** button.

NOTE

The current device license for UIC detection and recognition is displayed next to the currently selected camera server.

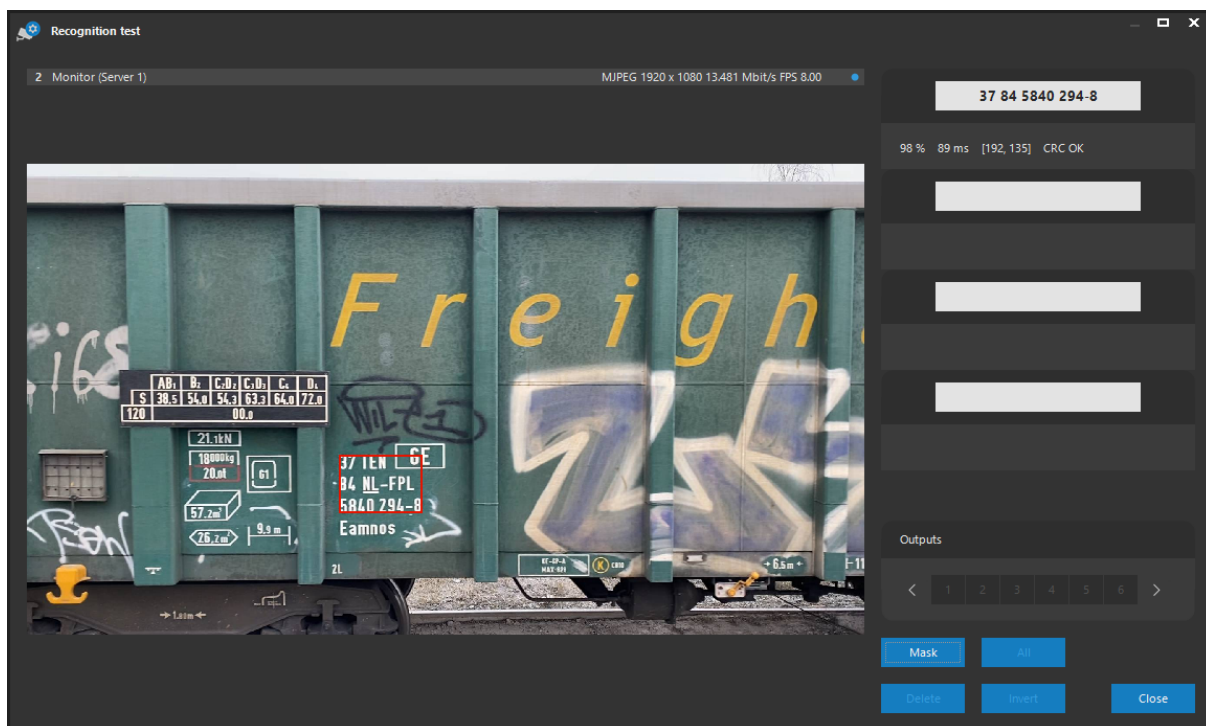
When extending the UIC engine license (upgrade to a higher edition or increasing the number of cameras) use the **LICENSE** button to display a dialog where you can upload a new license to the selected camera server.



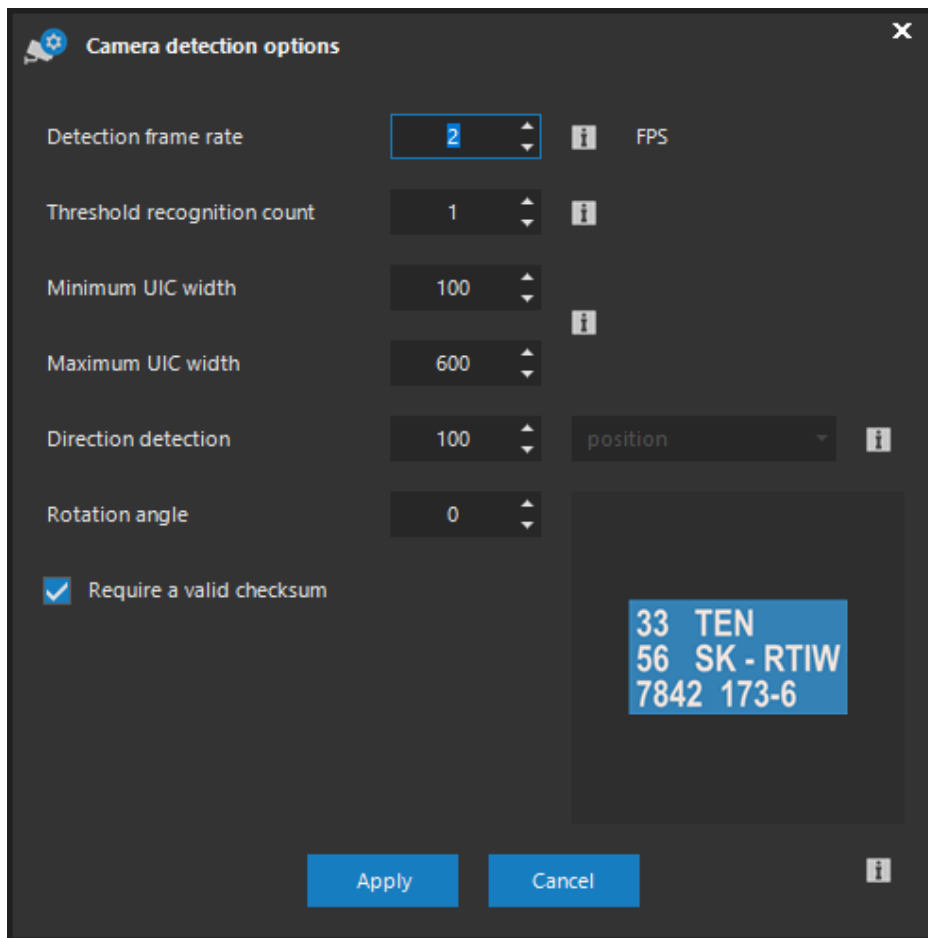
In the upper text field, the ID of your hardware key is displayed, which you are going to need when extending your license. In the License file section, a single or double click opens a dialog for selecting a new license file.

The dialog shows some important version information including the highest version that can be used with this UIC ID without ordering upgrade.

The **TEST** button opens the detection test window.



Displayed details are basically the same as for LP with the exception of the Checksum validity. This holds even for configuring a mask with the **MASK** button or configuring the detection using **OPTIONS**.



In the case of UIC detection, a higher default maximum width is used and the direction detection refers to a pixel shift to the right or left.

For UIC, specifically, the Require a valid checksum option can be used to decide whether a detection without a valid checksum should be published calculated based on the Luhn formula. If not enforced and the detection does not pass the checksum test, the event text and API will contain this information.

11.9.2. Event management

UIC detection has no predefined event sources in the system. Therefore, it is necessary to create a custom event with the UIC code name and add the corresponding time schedules.

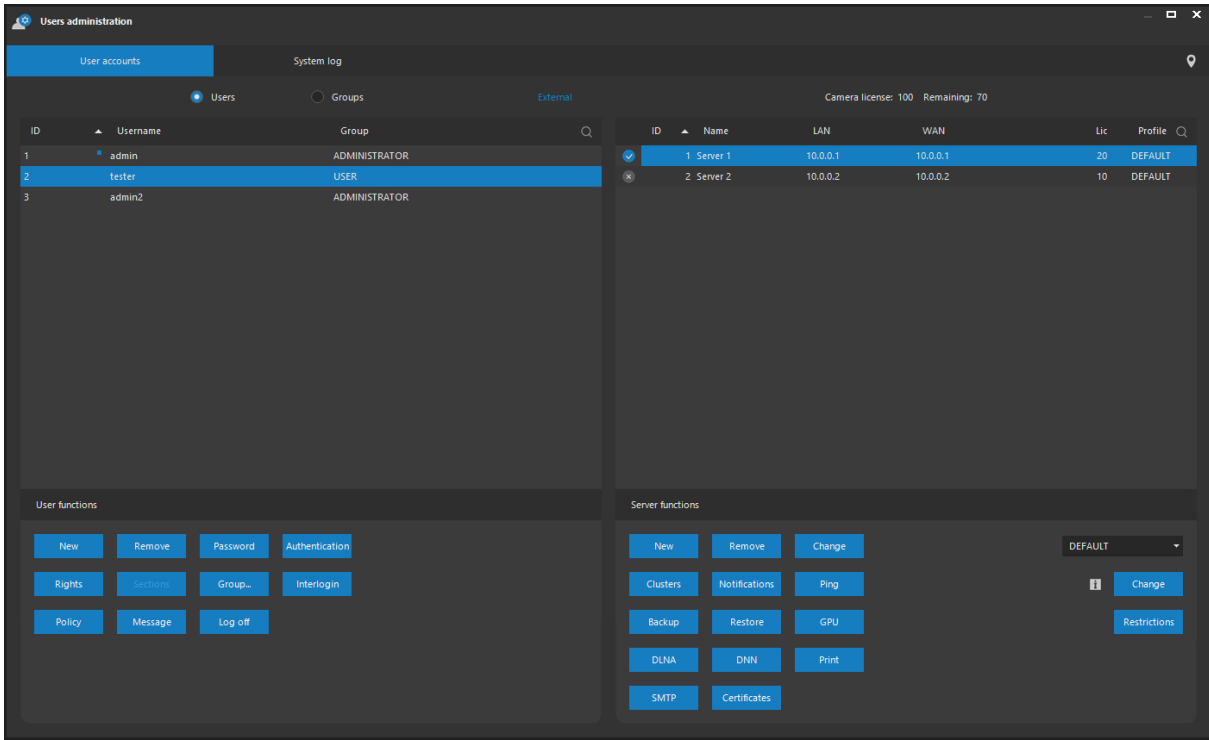
TIP

Events can be bound to a specific UIC direction, if detected.

11.10. Server and user management

11.10.1. Basic server management

Server and user management is performed in the Users administration section. HOME and PROFESSIONAL editions enable adding one camera server at most, in most cases located on the same computer or server as the administration server. The UNLIMITED edition enables to add any amount of camera servers.



The screenshot displays the 'Users administration' window. It features a sidebar with 'User accounts' and 'System log' tabs. The main area is divided into two sections: 'Users' and 'External'. The 'Users' section shows a table of user accounts:

ID	Username	Group
1	admin	ADMINISTRATOR
2	tester	USER
3	admin2	ADMINISTRATOR

The 'External' section shows a table of camera servers:

ID	Name	LAN	WAN	Lic	Profile
1	Server 1	10.0.0.1	10.0.0.1	20	DEFAULT
2	Server 2	10.0.0.2	10.0.0.2	10	DEFAULT

Below the tables are 'User functions' and 'Server functions' buttons. The 'User functions' include: New, Remove, Password, Authentication, Rights, Sessions, Group..., Interlogin, Policy, Message, and Log off. The 'Server functions' include: New, Remove, Change, Clusters, Notifications, Ping, Backup, Restore, GPU, DLNA, DNN, Print, SMTP, and Certificates. A 'Camera license' status is shown at the top right: 100 / Remaining: 70.

System camera servers are included in the list within the Server summary section. Each server is provided with information about its unique ID, name, LAN and WAN IP addresses, number of currently assigned cameras and (if a user is selected simultaneously) a profile for the user assigned to this server. The symbol at the beginning of a camera server row indicates if a server is currently online or offline. Restoring server states within the list is automatic.

NOTE

The client application itself automatically refreshes connections to all servers in case connection has been lost. Therefore, if a server is momentarily offline, it will be automatically connected when it becomes available. The disconnection from and connection to the camera server is also automatically displayed to users in the live window on the events tab.

CAUTION

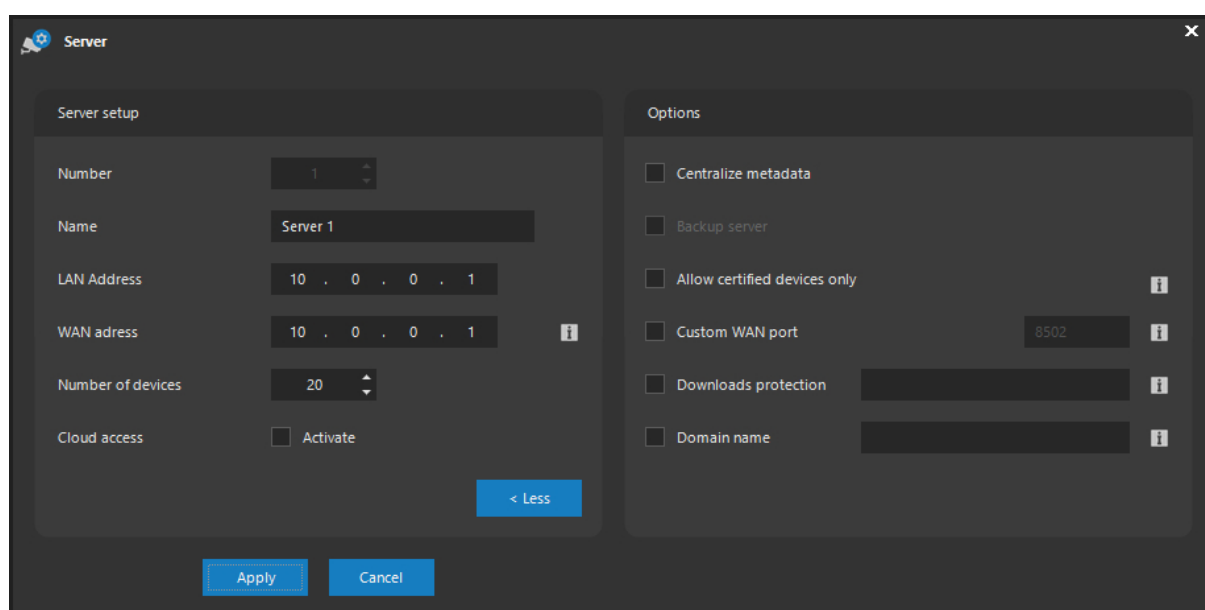
The client application cannot restore connection to the administration server (indicated in the bottom part of the window containing the application main menu). If the online connection symbol turns to offline, you must restart the application and authenticate yourself again.

NOTE

Above the server list you will find a summary of the total number of camera licenses and the number of remaining available licenses, which can be used for the existing or new camera servers.

Adding and removing camera servers

A new camera server can be added to the system by pressing the **NEW** button in the Server functions section. A dialog will appear, requesting the server name, its LAN and WAN addresses (see below) and a maximum number of cameras operating on the server. Assigning a higher amount of cameras than entered will not be possible. This value must correspond with the total number of cameras you are allowed to use in the system based on your license number. The licensed number of cameras cannot be exceeded by a sum of all cameras assigned to individual servers. A warning message will be displayed if this rule is violated.



When this dialog opens, the application proposes the first available identification number for new server to be added. UNLIMITED edition has the option of changing this number to a random value, and therefore group newly added servers in suitable fashion. The highest identification number possible for a server is 999, which is also the limit for the total number of servers in the system.

NOTE

The server identification number can only be changed in UNLIMITED edition. All other editions allow adding only one camera server with identification number 1.

LAN and WAN addresses have to be set with respect to network configuration and client connections. In order for the camera server to successfully identify itself to the administration server, it must connect from addresses entered in this dialog, otherwise the camera server is not identified within the system and cannot begin operation.

The LAN address shall always be entered, for it is the primary server identification for user connection. The WAN address is used only for users with REMOTE profiles, who can access the given server outside their local area network.

NOTE

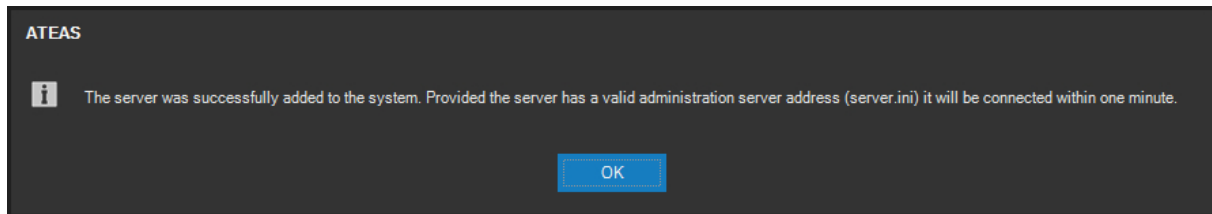
Entering the WAN address in HOME and PROFESSIONAL edition is not necessary. If a user with a REMOTE profile accesses the system remotely, the WAN address of the camera server is that of the administration server to which the user logs into. This way, the configuration of dynamically assigned public addresses is supported by default, because the user can access the server even by entering its name.

Therefore, the WAN address is only necessary to be entered with the ULIMITED product version, only if users with REMOTE profiles intend to access the system remotely.

NOTE

Setting the LAN and WAN addresses is not related to the number of network interfaces (cards) in the computer or server. For more information, see the system installation chapter, which describes the case of having multiple network cards in the computer.

The following message will be displayed when the server is successfully added to the system.



If an added camera server has already been successfully installed, the identification process of this server towards the administration server (ATEAS Administrator) will be executed. This will enable clients to connect to the camera server. Camera server connection to the system and to the client should be confirmed within seconds automatically. If the camera server is not connected to the administration system core, you will not be able to access it, assign cameras etc.

Any camera server can be removed by pressing the **REMOVE** button. This action has to be confirmed by pressing the **YES** button. The successful removal will be confirmed by a message dialog.

The dialog shown when adding a new or changing an existing camera server contains alternating buttons **MORE** and **LESS**, used to display or hide additional server options.

Central metadata storage

Metadata is descriptive data that provides additional information for stored camera video and audio data. For example, this data may include motion detection data, activation of alarm inputs, camera events together with any particular additional data or vehicle license plates. The metadata is obtained by individual camera servers within the system and therefore requires selecting the relevant camera server when performing metadata searches.

Should you need to search for specific metadata across all servers (e.g. when having many camera serves), you can activate the Centralize metadata option. Then all metadata of the selected server will be uploaded and stored on the system administration server.

Backup servers

Servers can be created to serve as backup servers. Backup servers are special servers only useful in cluster mode. For more information, please see the cluster documentation.

NOTE

This option cannot be changed after the server has been created.

Backup servers are not available for direct administration with some exceptions like e.g. media stores, which shall be configured for the backup servers. However, even with media stores configured, additional options such as assigning cameras to stores or metadata age setting are not available. These items are inherited during the cluster backup sequence. Another exception is the basic configuration of LP detection and recognition (excluding the camera options).

Device certification

By using the Allow certified devices only option, you can activate the certificate verification of all devices connected over https protocol. For the device to be able to enter the system, it must prove its identity with a certificate cryptographically derived from the certificates an administrator uploaded to the server (with other words, the same or a higher-level certificate must be found).

TIP

Therefore, it is recommended to provide root certificates of camera manufacturers.

CAUTION

Higher-level certificates and especially any root certificates must also be imported on operating system level.

Using custom camera server WAN ports

The camera server operates on the ports defined in the appendix to the product documentation about the network configuration. However, provided a situation occurs where two or more camera servers are to be accessible via the same WAN address, the default network ports used by the camera server must be changed. Upon activating the Custom WAN port checkbox, a new value can be entered for the default network port.

NOTE

This port must not be occupied by another application.

NOTE

The port is always used only in combination with the WAN address of the server, i.e. for users with the REMOTE profile for the given server.

NOTE

Together with the default camera server communication port, other camera server ports are also shifted by the same value compared to the default value (see appendix about the network configuration).

The administration server identifies camera servers according to their IP addresses. If, however, there are two or more servers connecting to the administration server via its WAN address (e.g. two camera servers in one local network of a large enterprise system connect via WAN to headquarters to the administration server), in order for the administration server to distinguish them and assign them proper identification, the FORCEDSERVERID key must be entered into the server.ini file of these camera servers, where the numerical server identification is directly recorded.

Downloads protection

By default, users who have been assigned the download recordings option can obtain ATS files without any password protection and may further export them. If we need users to keep the possibility to download recordings but, at the same time, want to restrict them in using these downloads, we can specify a password using the Downloads protection option for a camera server to be automatically applied for all downloads.

If such a password is set, a user must be assigned an additional permission to export data outside the system in order to obtain plain media files.

Changing a server and a division of licensed amount of cameras

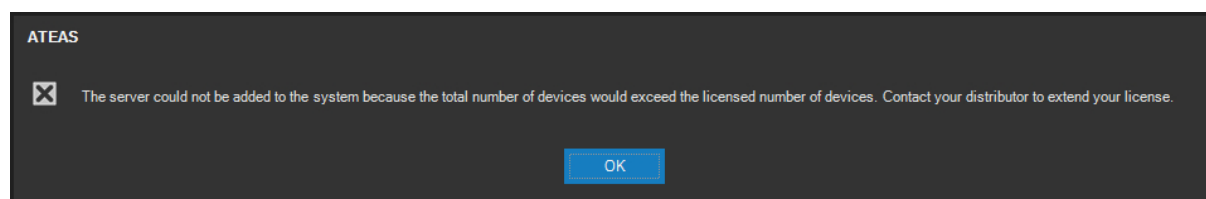
The total amount of cameras which can be included in the system, according to the license number, can be divided amongst individual camera servers in the system. This division is insignificant for the HOME or PROFESSIONAL edition, because all cameras are assigned to a single camera server. However, you can divide the licensed amount of cameras amongst individual camera servers when using the UNLIMITED edition. Therefore, if the maximum amount of cameras is limited to 40, the system can hold two camera servers with 30 and 10 cameras, 10 servers with 4 cameras etc. The maximum number of connectable cameras can be modified by pressing the **CHANGE** button. The amount of cameras can be changed in the displayed dialog. Besides changing the number of cameras assigned to a specified server, you can also change server names and both IP addresses (both LAN and WAN).

CAUTION

The amount of cameras connected to the server should be reduced so their final amount will be equal (or lower) to the maximum limit. Otherwise video distribution from cameras can be blocked after a certain period of time (not instantly).

If the previous request is not satisfied, the application will highlight the values in the column containing the number of cameras as a warning. The administrator must subsequently resolve this issue, otherwise the camera server may start limiting its functions.

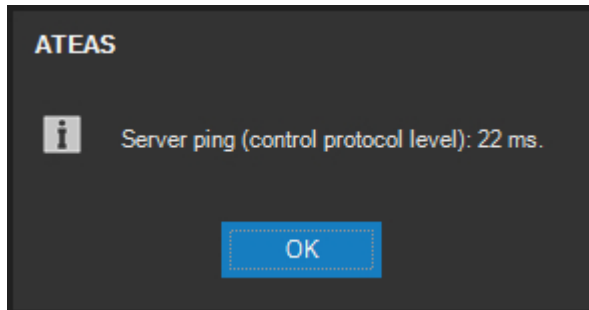
Keep in mind that the total amount of cameras must not exceed the licensed amount of devices. Otherwise, a warning message will be displayed.



NOTE

When changing a camera server, the identification number (ID column) of this server cannot be changed.

The current server ping can be tested by pressing the **PING** button. This latency is on the control protocol level. Therefore, it cannot be compared with values obtained using, for example, the PING command etc. The application ping will be displayed in a dialog.



11.10.2. Camera server connection in cloud mode

The ATEAS platform supports a special cloud mode for connecting camera servers to the system. If this mode is enabled for the camera system, the camera server can be deployed in any location with internet access, allowing for immediate full access to the server including video, audio and all other functions.

NOTE

This applies even when the server is part of a local network, without a public address, without port redirection (NAT), with enabled firewall, and copes with dynamic address changes and similar.

The fundamental advantage of cloud mode connection is the absolute independence from having to configure the network in which the camera server runs. The only precondition is the availability of the administration server.

NOTE

In order to work, this mode may require updates to the network settings within the environment in which the administration server runs, specifically opening the port used by the cloud mode. These ports are listed in the network configuration appendix document.

Connecting to a camera server in cloud mode is very easy to achieve:

- In the camera server dialog, check the Activate option for Cloud access.
- The WAN address item is automatically updated to the WAN key and a unique key for the given camera server will be generated in the relevant text field.
- The generated key must be used in the server.ini configuration file of the camera server service (WANKEY key), followed by a restart of the camera server service.

NOTE

Some camera server settings are not available or effective in cloud mode, such as LAN address input, availability for offline users or custom WAN port input.

NOTE

In cloud mode, clients of the camera system always use the administration server service to access camera server data. Streams, therefore, do not necessarily have to respect the optimal route.

11.10.3. Using a domain name for camera server

A domain name can be added to the server when creating a new or updating an existing server. The domain name will be used, for example, when accessing servers from the web client for the purpose of simplifying the deployment of certificates in an UNLIMITED edition for https access. The following applies within the ATEAS system:

- Independent from the configured WAN address of the camera server, the address entered during the authentication process is used for accessing the camera server for a REMOTE profile user in editions with one server. This automatically ensures support for dynamic DNS names of your camera system.
- The client connects to both the administration and camera servers when accessing from the web client. Https access requires certificates to be installed on all system servers.
- This means that for editions other than UNLIMITED, you can use the same certificate for an IP address or domain name installed for both server services without having to enter it anywhere.
- This means that for editions other than UNLIMITED, you can use the same certificate for an IP address or domain name installed for both server services without having to enter the domain name anywhere.
- The previous point can be bypassed by activating the cloud mode, which only requires the same certificate to be installed on the administration server and all camera servers in the

system. Nevertheless, in this case all data will flow through the administration server of the system.

- The above implies that entering the domain name for a camera server is only required in the case of UNLIMITED edition, when you are not using cloud mode, when you would like to use the web client over https and have certificates issued for the domain name.

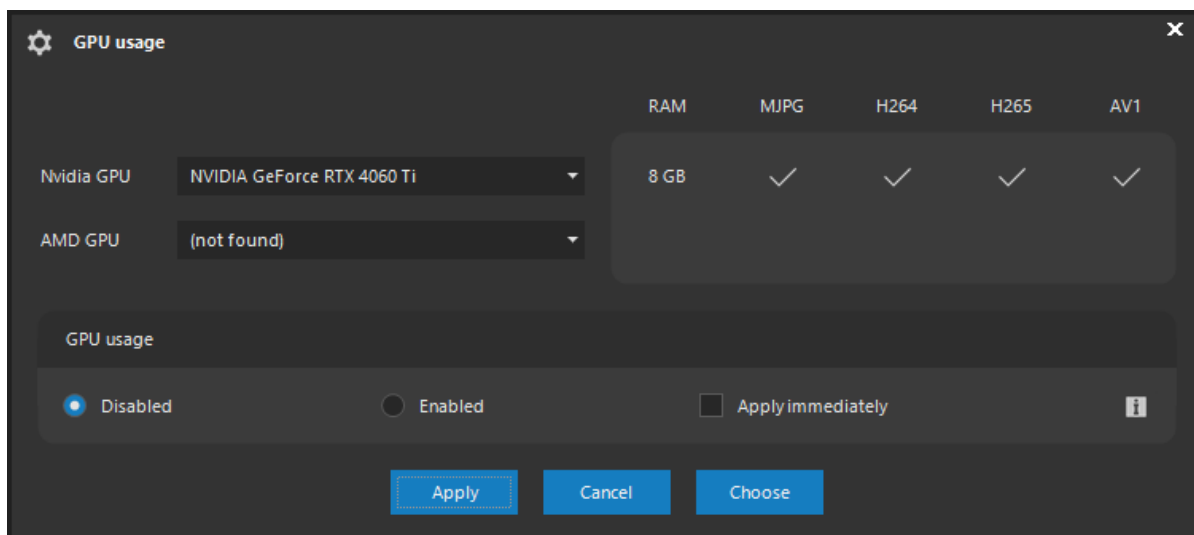
11.10.4. GPU acceleration in the server service

ATEAS Server, similar to the client application, can utilize GPU acceleration for increasing the performance of certain operations. In particular, this includes video decoding of all video formats or color space conversions which has great impacts on the performance e.g. of server based motion detection, LP detection or video analytics.

NOTE

Unlike the client application, Intel GPU graphic processors cannot be used for acceleration on the server side.

GPU usage can be configured by pressing the **GPU** button under the list of servers.

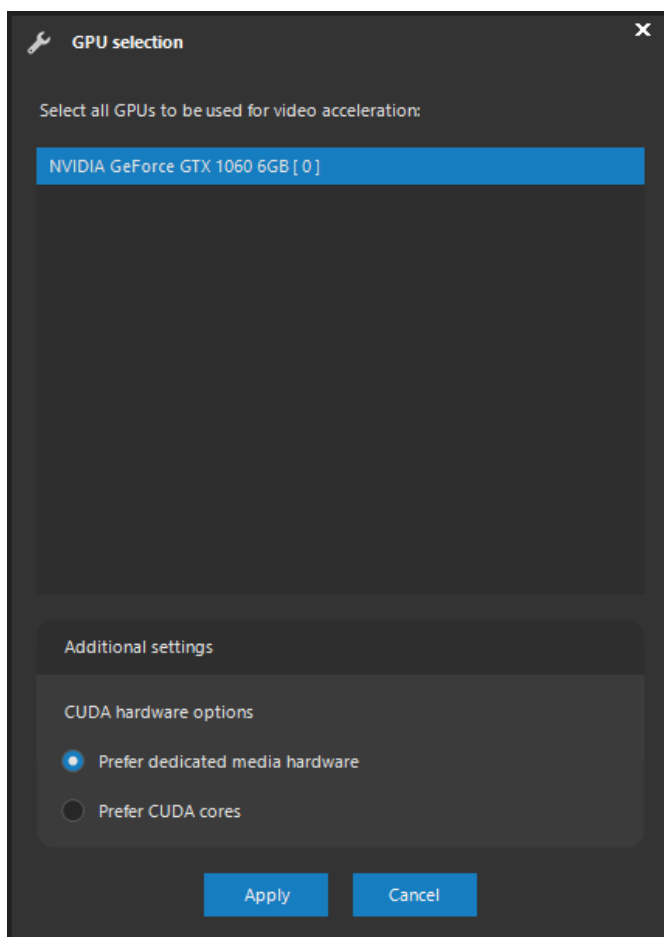


The GPU acceleration setting can be immediately enforced by checking the Apply immediately option. In this case, all cameras on the server will be disconnected and reconnected as it would happen after a configuration change.

The **CHOOSE** button displays a dialog with the list of all graphic cards. One or more graphic cards to be used for video acceleration must be selected from the list. In order to achieve maximum performance, the server is capable of utilizing various GPU acceleration technologies, as well as multiple GPUs, even within a single application.

NOTE

With respect to CUDA, the user can also specify certain hardware preferences. In particular, it can be specified whether CUDA cores will be used for acceleration, or whether dedicated media decoding hardware will be used.



NOTE

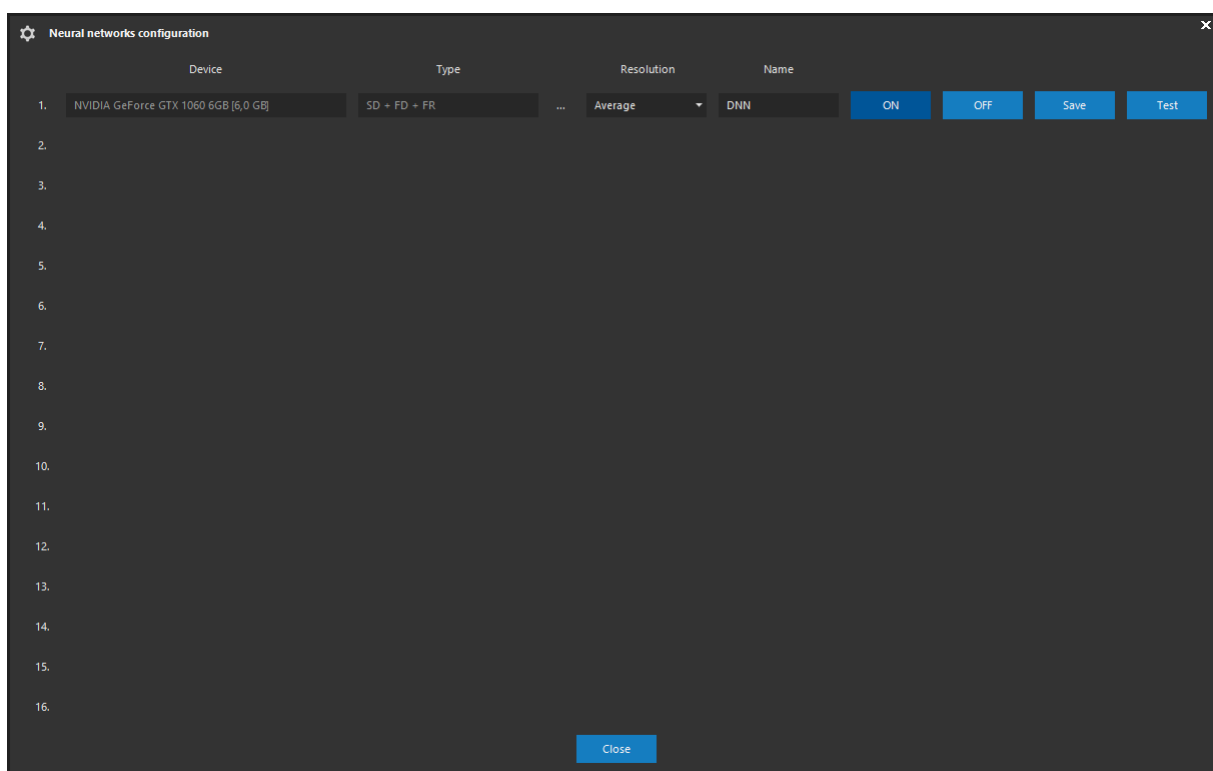
If, at the same time, a neural network is running on a GPU, the GPU acceleration for the cameras assigned to this network will be performed on that GPU irrespective of your selection here. This is necessary to optimize the data flow through the buses.

11.10.5. Starting a neural network on the server

The camera server supports starting a neural network, provided it features the hardware required to do so. ATEAS uses various types of deep convolutional neural networks suitable for video analysis. To configure a neural network, press **DNN**.

NOTE

Using neural networks is available starting with the ATEAS Security PROFESSIONAL edition.



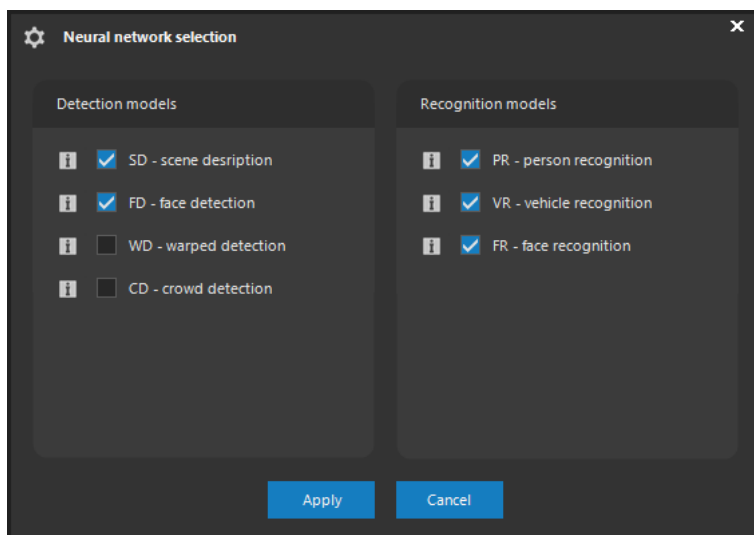
The neural network configuration is divided into the following columns:

Device – Indicates the name of the device recognized on the server and capable of running a neural network.

NOTE

A neural network can run on any Nvidia GPU with Pascal architecture or higher and a minimum graphic memory of 4 GB. Volta and higher architectures, which feature tensor cores, provide more performance that ATEAS can use.

Type – Here you can select one or more types of the neural network. Selection can be performed in the Network type selection dialog.



The detection models include:

- Scene description. This network is trained for classification of eight types of objects (person, car, truck, bus, bicycle, motorcycle, train, boat) with the ability to detect these objects in zones, crossing lines, determining counts, zone stay times etc.
- Face detection. This network is trained for detecting faces enabling all the features of the Scene description network.
- Warped detection: The network is trained for detecting people in 360 degree video (fish-eye cameras).
- Crowd detection: The network is trained to accurately estimate the size of crowds. A crowd is defined as a group of people where it is no longer possible for the scene description network to distinguish individual people from each other.

The recognition models include:

- Person recognition: This network is trained for recognizing persons from different cameras, angles and sizes.
- Vehicle recognition: This network is trained for recognizing vehicles from different cameras, angles and sizes.
- Face recognition. This network is trained for recognizing faces possibly assigning them names according to face database.

The Face recognition network depends on the Face detection network; therefore, recognition is not possible without detection. However, it's ok the other way round. Similarly, the Person or Vehicle recognition networks are connected to the Scene detection results and cannot be run as stand-alone networks.

The same goes for the Person or Vehicle recognition network using the results of the Scene detection network.

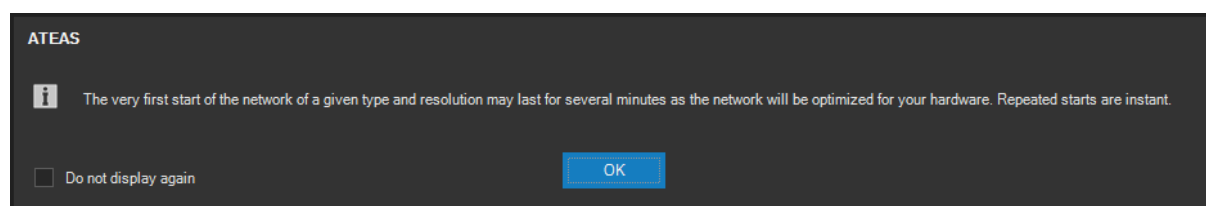
For successful face recognition, a face with its width and height greater than 100 pixels is expected. The network can easily handle face rotations around the z-axis, rotations around the y and x axis, however, reduce the number of recognition markers and reduce the overall recognition reliability.

Resolution – A sufficient number of pixels per object is especially important for detecting smaller objects. Based on the specific scene and other requirements, you can choose from three predefined normalized resolution options for the neural network.

Name – Specifies the name of the network that can be found under the analysis configuration.

Buttons – The **ON** and **OFF** buttons are used to indicate whether a neural network is running or stopped. Pressing the **SAVE** button saves all changes including whether the network should be started or stopped.

Starting a neural network of a given depth and resolution for the very first time on each GPU involves an optimization step compiling the network into an optimized image according to the specifics of the GPU which increases the detection speed afterwards. The very first start may last for several minutes.



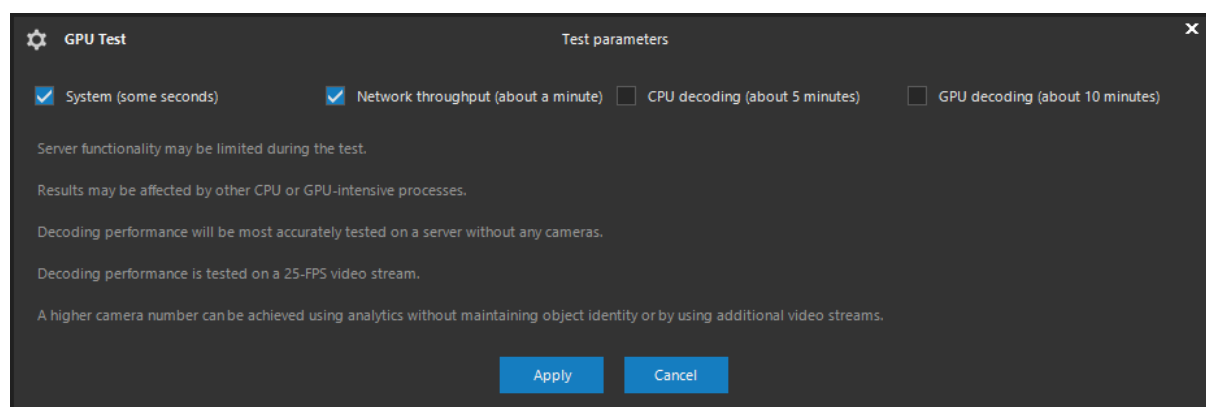
Subsequent starts of the network using an already compiled configuration on a GPU, which has already been used for the network, are instant.

Using the **TEST** button an AI performance test can be initiated for the current GPU.

CAUTION

During the tests, the configured neural network functions may be limited.

Before starting the tests, you can select the type of tests to be performed.

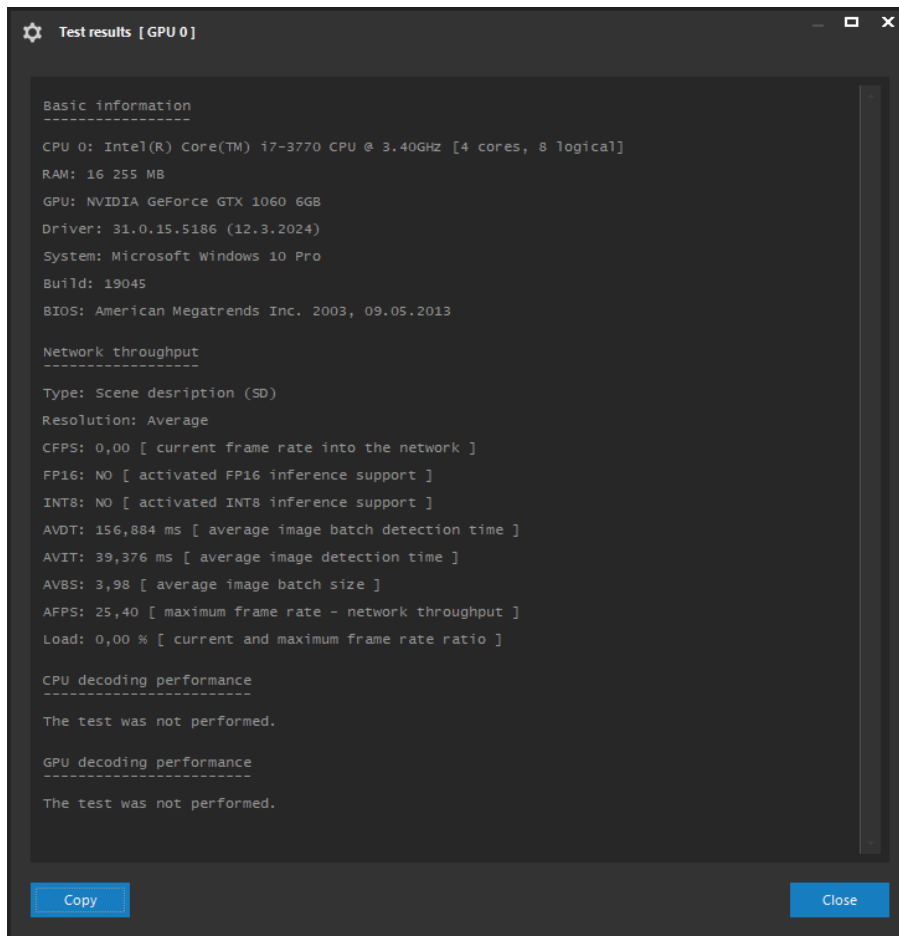


The system test will return basic information about your operating system, hardware configuration including e.g. the GPU driver version or BIOS version.

The network throughput test measures the current and maximum neural network throughput. To perform this type of test, a single independent network (e.g. SD or FD) must be selected optionally with a dependent network (PR or FR).

The CPU or GPU decoding tests perform decoding tests for all major video formats to give you the complete idea of what your configuration may look like.

A possible test result is shown here.



11.10.6. Cluster administration

Using clusters, you can ensure redundancy in the system in the case a server, which is part of a cluster, fails.

A backup server should always be part of a cluster. If any of the other remaining servers experience downtime, the backup server will fully take over all functions of the original server, including event management and neural networks. You can add up to one backup server to one cluster.

CAUTION

In order for the users to have access to cameras even after the camera server failure, you must have a profile created on the servers that are part of the cluster.

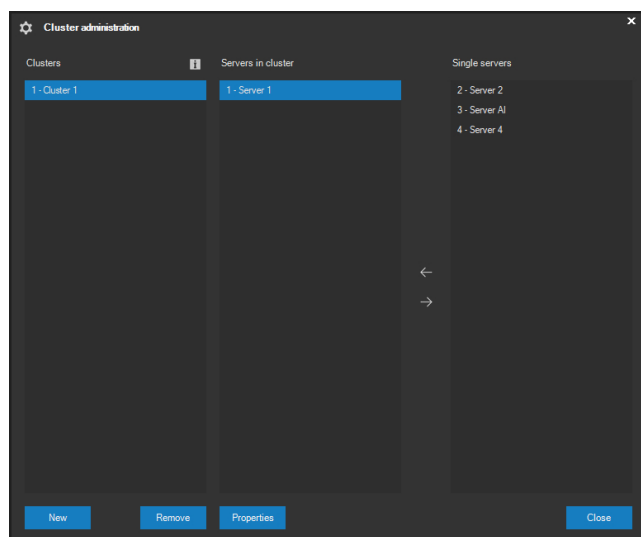
NOTE

Each cluster is capable of coping with a maximum of one server failure per cluster. If a second server that is part of the same cluster fails, its functions will not be backed up. However, individual servers can malfunction gradually and if they do not fail at the same time, the server that fails will always be backed up.

Clusters are managed by the system administration server. In the event that the administration server itself experiences downtime, camera server functions are preserved (with the exception of event scenarios that extend one server). Offline login and online availability of camera servers is also available in the event of such downtime. The administration server can be backed up, for example, using operating system tools, by installing in a virtual environment etc.

Creating a cluster

Providing you have purchased the UNLIMITED edition, you can create and edit clusters by pressing the **CLUSTERS** button.



Three lists make up the main part of the window. All currently created clusters are available in the left list. The middle list contains camera servers pertaining to the currently selected cluster in the left list. Finally, the right list contains camera servers, which are not currently part of any cluster.

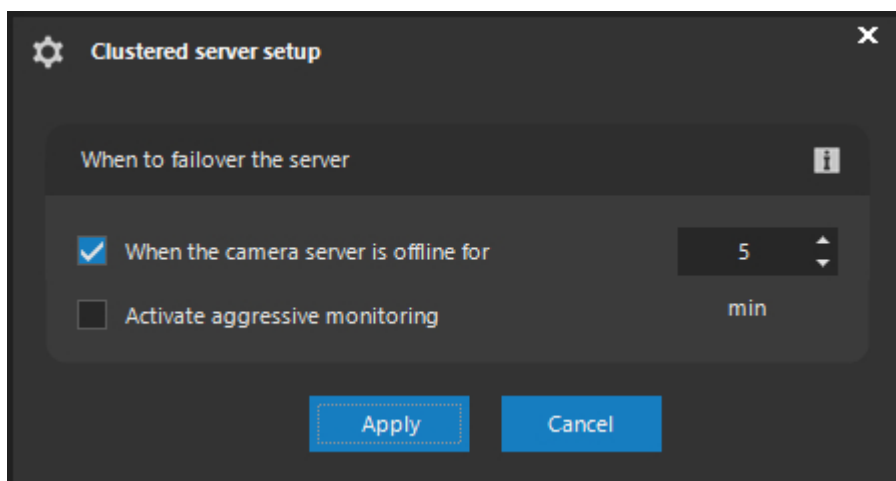
After entering the name, pressing the **NEW** button leads to a creation of a new cluster. You can remove an existing cluster by pressing the **REMOVE** button. In this case, all camera servers, which are part of the cluster, will again be assigned amongst individual servers without cluster affiliation.

Two white arrow buttons are situated between the Servers in cluster and Independent servers lists. Using these buttons, you can move the selected camera servers between these lists. You can then assign individual camera servers to clusters or remove them again and for example add them to a different cluster.

The final option in the window is the **PROPERTIES** button, which is available for the selected camera server that is already part of a cluster.

NOTE

This option is not available for backup servers, which themselves are not backed up.



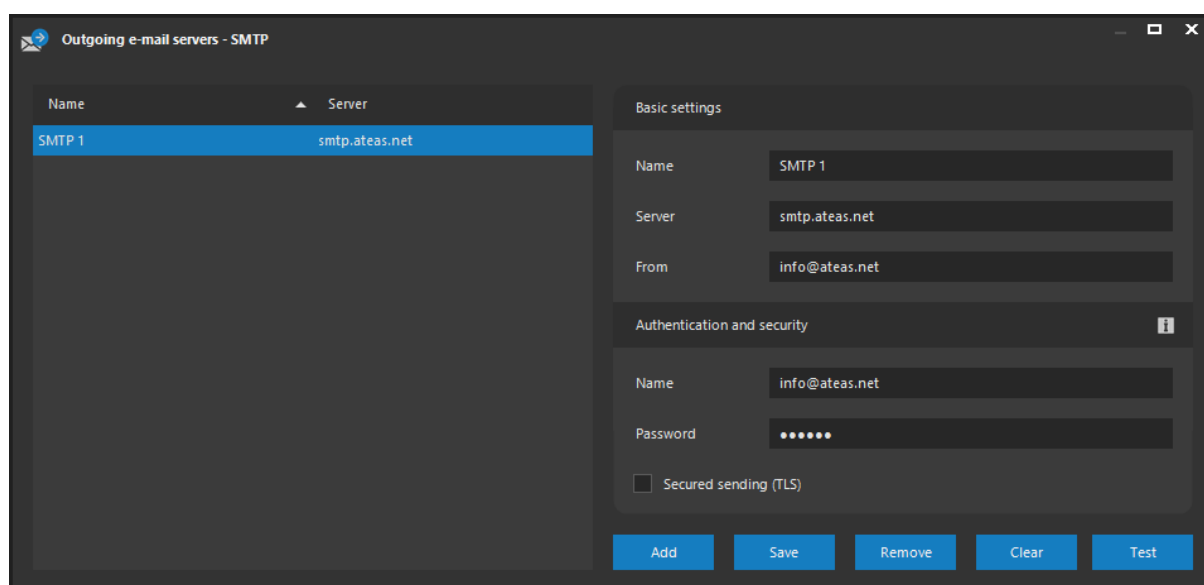
In this dialog, the server downtime interval can be configured during which the server does not respond to system administration server. By default, the time interval is configured in minutes, by activating the aggressive monitoring strategy, it can be reduced to as low as 5 seconds for critical systems.

CAUTION

With aggressive monitoring enabled, server failovers can occur even with very short network down periods, thus it is recommended to activate this option for stable and properly working local area networks only.

11.10.7. SMTP accounts

Using the **SMTP** button, it is possible to display the list of all outgoing mail server accounts, that are used throughout the system for various tasks like sending events information including image attachments, sending system notifications or automatic distribution of charts and metadata reports.



The **ADD**, **SAVE** and **REMOVE** buttons are used for basic e-mail account management. Use the **CLEAR** button to quickly empty all text fields. For any selected account, the **TEST** button can be used to send a testing e-mail to an arbitrary address using that account.

In the Basic settings section, the name and address of an SMTP server must be provided as well as the From address. The Authentication and security section allows you to enter credentials for an SMTP authentication and to activate encryption using TLS protocol.

NOTE

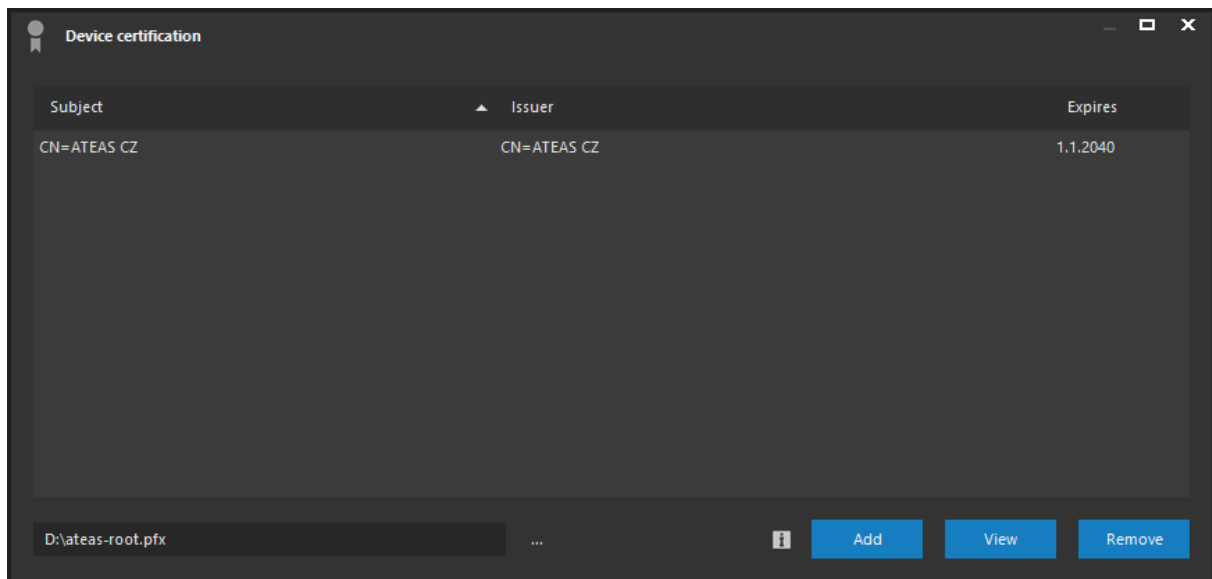
When sending encrypted e-mails, the SMTP protocol together with the STARTTLS scheme is used, by default operating on port 587. The other commonly used SMTPS alternative with port number 465 provides the same level of security using the TLS protocol as well.

11.10.8. Device certification

Using the **CERTIFICATES** button, administrators may upload certificates to the system to be used to verify devices connecting to camera serves.

NOTE

Using and validating device certificates is available starting with ATEAS Security PROFESSIONAL edition.



A certificate whose path has been entered into the Certificate path field can be uploaded by using the **ADD** button. All major certificate file formats like cer, crt, pfx or p12 are supported.

NOTE

Some file formats may require a password to open the file which can be provided in the Access password text field.

Use the **VIEW** button to display a window with detailed information about the certificate. Use the **REMOVE** button to remove the certificate from the server. Of course, the certificate is not required to contain the private key but the public key only necessary for validation.

Certificates can be applied on both camera server level and device level. They provide a solution for video and other content certification. See more on this topic in the camera server dialog or camera configuration section.

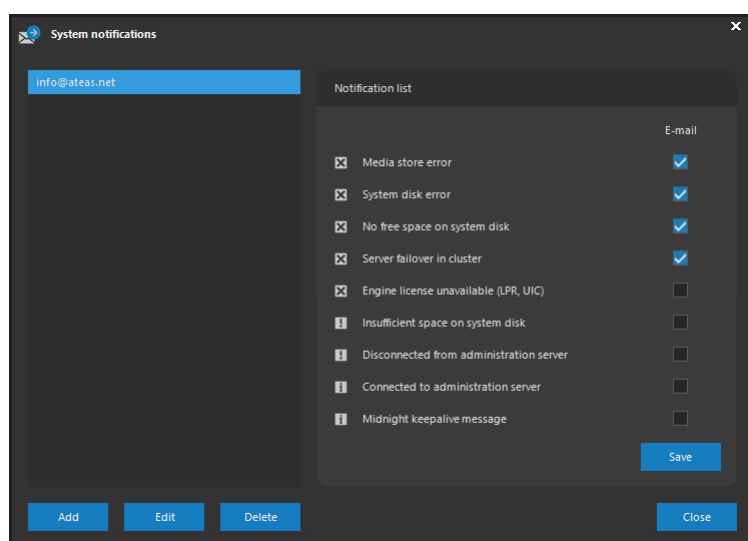
11.10.9. Notifications

The notification function is available for camera servers during a system event. Sending e-mails is possible during a system event. The ATEAS camera server can send e-mails in several languages to any number of e-mail addresses.

NOTE

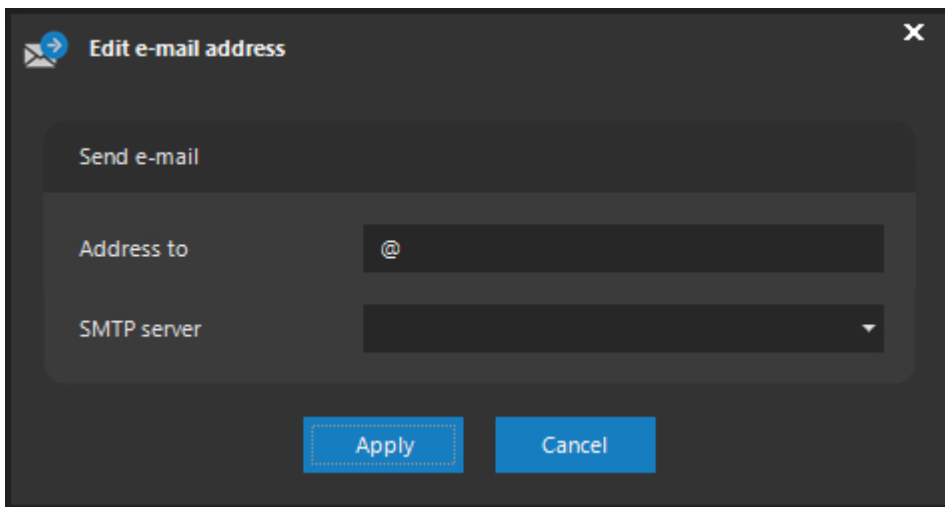
Here, we do not refer to the e-mail sending option during a system event of alarm (for example when activating the camera alarm input, camera failure or the recognition of blacklisted LPs). This reaction can be part of an event scenario for camera reactions to an event, see chapter on event management and creating event scenarios.

You can open the notification settings window by pressing the **NOTIFICATIONS** button. The camera server shall be online when using this button.



E-mail addresses

The list in the left part of the window contains e-mail addresses to which an e-mail will be sent informing of an occurrence of a system event. Use the **ADD** button to insert new e-mail addresses into the list according to the following picture.



Mandatory fields to be filled in include the recipient's address and an SMTP server.

NOTE

E-mail address syntax is checked according to valid standards and notifies you of any addresses with invalid format,

You can edit the inserted address at any time using the same dialog as for adding a new address by pressing the **EDIT** button. You can remove any address from the list by pressing the **DELETE** button.

Notification list

The camera server sends e-mails during the occurrence of any system events, which have the send e-mail option checked in the list. Therefore, you can receive an e-mail notification, for example during a media store failure (or if not available after the server starts), a server within a cluster fails (the message is sent by servers with delegated functions), ATEAS Server service system disk error, running out of space on the system disk etc. Both the installation location as well as the metadata location (if it resides on a different disk) are considered to be system disks.

Also available are purely informative messages such as reconnection to the administration server (after a disconnection) or the midnight keep-alive message, which is automatically sent everyday at midnight and indicates the server is operating.

TIP

The LPR engine license not available notification can also be used to be notified of the time limited demo license expiration.

Different types of notifications can be sent to each address. After an e-mail address is added, only sending of critical messages to this address will be activated by default. To activate sending of selected notifications only for the selected e-mail address, check the desired notifications and press **SAVE**.

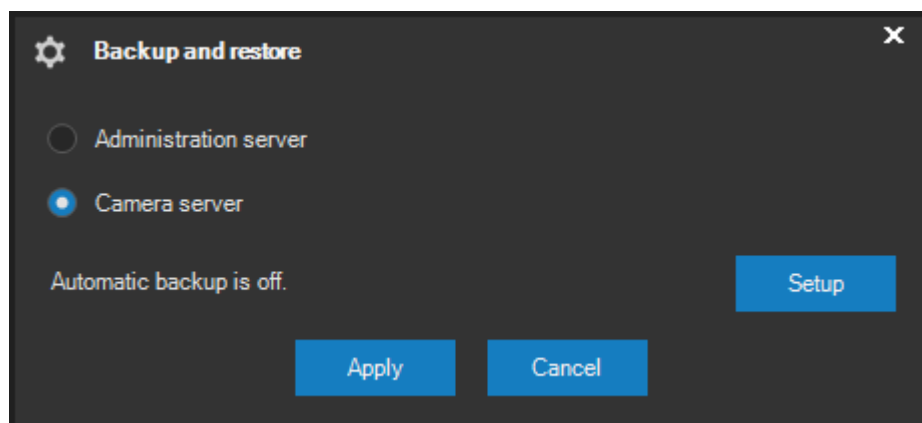
NOTE

Since the Disconnected from administration server notification can be caused by the connectivity loss of the camera server, the camera server may not be able to properly send this notification. Therefore, this notification is sent in parallel also by the system administration server.

11.10.10. Configuration backup and restore

Configuration backup and restore can be performed using the **BACKUP** and **RESTORE** buttons in Server functions. Using these two buttons allows the user to backup or restore the complete configuration of the administration server or selected camera server at any time. Settings are stored as an XML file.

When backing up the configuration, you must select the respective server, see following figure. After the location of the final XML file is defined, the complete settings for the given server application will be exported.



When restoring your configuration, all you have to do is search for the respective XML file, confirm your selection and the configuration for the given server will be restored. When restoring camera server configuration, the target camera server must first be selected from the list of servers.

NOTE

Only system administrators can backup and restore the configuration. The administration server configuration can only be backed up and restored by the master administrator (administrator number 1).

CAUTION

When restoring configuration from an XML file, the configuration versions in the file and in your system must match.

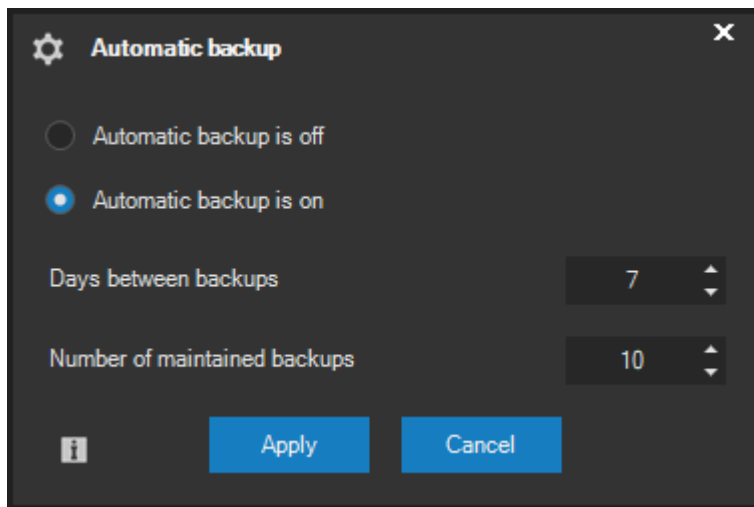
TIP

The **RESTORE** button can also be found in the license dialog, from where, after a clean installation, it is possible to restore the configuration more quickly and without activating the license.

Automatic configuration backup

The configuration of the administration server and all camera servers in the system can also be comfortably backed up automatically. This is particularly useful if the configuration is changed often or we have a greater number of camera servers for which a manual backup would take longer.

Automatic backup can be activated in the dialog displayed when **SETUP** is pressed in the dialog, where manual backup is performed.



Automatic configuration backup can be enabled or disabled from this dialog. If automatic backup is on, you can specify the number of days between individual automatic backups and the maximum number of maintained backups (old backups are automatically deleted).

NOTE

When performing automatic backups, XML files containing the configuration are always stored on the system administration server in the configuration-backup subfolder, where they are automatically divided into folders based on the server and individual files are labeled with the date when the backup was performed.

NOTE

On the date when the backup is scheduled to be performed, it is performed at midnight. If the server is not online during this time, the automatic backup is performed as soon as the server is connected.

Configuration cannot be exported and imported in systems with different versions. Therefore, during manual backup, the application suggests a filename containing both the export date and the system version. Identical names are also used during automatic backup.

Not dependent on the automatic backup settings, the configuration backup is always saved in the recover folder when upgrading both the administration and camera server to a higher version.

11.10.11. DLNA streaming support

DLNA streaming can be activated for the given camera server by pressing the **DLNA** button under the list of servers. DLNA denotes a technology that allows devices such as televisions and other (e.g. VLC) to automatically detect the source of video streaming on the network, including names and other parameters, and to connect to these video sources.

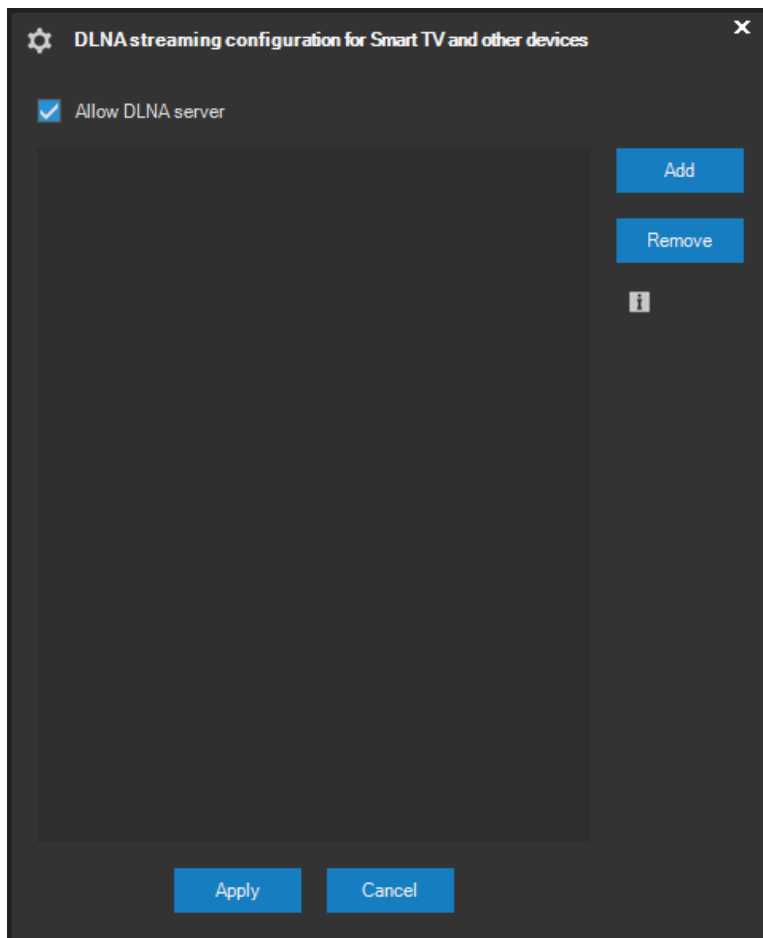
NOTE

ATEAS Server uses port 8509 for DLNA streaming, as well as the SSDP protocol for publishing DLNA streaming channels.

CAUTION

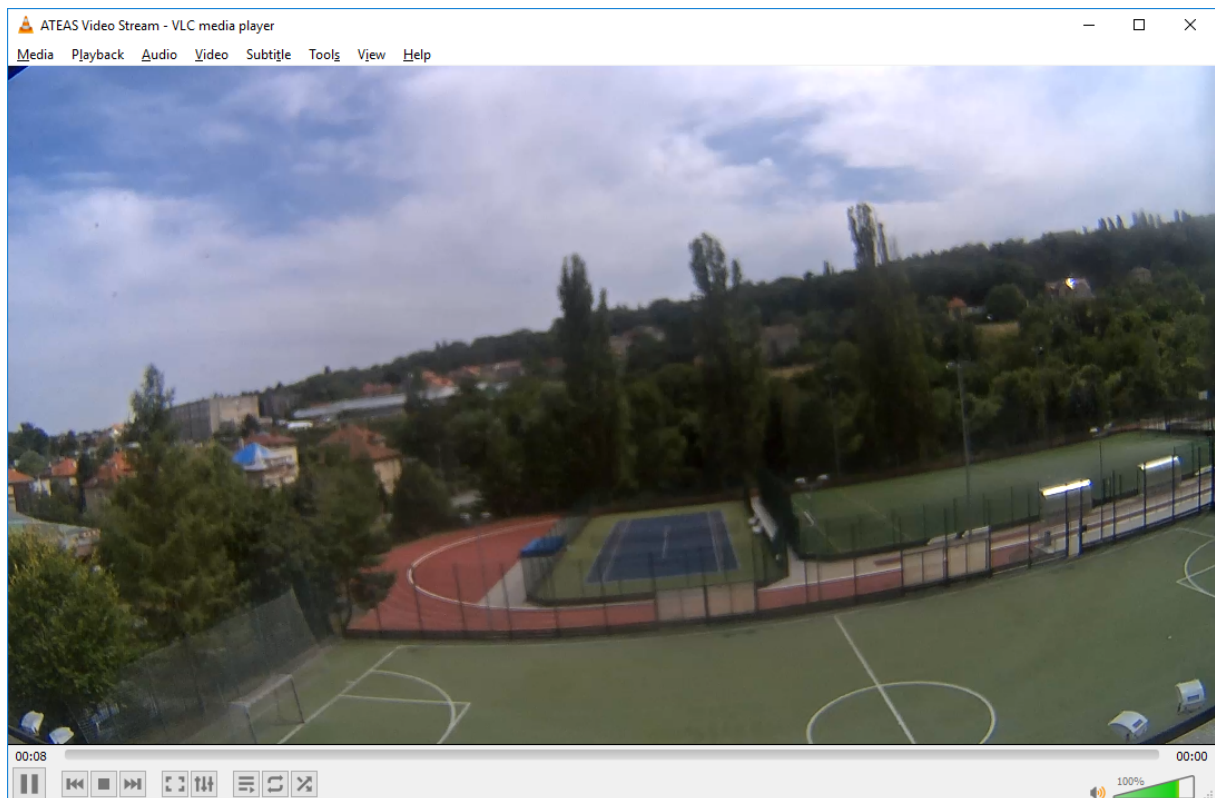
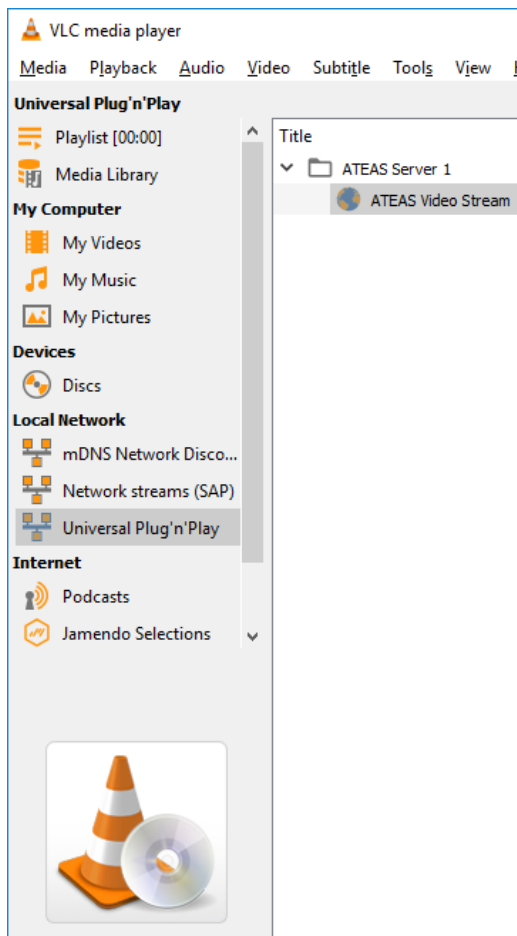
ATEAS uses a new MP4 container for live DNLA streaming (fragmented MP4 transmission). Devices, which do not support this format, will not be capable of playing video.

The following dialog will appear after the DLNA button is pressed.



The Allow DNLA server option enables and disables the DLNA server. DLNA streaming channels must be created in order for clients to receive video from cameras. To add a streaming channel, simply press **ADD** and enter the name of the channel, followed by the camera number in brackets, e.g. a channel with camera 1 can be created by entering Camera 1 [1].

The figures below show the VLC player accessing the ATEAS DLNA server.



CAUTION

DLNA clients do not authenticate in any way. Therefore, only streaming channels should be created that can be accessed anonymously.

NOTE

DLNA server is available starting with ATEAS Security PROFESSIONAL edition.

11.10.12. Server migration

If it is necessary to migrate ATEAS services to a new server, you can use the XML format configuration to migrate all the settings as described above. After the relevant ATEAS service is installed, the XML configuration of the previous server is imported.

CAUTION

In case camera recordings shall also be available after the migration to a new server, you may have to perform the additional steps described below.

If the media stores remain available at the same location as on the previous server, after the new server installation you should copy the contents of the camera server data subfolder from the previous server to the new server and restart the camera server service.

If the media stores are at different locations, the original media stores can be removed and new media stores can be created using existing data. This procedure is described in the media store management chapter.

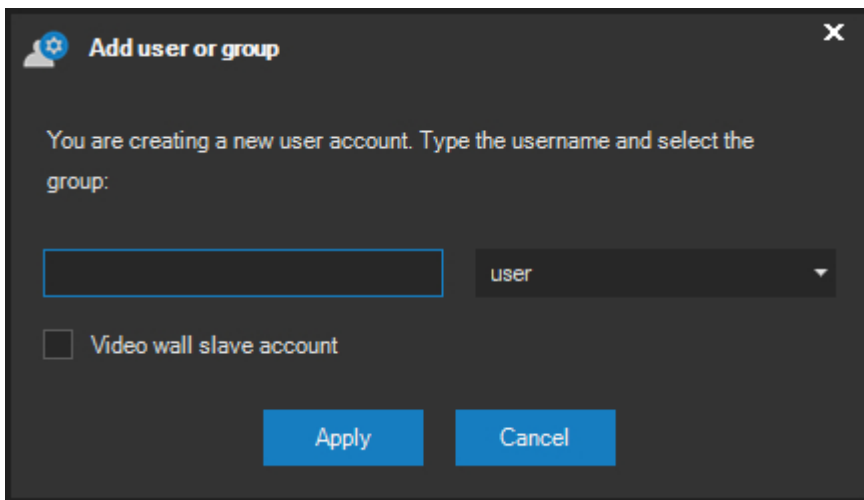
11.10.13. User administration

The list of all users is displayed in the Users Administration section. Each user in the list is given a unique ID, username and assigned to a group - either USER (ordinary users) or ADMINISTRATOR (administrators) or another group created by the administrator. See the group administration subchapter for more information on groups. The amount of users and administrators created in the system is unlimited. User accounts can be sorted by any of the columns in the list either ascending or

descending. The list also contains an indicator that distinguishes users currently logged into the system from offline users by using different indicator colors.

Adding a user

To add a user, press the **NEW** button in the Users Administration section. A dialog will be displayed requesting the user name and group.



Each username is checked for duplicity before a user account is created. If duplicate, the application will display a message dialog informing the user that the user account is already created. After the account is successfully created, the list of users will be updated and the application will display the respective message dialog. The Video wall slave account checkbox is used for creating special user accounts related to slave video stations that can be controlled from other client stations. For further information, see the chapter regarding views administration, namely the part on video walls.

User operations where a batch configuration makes sense and has a meaningful visual interpretation can be performed for a multiple selection of users. Therefore, it is possible to remove multiple users with one click or assign a new group to them. However, these batch operations cannot be performed for a mixed selection of administrators and users for example.

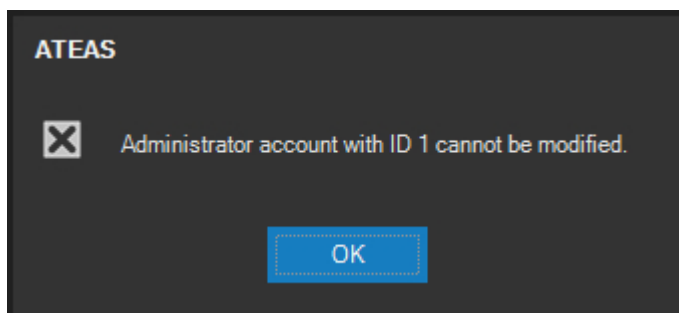
TIP

A user can be renamed directly in the list by clicking on its name.

Removing a user

Any user account (both the ordinary and administrator) can be deleted from the system. After pressing the **REMOVE** button in the User functions section, you must confirm the action and wait for system confirmation.

The only exception is for the administrator account assigned the number 1 (admin), which cannot be removed or modified. When attempting to remove or modify this account, the application will display an error message and the account is not removed.



NOTE

The administrator account with the admin username and ID 1 assigned has a special significance for whole system. This account differs from other accounts as follows:

- This account cannot be removed and its rights cannot be modified.
- This account has a profile created on each newly added camera server. This profile cannot be deleted. Other users (including administrators) do not have any account on newly created camera servers (default setting). This profile is invisible to them.
- It is the only administrator account authorized to manage camera servers and users (with the exception given by the tool for controlling access to the administration sections - see below). Other administrators can only manage servers they can access.
- It is the only administrator account authorized to perform an upgrade of the system license number.
- It is the only account authorized to control other administrator accounts and the tool for controlling administrator accounts using sections - see below).

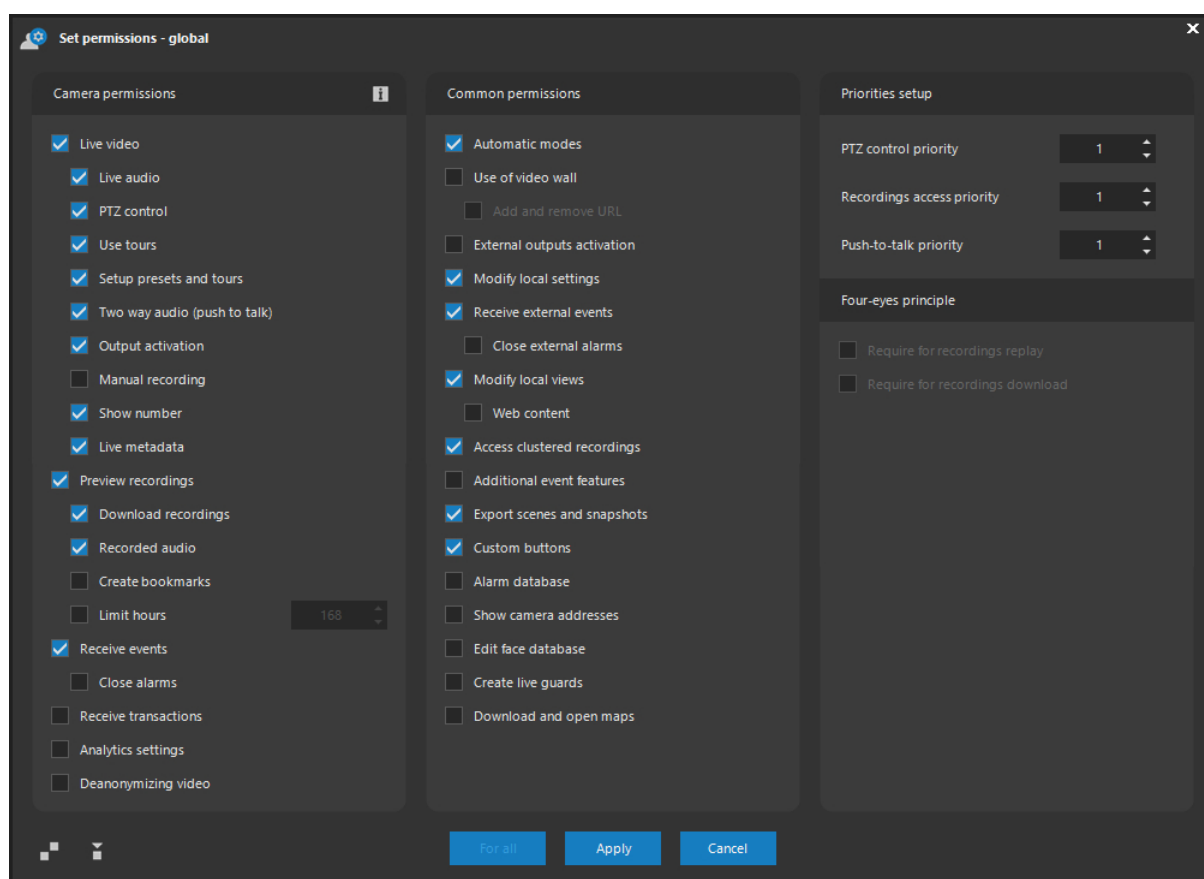
Passwords and resetting passwords

A password for a newly added user is always the same as the username. Since the system does not permit identical usernames and passwords, each user must change his password during the first login. If a user forgets his password, it can be reset using the **PASSWORD** button. The password of a

selected user will be reset to the default value (same as username) after confirming the following message by clicking the **YES** button.

User permissions

Permissions can be defined for each selected user. These permissions will be applied to the user globally (i.e. they will be applied for all cameras on all camera servers to which the user has access) except for cases where user permissions are created with the option of defining camera permissions for each camera independently. User permissions in the permissions list can be modified using the available checkboxes. All changes can be saved using the **APPLY** button. A message will be displayed after saving process is successful.



User permissions are divided into two groups. The left section contains camera permissions (permissions directly associated with cameras), the right section contains general permissions (not directly associated with cameras).

CAUTION

If a user has some restrictions, the specific camera permissions configured there will take precedence over the common permissions configured in this dialog.

The majority of general and camera permission list items do not require additional remarks. We only add selected comments below.

The Show number permission refers to displaying the camera number within the camera number overview in the primary live window, and does not affect the ability to access the camera within a view, replay etc. However, the permission can be used when cameras are added multiple times to the server and when their offset values are set to display a camera detail and recordings (see basic camera setup). In this case, for better transparency, we can revoke permissions to display camera numbers in the live window for duplicate camera entries.

If you wish to enable a certain user to use the video wall (if available in the system), respective permission must be selected in this window. In particular, a user must be granted a special permission to be able to create URLs for displaying web based content on the video walls.

The Additional event features permission relates to the option, for some event types received in the live windows or found in the recordings by right-clicking the mouse, to invoke a context menu with additional options for the given event. It is used, for example, in order for an ordinary user to be able to change the classification of a vehicle LP into the registered LP lists (white list, black list etc.). This permission also applies, when the user tries to activate the context menu of a counter to reset its value.

The PTZ control priority value (from 1 to 20, where a higher number represents higher priority) can be set in the Priorities setup permissions section. This priority (set to 1 by default when a new user is added) is important when two (or more) users are trying to simultaneously control one camera. In this case, the user with lower priority yields to the user with higher priority. However, if a user with the highest priority does not control the device for a certain period of time, a user with a lower priority can also start controlling the camera (after a certain period of a time referred to as the PTZ time window). A “first come, first served” rule applies when two users with a same priority level are accessing one device simultaneously. The user which starts controlling a camera earlier gets his personal time window and has priority over the other users.

The name of the user, who obtained control over the camera, will be displayed to other users under the user control for controlling cameras. Other users, who may not control the camera, can at least be

notified who is currently using the camera and potentially verify the controlled camera is available for use by another user.

In terms of control priorities, a tour has the lowest priority. Higher priority is assigned to manual control (positioning or moving a device to a preset point) which interrupts a tour for a certain period of time. However, if the tour is launched in reaction to an event, the interruption time for this event tour when manually controlling the camera, is reduced to a very short period of time (seconds), for the event tour has a higher priority than a standard tour.

Likewise, the Push-to-talk priority value determines the priority of the user or group to transmit audio to the camera. A user with a higher priority can start talking to the camera even in case another user with lower priority is currently using the camera for talking, in which case his audio transmission is automatically stopped. The priority can again be set between 1 – 20 whereby a higher value indicates higher priority. If a user has a lower or equal priority, he must wait until another user stops his audio transmission.

Recordings access priority determines the priority of the user or group to access recordings intervals with applied restrictions and also define such restrictions. For example, if a user has the priority of 10, the user cannot display data restricted for access priorities of 11 or higher, however, the user can configure restrictions on parts of the recordings and specify the minimum access priority of 10 or lower. The priority can again be set between 1 – 20, whereby a higher number indicates higher priority.

NOTE

The user must have the permission to receive external events in order to accept events generated by the system administration server – events sent via the ATEAS API from an arbitrary communication channel described and related to the created virtual object structure. This condition, however, is insufficient. If a non-empty event scenario is created for an event, the client will only accept the event if it has access to at least one of the cameras belonging to the event. This way, external events can be intelligently distributed throughout a system with a greater number of servers and clients.

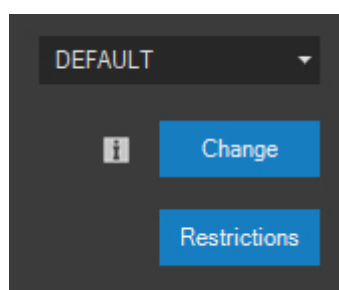
Users authorized to access the recordings can be further limited to a given amount of hours (Limit hours item) they can actually access the recordings. For example, you can configure the permissions so that only selected users will be able to view data older than one day etc. The value can be set in the range from 1 hour to 100 days (2400 hours).

For a group, the four eyes principle can be activated, which is described further in more details.

To make the configuration of user rights or group rights easier, rights can be copied among users. Thus, if we plan to give a user rights identical or similar to another user, copying the entire set of rights and subsequently adapting them is beneficial. The two buttons in the bottom left corner of the window are used to copy and paste sets of rights.

User profiles

Any user who needs to access a camera server (or servers) must have a profile created. The user profile for a selected server can be set in the User profile section.



The drop-down list includes several options with following purposes:

NO – No profile, selected user will not be able to access a selected server.

LOCAL – Local profile, the selected user will be able to access media data (video and audio) through multicast addresses using the camera server LAN address.

DEFAULT – Default profile, the selected user will be able to access camera server's media data through unicast connection using the camera server LAN address.

REMOTE – Remote profile, the selected user will be able to access camera server's media data through unicast connections using the camera server WAN address.

NOTE

Setting the WAN address for camera servers under HOME and PROFESSIONAL editions is not necessary. It is necessary under UNLIMITED edition only if the user accesses the server outside his local area network. For more information, see subchapter Basic server management.

Therefore, modifying the profile can prevent users from accessing camera servers located outside their local area network, only users with REMOTE profiles will be able to connect to the given server. The profile can be modified by pressing the **CHANGE** button. A confirmation message will be displayed after the change is successful.

NOTE

Before changing the profile, a message will be displayed allowing the administrator to apply the change just for the selected server or for all servers which the administrator can access.

NOTE

The default user profile for a newly added server is the NO profile. The default profile of a newly assigned user to any camera server is also the NO profile. The only exception is the admin user account (with ID 1 assigned) whose default profile for accessing all newly added servers is the DEFAULT profile.

NOTE

The admin account with ID 1 assigned cannot be deprived of access to any of the servers. This account has to have either the LOCAL, DEFAULT or REMOTE profile set for accessing all of the servers. The application does not permit changing the profile of this account to the NO profile.

Using the LOCAL profile for all (or selected) users can have a very positive effect on network utilization and the amount of transmitted data during simultaneous user access. This is due to the use of multicast transmissions. This means that the multicast transmission is performed by a camera server instead of individual cameras (even though cameras also enable this option). This might increase the performance of all network-related operations (multicast data streams proceed through a camera server). The following advantages are offered by this conception:

- Multicast can be used even if client and camera networks are separated and clients cannot see camera addresses. When requesting a multicast transmission of an individual camera e.g. through the RTSP protocol, the client would have to access the camera address.

- Video and audio data are marked with a time stamp which is valid for entire system. Therefore, there is no dependency on camera time synchronization if a user, for example, saves snapshots from a live view.
- Multicast transmission can be used even if not supported by the camera.

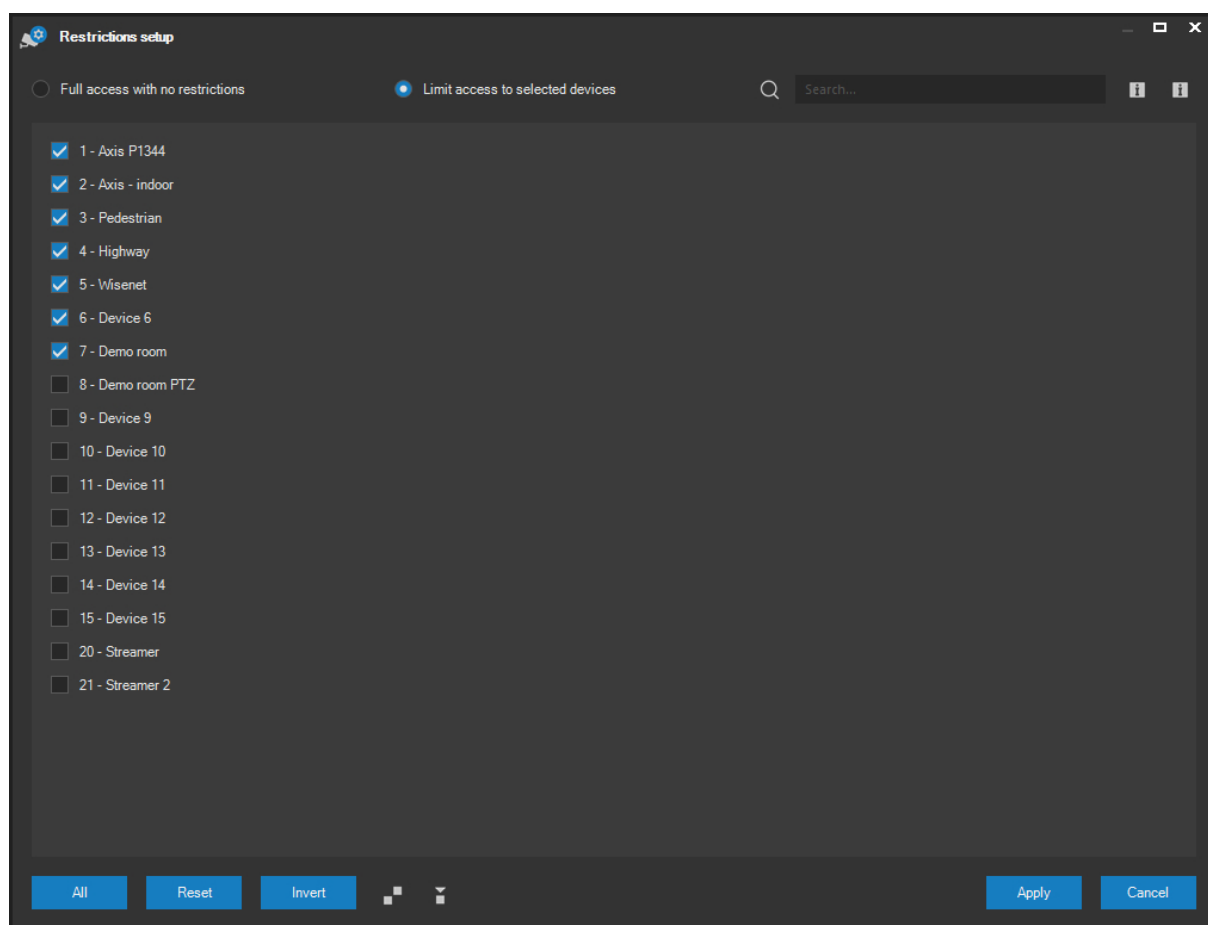
CAUTION

In order to enable multicast transmissions in your network, all active network devices (switches) have to support this type of transmitting. This information can be found in the documentation or datasheet regarding your switch. The second version of the IGMP protocol has to be supported. To make multicast transmissions work even within several interconnected networks, the multicast support has to be ensured on network routers as well. When switching to the LOCAL profile, the application will display an information dialog for this warning.

User restrictions

If a selected user able to access a selected server (the profile is set to either LOCAL, DEFAULT or REMOTE), he can also automatically access all cameras on this server. If you wish to restrict a certain user from using some of cameras on the server, press the **RESTRICTIONS** button.

Using restrictions you can limit user access to selected (or all) cameras on the camera server, but also define camera permissions in detail for each camera independently. Therefore, if we want camera permissions, modified by pressing the **RIGHTS** button, to apply uniformly for users, the user cannot have any restrictions created for him on the relevant camera server.



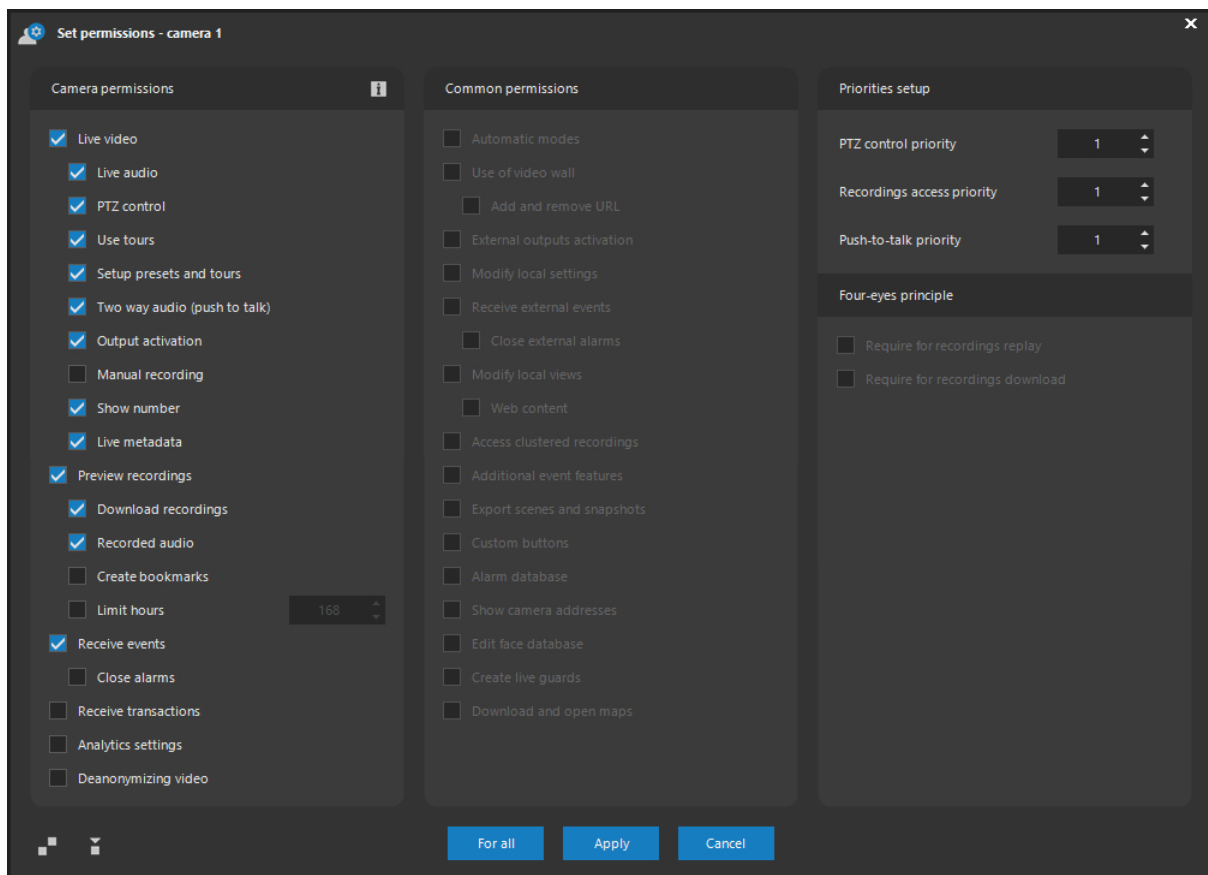
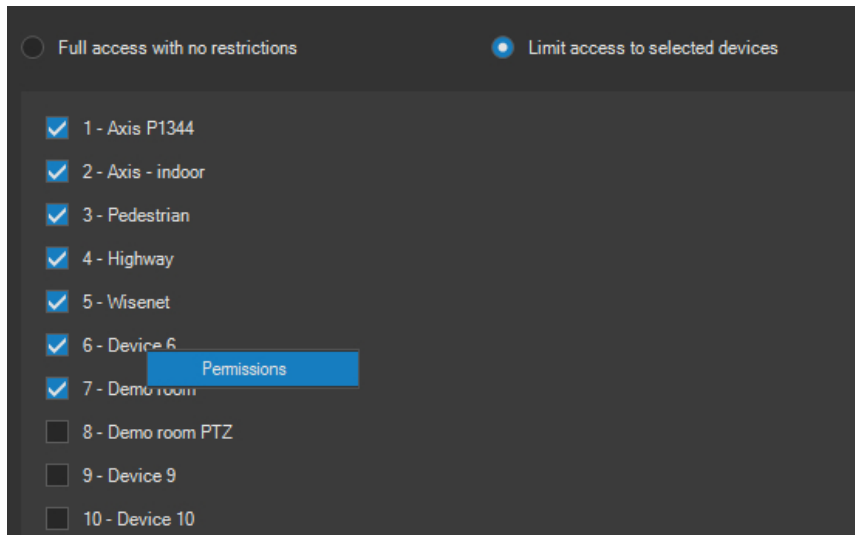
You can apply filters to the displayed list of cameras by using the search field. You can enter multiple character groups, which all must appear in either the number or name of the cameras. To search for exact phrases with whitespace, surround the phrase by quotes.

You can select between two switches, namely Full access with no restrictions and Limit access to selected devices. If full access is selected, the user will be able to access all cameras on the server, including cameras added in the future. If access is restricted, the user will only be able to access selected (checked) cameras and will not be able to access newly added devices (unless they are checked).

Using the **ALL**, **RESET** and **INVERT** buttons, you can modify the selection of cameras in three different ways. The **ALL** button selects all existing cameras on the server. Press the **RESET** button to deselect all cameras. The **INVERT** button inverts the selection making selected cameras become deselected and vice versa.

If the window is in the restrictions setting mode (the Limit access to selected devices radio button is checked), you can use the right mouse button to display the context menu and select the Permissions

item for a random camera, which the user has access to and is checked. A window is then displayed containing the permissions for the given camera.



This window is similar to the user permissions window after pressing the **RIGHTS** button with the only difference being that you cannot make any changes in the Common permissions list and all changes

in the list of camera permissions including PTZ priority settings will be applied only for the selected camera upon saving changes in the restrictions window.

NOTE

This restriction can never be set for administrator with ID 1 assigned.

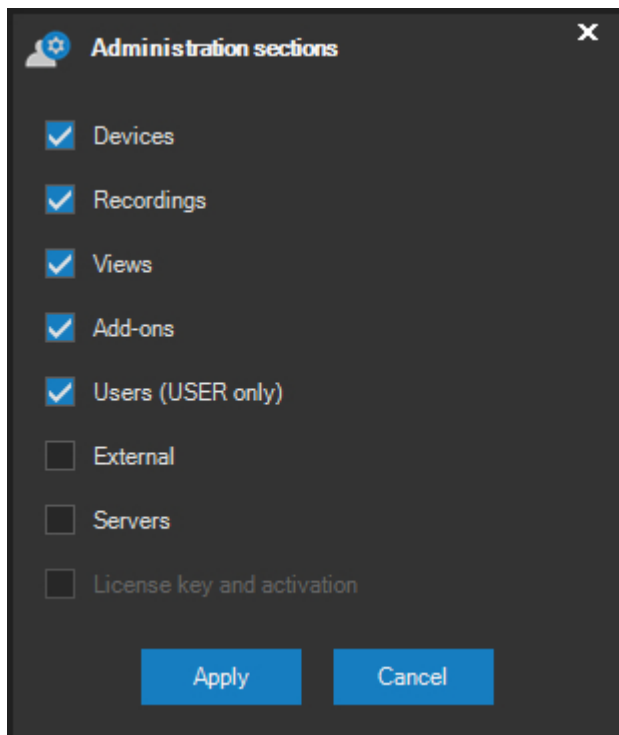
To make the configuration of user rights or group rights easier, rights can be copied among users. Thus, if we plan to give a user rights identical or similar to another user, copying the entire set of rights and subsequently adapting them is beneficial. The two buttons in the bottom left corner of the window are used to copy and paste sets of rights. The same two buttons are also available in the main restriction administration window, where you can copy restrictions for all cameras among users or user groups.

As often is the case, we also require the same rights for certain cameras for which restrictions have been established for a user. The **FOR ALL** button has this purpose exactly.

Administrator access control - administration sections

The method for creating new user accounts within a group of users or administrators was described above. The fundamental difference between the user and administrator is in the ability to access the menu items in the Administration section of the application main menu. We have also described the specifics of the administrator account with identification number 1 and username admin, which we can also refer to as the master administrator account.

The master administrator can create additional administrator accounts in the system to which he can delegate the permissions to manage the cameras or recordings on individual camera servers. Therefore, administrators can divide their scope of authority according to the camera server they have been granted access to. ATEAS Security version 4.0.0 enables setting the scope of administrator authority, not only according to servers, but also according to the activities performed on them. The Administration sections tool serves this purpose and can be displayed by pressing the **SECTIONS** button.



The picture shows the default set of accessible administration sections for administrators, as this was the default system behavior before the version 4.0.0. Newly created administrator accounts could access the devices, recordings, views and add-ons administration sections— of course only on camera servers with a profile for the administrators.

With the help of this tool, the master administrator can restrict administrator permissions to access individual sections, such as devices, recordings, views or add-ons, but can also grant access to users, external and servers sections.

NOTE

In order to maintain the master administrator control over the scope of authority of other system administrators, other system administrators cannot affect users, within the users administration section, from the administrator group in any way (the same applies for their own accounts).

NOTE

For users without access to the users section, the administration section of users and servers remains available in read-only mode with the option of using some unessential functions only.

If administrators are granted access to the Servers section, they will be able to create, edit and delete camera servers from the system. They will also be authorized to allocate the licensed number of cameras among these servers. In this case, they will also be able to see all servers in the list, including those for which they do not have a profile established.

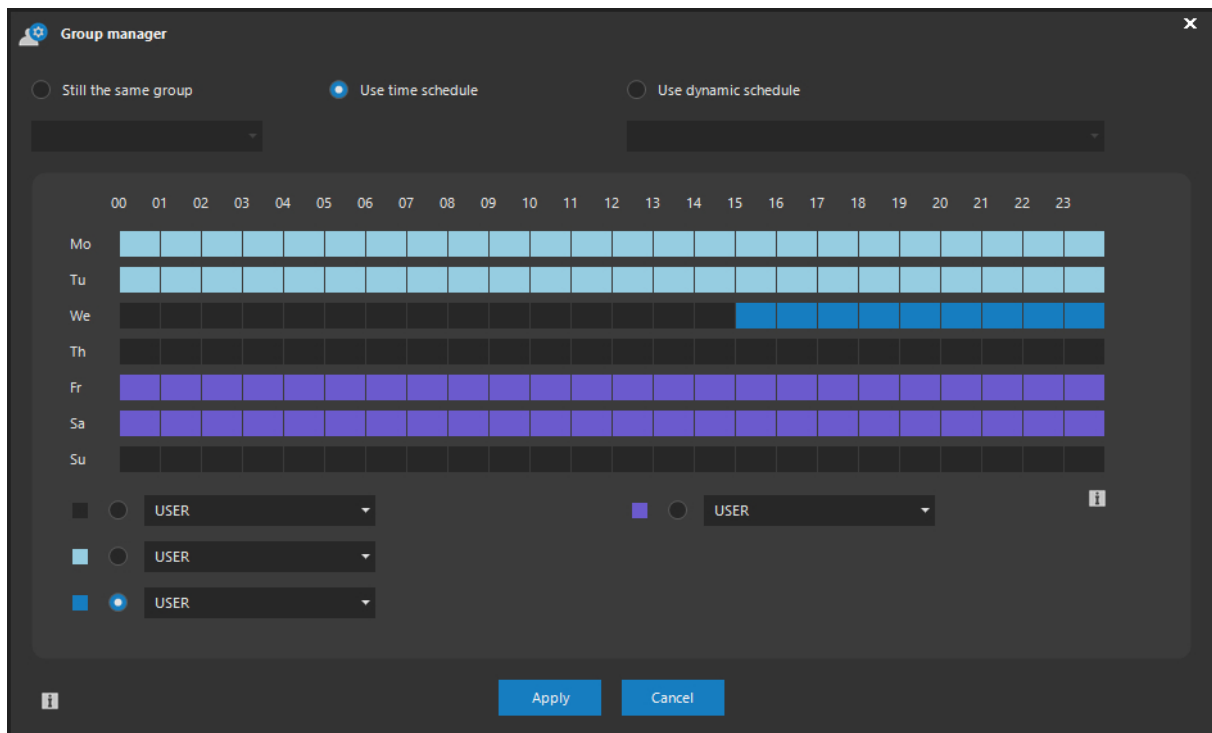
Despite the wide and intuitive configuration of the scope of administrator authority, some settings or activities can only be performed by the master administrator, i.e. the administrator with number 1 and username admin. These activities include:

- The master administrator is the only user that can create, delete and change the settings of user accounts from the administrators group.
- Master administrator is the only user that can create and delete custom camera event sources due to central validity of names for the entire camera system.
- The master administrator is the only user that can enter the license key and generate an activation key online including the initial system activation and all later reactivations when upgrading to a higher system version, or when expanding the license.

Assigning users to groups

Each user account becomes part of a group after being created. The group is either a predefined system group of common users (USER) or administrators (ADMINISTRATOR) or a randomly named group defined by an administrator. If a user is part of group defined by an administrator, his rights and restrictions are always derived from the rights and restrictions of the given group and cannot be individually changed. In this case, the application responds with a warning message.

If a user is part of one sole group, this is referred to as a static group assignment. If the user is part of multiple groups, this is referred to as a dynamic group assignment. . Dynamic group assignment can be based on time or on the dynamic schedule specified by event in the system. This setting can be performed upon pressing the **GROUP** button.



The picture shows the option of static or dynamic group(s) assignment for the selected user. For a static group, it is necessary to select one specific group (including predefined system groups) to which the user will be assigned. For time based dynamic assignments, it is possible to select as many as four different user groups and plan time frames when the user's group assignment is automatically changed. For dynamic assignments according to dynamic schedules, it is necessary to select the created dynamic plan from the list and specify, as well as differentiate by colors, two different groups between which the user will automatically be reassigned based on whether the respective dynamic schedule is inactive (first group) or active (second group).

TIP

To quickly select a day or entire week, double or triple-click the area.

TIP

To quickly schedule working hours in multiple days, use the ALT key.

In practice, the dynamic group assignment can, for example, be used for limiting daily monitoring of populated areas, or restricting the control of PTZ devices during some time frames etc.

NOTE

If a user is assigned to one group (static assignment), the name of the group is displayed in the user list in the Group column. However, if the user is assigned to multiple groups (dynamic assignment), the column will contain system value <dynamic>.

NOTE

Changes to group rights or restrictions are registered immediately, regardless of whether the user's group assignment is static or dynamic.

NOTE

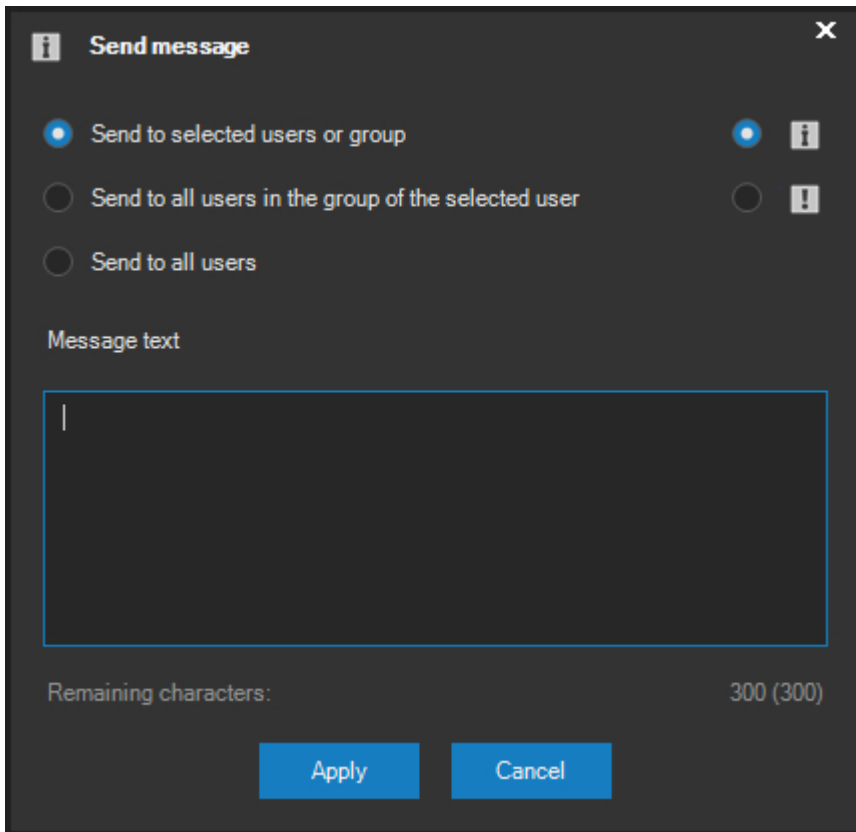
By rule, users created in the predefined USER group or in a group based on this group, can only have a static or dynamic assignment to the USER group or groups based on this group. Similarly, the same applies for the predefined ADMINISTRATOR group.

User logout

Pressing the **LOG OFF** button will induce a forced logout of the user from the system. This can be performed for a user logged into via the standard client or any other client including mobile applications.

Sending messages

Internal system messages can be sent to a selected user or group of users by pressing the **MESSAGE** button. These messages are displayed to the user in standard fashion within their client applications; this way the administrator can inform them, for example, of a forthcoming system restart etc.



The image shows a 'Send message' dialog box with a dark background. At the top left is an information icon and the title 'Send message'. At the top right is a close button 'X'. Below the title are three radio buttons for selecting the recipient: 'Send to selected users or group' (selected), 'Send to all users in the group of the selected user', and 'Send to all users'. To the right of these radio buttons are two icons: a blue circle with an 'i' and a red circle with an exclamation mark. Below the radio buttons is a text input field labeled 'Message text'. At the bottom left, it says 'Remaining characters:'. At the bottom right, it says '300 (300)'. At the very bottom are two buttons: 'Apply' and 'Cancel'.

The radio buttons in the upper part of the dialog are used to select the recipient of the message. The first option will send the message to one selected user or one selected group. The second option will send the message to all users that are currently in the same group as the selected user. This does not refer only to groups which the administrator created, but also the basic USER or ADMINISTRATOR groups. The third option will send a message to all system users currently logged in.

NOTE

Messages are not sent to video wall clients, unless they are explicitly selected as recipients (user or created group).

The length of the message is limited to 300 characters and can be assigned a certain level of importance that will be displayed to users by selecting the respective radio button (icon) - normal information or warning.

11.10.14. Group administration

In order to manage user groups, it is necessary to select the Groups option. User groups can be sorted by any column in the list either ascending or descending. Assigning individual users to groups is described in the previous subchapter.

Adding groups

Press the **NEW** button and enter a group name to create a new user group. The group must always be based on one of the two predefined system groups – common users or administrators (USER or ADMINISTRATOR). The difference is whether or not the group members will have access to the administration section.

TIP

A group can be renamed directly in the list by clicking on its name.

Deleting groups

Any arbitrary user group can be deleted by pressing the **DELETE** button.

NOTE

If a group containing users is deleted, the users' affiliation to the group will be reset to the predefined system groups USER or ADMINISTRATOR. The basic rights for these users will be taken from the group rights and their restrictions will be renewed to the state prior to creating the group. This not only applies to situations when the user is assigned to only one group, which is then deleted, but also to situations, when the user is assigned to multiple groups and is part of deleted group at the given time.

Group rights and restrictions

Setting the basic rights and restrictions for a selected group is identical to setting the rights and restrictions for a specific user.

NOTE

When a change is made to the rights or restrictions of a group, this change is registered immediately by all users that are part of the group at the given time.

Group profiles

User group profiles can be created, edited or deleted for individual camera servers, while the same applies as mentioned in the User profiles paragraph. Defining a group profile, however, allows you to change the profile of all users in the group at once.

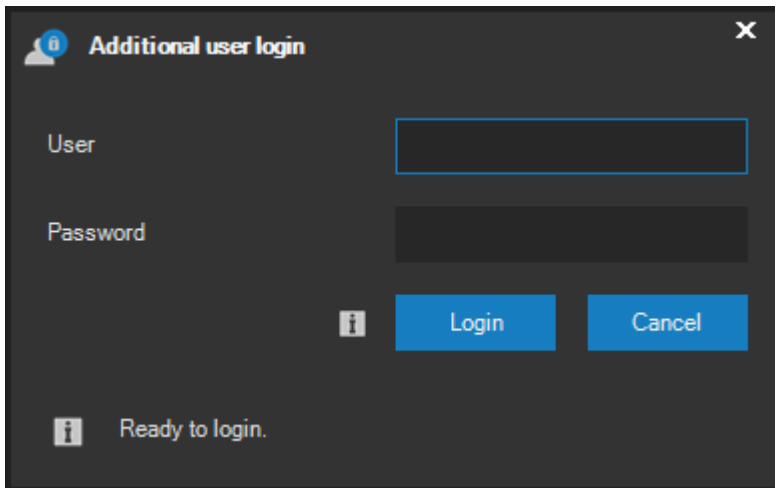
NOTE

Since the group itself does not carry the profile to servers, changes to the profile are made directly for all users statically assigned to the selected group. The profiles of individual users can subsequently be updated.

11.10.15. Four eyes principle

In the group permissions dialog, the so called four eyes principle can be activated, which can be applied to downloading recordings or even to displaying them. This principle ensures that to be able to access the recordings, two users from the same group will have to log in from within the same client station. Despite the permission to access recordings, none of the users will be able to actually access them separately on his own.

When this principle is active and the user tries to access or download the recordings, a dialog will be presented automatically to allow a second user to log on.



Only after a second user from the same group and with a created server profile logs in, the first user will be allowed to proceed. When the second user logs out, the feature will no more be available.

NOTE

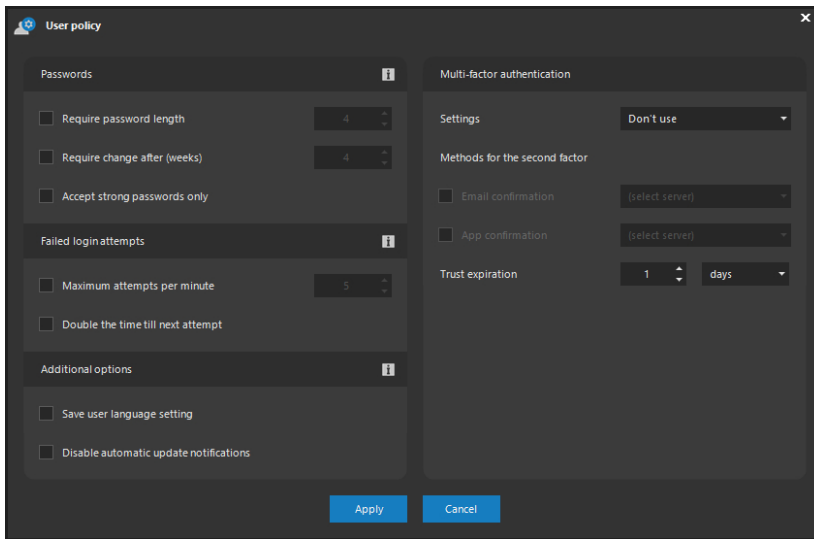
The additional login of the user does not collide with his regular application login so no duplicate login error message will ever be displayed.

NOTE

Accessing recordings with a four eyes principle activated is always logged with information about both of the users.

11.10.16. User policy

Besides being able to set the rights and restrictions of every user or group, the administrator can also configure some global parameters concerning all system users. These settings are referred to as user policy. These settings can be accessed by pressing the **POLICY** button.



In the Passwords section, you can change the global settings for the minimum password length required for each user. You can also check the Accept strong passwords only option, forcing the user to select a strong password, meaning the password must contain at least one lowercase letter, one uppercase letter and at least one digit.

NOTE

After applying the new user policy rules for passwords, new and existing users will be forced to change their passwords during their next login, providing their current passwords do not satisfy this policy.

You can also set a time limit for the validity of users' passwords. If this feature is active under user policy, all users will be prompted to enter a new password after the configured number of weeks have expired since the last password change.

NOTE

The new password must not be the same password that was valid prior to this change.

In the Failed login attempts section, two important security features are located telling the system what to do in case of failed login attempts. By activating these features, password brute force attacks can be effectively mitigated. The first option enables to set a maximum amount of failed login attempts per minute (all attempts are logged together with the information about the IP address). The second option is even stronger and allows to successively double the time until the next attempt is accepted.

Therefore, a relatively small amount of failed login attempts is sufficient to hit the maximum lock time of the account, which is topped at one year. The only way to reset this lock time is to reset the password of the user. For the master administrator account with ID 1 the lock time can only be reset by restarting the administration server service.

In the Additional options section, you can activate the option of saving the user language settings. If this option is active, the system will remember the language settings for all users and automatically switch to the respective language after logging in from any station.

NOTE

This language setting has a higher priority over the language settings in the local setup of the station.

In this section, it is also possible to turn off the version update notifications of the client application, which is performed by the client by checking ATEAS web servers.

In the Multi-factor authentication section, the possibility or obligation to use the multi-factor verification during login can be activated. Supported methods for the second factor (i.e. apart from username and password knowledge) include access to the predefined e-mail address or mobile device.

In the case of an e-mail address, it is necessary to select an outgoing e-mail server responsible for sending the verification e-mails. In the case of a mobile verification, it is necessary to select a server configured as a mobile notification gateway supporting the Firebase protocol.

The client application which passed the multi-factor authentication can log in faster during the next login attempts with the same account once such a client is trusted. This trust is subject to expiration, if the account in this client application is away for the time interval configured in the Trust expiration setting.

NOTE

If the time interval is set to zero, users will always need to go through the multi-factor authentication.

If the user cannot complete the multi-factor authentication, a password reset process must be initiated. This might be necessary, if the user lost access to his e-mail address or the linked mobile device or removed the mobile app from this device.

NOTE

In case of an e-mail verification, the user has to be able to reach the administration server where the confirmation link is referring to. In the case of a mobile verification, the administration server must be able to perform outgoing internet connections, mobile devices must be online too.

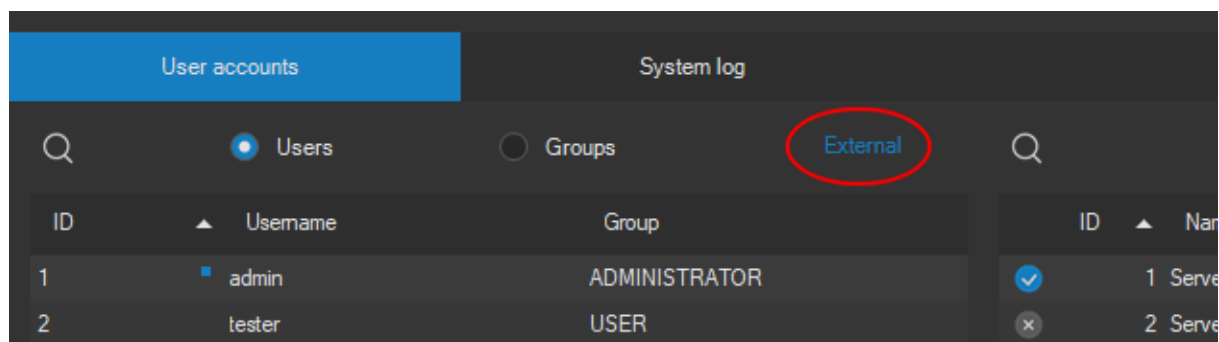
11.10.17. Users integration with external sources

The integration of user administration with an external source serves as an alternative to manual user administration, which requires all user names to be added to or removed from the system manually. The integration with external sources tool allows you to add or remove system users in batches based on user information loaded from external sources. This feature currently supports Active Directory connections via the LDAP protocol (Lightweight Directory Access Protocol).

NOTE

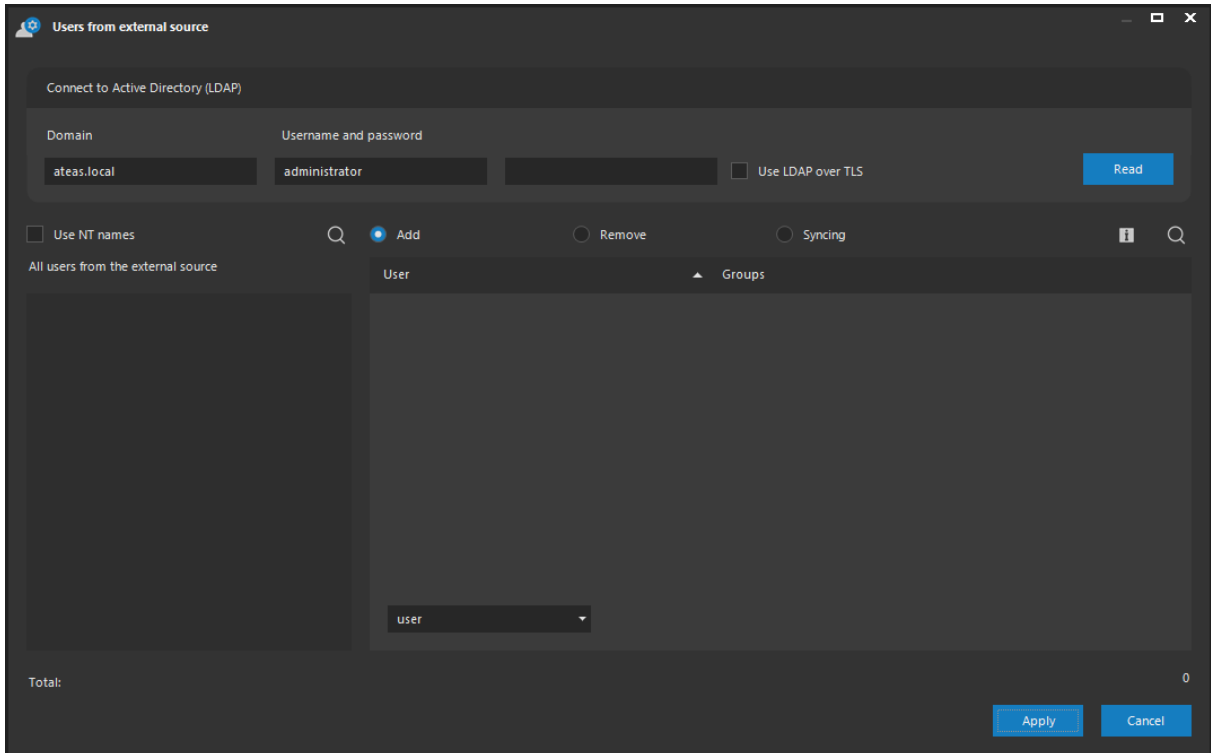
Integration with Active Directory is available starting with ATEAS Security PROFESSIONAL edition.

The tool can be activated by clicking on the External link next to the users and groups radio buttons.



Credentials for connecting to Active Directory can be entered in the top part of the following dialog. The domain, username and password are required for accessing the domain. Press **READ** to connect

to the domain and get the actual list of all user accounts, which are displayed under User lists on the left.



NOTE

The ATEAS administration server must be capable of resolving the domain name in order to fetch this list. Therefore, the ATEAS administration server shall be part of the domain or shall be granted access to the domain.

NOTE

After the user accounts in the domain are successfully read, the domain name and user name are stored and automatically displayed next time when this dialog is opened. However, the password must always be re-entered.

You can activate the Use LDAP over TLS option to enforce a secured communication. Instead of using the default LDAP port 389, a secured connection will use the LDAP port 636. For TLS to be working, the domain controller must have the correct certificates installed. Encrypted connections are then used for external authentication as well.

Based on the comparison made between the user accounts read from external sources and user accounts created within the ATEAS system, you can use the Add and Remove radio buttons to generate comparison lists. The Add option displays a list of all user accounts from external source not yet created in ATEAS Security. The Remove option displays a list of all user accounts in ATEAS Security not yet created in the external source.

Searching can be performed in all lists in this dialog using the corresponding buttons. This can be especially beneficial in the list of accounts to be imported from the domain, where you can filter out specific groups only.

Press **APPLY** to add or remove the selected user accounts in a batch, thus synchronizing user accounts created in an external source and ATEAS Security with one click. When adding users to ATEAS Security, you can also select the user group to which the users will be added.

NOTE

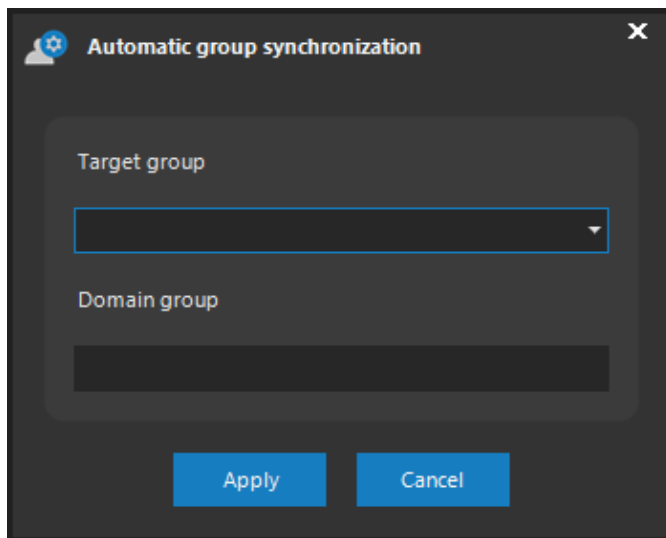
Using a custom user group for adding users from an external source is beneficial, because you can then configure profiles to camera servers for the entire group and manage their rights and restrictions within the system all at once.

NOTE

The master administrator account is excluded from any batch operations via this feature.

Automatic synchronization

Use the Syncing option to view the current set of synchronization rules for ATEAS and domain groups. Use the **ADD** button to create a new rule.



Once some synchronization rules have been created, the synchronization will take place periodically every few minutes. This time interval can be configured in the right bottom part of the window and must be confirmed with the **SAVE** button. The default value is 5 minutes. Use the **REMOVE** button to delete any rules you wish to deactivate.

NOTE

The synchronization involves all users in a domain group regardless of whether they are part of other groups as well.

Username forms

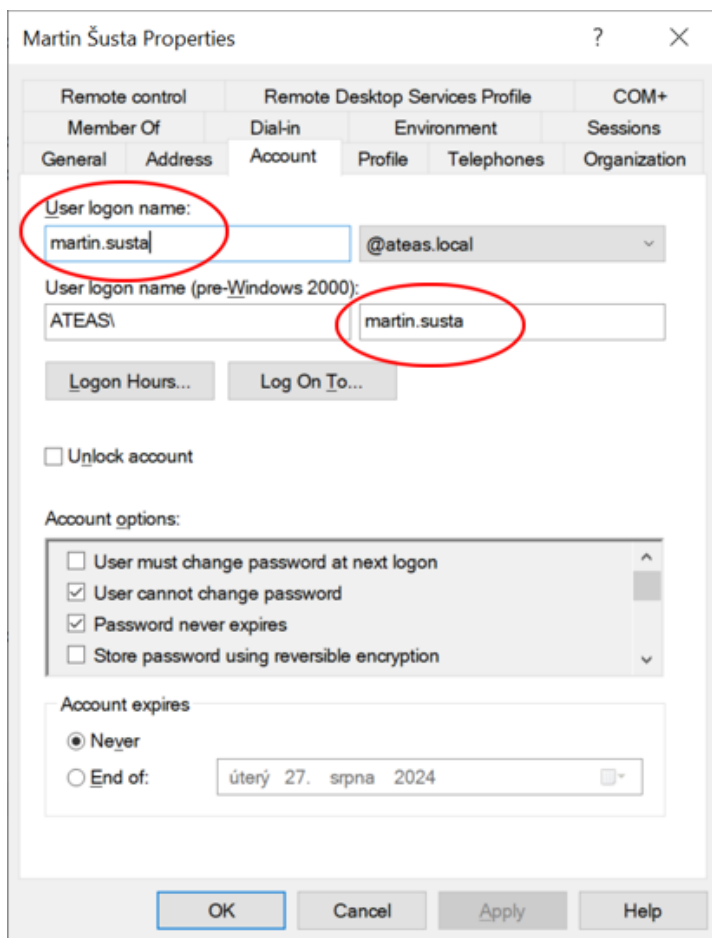
The AD user administration tool allows entering two different forms of usernames. In the past, usernames typically consisted of surnames and the leading character of first names which followed the domain name, e.g.

ATEAS\DoeJ

Later, usernames in the form of e-mail addresses gained more common usage, where the @ sign is used to separate the username and the domain parts, e.g.

john.doe@ateas.net

We are talking about the following two items:



Martin Šusta Properties

Remote control Remote Desktop Services Profile COM+

Member Of Dial-in Environment Sessions

General Address Account Profile Telephones Organization

User logon name: martin.susta @ateas.local

User logon name (pre-Windows 2000): ATEAS\martin.susta

Logon Hours... Log On To...

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☒ User cannot change password
- ☒ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of: úterý 27. srpna 2024

OK Cancel Apply Help

CAUTION

For external authentication, ATEAS adds the domain name automatically, the user is not supposed to use it during login.

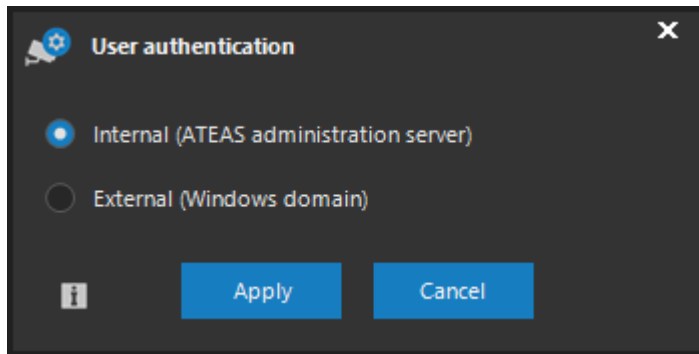
If an organization uses two different username forms, you should select one of these forms for both the manual and automatic user account synchronization. The Use NT names checkbox serves this purpose. By activating this option, the old (NT) usernames will be used and synced.

11.10.18. Authentication methods

The default user authentication method in ATEAS is the internal authentication, which means the user name and password are verified by the ATEAS administration server. For the purpose of an in-depth integration with Windows domains, it is however possible to switch the authentication mode to external. This change is made by pressing the **AUTHENTICATION** button.

NOTE

External authentication is available starting with ATEAS Security PROFESSIONAL edition.

**NOTE**

This change can be performed at both the user level and group level.

Upon switching to external authentication, the user name and password will be verified directly in the Windows domain, which is specified as the external source for user accounts. See the previous sub-chapter to find out how this external source is created.

NOTE

Account verification with external authentication is, by default, performed by the administration server. This means that even mobile or web clients can use and benefit from external authentication.

NOTE

External authentication cannot be used for administrator account number 1.

NOTE

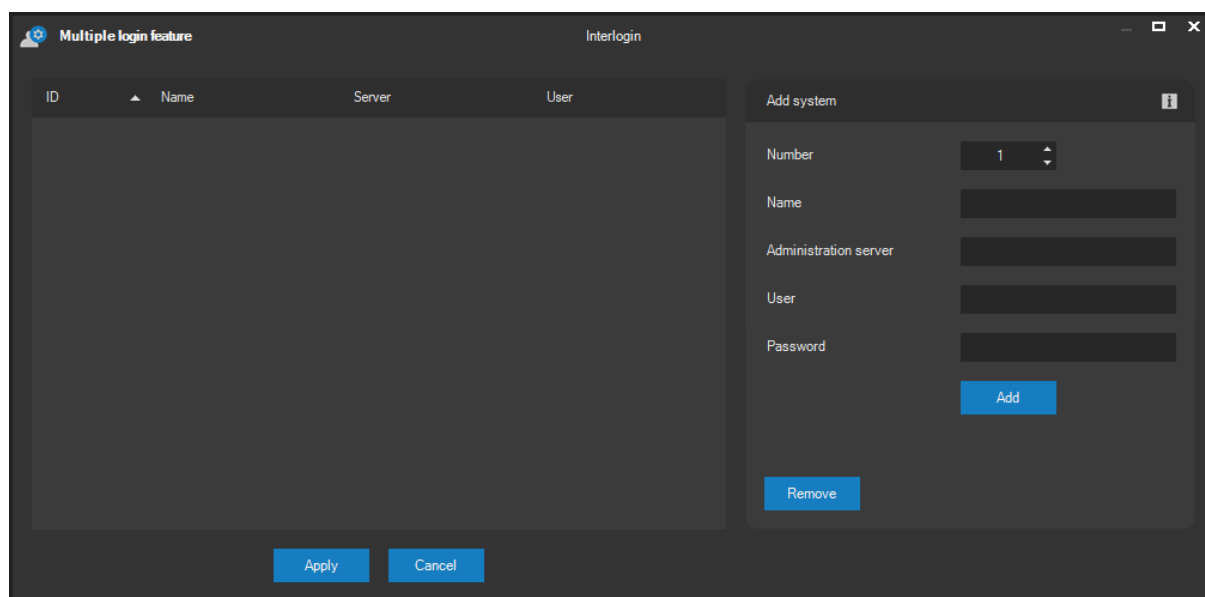
The auto login feature cannot be used in combination with external authentication.

11.10.19. ATEAS Interlogin feature

Usually, users log in to a single camera system. This camera system can, of course, consist of any given number of camera servers within ATEAS Security UNLIMITED edition. But it is often the case that the user would like to log in to multiple camera systems simultaneously. For example, security agencies can receive an account from ATEAS license holders with limited rights for the purpose of remote monitoring. The multiple login feature can be configured by pressing the **INTERLOGIN** button.

NOTE

Using this function does not require installing any additional components as it is a native part of the ATEAS platform.



The Interlogin feature can be activated both for individual users, as well as for entire user groups. In the previous dialog, you can enter a unique number, a custom name, address or network name of the ATEAS administration server and login information. By pressing the **ADD** button, you can add a camera system to the list. Next time after the user logs in (primary login), he will automatically be logged in to additional camera systems (secondary login) with access to cameras, recordings and events according to the user's granted rights.

NOTE

Before adding an account in this dialog, users must go through primary login and change their password.

NOTE

ATEAS Interlogin feature is only available in ATEAS Security UNLIMITED edition. All systems added within the previous dialog must be PROFESSIONAL or UNLIMITED editions.

The Interlogin feature differs from an UNLIMITED license as follows with all servers connected in one system as follows:

- All systems remain independent with their own license and administration.
- Event scenarios cannot be created by integrating servers from different systems.
- The user profile cannot be LOCAL (is automatically changed to DEFAULT).
- Cameras in the views must always belong to the same camera system.
- Views with cameras from others than the primary system cannot be shared.

NOTE

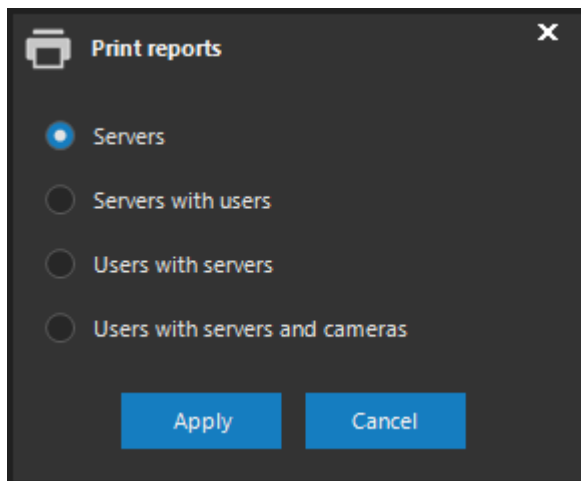
The ATEAS Interlogin feature cannot be chained. If the function is activated for a user that is already logged into the system with a secondary login, the settings do not take effect.

CAUTION

The version of systems for multiple login can be lower than the version of the system to which the user logs in primarily, however the minimum supported version is 4.5.0.

11.10.20. Print reports

The following image shows that several print reports can be created for camera servers by pressing the print button in the top right corner of the window.



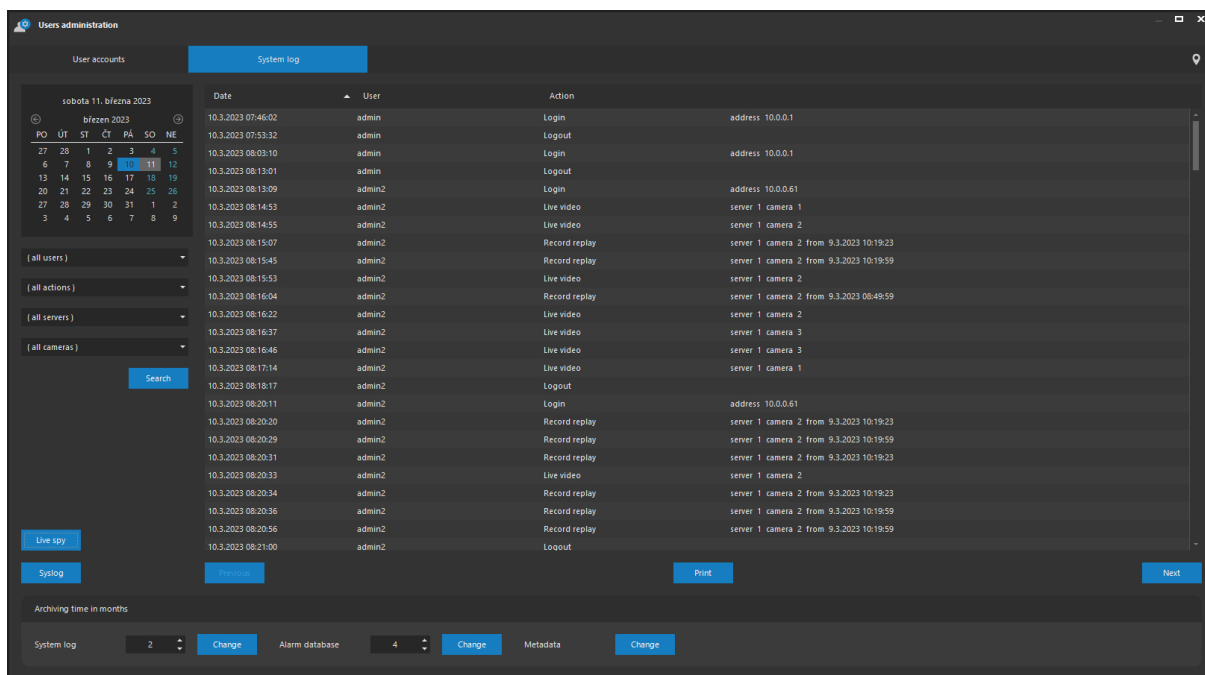
The first report displays a summary of all camera servers together with their basic information. The second report adds all user accounts to the server that can access the server. The third report, on the contrary, displays a sorted list of users together with all servers accessible by each of the users. The fourth report adds camera information to the previous report, which the user can access.

CAUTION

If the user is part of multiple groups with different permissions and his group membership is controlled by time or events, the camera list cannot be determined and the default camera list will be displayed as if the user were not part of any group.

11.10.21. System log

The system (or the administration server to be more specific) saves important events to the system log. Therefore, it is possible to check which user controlled a camera and when, or which of the users logged into the system and downloaded a record etc. The entire system log is available in the Users administration section on the System log tab.



The screenshot displays the 'Users administration' window with the 'System log' tab selected. On the left, there is a calendar for February 2023 and filters for users, actions, servers, and cameras. The main area contains a table of log entries:

Date	User	Action	address
10.3.2023 07:46:02	admin	Login	address 10.0.0.1
10.3.2023 07:53:32	admin	Logout	
10.3.2023 08:03:10	admin	Login	address 10.0.0.1
10.3.2023 08:13:01	admin	Logout	
10.3.2023 08:13:09	admin2	Login	address 10.0.0.61
10.3.2023 08:14:53	admin2	Live video	server 1 camera 1
10.3.2023 08:14:55	admin2	Live video	server 1 camera 2
10.3.2023 08:15:07	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:23
10.3.2023 08:15:45	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:59
10.3.2023 08:15:53	admin2	Live video	server 1 camera 2
10.3.2023 08:16:04	admin2	Record replay	server 1 camera 2 from 9.3.2023 08:49:59
10.3.2023 08:16:22	admin2	Live video	server 1 camera 2
10.3.2023 08:16:37	admin2	Live video	server 1 camera 3
10.3.2023 08:16:46	admin2	Live video	server 1 camera 3
10.3.2023 08:17:14	admin2	Live video	server 1 camera 1
10.3.2023 08:18:17	admin2	Logout	
10.3.2023 08:20:11	admin2	Login	address 10.0.0.61
10.3.2023 08:20:20	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:23
10.3.2023 08:20:29	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:59
10.3.2023 08:20:31	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:23
10.3.2023 08:20:33	admin2	Live video	server 1 camera 2
10.3.2023 08:20:34	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:23
10.3.2023 08:20:36	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:59
10.3.2023 08:20:56	admin2	Record replay	server 1 camera 2 from 9.3.2023 10:19:59
10.3.2023 08:21:00	admin2	Logout	

At the bottom, there are controls for archiving time in months (System log: 2, Alarm database: 4, Metadata) and buttons for 'Live spy', 'System log', 'Post', and 'Next'.

The main list of events, recorded in the log, shows the exact time of the action, username and a description and details of the action. If a live video request is logged, additional information can provide details about the exact camera server and camera. When downloading a recording, you can search for the exact time of the sequence. Actions related to movement can be provided with information about a number of a preset point etc.

NOTE

The Login action also contains the IP address used to access the system.

NOTE

Some events in the log do not necessarily require a user to be assigned, e.g. an invalid attempt to login to the system.

Log filtering

Using a calendar in the left part of the window, you can display the part of the log for the selected days. The calendar enables switching between different months. The date is always set to the current date after opening the calendar window. Under the calendar control, it is also possible to filter the system log by user, type of action, camera server or individual cameras.

NOTE

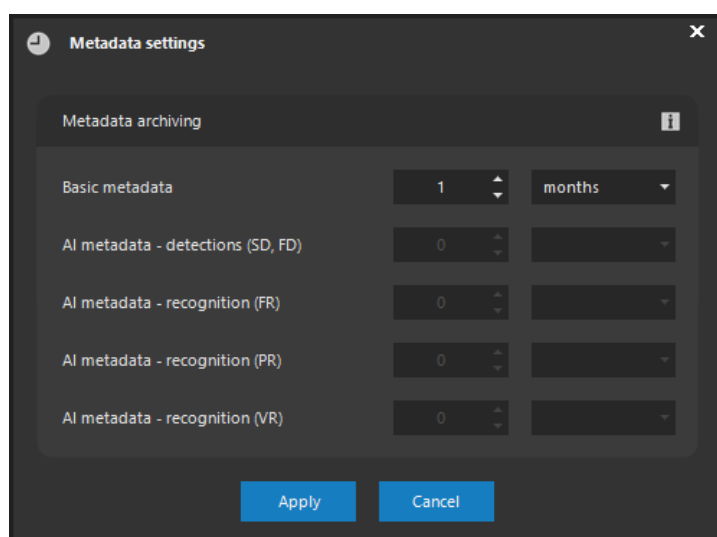
If there are too many events for a selected day, listing buttons are activated in order to ensure better orientation. These buttons enable switching between individual system log pages.

The system log is regularly cleared to ensure the size is not excessively big after a certain period of using the system. The archiving time can be set by clicking the **CHANGE** button in the bottom part of the window. The default archiving time is set to two months and can be modified from one month to one year.

Besides the option of changing the archiving time of the system log, you can also change the default archiving time of the alarm log in the bottom part of the window. The archiving time can be set by clicking the **CHANGE** button. The default archiving time for the alarm log is set to four months and can be modified from one month to four years.

Metadata archiving

Similarly to each camera server, under active metadata centralization, metadata archiving can be configured for the administration server using the **CHANGE** button. In administration server context, only those metadata groups can be altered that can also be centralized.



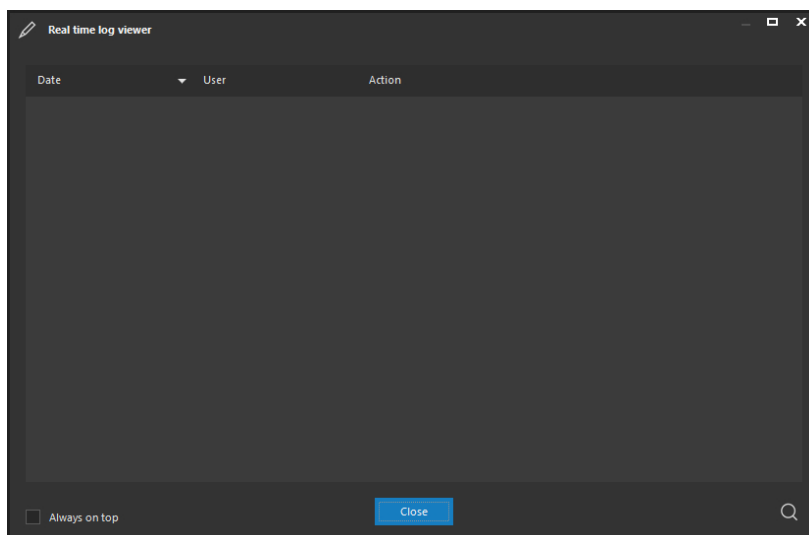
Printing the log

The system log can be printed on any printer including a PDF file printer by pressing **PRINT** in the top right corner of the window. Once the print report is displayed, you can move between pages using the Page up and Page down keys.

NOTE

Given that the log can be very large, only the current section displayed in the window is printed. The print process must be repeated to print additional sections. The section of the log and their total number is included in the header of the print report.

The system log, displayed in the basic window, is static. Therefore, it is not automatically updated for actions to be recorded appear. To refresh log data, select either a day in the calendar or a user. If you wish to view the log online including the automatic refresh feature, press the **LIVE SPY** button.



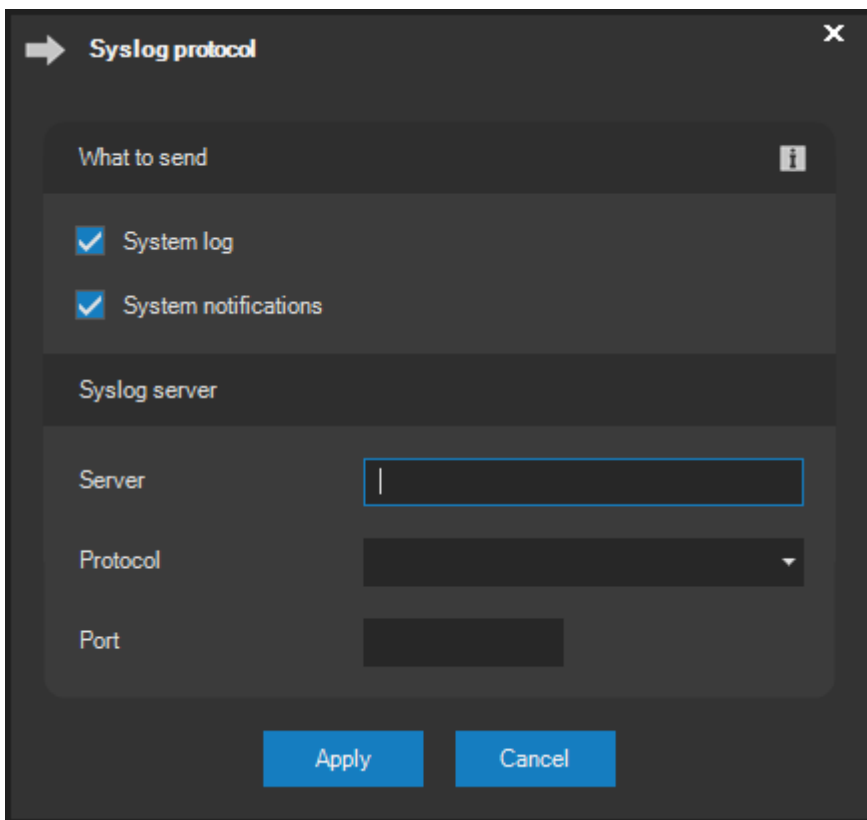
This window can remain opened even after finishing work in the administration section. It provides a live and automatically updated preview of actions recorded in the system log as well as additional information for individual actions. The Always on top checkbox ensures that this window will not be overlapped by other windows.

NOTE

The maximum log history size is modified in the live spy window. When the maximum size is reached, the oldest actions will be constantly removed, preventing the list from growing disproportionately. Deleted actions will remain searchable in the history of the log.

11.10.22. Syslog protocol support

ATEAS supports the Syslog protocol, which is used for standardized log reporting from any system to Syslog servers. These servers collect logs from all types of systems and feature options to filter, search etc. To configure the Syslog connection server, press the **SYSLOG** button.

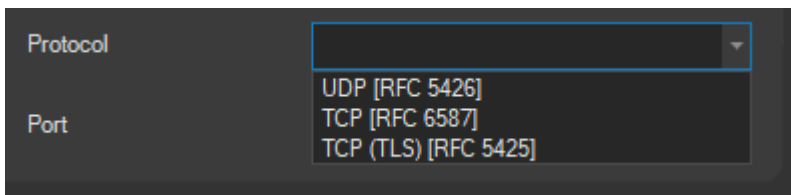


The image shows a 'Syslog protocol' configuration dialog box. It has a title bar with a back arrow, the text 'Syslog protocol', and a close button (X). The dialog is divided into two main sections. The first section, 'What to send', contains two checked checkboxes: 'System log' and 'System notifications'. The second section, 'Syslog server', contains three input fields: 'Server' (a text box), 'Protocol' (a dropdown menu), and 'Port' (a text box). At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.

ATEAS implements the Syslog protocol compliant with RFC 5424, which is a newer version of the protocol, compared to the originally defined standard.

The Syslog dialog allows you to select whether only system log items will be sent, as shown directly in the ATEAS system log, or if also system notifications such as camera server disconnections, media store failures or midnight keep-alive messages will be included.

Under Syslog server, you can enter the address or name of the Syslog server, choose the transfer protocol, as well as the port. The following options are available for the protocol selection. Each option is associated with a different RFC document.



Your Syslog server must therefore fully support the selected protocol in order to receive messages.

CAUTION

The options not only differ by transport protocol, but also by the method of concatenating individual Syslog messages as per the respective RFC, resulting in slightly different data to be sent out on each occasion.

If the UDP protocol option is selected, the standard Syslog port 514 is automatically pre-set, but can be changed.

If the TCP over TLS protocol option is selected, the standard Syslog port 6514 is automatically pre-set, but again can be changed.

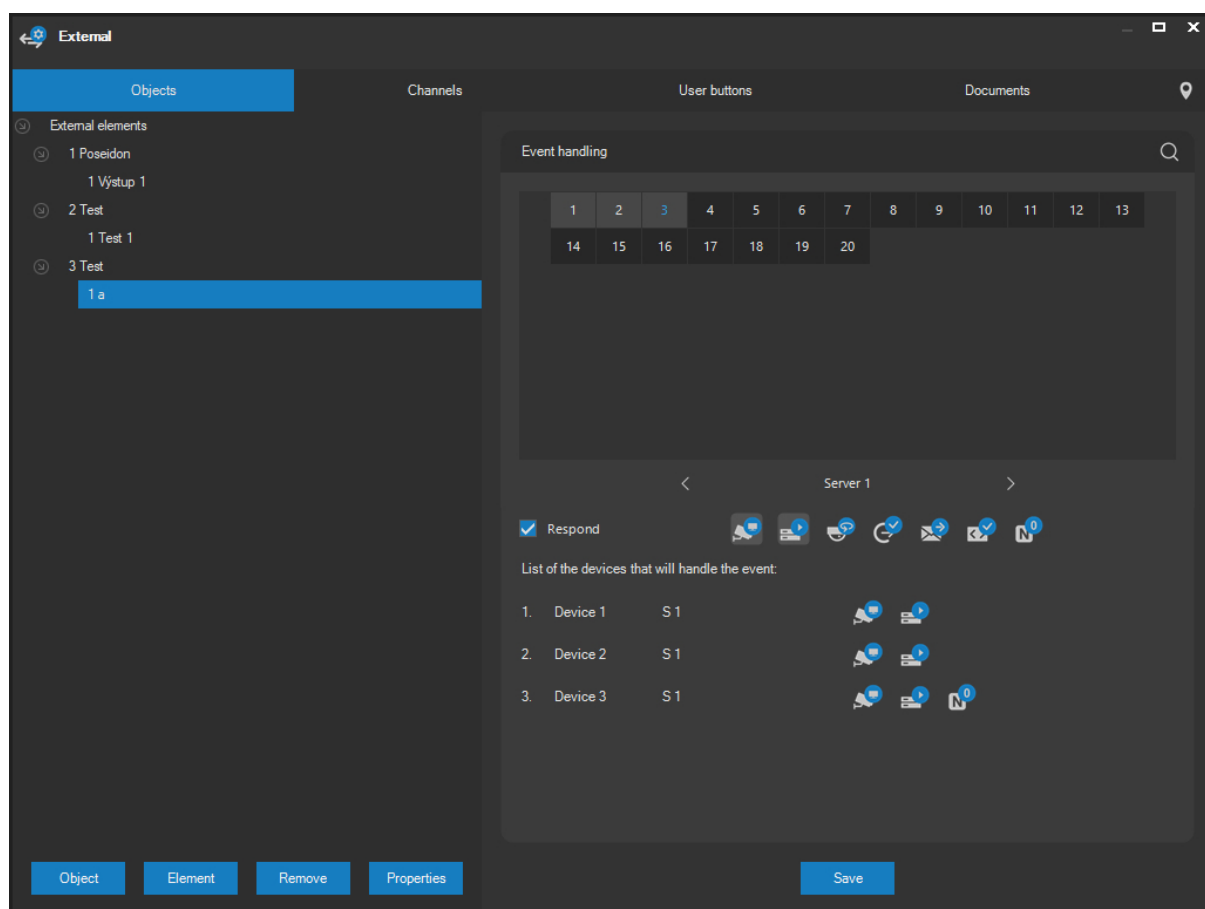
The standard does not specify any port for the TCP option. Nevertheless, the port is pre-set to 1514, which (as with other values including 2514 and 3514) is the most commonly used value.

11.11. External

The External item of the Administration menu opens a section where you can create and edit the virtual structure of objects and their elements. Based on messages received and information pertaining to these objects, you can start previously prepared event scenarios. This way, you can force a reaction within the camera system depending on external events within another system.

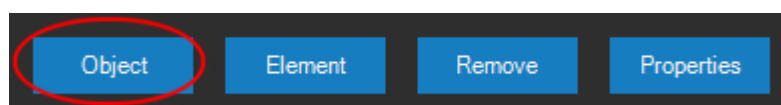
11.11.1. Virtual structure of objects

Virtual structure of objects can be created on the Objects tab. The structure has two levels as shown in the following picture.

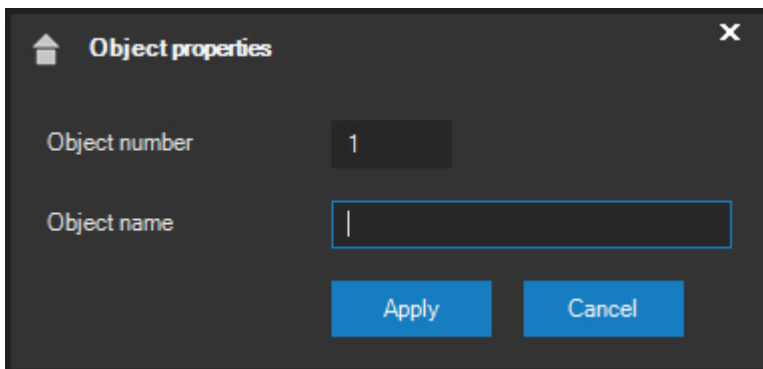


With respect to the terminology used in ATEAS Security, the first level is called an object or a group, while the second level is called an element. The external object structure can be associated with any given remote security system, securing objects with security devices etc.

In order to add a new object (group), use the corresponding button under the list of objects.



It is necessary to enter the object's number and name into the following dialog.

A dark-themed dialog box titled "Object properties" with a close button (X) in the top right corner. It contains two input fields: "Object number" with the value "1" and "Object name" which is empty. At the bottom are two blue buttons labeled "Apply" and "Cancel".

The system will automatically offer the lowest positive unassigned group number. The number offered does not have to be accepted and can be changed. However, it has to be unique (system will display a warning message if it detects duplicity). The system also works with an internal limit for the total number of groups and elements. The maximum number of groups is 10 thousand with up to 99 elements in each group, while the maximum number value for the element can be a five-digit number. The application will display a warning message if these limits are exceeded.

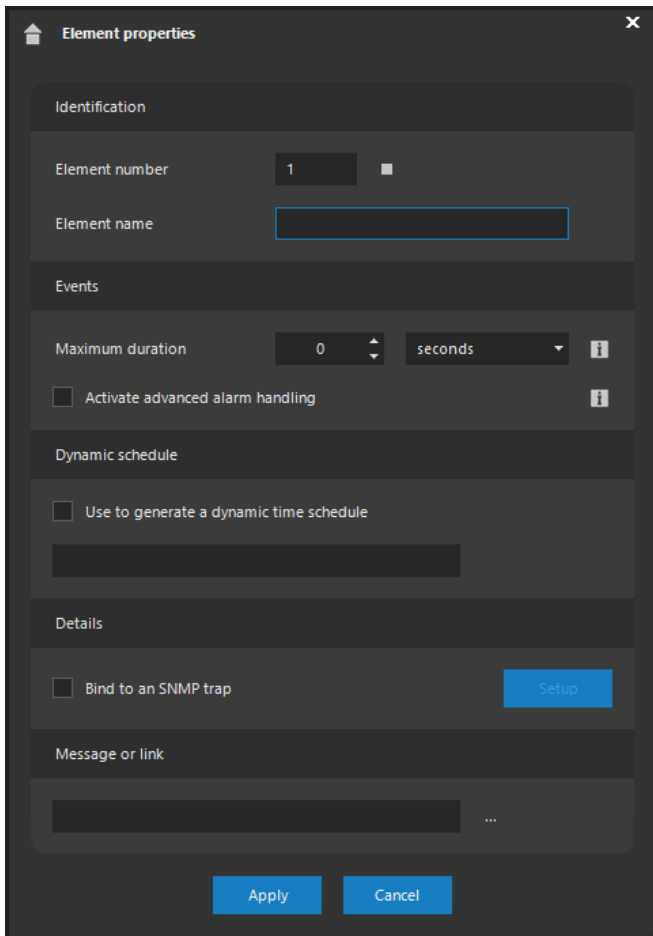
Click the corresponding button to create a new element.



However, to successfully use this button, you need to create a group (or its element) where the new element will be placed. Otherwise, a warning will be displayed and it will not be possible to create a new element. A dialog will be again be displayed where you will be asked to enter a number (or accept the offered number) identifying the element, name of the element and the maximum event duration in minutes. The purpose of this parameter is consistent with camera event input configuration. It specifies the maximum event duration unless the event is ended by the ATEAS API interface with a SNMP message.

An element can be bound to any given SNMP trap by checking the corresponding option. A separate subchapter devoted to SNMP is included further.

An element will be added to the specified group after confirming the message dialog by pressing the **APPLY** button.



Next to the element number, the currently assigned color is displayed. The color can be changed by clicking on the color symbol and selecting any user-defined color. The color is then used for events displayed on the replay timeline when replaying recordings.

TIP

You can quickly restore the original default color by using the right mouse button.

Checking the Activate advanced alarm handling option activates the extended alarm handling mode for the given event source. See also the separate Alarm handling mode subchapter for more information.

Similar to camera events, an object event may include a message to the user, which can be entered in the Message or link section. A different text message can be added to each element, or – using the button next to message – you can also add an entire PDF document or a hyperlink (must start with

http or https protocol). The method of inserting a document and the syntax for attaching the document are the same as with camera events, where the method of inserting documents is described.

Any element or entire object can be removed by pressing the button with the remove symbol. A message dialog must be confirmed before the actual deleting process takes place. All elements of a deleted object will also be removed beyond recovery.



Basic parameters of a selected object or element can be modified by pressing the button labeled Properties.

NOTE

The dialog for adjusting basic properties is identical to the dialog for creating a new object, the only difference being that this dialog does not enable editing certain information.

11.11.2. Creating event scenarios

As is the case for creating camera event inputs (motion detection, alarm inputs, failure, custom events such as sabotage or sound detection), you can create event scenarios for individual elements, divided into groups. If a sensor, connected through a central and ARC triggers an alarm, you can automatically send selected camera feeds to operators, trigger alarm recording, position cameras or switch them to an alarm tour, send an e-mail, activate outputs etc. All of mentioned actions can be performed on several camera servers. Setting an event scenario is completely identical with the procedure for setting the scenario for individual cameras. For further information about setting and modifying event scenarios, see the subchapter regarding camera management

Event handling

1234567891011

121314151617181920

<Server 1>

☒ Respond



List of the devices that will handle the event:

1. Device 1S 1

2. Device 2S 1

3. Device 3S 1

4. Device 4S 1

The only significant difference is the **SAVE** button which is placed under the virtual structure of objects. This button explicitly saves the changes performed in the event scenario. If you attempt to close the form or switch to another element without saving your changes, the application will display a warning message. If you press the **NO** button, the application will not continue in started action and you will be able to save all performed changes.

ATEAS

?

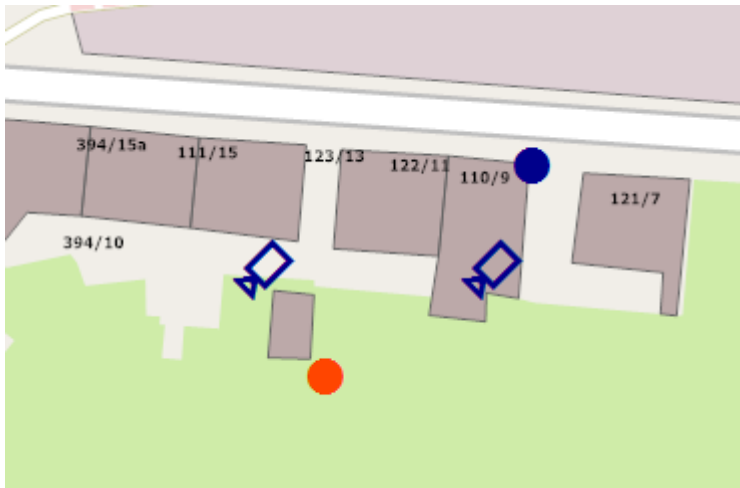
The event scenario of an element has not been saved. Continue without saving changes?

Yes

No

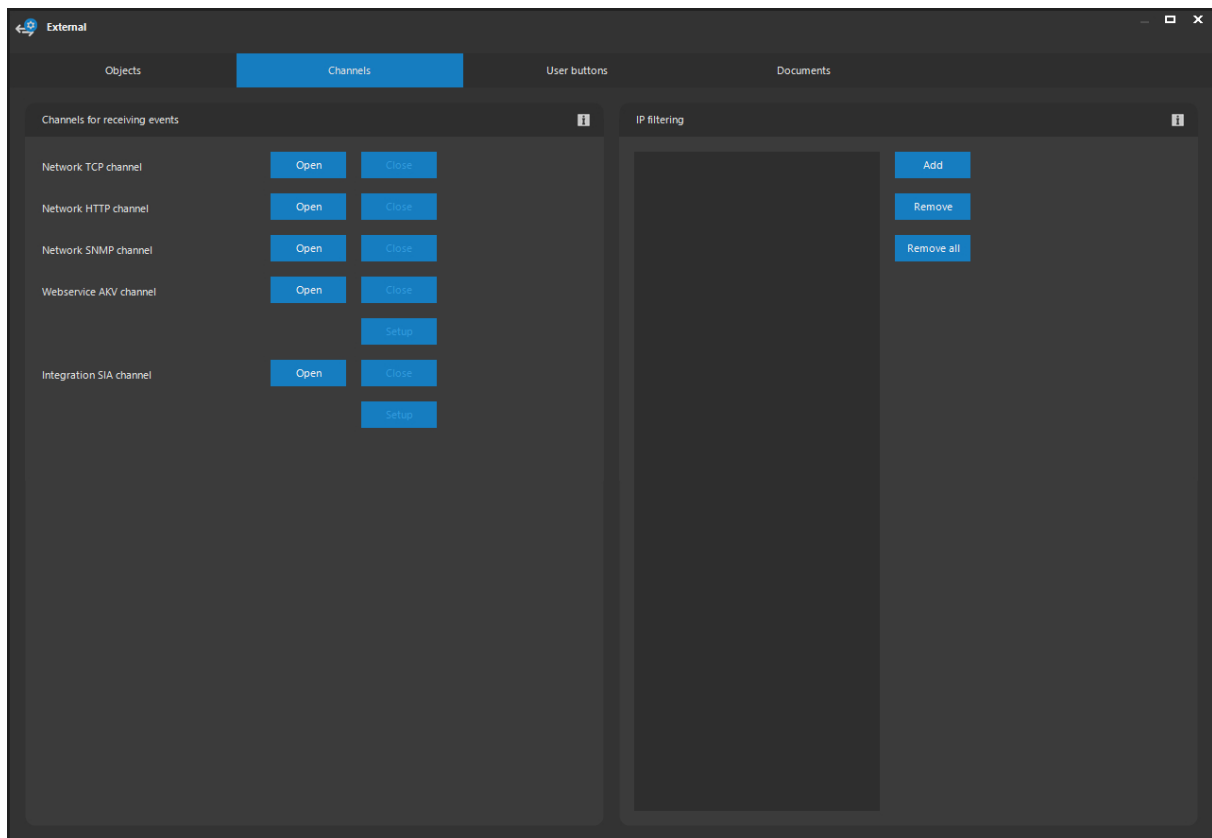
11.11.3. Locating elements in the map

Similar to cameras, external elements can also be located in maps. The process of placing an element into the map is analogous to the process used for cameras and is described in the chapter Locating cameras in the map.



11.11.4. Communication channels

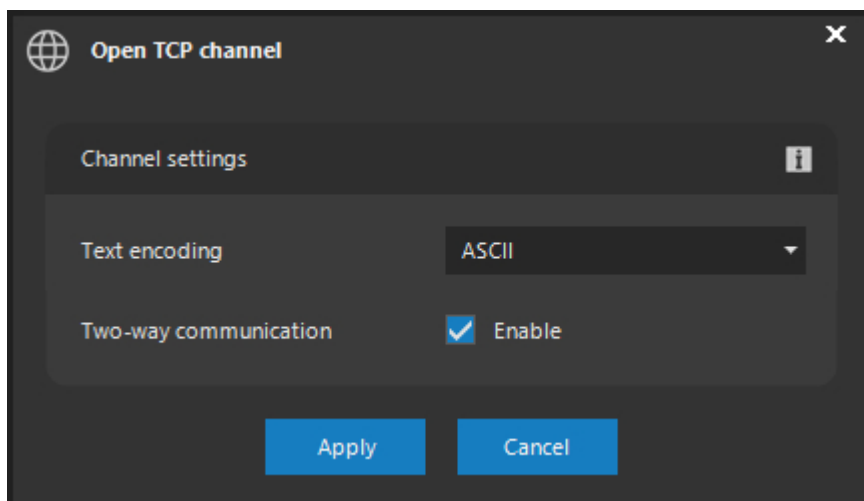
Using ATEAS API, you can forward information to the ATEAS Security system. This information is related to an event (alarm) triggered by any of the elements. You can eventually forward information related to end of an event (not necessary if maximum event duration is configured properly). External systems can use various communication channels to forward this information in text format. Use the Channels tab to manage the channels.



11.11.5. Network TCP and HTTP channels

The TCP and HTTP channels use the ATEAS API interface described in an appendix to this manual. The SNMP channel uses SNMP traps and is described further below in this chapter. After administration server installation, all channels are closed and must be opened using the **OPEN** button.

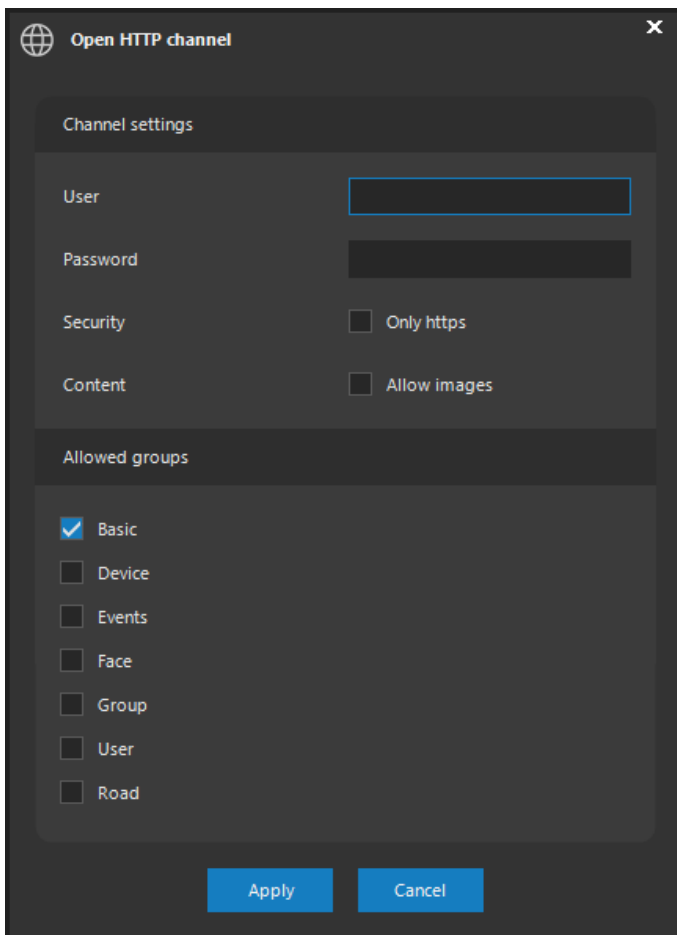
When opening the TCP channel, text encoding must be chosen. Optionally, two-way communication can be enabled.



TIP

When two-way communication is disabled, you will be able to receive data using the connection, but you won't be able to send any commands.

When opening the HTTP channel, you may enter a username and password. If set, they will be required for authenticating the request. Additionally, you can enforce an encrypted connection using the TLS protocol. The Allow images option allows attaching overview or detail image data to the HTTP interface. This can be used e.g. for publishing an overview image of the car and a detailed image of the license plate after it was recognized.



Open HTTP channel

Channel settings

User

Password

Security ☐ Only https

Content ☐ Allow images

Allowed groups

☒ Basic

☐ Device

☐ Events

☐ Face

☐ Group

☐ User

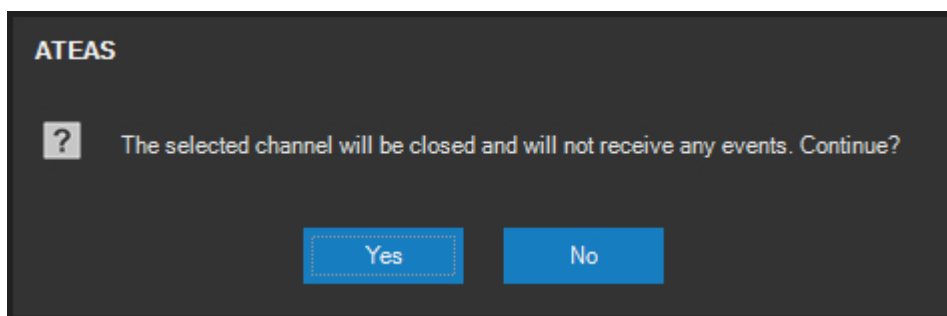
☐ Road

Apply Cancel

In the Allowed groups section, you can restrict the allowed API groups to the required groups only thus preventing other sensitive groups from being exploited.

A button providing information on communication channel parameters will become available together with each successfully opened channel.

The **CLOSE** button will also become available. Using this button, you can close the respective communication channel. This action requires confirmation. Events cannot be received through a closed channel.



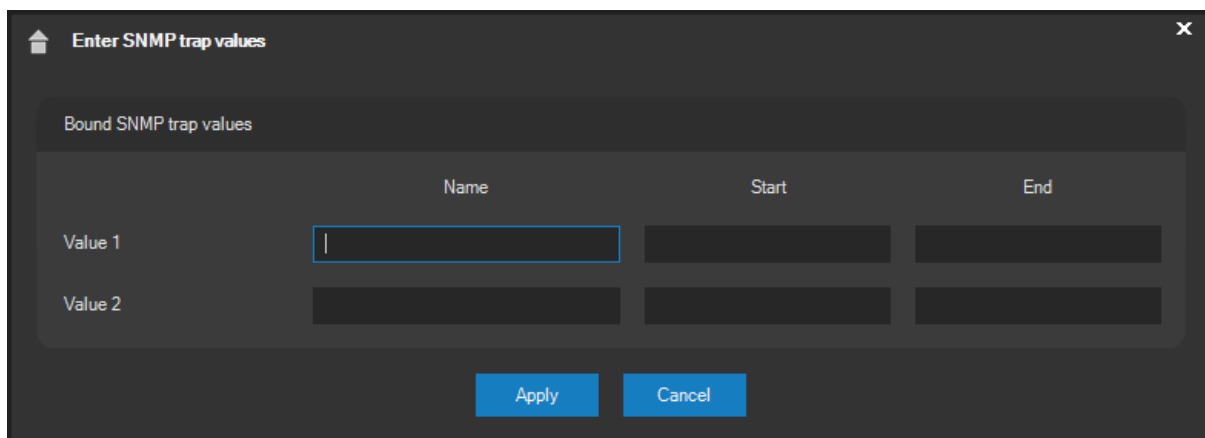
NOTE

The reception of commands through the TCPIP channel can be restricted using the IP filter feature (see the respective subchapter).

11.11.6. Network SNMP channel

The administration server can receive events and respond with complex event scenarios. The type of external device providing events does not matter, assuming the external device can send an event notification in a way supported by the server. Events can be received using either an established TCP connection, HTTP commands or the SNMP protocol. Receiving an event over SNMP is based on SNMP standards, so an event is received in the form of an unsolicited SNMP message (SNMP trap), port 162 by default.

SNMP message values activating the element can be assigned to any particular object and its element. Use the Bind to an SNMP trap option to connect the element to specific SNMP values and click the **SETUP** button to display the dialog window as follows.



	Name	Start	End
Value 1			
Value 2			

NOTE

Binding elements to random SNMP traps is available starting with ATEAS Security PROFESSIONAL edition.

At least the name of the first value and its Start field shall be entered in this dialog. An event occurs when the value entered in the Start field and name entered in the Name field appear in the received SNMP trap. If the device is capable of informing about the end of an event using an SNMP trap, the expected end value of the event can be entered into the End field.

NOTE

If the device cannot terminate events using separate SNMP traps, it is recommended to set the maximum event duration in element settings. The event will terminate after the specified interval expires.

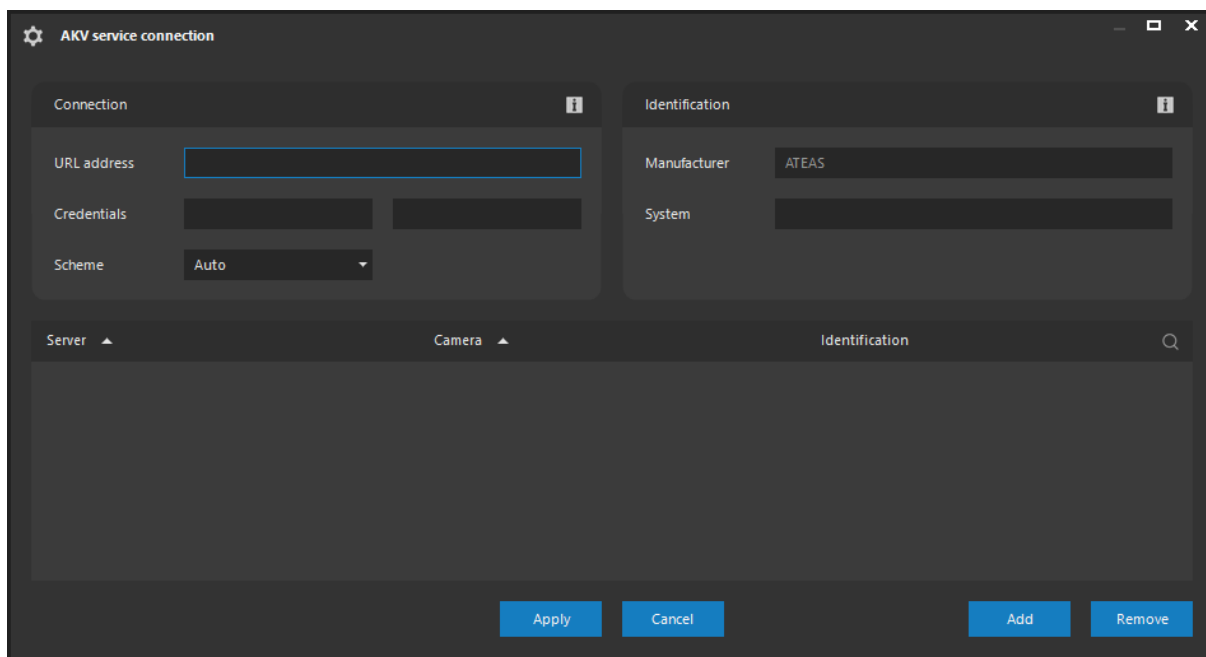
The SNMP traps of some devices can consist of many values and evaluating the start of an event solely based on a single SNMP trap value is not always possible. Therefore, two values may be entered. In order for an event to occur (or end) when two values are used, the SNMP trap must always contain both names with the Start (or End) values.

NOTE

If both values are used, the actual order of the values within the SNMP trap does not matter. Moreover, the values are not required to appear immediately one after the other.

11.11.7. Web service AKV channel

The AKV web service is operated by state administration bodies of the Czech Republic and centralizes data about LP detection and recognition from various systems.



The screenshot shows a window titled "AKV service connection" with a settings icon. It contains two main sections: "Connection" and "Identification".

- Connection section:** Includes fields for "URL address", "Credentials" (split into two input boxes), and a "Scheme" dropdown menu currently set to "Auto".
- Identification section:** Includes fields for "Manufacturer" (set to "ATEAS") and "System".

Below these sections is a table with three columns: "Server", "Camera", and "Identification". The table is currently empty. At the bottom right of the window are four buttons: "Apply", "Cancel", "Add", and "Remove".

To connect to the service, it is necessary to receive the address where the service is running, login details, and also the identification of the system and cameras that will be able to send data. Using the **ADD** button, it is possible to display a window to search for a camera to assign to the service. After assignment, it is necessary to add the identification of the given camera to the Identification column. The camera can be removed at any time using the **REMOVE** button.

NOTE

The respective authority is expected to register ATEAS as an approved product to send data.

Afterwards, camera details, time data, LP in plain text format together with an image detail of the plate and an overview image will be published using this web service.

CAUTION

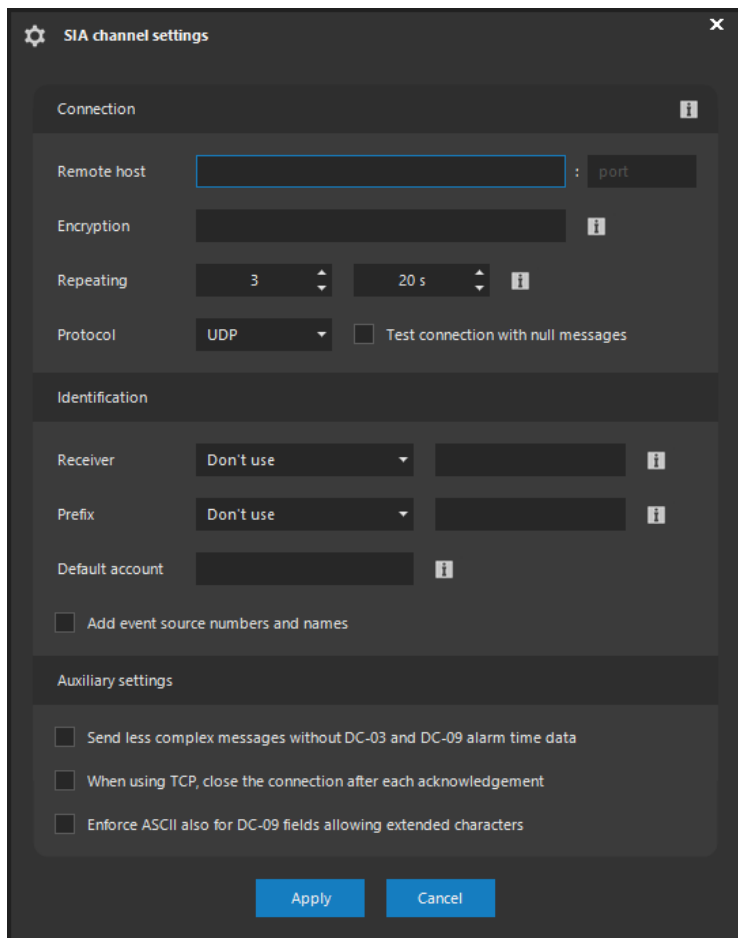
Sending image data will be active regardless of the send image data option configured for the HTTP communication channel.

11.11.8. SIA integration channel

This channel allows sending alarm information using the SIA protocol, which is an industry standard for devices that aggregate alarms from different systems for centralized reception, processing, and clearing. ATEAS supports the DC-03, DC-07, and DC-09 standards for transmission over IP.

NOTE

Opening the SIA integration channel is possible starting with the ATEAS Security PROFESSIONAL edition.



SIA channel settings

Connection

Remote host: [text field] : port

Encryption: [text field]

Repeating: 3 [dropdown] 20 s [dropdown]

Protocol: UDP [dropdown] ☐ Test connection with null messages

Identification

Receiver: Don't use [dropdown] [text field]

Prefix: Don't use [dropdown] [text field]

Default account: [text field]

☐ Add event source numbers and names

Auxiliary settings

☐ Send less complex messages without DC-03 and DC-09 alarm time data

☐ When using TCP, close the connection after each acknowledgement

☐ Enforce ASCII also for DC-09 fields allowing extended characters

Apply Cancel

Connecting to a remote host includes entering its address or name and its port number, optionally the network protocol or encryption.

NOTE

SIA uses the AES encryption with 128, 192 and 256-bit keys. Therefore, an identical key with 32, 48 or 64 characters in hexadecimal form is expected to be entered on both sides.

According to the SIA standard, unacknowledged messages are repeated several times, the number of trials and the time interval are adjustable. For TCP connections, it may be appropriate to test the connection with zero SIA messages, to ensure lower latency of alarm reception after a connection failure.

In the Identification section, it is necessary to fill in the default account (object) as a unique identification for the central receiver. This value can be in the range of 16 bytes. Optionally, the identification and name of the event source can be added.

TIP

The account value can also be entered in hexadecimal form using the 0x prefix.

If required by the central receiver, it is possible to extend the identification by entering a Receiver (least specific identification) or a Prefix. ATEAS offers here the possibility to inject some other identifiers automatically (ATEAS ID, Server ID).

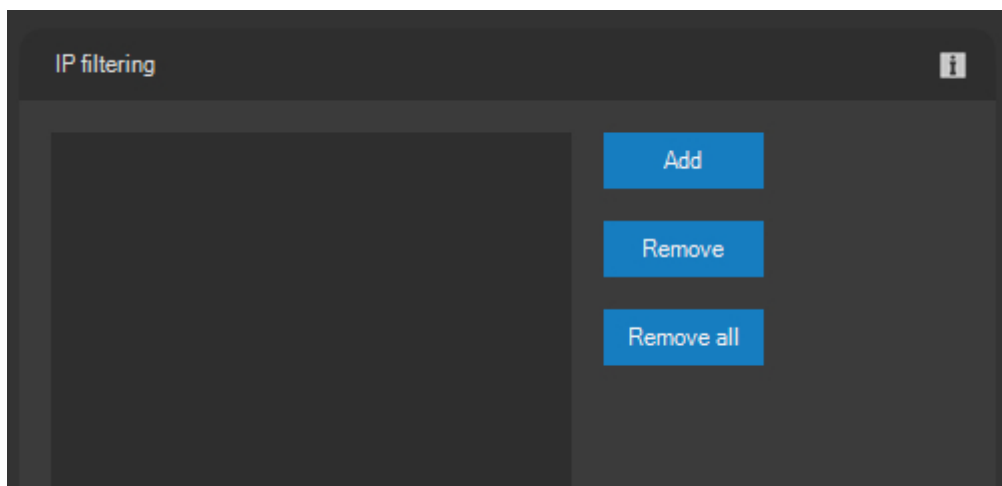
In the Auxiliary settings section, you can adjust the behavior to better suit some devices. For example, you can omit the event time (the message sent time will be used), create a new TCP connection for each message, or force ASCII characters even in parts of the message where the DC-09 standard allows extended encoding.

NOTE

Moreover, the camera identification can be adjusted for each camera in the SIA identification camera settings section.

11.11.9. Filtering IP addresses

The TCP channel is not secured so an IP filtering tool can be used to restrict the communication to selected addresses only.



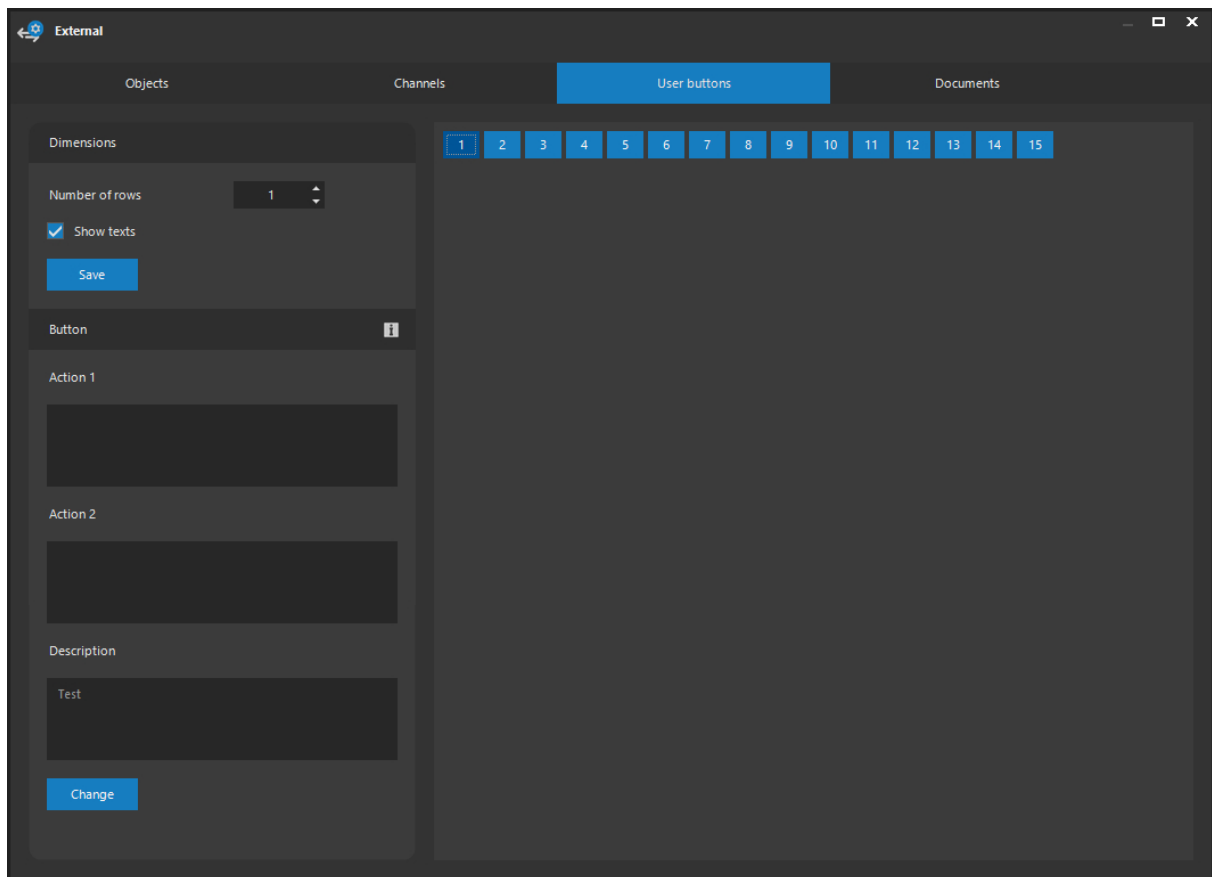
IP address can be added to the list by pressing the **ADD** button. If at least one IP address has been added to the list of allowed IP addresses, the administration server will only accept external events forwarded through the TCPIP protocol from a specified IP address. The list can contain any number of IP addresses. Address can be deleted by pressing the **REMOVE** button. Press the **REMOVE ALL** button to delete complete list.

CAUTION

If there is no IP address in the list, all events or other ATEAS API commands forwarded through TCPIP from any network address will be accepted without going through the verification process.

11.11.10. User buttons

User buttons can be configured on the third tab of the administration window under the External section. User buttons are then displayed to authorized users in a separate window and these users can execute predefined commands over the http or https protocol via these buttons. These commands can affect the functions of IP cameras, which could otherwise not be able to be controlled, or can affect any external device available over the http protocol.



In the first step, it is necessary to set the number of user button rows that will be displayed to the user. After pressing the **SAVE** button, a preview of user buttons is displayed in the main window area.

NOTE

When the number of rows is changed, the changes in open windows with user buttons are reflected immediately, including the situation when the number of rows is set to zero, after which the window is automatically closed.

NOTE

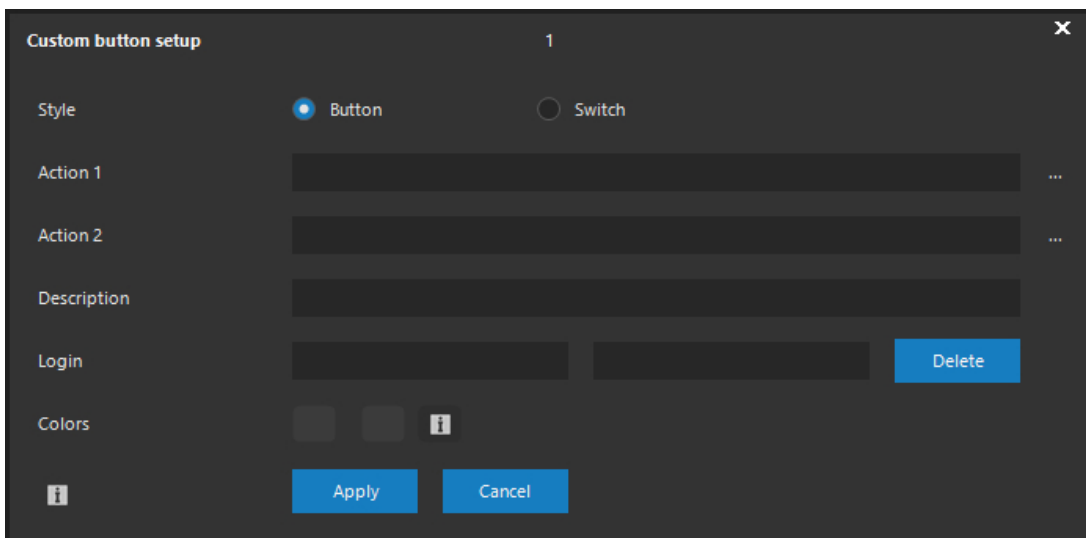
The window containing user buttons can only be displayed by a user having the relevant rights or who is part of a group, which has these rights assigned.

NOTE

The use of user buttons is automatically logged into the system log.

In order for the user button to hold a function, style, specific actions and description must be defined for the button using the **CHANGE** button. Entering login credentials is optional and only needed for an action that requires authentication.

If the Show texts option is active, users will be able to see the description directly, instead of seeing the button number only with its description in a tool tip.



The image shows a 'Custom button setup' dialog box with a dark theme. It has a title bar with 'Custom button setup' and a close button 'X'. The dialog is divided into several sections: 'Style' with radio buttons for 'Button' (selected) and 'Switch'; 'Action 1' and 'Action 2' with text input fields and a three-dot menu icon; 'Description' with a text input field; 'Login' with two text input fields and a 'Delete' button; 'Colors' with two color swatches and an information icon; and a bottom section with an information icon, an 'Apply' button, and a 'Cancel' button.

The user button can be configured as an actual button or switch button. The button can be used to start an action, while the switch button remains pressed when clicked and a different action can be started after the switch button has been released. The user button configured as a switch button is therefore ideal for controlling external devices that can be switched on and off.

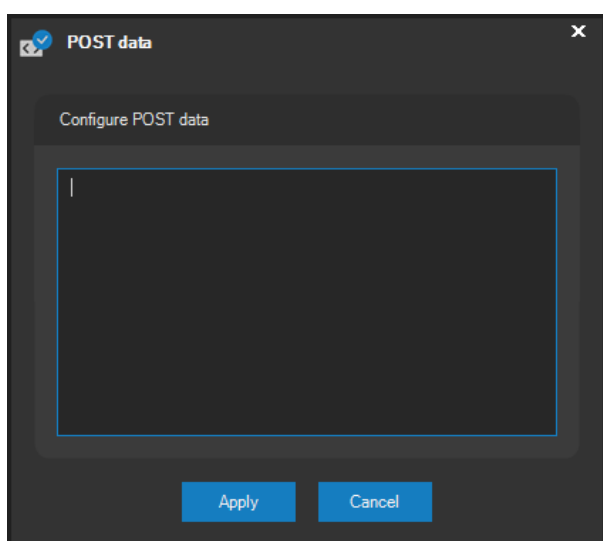
NOTE

The ATEAS administration server maintains the states of all user buttons of the switch button type. The switch button states are therefore automatically synchronized for all users that are currently logged on.

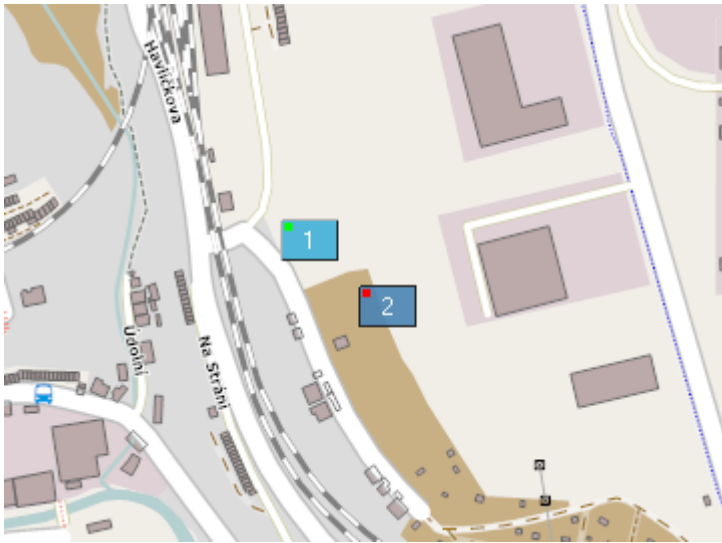
After filling out the dialog for each button, the actions and descriptions are displayed in the relevant text fields in the main administration window.

Up to four parameters can be included with an action. To add a parameter to the command, use <P1> through <P4>. These parts of the command are variable and can be filled with a concrete value during the execution of the user button. It is convenient to use parameters for commands, where we would like to give the user freedom to define any of his parts (e.g. determining the activation period of a device etc.).

Even though you can pass complex URLs with CGI command parameters etc., some devices may require a different HTTP method than GET to invoke an action. Using the button behind the URL text box an additional dialog can be opened to insert data to be sent using the HTTP POST method.



User buttons can be localized in the map. This is beneficial in all cases, where user buttons control external devices, which can be localized into maps. The user can therefore control an external device directly via the button in the map. Another possible way to use the localized user buttons is to execute event scenarios linked to this button (for example positioning PTZ cameras to the given place via presets). In this case, a custom event with a system name ATSBUTTON<n> shall be created for a camera, see the chapter about custom camera events for more information.



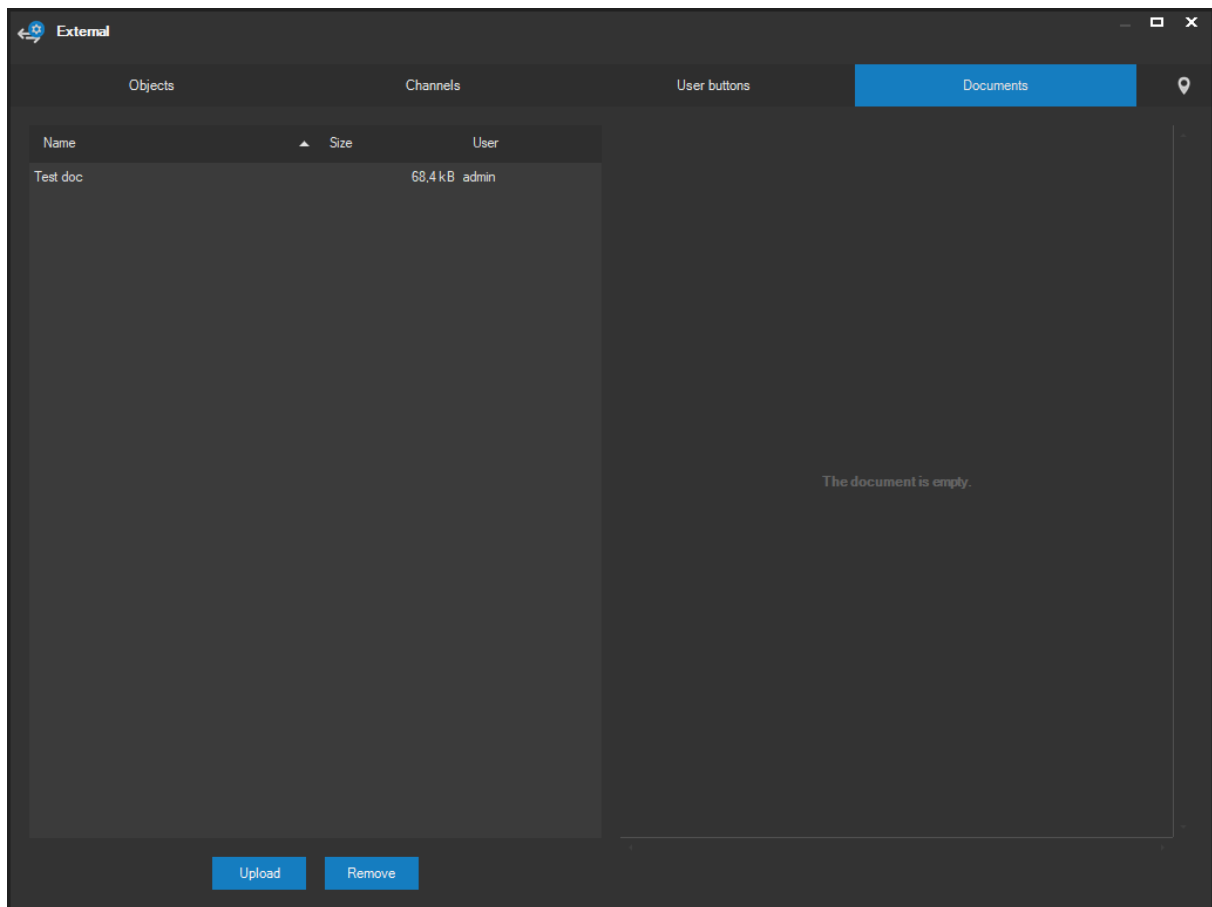
NOTE

The user button localization process is identical to the camera localization process.

By default, buttons placed in the map use some basic colors to differentiate the states of a switch button. These colors can be changed and also forced to appear in the user button window by configuring the colors in the Colors item. It is possible to configure different colors for a released or pressed state of a button.

11.11.11. Document integration

On the Documents tab, you can upload documents to the system and later use them in various situations that support camera security processes. For example, instead of displaying simple messages to users in alarm situations, one can display a document with more detailed instructions, building plans or any other helpful information.



The left part of the window shows a list of all uploaded documents including their name, size and the user who uploaded the document. Click on the document to show a preview of the document in the right part of the window.

NOTE

PDF documents are supported and can therefore contain various formatted text, images, diagrams, tables etc.

NOTE

No additional components are necessary to install to use the PDF documents as ATEAS natively supports the PDF format. Thus, all you need is to install the camera system client to have the full PDF support.

To upload a new document, use the **UPLOAD** button. After entering the name of the document, a standard dialog will be used to browse for the document and upload it. Use the **REMOVE** button to delete any given document.

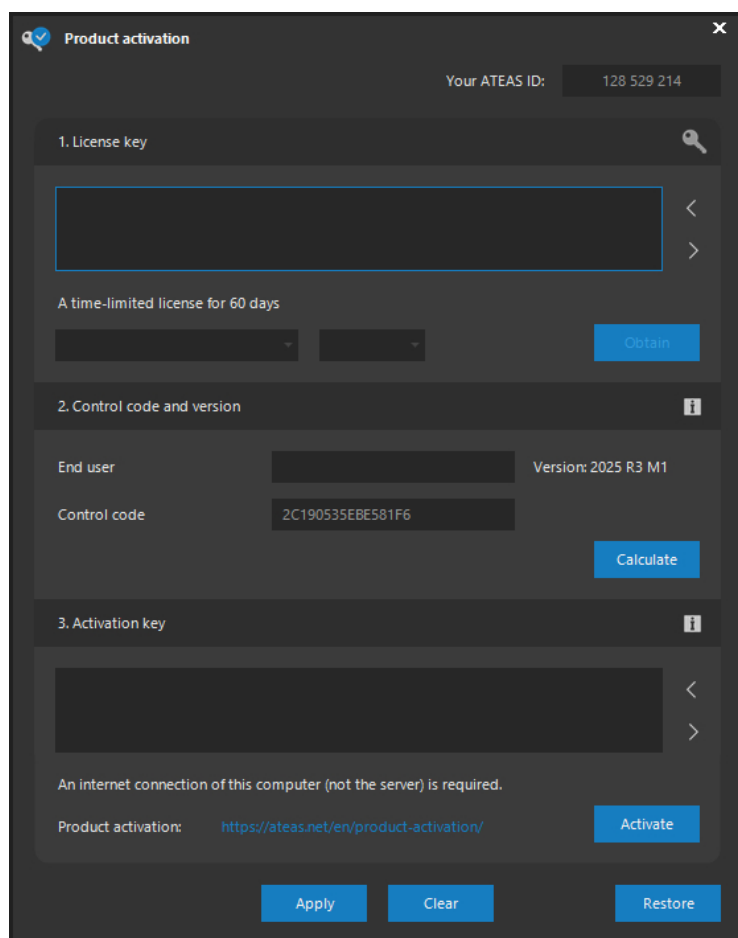
CAUTION

The size of documents to be uploaded is limited.

11.12. Licensing and activation

11.12.1. License keys and their activation

Entering the license key can be performed after the system (administration server) installation or anytime when working with the system. This will set the initial (or upgrade the existing) product edition, number of cameras and simultaneous client access licenses. You must activate every license number over ATEAS servers.



The screenshot shows the 'Product activation' window with the following sections:

- Header:** 'Product activation' title bar, 'Your ATEAS ID: 128 529 214'.
- 1. License key:** A large text input field for the license key. Below it, a note states 'A time-limited license for 60 days' with two dropdown menus and an 'Obtain' button.
- 2. Control code and version:** Fields for 'End user' and 'Control code' (containing '2C190535EBE581F6'). The 'Version' is set to '2025 R3 M1'. A 'Calculate' button is present.
- 3. Activation key:** A large text input field for the activation key. Below it, a note states 'An internet connection of this computer (not the server) is required.' and a link for 'Product activation: <https://ateas.net/en/product-activation/>'. An 'Activate' button is present.
- Footer:** 'Apply', 'Clear', and 'Restore' buttons.

When upgrading a license key, the administration server will increase the total amount of cameras which can be connected to the system. This amount is automatically increased for HOME or PROFESSIONAL editions for an already existing camera server. License distribution for UNLIMITED edition, which allows creating multiple camera servers, however, shall be carried out manually.

The license key number you purchased shall be entered in the License key section. This license number can be copied or inserted from the license file that was attached to the activation e-mail. Importing the license key from the license file can be performed via the white arrow button. The license key is decrypted automatically and the edition and camera number appear above the key.

If you have not purchased a license number, you can automatically obtain a trial license for 60 days. To do this, simply select the edition, number of cameras and use the **OBTAIN** button. You can upgrade from a trial license to a commercial license without any time limit at any time.

CAUTION

It is not possible to downgrade the system license to a lower edition or number of cameras. This should be kept in mind if you plan to upgrade to a commercial license later.

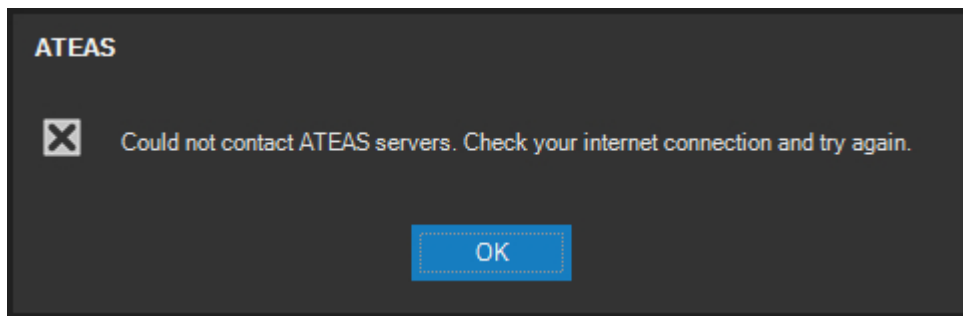
The control code section contains a reference number for your system. This number has to be used if you are activating the system manually through the manufacturer's website ateas.net.

Besides the basic information about the computer, the control code is also bound to the name of the end user of the purchased license, which shall be entered during activation followed by pressing **CALCULATE** to generate the control code.

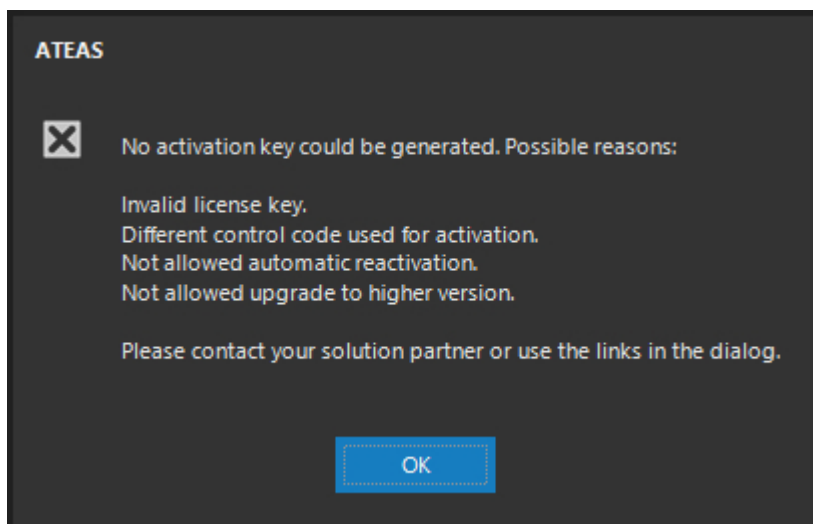
CAUTION

A valid end user name must be entered. System users can display the name at any time, and provided the name is incorrect, they shall request the name to be corrected. A system with an invalid end user name is considered to be improperly licensed.

Every license key needs to be activated. If your computer (the camera system client) has an internet connection, you can obtain the activation key within several seconds by pressing the **ACTIVATE** button. If you cannot connect to the ATEAS servers, the following message will appear.



If the connection is established successfully, but your attempt to activate your license fails, the warning message will look like the picture below.



In the first case, you will need to check your internet connection and eventually activate the license via the ATEAS website. In the second case, the attempt to activate the license was actively refused. This can happen if you attempt to activate the same license number for a second time with a different control code, or because you made a mistake while entering the license number. This could also potentially refer to an unauthorized upgrade to a higher version. If you have no upgrades available, your license number cannot be activated with the new product version. If the activation continues to fail, try to activate the product directly over our website, which will provide you with a more detailed error description causing your activation attempts to fail.

NOTE

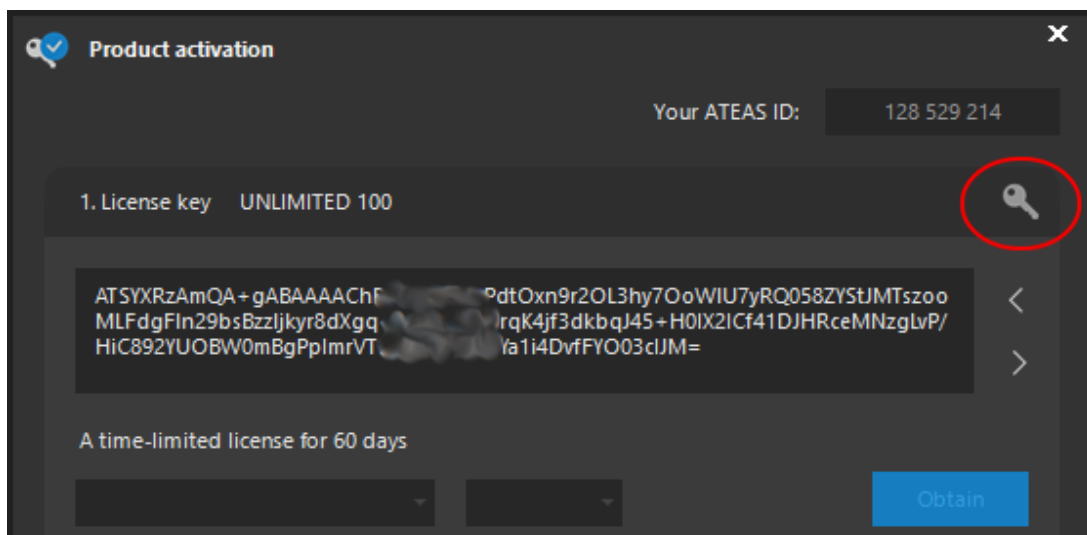
If you reinstall ATEAS software completely within the current environment of your computer and operating system, you will still be able to activate the license again.

With the exception of the trial licenses, activated systems display the ATEAS ID in the license dialog, which unambiguously identifies your system. This ATEAS ID is required for most tasks associated with the given installation, such as extending the license etc.

11.12.2. System extensions

In case of extending the system by additional cameras or moving to a higher edition it will be necessary to provide new license key and activate it. The license can be inserted as described above, by copying it into the License key field or by importing it from a file.

If your camera client is online, the new license for your system is automatically recognized and will be indicated by a flashing license key symbol.



After clicking on this symbol, you will be prompted to confirm the insertion of a new key, which will automatically appear in the License Key field. After that, you can proceed with its activation.

11.12.3. Activating new versions

After updating to a new version, you will need to reactivate your existing license. Activation is possible without restrictions if the system uses a trial license. In the case of a commercial license, the system must have an active ATEAS PMA, which grants you access to all new ATEAS versions.

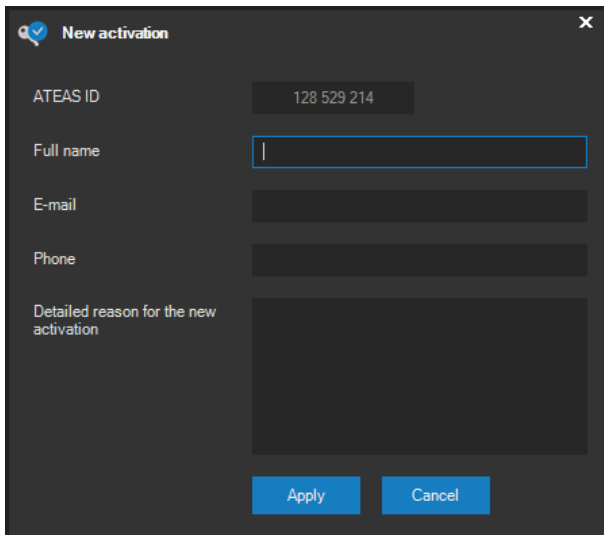
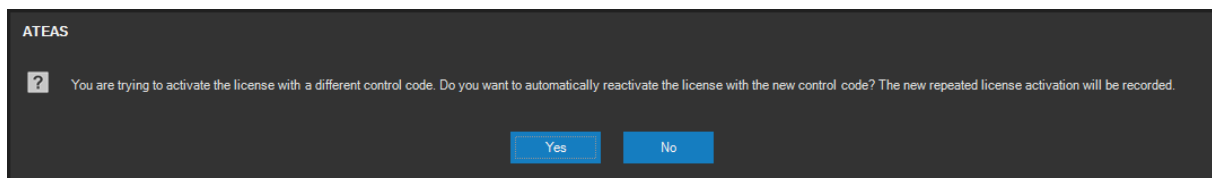
You can read more on this topic in the Version information and PMA information documentation chapters.

11.12.4. Automatic license reactivation

As soon as the system is activated, the license can no longer be activated on another computer, to be more precise, when the administration server is installed on a computer with a different control code. If a second or any later activation of the same license on a different computer meets the license agreement (e.g. in case of a hardware failure, OS installation etc.), the license can be deactivated by using a signed declaration submitted to the license supplier.

Customers with an active PMA service (unlimited access to new product releases), however, can take advantage of the automatic license reactivation feature on their new machine without having to cooperate with the license supplier and filling the license deactivation declaration.

Such a situation will be detected by the system and when a second activation is performed, upon confirming a query, the following dialog will be displayed.

A dark-themed dialog box titled "New activation" with a checkmark icon and a close button (X). It contains several input fields: "ATEAS ID" (pre-filled with "128 529 214"), "Full name" (empty), "E-mail" (empty), "Phone" (empty), and "Detailed reason for the new activation" (empty text area). At the bottom, there are two buttons: "Apply" and "Cancel".

To perform a new license activation, you must fill in all fields in the reactivation dialog and confirm by pressing **APPLY**.

NOTE

Automatic license reactivation for one ATEAS ID can only be performed once every several days. Additional attempts will be blocked.

CAUTION

Records are made for repeated deactivations and the relevant license supplier is informed automatically. If there is reasonable doubt that the information provided is not accurate or a situation that contradicts the license agreement is detected, further attempts to reactivate the license will be blocked.

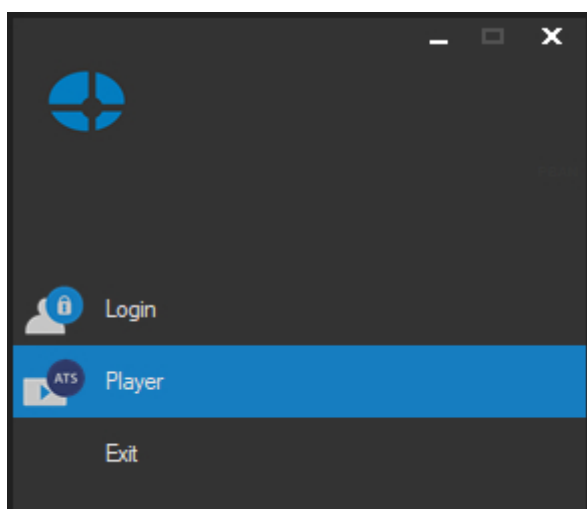
Chapter 12 - Player

12.1. Starting the player

The Player application is a simple and intuitive player, which supports the ATS format to which video and audio from cameras can be exported. The player also enables exporting images in JPEG format. Besides the ATS format, the client application can also export video to AVI or MP4 format, which is supported by a large amount of other players. To the contrary, exporting to the ATS format has its advantages:

- The export is several times faster, for the video is not recompressed using the selected codec.
- The output file may contain up to 16 cameras including audio.
- The target file can contain video compressed by various video and audio formats.
- The exported video supports dynamic changes to frame rate and video resolution.
- ATS files can be digitally signed via an integrated tool.
- The file can be encrypted and password protected.

There are several ways to start the player. If the ATEAS Observer client application is running, you can select the Player item directly from the application main menu. This option is also available before logging into the system.



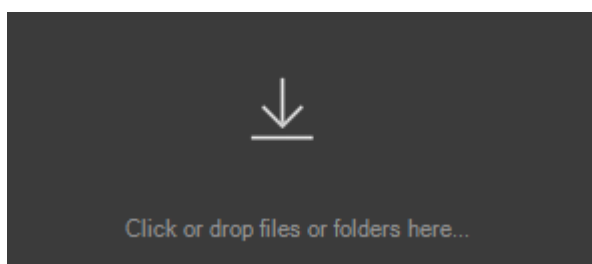
If the client application is not running, the player can be started by double-clicking on a file with an ATS file extension wherever in the Windows system. Upon installing ATEAS Security software, the ATS file extension is recognized as a registered file type and the player will be started automatically.

It is also possible to launch the player on a computer without installing the full ATEAS client software using a stand-alone executable of the player. This executable is available as a part of the ATEAS installation image and can also be downloaded from your administration server's web page. If the player is exported together with the exported data, the replay process will be started automatically.

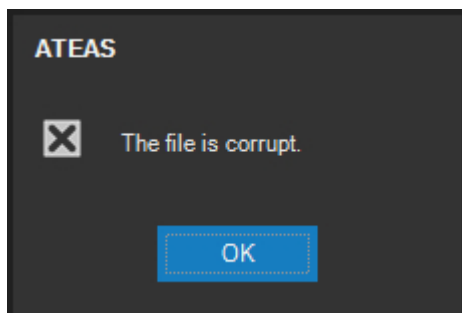
12.2. Replaying video in ATS format

12.2.1. Opening a folder

If the player is run automatically by selecting an ATS file directly in the operation system, this file will be opened automatically. The file can also be opened using the file list in the right part of the player window, described in an independent subchapter. Another and usually the fastest method of opening a folder or file in the player is using a drag-and-drop operation directly from a folder to the play list. The active area below the list of files and folders can also be clicked to display a folder browser dialog.

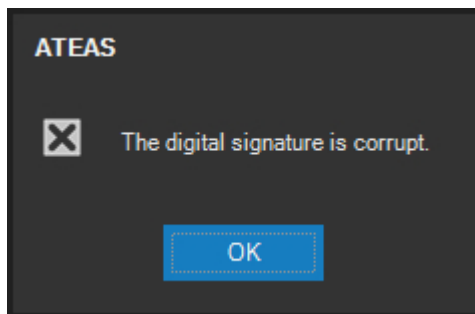


Several situations may occur when opening a file. If the file is not a supported file type, it will not be opened and a warning message will be displayed.



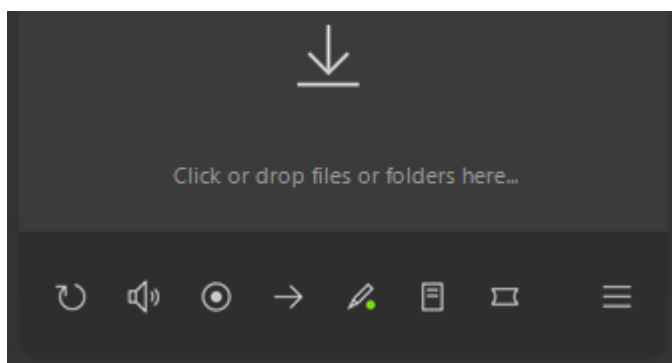
If the file structure is intact, the file will be checked for digital signatures. If the replayed file does not contain a digital signature, it will be played automatically. In this case, the digital signature indicator, located in the bottom right corner of the player, will show up in grey color. If the file is digitally signed, the signature will be automatically verified. Three cases can occur.

The first case is a situation when the digital signature is evaluated as invalid. That means that someone manipulated with file data after the digital signature was appended. The file cannot be considered valid even if any part of the file, even a single bit, is changed, regardless of the file size. The application will display the following message and the digital signature indicator will show up in red color.

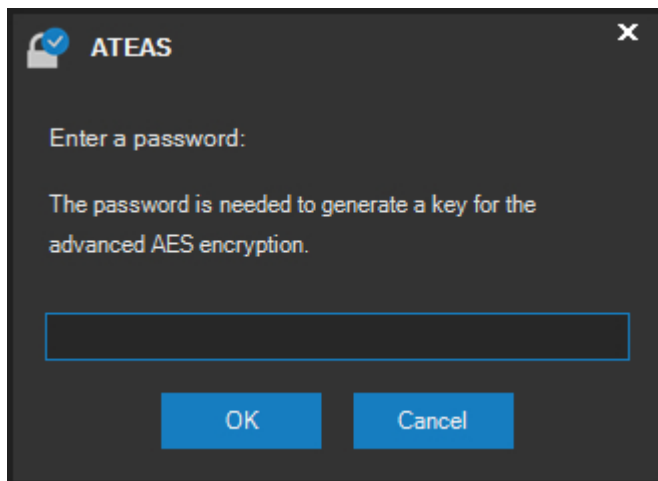


In the second case, the digital signature is verified positively, however, the receiving party cannot evaluate the content of the file as credible, because not all required certificates are available, or because the path to the signing certificate on a computer of the receiving party does not lead to the root certificate, installed in the storage of trustful root certification authorities. If this happens, the receiving party may install the relevant certificates (either directly from the file signature or externally). In this case, the digital signature indicator will show up in orange color.

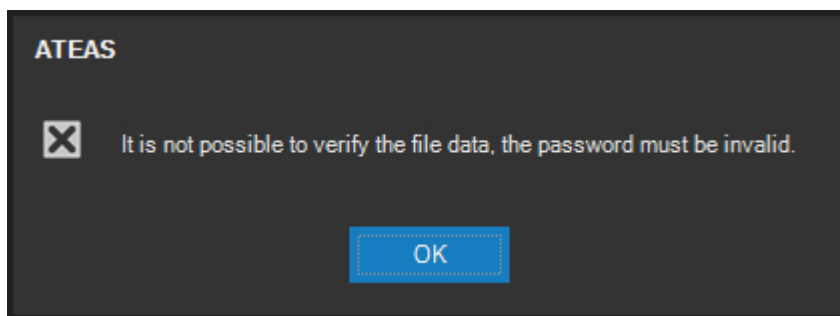
In the third case the digital signature is recognized as valid and it also contains a trusted signature certificate. In this case, the digital signature indicator will show up in green color.



If the ATS file was protected during export with advanced AES encryption, a password will be required after the digital signature verification to open the file, which is the input for a one-way mathematical function, through which the key to decrypt the file data is obtained. If the file data is encrypted, the following dialog will be displayed automatically.



If a valid password is entered, the file replay will be initiated. Otherwise access to file data cannot be granted and the application will display a critical message.

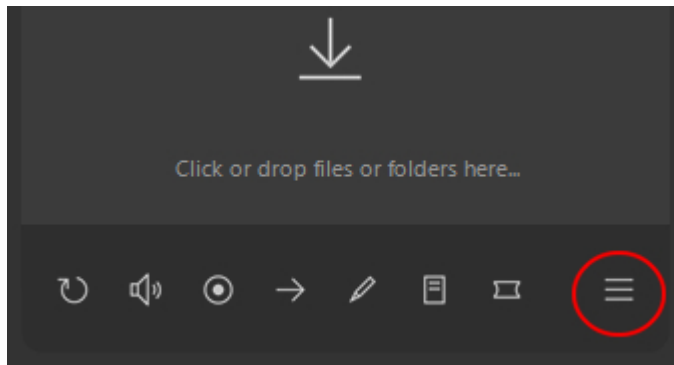


NOTE

Without knowing the correct password and using today's technology, there is no way of obtaining access to decrypted file data and replaying the content in reasonable time.

12.2.2. File list

After opening a folder, the player will automatically create a list of all ATS files in the given directory. This list can be displayed or hidden using the in the bottom right corner of the player. All subfolders are also automatically searched, creating an organized tree structure.

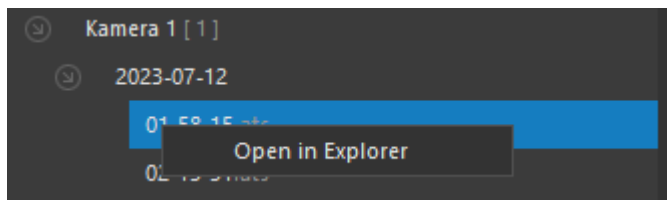


Any file can be opened by easily clicking it in the file list. The bottom edge of the file list contains a button for activating the automatic replay. If this option is activated, the player will replay all files in the list automatically one by one.

Above the list of files, there are buttons for refreshing the playlist and for activating search.

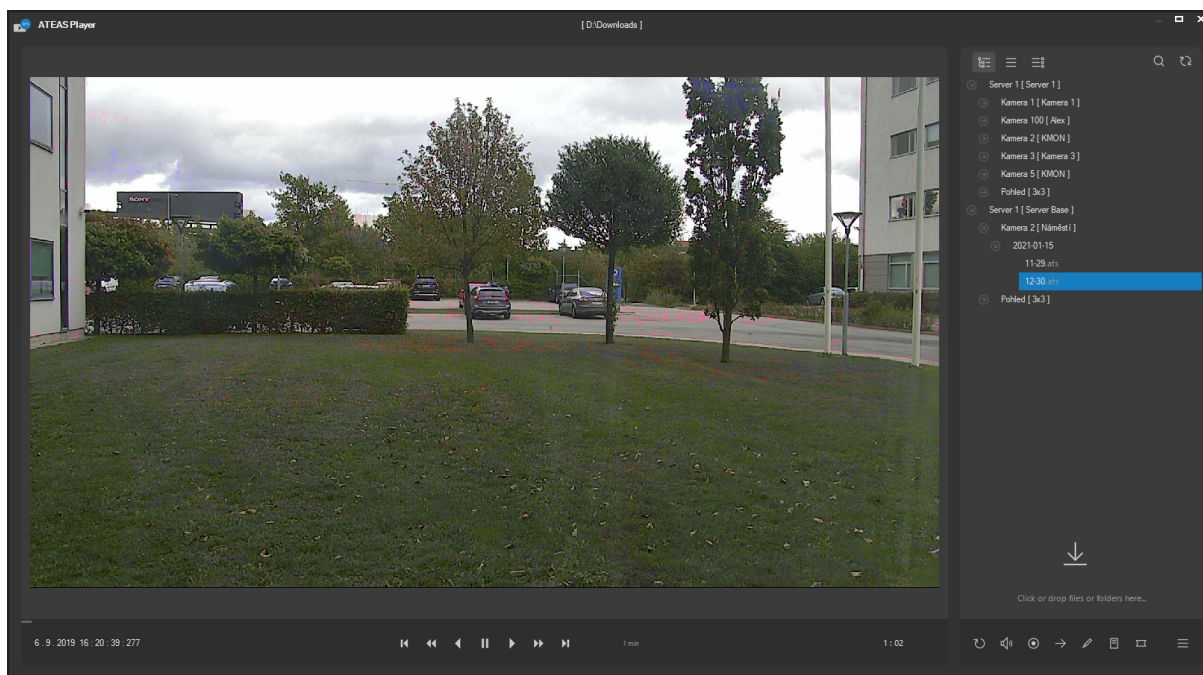
By placing the mouse between the video replay area and the playlist a drag operation can be initiated to update the widths of these window parts. Use a double-click to restore the default ratio.

Each file has a context menu allowing you to quickly open the folder containing the file.

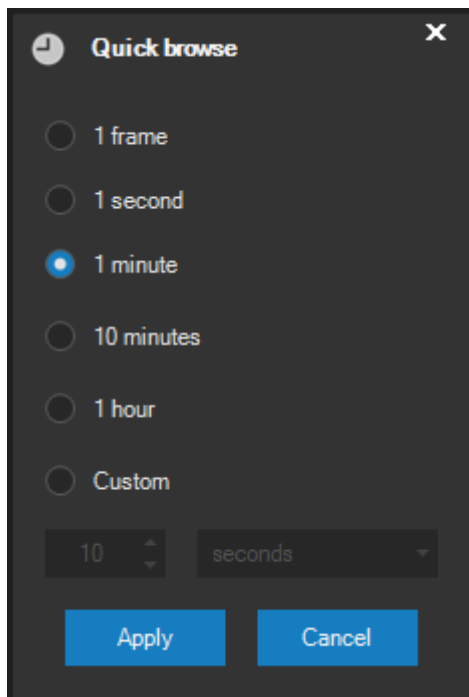


12.2.3. Replaying a file

You can change the speed and direction of the currently replayed sequence. You can also perform one-shot shifts using the replay control placed in the centre of the bottom part of the window.



The two buttons located in the left part of this control are used to change the replay speed ranging from sixteen times slower to sixteen times faster. The three bigger buttons in the middle of this control change the direction or stop the replay. The two smaller buttons on the right can be used for fast scrolling (forwards or backwards) by increments of a specified time interval. This interval can be changed by clicking on its current value. The user can either select a predefined interval or create a new one in the following window. To assign a selected interval to the scrolling buttons, press the **APPLY** button. Value 1 frame is time independent and allows moving between individual video frames.

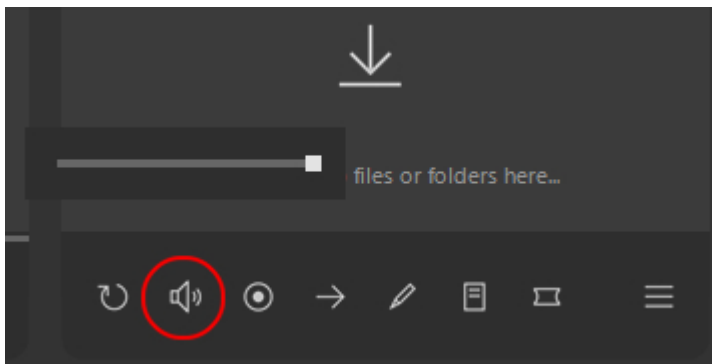
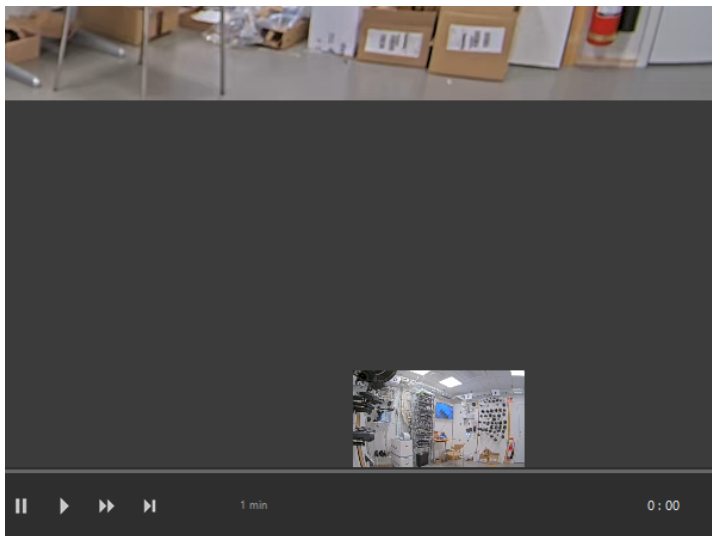
**NOTE**

If the open ATS file contains multiple cameras, one camera shall be selected before starting the process of moving by single frames. Other cameras in the view are synchronized with the selected camera throughout the entire frame by frame moving process.

During the replay process, the replay time is displayed in the bottom left corner whereas the bottom right corner shows the time remaining till the end of the file. A control showing the replay progress is located directly under the window of the replayed sequence. Replaying is automatically stopped when the right end (or left end when replaying backwards) of the control is reached. You can also click on a specific point of the progress bar to instantly shift to that point. This can be done whether the replay process is running or stopped.

If you hover over this bar with your mouse, a small time synchronized preview will be displayed automatically.

If audio is available for a scene, it is automatically replayed together with the video. The audio volume can be adjusted using the relevant control.

**NOTE**

If the open ATS file contains multiple cameras, audio will always be played for the selected camera.

NOTE

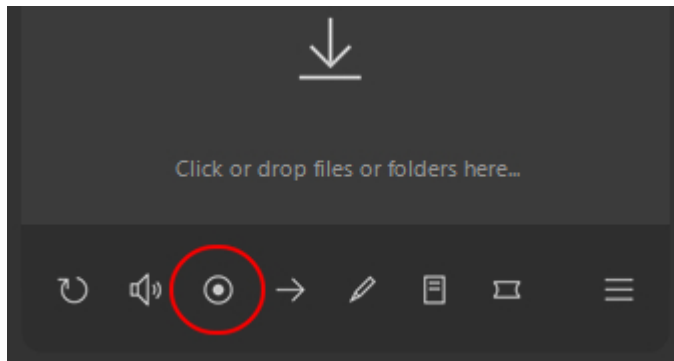
The right button can be used to quickly mute the audio and restore to the last volume setting.

During the replay process, gaps in the recordings are automatically detected and the player automatically skips the gaps, which makes the replay process more comfortable.

The button for saving a snapshot can be used at any time during replay. Not dependent on the format of replayed video, a snapshot will be created and inserted into a new window (which will become active) upon pressing this button.

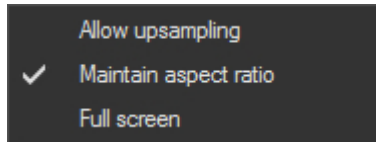
NOTE

If the open ATS file contains multiple cameras, you have to select a camera for which the snapshot will be taken.



There are two buttons available in the snapshot window. A dialog enabling the export of a snapshot to JPEG can be opened by pressing the **SAVE** button. The window with a snapshot can be closed pressing the **CLOSE** button. After closing, the ATS media player will again become the active window.

The context menu, containing several extended replay options, can be displayed at any time during the replay process by right clicking the mouse in the video display area.



The Allow upsampling option is disabled by default. By enabling this option the video will be displayed in the maximum possible size the player window will allow. If the option is disabled, the width and height of the video will never exceed the native resolution of the video, i.e. the player will not calculate any additional pixels during the replay process.

The Maintain aspect ratio option is enabled by default and enforces that the width to height ratio of the displayed video is maintained according to the native video resolution, and therefore the displayed people or buildings will not be deformed in any way.

The Full screen option enables toggling the player to full screen mode and back.

NOTE

Full screen mode can smartly adapt to the monitor setup, provided that there are multiple monitors connected to the station.

NOTE

Alternatively, you can leave the full screen mode can by pressing the Escape key.

NOTE

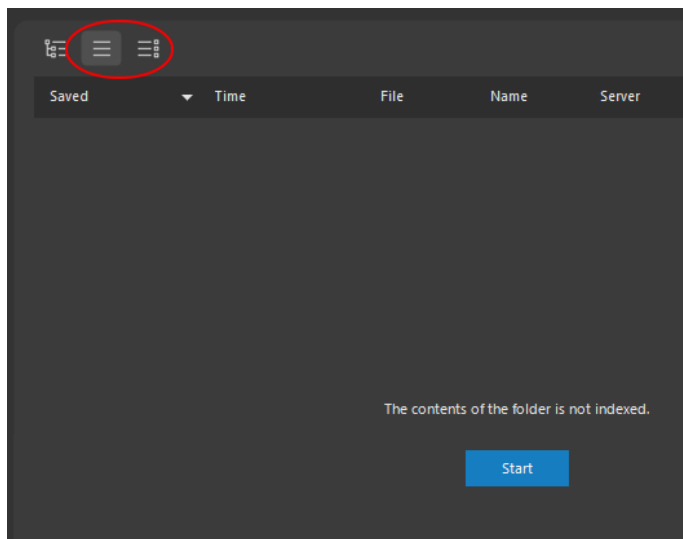
The Allow upsampling option is automatically activated when switching to full screen mode as its use in full screen mode is logical.

Some control keys are available during the replay mode in full screen. The space bar toggles the pause and play in the forward direction. The media pause button and media play button have the same function, provided the keyboard contains these media buttons. Reverse replay can be activated

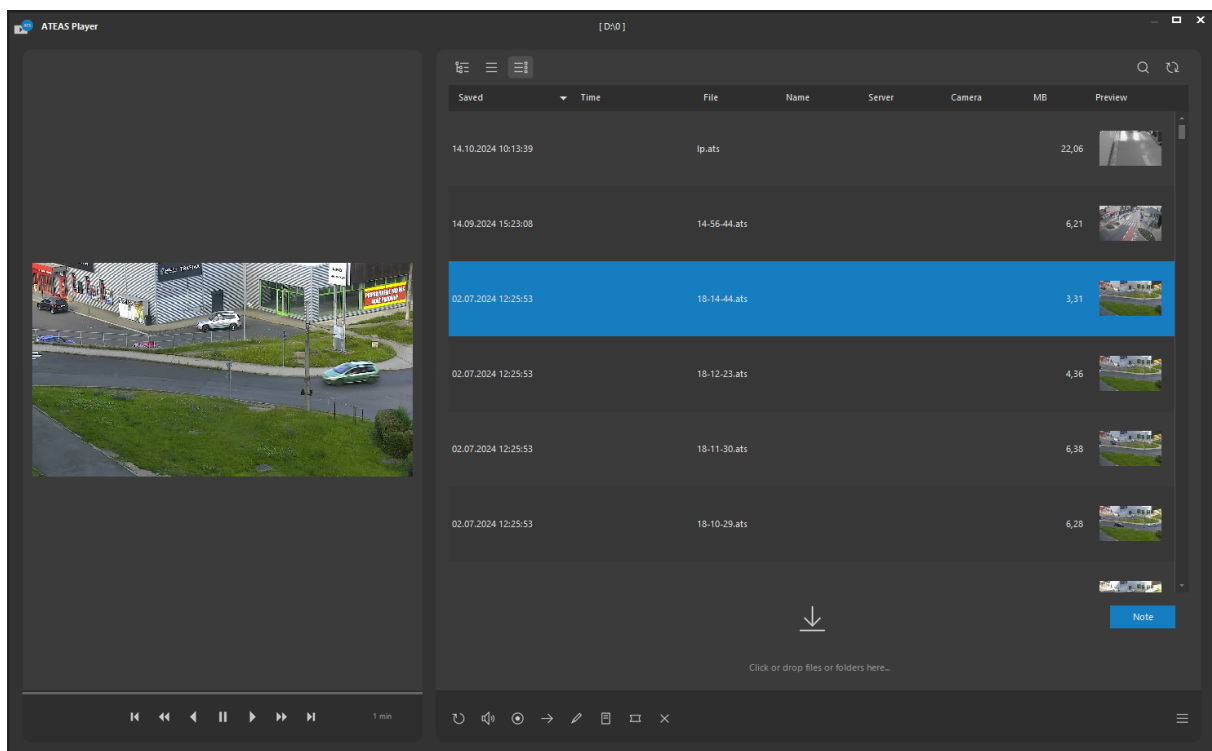
via the Backspace button. The plus and minus keys on the numerical keyboard increase and decrease the replay speed.

12.2.4. Indexed folders

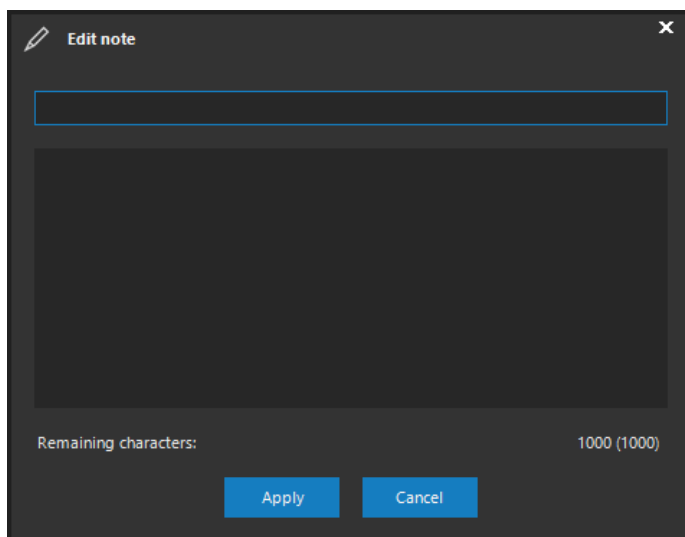
You can perform some basis searching in the default tree view of the selected folder. It is not possible, however, to sort the files by all criteria or add some longer descriptions to the files. For these features to work, you might want to switch to the list view or preview mode and if the folder is not indexed, start the indexing process with the **START** button.



Indexed folder content allows sorting according to all column headers, adding titles or longer descriptions using the **NOTE** button, searching or showing preview while hovering over a file with the mouse. In the preview mode, previews are displayed automatically for all files.

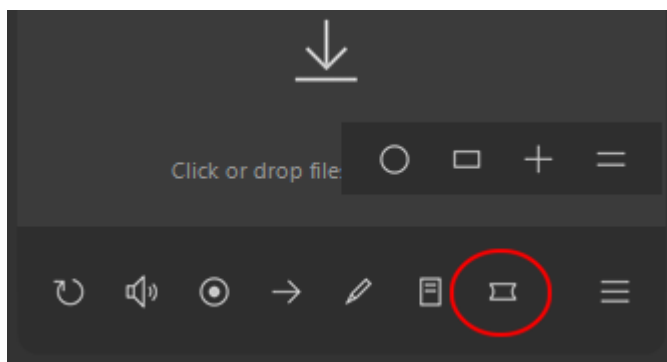


After editing the title or description using the **NOTE** button, you can then search for any text that this text data contains.



12.2.5. Fish-eye image dewarping

Additional buttons for choosing the dewarping mode can be displayed or hidden during the playback of exported files from cameras, which the system administrator configured as fish-eye image cameras.



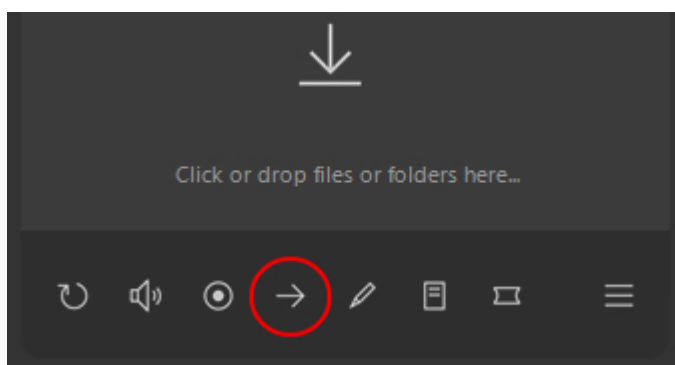
The fish-eye image dewarping feature and individual dewarping modes work in the exact same way as in the live window and are described in the Fish-eye image dewarping subchapter under the Selected camera functions subchapter.

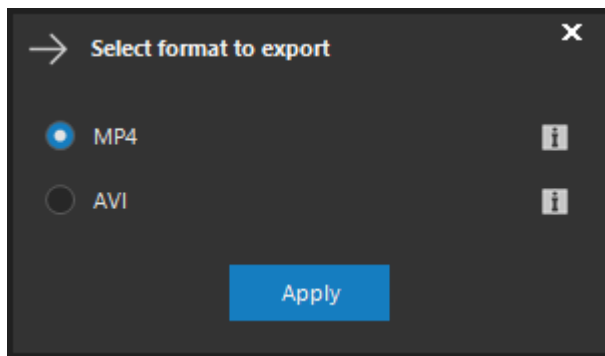
12.2.6. Video export

All the selected ATS files can be exported to other formats. The file selection is not limited to a single folder. It is possible to select multiple files from various folders. Pressing the button for exporting video and selecting the format for export will display the video export dialog in compact mode. The **MORE** button displays additional export options. When exporting a single file, the user can select the target folder and enter the name of the exported file. When exporting multiple files, the user can specify the target folder, names of the exported files, and placing into subfolders will automatically correspond to input files.

NOTE

When exporting a single file that contains multiple cameras, a camera must be selected first, that will be exported.





AVI is a widely used platform-agnostic format, easily portable, disadvantages include slower export speed (video re-compression required) and the inability to change the resolution or video and audio format of a file. Frame rate changes are balanced automatically by the export module.

MP4 similarly to the AVI format is easily portable. When exporting to MP4, export does not use video re-compression, therefore, the export speed is about the same as the export to ATS format.

The MP4 output is best performed from a higher FPS video, which makes the output playable even in some less robust third party players.

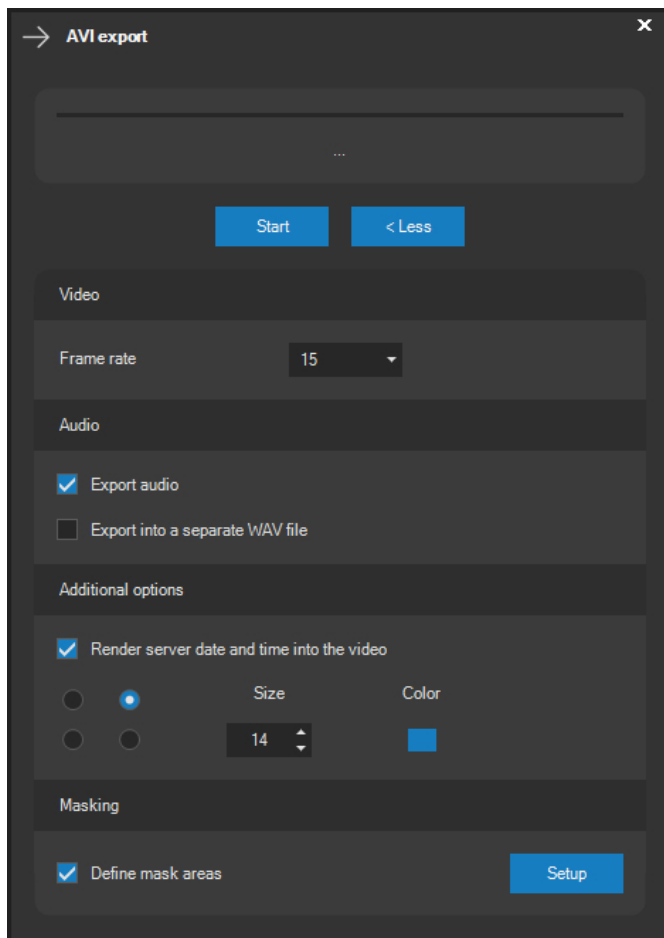
CAUTION

AVI and MP4 formats do not support integrated security of ATEAS, meaning the contents are not encrypted during export and the data cannot be digitally signed.

12.2.7. AVI video export

Basic setup

Pressing the button for exporting video and selecting the AVI format will display the compact AVI video export dialog. The **MORE** button displays additional export options.



Upon pressing the **START** button, a dialog will appear requesting the destination and name for the new AVI file.

NOTE

If more local media scenes are selected before exporting, there is no sense in entering a specific file name, however, a target folder can be selected. The names of each file will then be created in general format (e.g. Scene1, Scene2) or the name of the scene will be used as the final name of the file, provided the user created it.

Upon starting the export process, the **CLOSE** button will turn into the **CANCEL** button which can end the video export process prematurely. A control next the **START** button provides information about the video export. After finishing the export, a confirmation message will be displayed.

Before starting the export, several additional export options can be set:

NOTE

These additional options will automatically be configured to the last used values the next time the dialog is opened.

The frame rate for the exported video can be selected from the Frame rate drop-down list. If you do not want to lose any frames during the export, always select a higher frame rate than the highest frame rate in the exported media sequence. The final size of the file will be (depending on the selected codec) smaller if you select a lower frame rate.

Audio

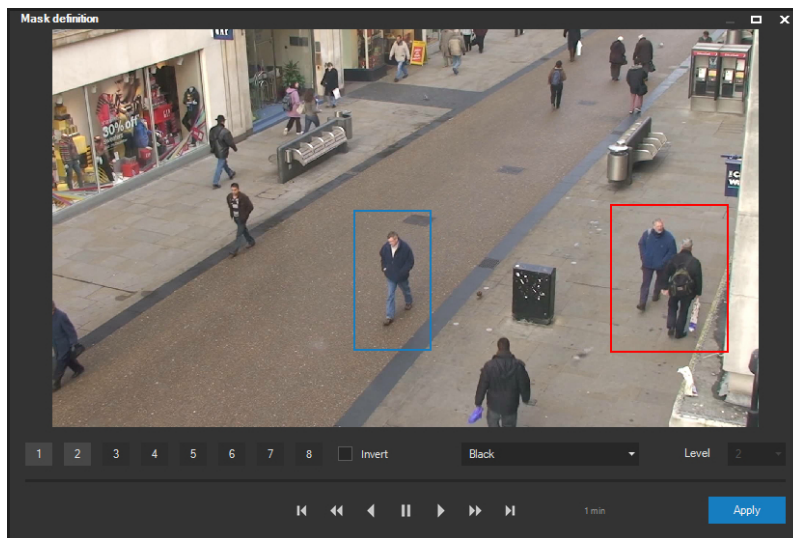
It is possible to check the Export audio and possibly also the Export into separate WAV file option. If you only check the Export audio option, the audio track will be exported together with the video track into the final AV file. In contrast, if you additionally check the Export into separate WAV file option, an identically named file but having a WAV file extension will be created with the audio track.

Additional options

The Render server date and time into the video option can be activated under Additional options. This will render the server date and time directly into the exported file. If this option is selected, you can select one of the four corners where the date and time will be displayed in the exported video. If necessary, you can also change the font size and color. The font size can be set from 8 to 60 points, the color can be either picked or created in the color selection dialog, opened by pressing the button next to the selected color.

Masking

After the Define mask areas option has been activated, pressing the **SETUP** button will display a dialog containing a preview of the video, in which the mask can be created.



It is possible to create up to eight independent dynamic masks, which can be moved, resized or completely hidden and displayed again during the replay process. This way, you can anonymize selected persons or faces in exported material even if they are moving.

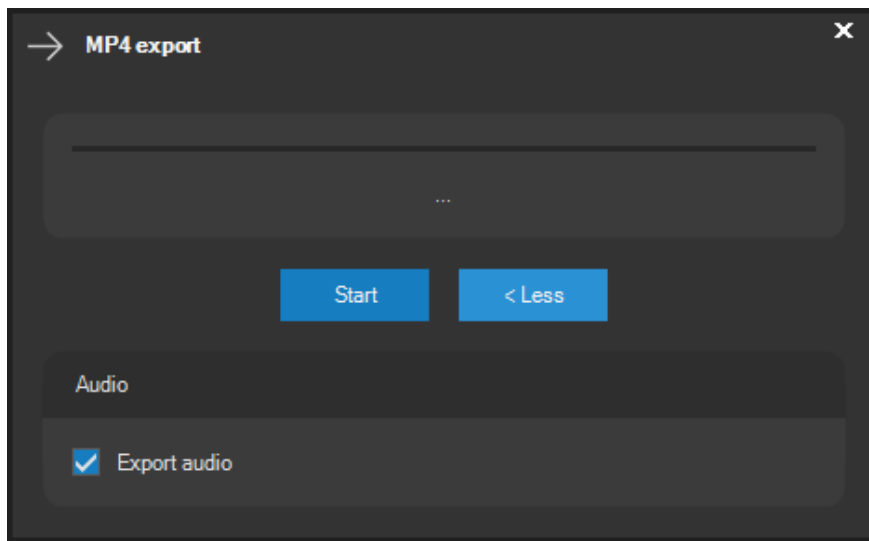
The masked areas can be rendered completely black or they can be pixellated or blurred. For these two more advanced effects, the strength of the effect can be chosen from 1 to 3 (strongest).

Once the Invert option is active, all configured masks will be applied outside the masked areas. This way, you can unmask e.g. just one or more selected moving objects more conveniently.

12.2.8. MP4 video export

Basic setup

Pressing the button for exporting video and selecting the MP4 format will display the compact MP4 video export dialog. The **MORE** button displays additional export options.



Upon pressing the **START** button, a dialog will appear requesting the destination and name for the new MP4 file.

NOTE

If more local media scenes are selected before exporting, there is no sense in entering a specific file name, however, a target folder can be selected. The names of each file will then be created in general format (e.g. Scene1, Scene2) or the name of the scene will be used as the final name of the file, provided the user created it.

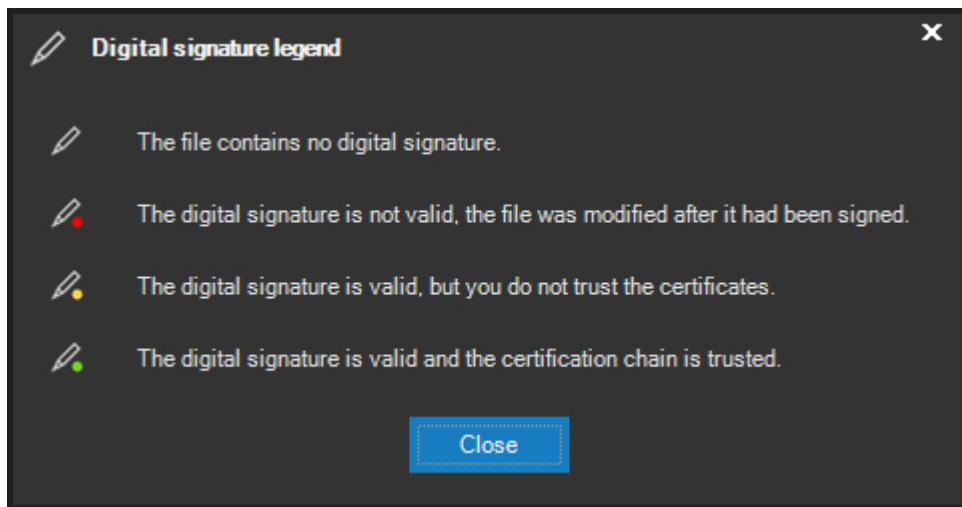
Before initiating the export, you can select whether or not the final file will contain the audio-track, or if it will be omitted during the export.

NOTE

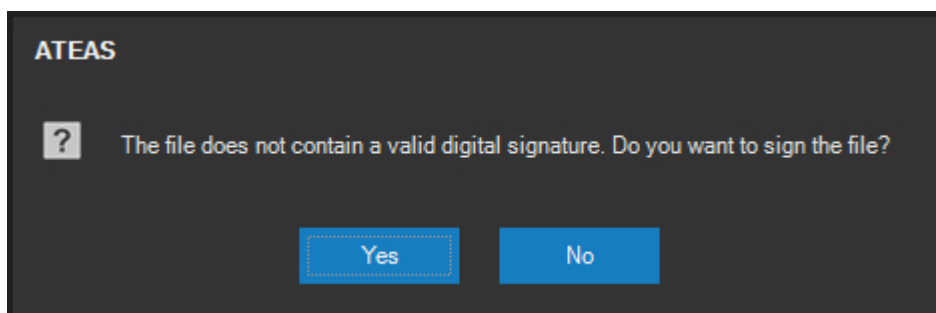
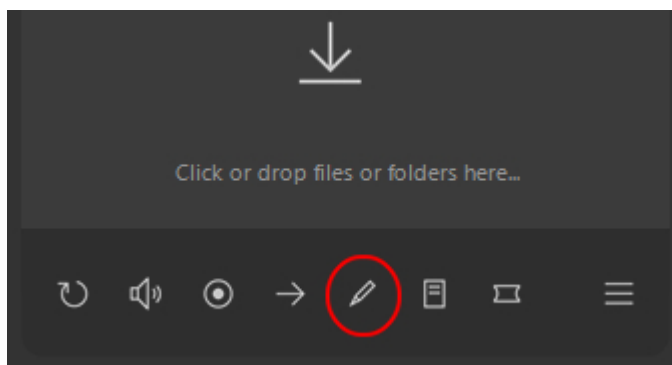
These additional options will automatically be configured to the last used values the next time the dialog is opened.

12.3. Digital signature

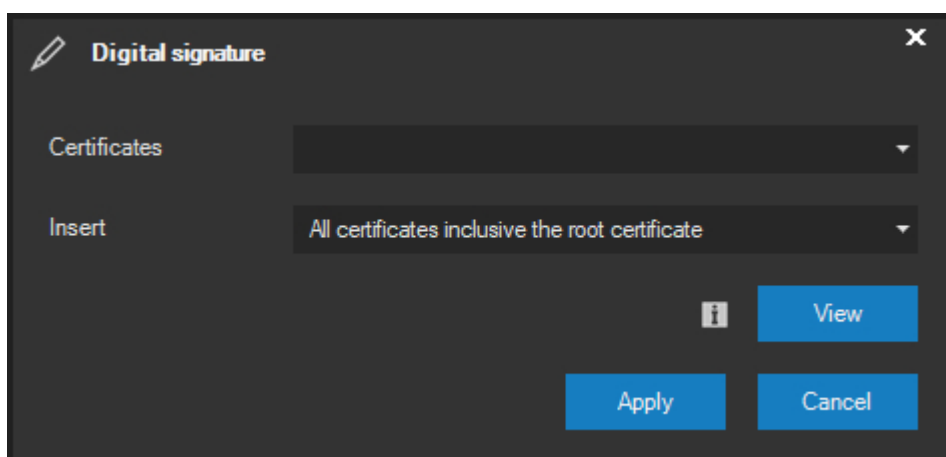
The result of the digital signature verification of various video and image files is displayed using the digital signature indicator. If we right-click this color indicator, a dialog with the legend containing all digital signature states will be displayed, as shown in the following picture.



If not already signed, the sign button may be used to initiate the signing process.



If we answer this question by pressing **YES**, the file can then be signed. A signature certificate and the insert option can be selected on the following dialog.

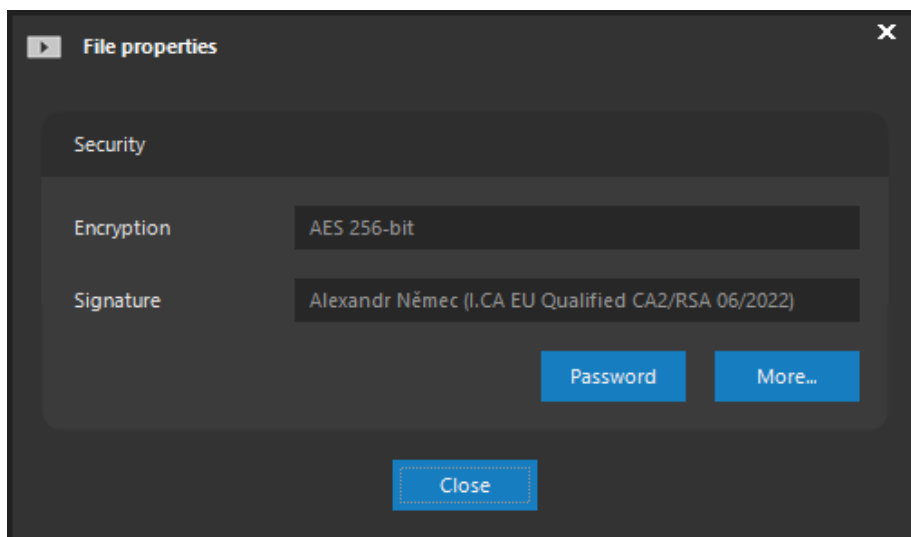


It is possible to use any certificate installed in your Windows certificate store (from where they are obtained by ATEAS Observer) together with a digital signature.

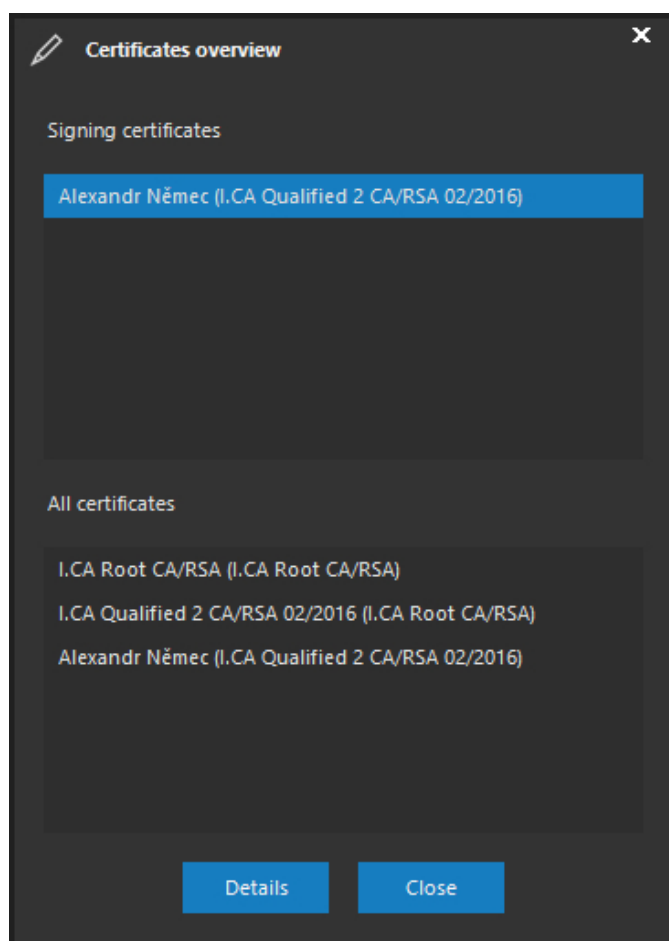
If already signed, the Properties button can be used to display the signatures and all corresponding certificates.

12.4. File properties

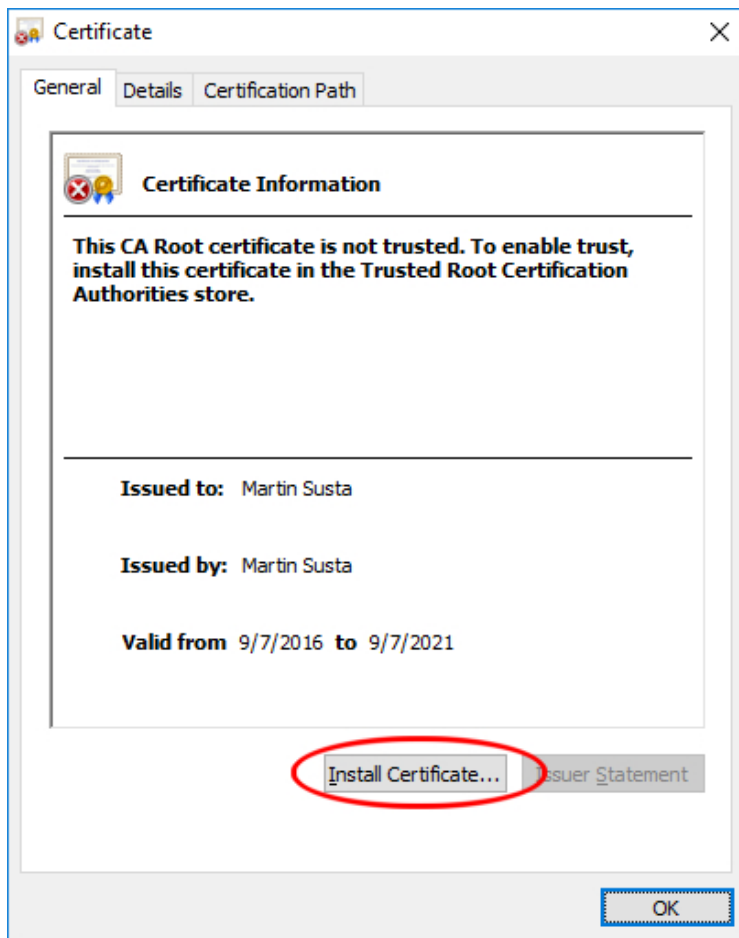
The Properties button opens a dialog with additional file information.



The Security section contains the type of encryption (i.e. whether or not a password is necessary for opening the file) and the signature certificate. If the file is signed, the **MORE** button can be used to display a detailed list of all certificates in the file.



Signature certificates are listed in the upper part of the window. All certificates included in the signature are listed in the bottom part of the window. Using the **DETAILS** button, you can open a selected certificate within the standard Windows dialog which provides detailed certificate information including the certificate path as well as justification why it is not credible. A button for importing certificates to third party certificates or to trusted root certification authorities will automatically become available. An automatic guide which adds a certificate to the Windows operating system can be started by pressing the **INSTALL CERTIFICATE** button.



The **PASSWORD** button can be used to remove or change the password of the file. This might be useful, if the administrator has activated password protected downloads and a file must be unlocked without revealing the original password.

CAUTION

When changing the password, any digital signature will be invalidated and removed automatically so that a new signature will be necessary if appropriate.

Chapter 13 - Map window

13.1. Map window basics

The map window is an intelligent component integrated in the ATEAS Security system making it possible to visualize the geographic context of your system. Coordinate orientation enables all map functions including map zoom, centering according to coordinates, centering to defined cuts, creating and switching map levels and many others. Using this component, you can integrate your map data (maps, drawings, plans) with the camera system. The following pictures show examples of imported maps.

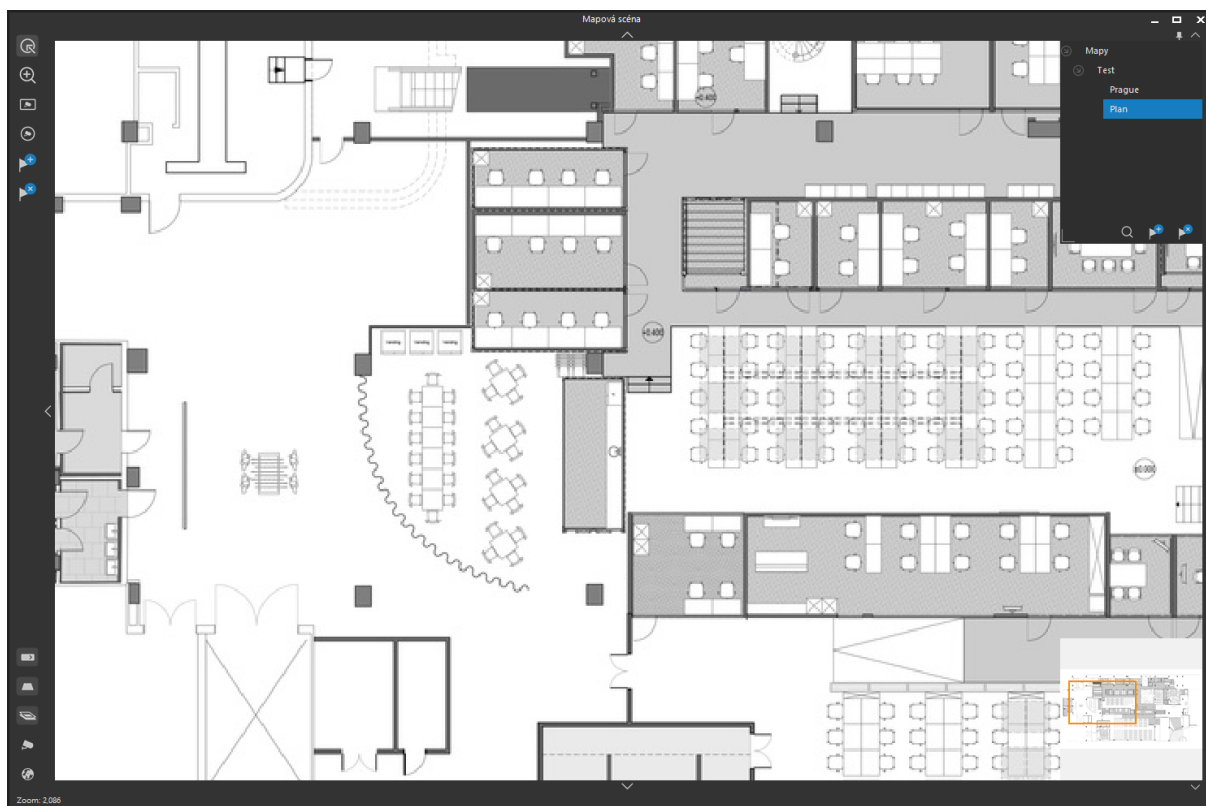
The map window is also compatible with OpenStreetMap map data. The maps you can be provided, may contain free map data from this source. These maps are real, precise, multi-layer and georeferenced maps, which provide zoom levels up to low map scales (detailed view of buildings) and high performance. The fundamental advantage is their availability for free and the lack of dependency on any third party maps. Therefore, detailed maps for the entire city or region can be added to your system easily.

NOTE

The map window seamlessly supports various maximum zoom levels for different parts of the map. You can therefore add a map that contains, for example, an entire region at overview level, and selected parts or cities with maximum details.

NOTE

Using OpenStreetMap sources is available starting with ATEAS Security PROFESSIONAL edition.



NOTE

This chapter describes the basics how to control the map window. However, certain functions related to the map window are also mentioned in other chapters. These functions include placing a camera to coordinates (camera setup section), adjusting map behavior, history of events shown within the map, selections (local setup section) and displaying event symbols (live window and receiving events section).

13.2. Map data distribution

The map data distribution is an automated process. An administrator with access to the administration server can create or update the map data folder structure and publishes it for distribution to clients, who save the maps locally.

NOTE

For the client to synchronize the maps, a corresponding permission is required.

The system administrator can create the map structure in the `httproot\maps` folder on the administration server. There, up to three map levels can be created in the forms of subfolders. Each folder can contain a raster image in JPG, TIF, PNG or BMP format or an OSM map model based on the freely available OpenStreetMap sources covering the entire world. Thus, you can export any region of your interest. There are more tools and ways of exporting the data, one of them is described in an annex to this documentation.

TIP

Large raster images with very high resolution should be converted to OSM map model as described in the appendix for working with extremely large raster images will be slow.

The folder name consists of a unique ID of the map layer and its name separated by a hyphen, e.g.

10-Prague

By default, the order of the map layers is determined by the ID. If this is not the desired order, it is possible to append a sequence number in square brackets, e.g.

10-Prague[1]

When determining the order, these additional sequence numbers will take precedence. The sequence numbers are not required to be strictly continuous, to determine the order unambiguously, on any given map level, duplicate values should not appear.

CAUTION

The map data structure must not, however, contain duplicate ID values of the map layers. These must be unique not only on a folder level but in the entire map structure.

For the changes to the map structure to be distributed to the clients, it is necessary to increase the version of the map data in the maps.ini file in the map root folder. The rest is fully automatic. Every change to the map structure or content has to be followed by incrementing the map version. Otherwise, the clients may not be propagated these changes.

TIP

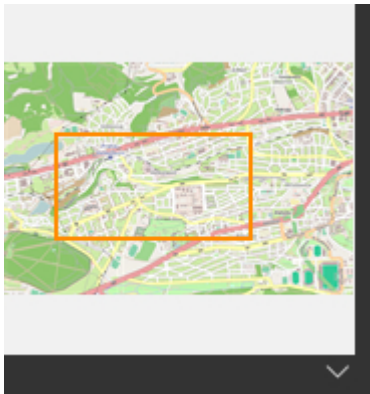
Some test map data is part of the system installation so that you can start experimenting with it immediately.

13.3. Map windows basics

13.3.1. Moving and zooming the map

The map can be smoothly moved by dragging the mouse. By clicking the left mouse button with the cursor placed anywhere in the map, the map will move together with the cursor. This is considered the fastest and the most intuitive way of moving a map. A map can be also moved using arrows located in the centre of all four map area sides.

When working with a map, a preview window is available in the top right corner containing a maximized map (or the current map level to be more specific). A border indicating the currently selected map section is highlighted in this preview. The preview window can be either closed or displayed using the arrow under the bottom right corner of this control.



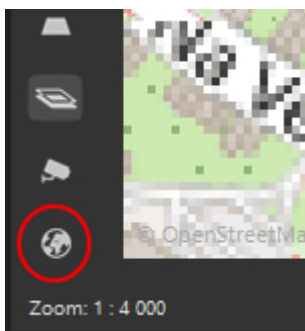
Another way of quickly moving throughout the map is by dragging the highlighted border (by left-clicking anywhere within the border) and moving it within the preview window. The contents of the main map surface will be displayed according to the current position of the border.

The easiest way of zooming is by using the scroll wheel to perform a smooth zoom in or zoom out. When using the mouse scroll wheel to control the map zoom, the center of the map zoom in or out operation is determined as the current position of the mouse cursor. If the mouse is not equipped with a scroll wheel (or even if a scroll wheel is available), you can zoom by using the Rectangle zoom function.



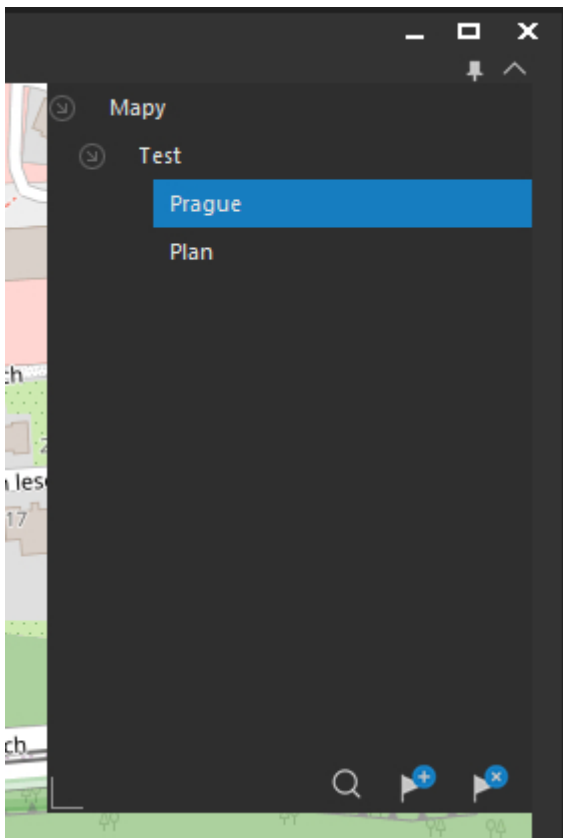
This function will become active after pressing the button. You can then create a selection by holding the left mouse button and dragging the mouse. This selection will turn into a zoomed area after the mouse button is released. Press the right mouse button to zoom out. Information for the current zoom is displayed in the map window status bar.

The button in the bottom left corner of the map window is used to instantly open the maximized map view (the map is zoomed out as much as possible with regard to the extent of map data).



13.3.2. Switching levels

Map data available in the map window can be separated into individual levels. The Map level is a third dimension of a map. Map levels are used everywhere, where it is necessary to integrate plans for multi-floor buildings or cover a large area with several map parts. In order to switch the map levels, use the Legend tool, which is placed in the top right corner of the map window. This tool can be either displayed or hidden using the associated arrow.



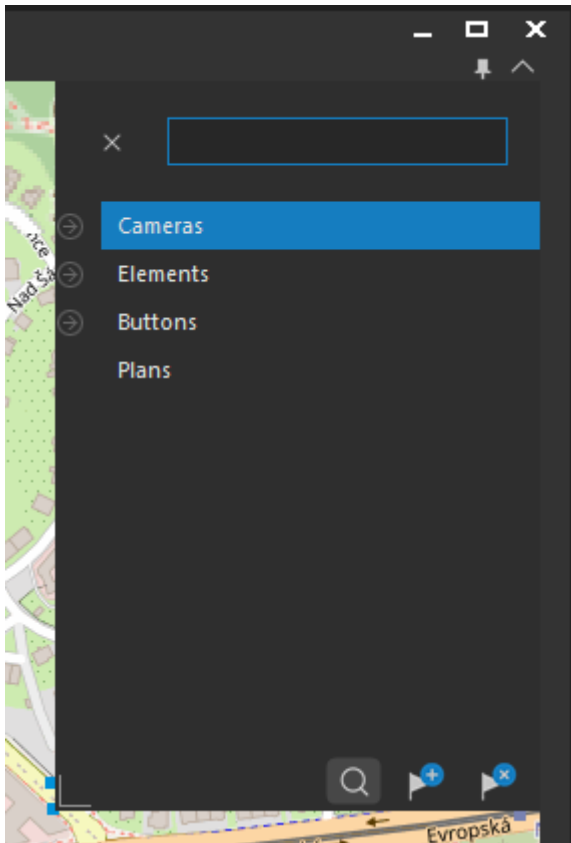
Controlling the legend is very simple. A specific map level is activated by simply clicking on an item in the tree map level structure. Drag the bottom left corner of the legend to change the legend size and save the final position that will be used the next time the map is started.

NOTE

Switching between individual map levels (floors of buildings) can be done manually as described above. However, this can also be done automatically by the application if the synchronization (full or event only) is turned on and the event is related to another map level than the level currently selected.

13.3.3. Searching the map

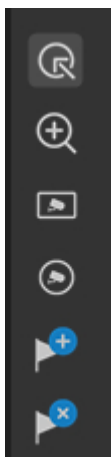
Cameras from all camera servers, their zones, user buttons, external objects and their elements or plans can be localized on the map. Using integrated search, you can search among all of these entities by name. The search button located below the legend is used to begin the search.



The search runs in real-time and results are immediately visible in the list. Click on any element to search and centre on the map.

13.4. Additional map functions

The control panel placed within the map window includes certain additional functions for controlling the map. A brief description is provided below.



Movement and selection function. If this function is active, it is possible to smoothly move the map as described above. Despite the fact that the control panel contains a special function for selecting elements (cameras), this function can be also used for making selections. This enables quick camera selecting without selecting another function from the control panel while searching in a map. If you use this function and simultaneously hold the CTRL key, the function will work the same way as the Rectangle select function, described below.



Rectangle zoom function. Using this function, you can create a section (rectangle area) to which the zoom effect will be applied.



Rectangle selection function (the same function is assigned to the movement button when simultaneously holding the CTRL key). When this function is active, you can create a rectangle area in the map from which all the camera units will be selected and then displayed in a certain live window (according to the local setup). One edge of the rectangle area is determined by the first click.



Circle selection function. When this function is active, you can create a circle area in the map from which all camera units will be selected and then displayed in a certain live window (according to the local setup). The centre point of the circle area is determined by the first click.



Place element function. Individual elements (e.g. camera units) can be placed into the map using this function. This function will be activated (or will invoke a corresponding action) only if you are in the administration section and have the necessary user rights.



Remove element function. This function removes already localized elements (e.g. camera units) from the map. This function will be activated (or will invoke a corresponding action) only if you are in the administration section and have the necessary user rights.

Apart from these functions, the left bottom corner contains functions for showing or hiding the active dynamic content. This refers to buttons, zones, maps and camera streams.

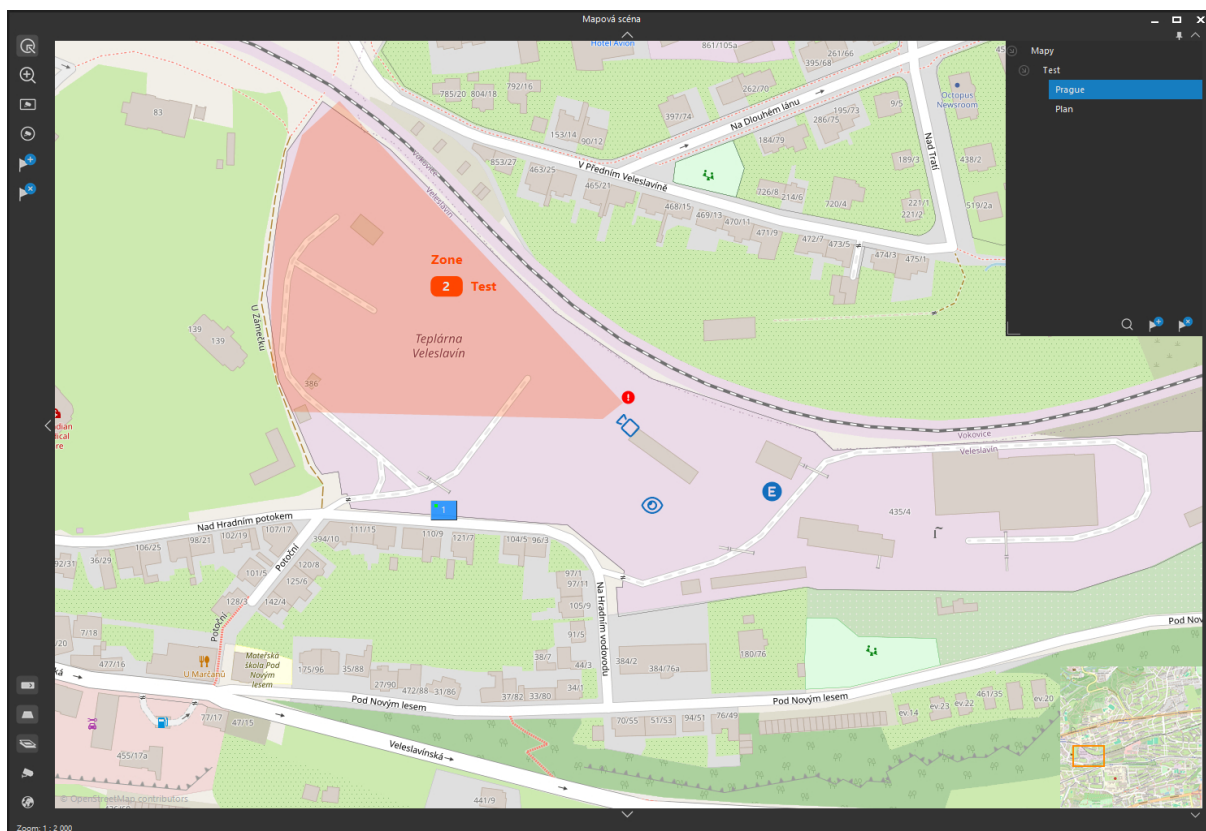


13.5. Dynamic map layer and video preview in the map

The map window always projects a dynamic layer over each map level that includes e.g.:

- camera symbols,
- camera zones,
- automatic zone counters,
- external element symbols,
- events with age differentiation,
- user defined buttons,
- live video of cameras,
- connections to other map levels.

This layer changes (automatically and for all users) depending on events in the system, adding, removing and dislocating cameras or user buttons, modifying the appearance of symbols, local definition of symbol sizes etc.



By default, cameras and user buttons are always displayed in the raster map and are only displayed in multi-layer maps (based on OpenStreetMaps) for scales from 1:35 000 and lower. For maps with larger scales (lower map detail), these symbols could inconveniently cover a large part of the map and make orientation within the map difficult.

NOTE

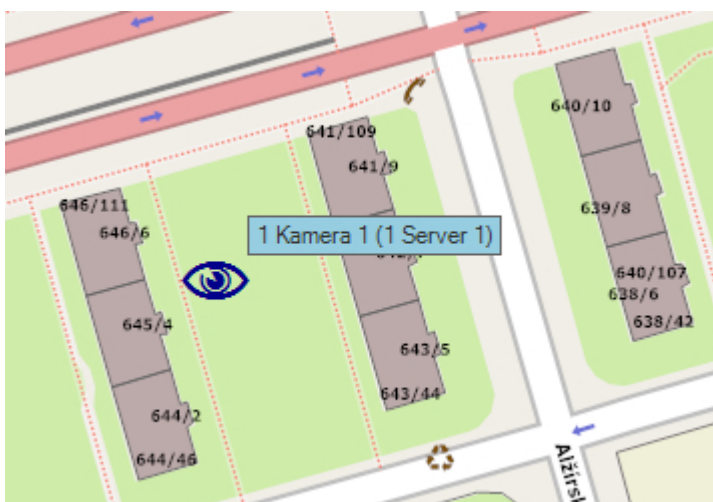
Changing the settings for this scale and other settings can be configured in the local settings section of your client application.

The map is also equipped with a smart grouping feature of map elements of the same type (cameras, external elements, events). This feature is helpful when symbols may overlap each other due to the current map scale setting. The grouped symbol shows a number, which indicates the number of elements it represents.

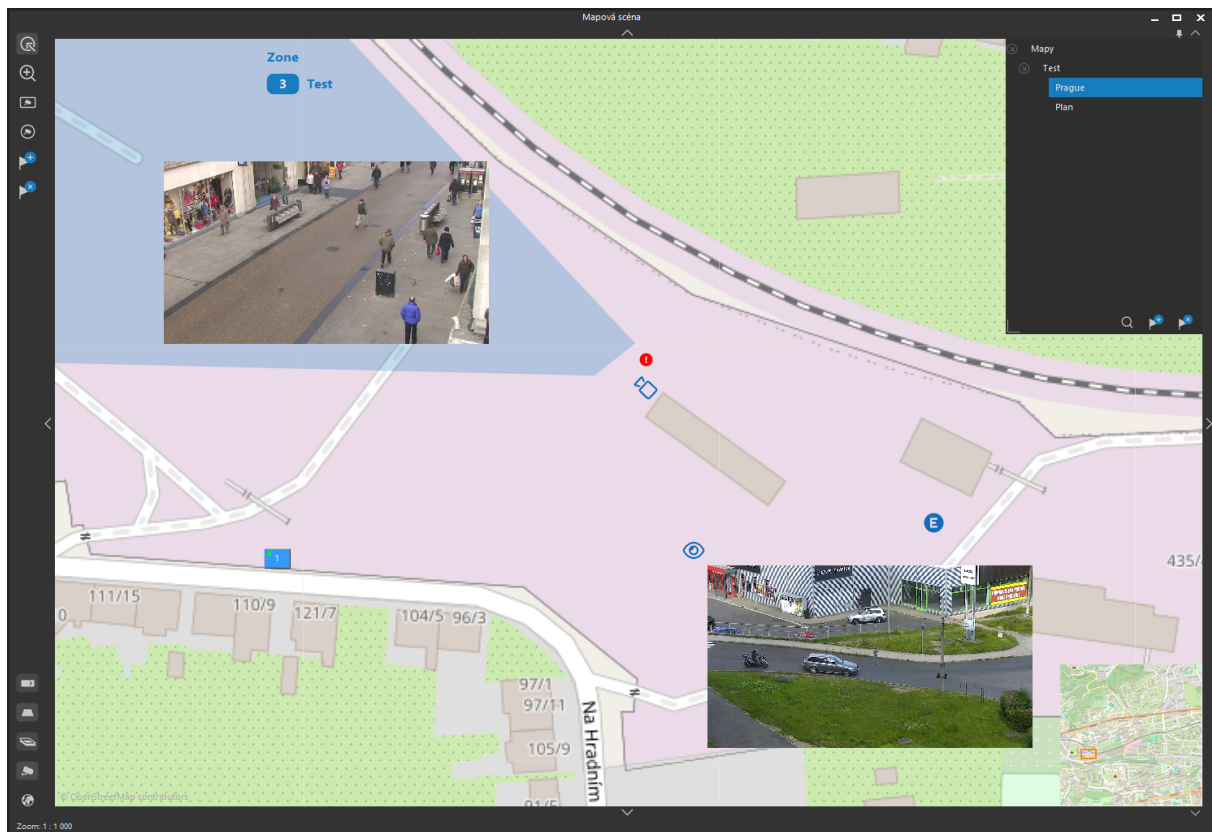


User buttons can be displayed and hidden independently of the current map zoom level via the button in the bottom left corner of the map window (above the camera symbol).

If the video preview function is turned off, each camera is provided with a text which identifies the camera. This text is displayed when you hover over the camera for a very short period of time.



The control panel of the map window also contains a function which activates a video preview directly in the map window. This button has a camera symbol and is placed in the bottom part of the control panel (above the Global view function). If this tool is activated, a video preview for the selected camera will be available in addition to the information box, directly in the map window.



If you position the mouse cursor on several cameras, the video preview will be displayed for up to 5 cameras at a time. Other cameras will then cause the video previews opened first to be closed.

TIP

Positioning the mouse over a zone has the same effect opening the camera video stream possibly extended by sending the camera to a preset, if the zone is bound to one.

If you wish to turn off any of the previews manually, just click on the preview. If you wish to close all video previews simultaneously, deactivate the Video preview function on the control panel. Video previews will also be closed if the map level (not the map layer) requires modification for any reason (manual or automatic switch).

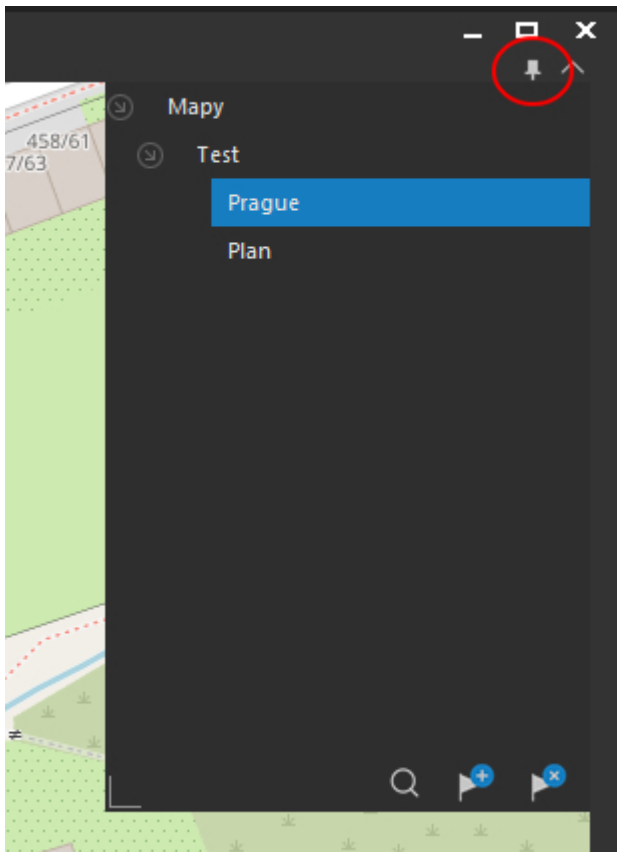
NOTE

Video previews are shown in the map geographically. That means that video previews will move in the same direction as camera symbols when moving or zooming the map. Therefore, video previews might overlap each other when the map is not zoomed enough. Overlapping can be eliminated by zooming in.

13.6. Displaying maps directly in the live windows

In most cases maps are displayed in a separate map window. This configuration is most suitable for workstations with multiple monitors. Providing you only have one monitor or you would like to have all monitors occupied by live windows, the map can be integrated directly into one of the live windows. In this case, the map can be displayed in any random position of the view.

Integrating the map into the live window is achieved by clicking on the pin symbol in the top right corner of the map window. The application will suggest that the next step is to select an empty position in the view of any random live window. After making the selection, the appearance of the map, which from now on will be displayed directly in the live window at the chosen position, will change. The map is removed from the view by clicking on the pin symbol again found in the top left corner.

**NOTE**

If the map is displayed directly in the live window, this setup will be saved together with the workspace.

NOTE

The location of the map is linked to the live window and to the selected position in the view, not directly to a specific view containing individual cameras. Therefore, when switching views, the map does not disappear and is displayed at its proper location in the view.

NOTE

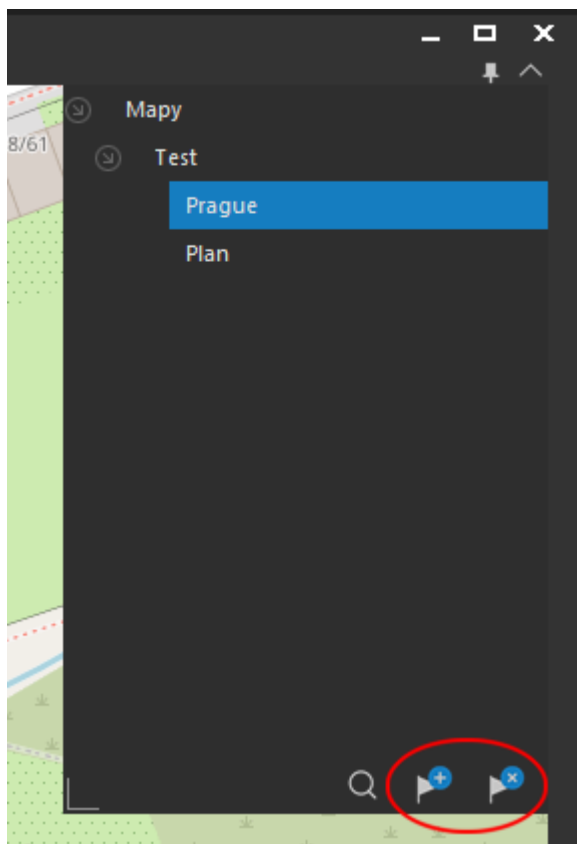
If the map is displayed directly in the live window, the camera selection in the map is automatically redirected to another live window.

13.7. Geographically linking the map levels

Individual map levels arranged in a well-organized tree structure provide a good overview of all imported map data. Of course, these levels are automatically selected depending on the selection of camera or event occurrence in the system.

If we, however, use map data from OpenStreetMap sources in our system together with e.g. building floor plans, we will intuitively expect that when we zoom the city map as close as possible, we will be able to automatically "enter" a building and display the building floor plan. This can be achieved through the geographical localization of map data, where building floor plans are localized into the OpenStreetMap data.

Map localization is carried out in a very similar fashion as the camera localization. In order to specify (or cancel) a localization, you must select the map or floor plan to be localized, press one of the buttons for defining the map localization (under the legend tool) and switch to the target map along with specifying the position where the map will be placed.



A door symbol will be displayed in the location where the map is inserted. This door will allow you to virtually "enter" the geographically oriented building floor plan.

NOTE

As an alternative and maybe faster way of localizing the map data, you can use a drag and drop operation, dragging a map level from the legend directly into the target map level.

**NOTE**

The geographically oriented plan can also be exited without having to select the superior map level via the Legend tool. Just use the mouse wheel and once you have zoomed out of the embedded map, continue zooming out. This additional zoom-out automatically switches to a superior map level.

Chapter 14 - Access from Apple devices

14.1. Supported features

The application for Apple iOS targets iPhone and iPad devices and is equipped with features as follows:

- highly effective displaying of video (supported codecs are MJPEG, H264, H265 or AV1),
- hardware video acceleration,
- displaying mobile views of up to 16 cameras simultaneously,
- secondary stream support in shared views,
- simultaneous replay of all cameras in the view with timeline preview,
- playing audio (supported audio codec is G711),
- transmitting audio to the camera,
- digital zoom and digital PTZ for all cameras including recorded video,
- highly sensitive PTZ camera control based on PTZ priority configuration and permissions,
- sending cameras into preset positions,
- camera output activation based on the permissions,
- intuitive viewing and replaying of recorded video including audio,
- event preview and replay,
- local video display settings,
- exporting of snapshots,
- live video (and audio) transmission from the camera of the mobile device including GPS,
- live displaying and replay of neural networks metadata,
- LP detection directly on the device display,
- face recognition directly on the device display,
- receiving and handling multi-factor authentication confirmations.

14.2. Launching and login

Valid user credentials must be provided to enter a camera system.

11:00

Please enter your login details:

Username

Password

10.0.0.1

Enter

Overview Live view Recordings Views Setup

11:36 AM Fri Mar 10 100%

Please enter your login details:

Username

Password

10.0.0.1

Enter

Clear

Hold a button to create a new name.

Overview Live view Recordings Views Setup

NOTE

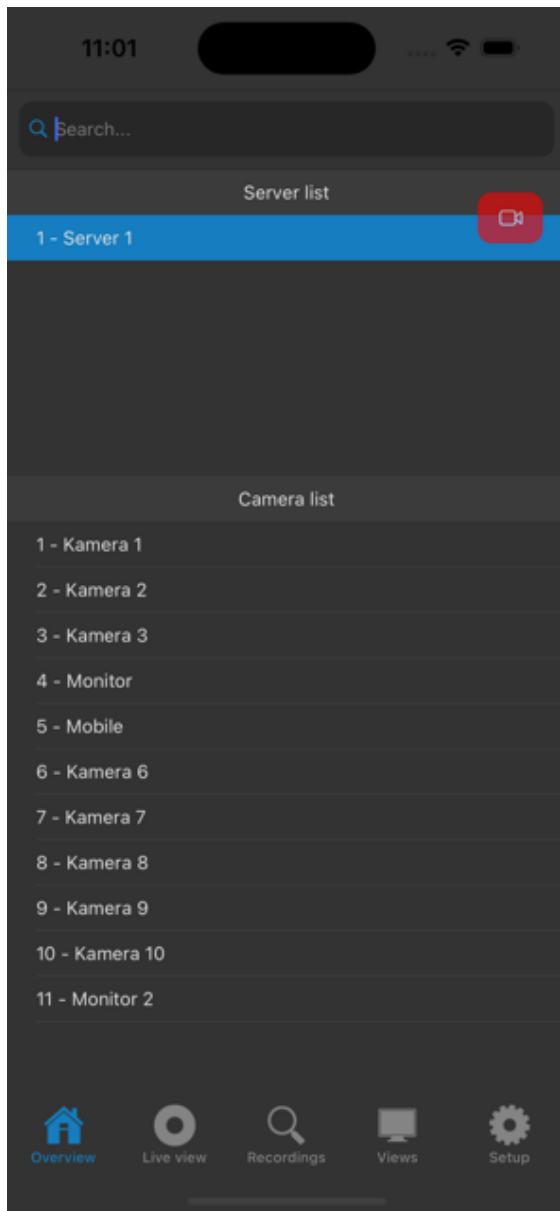
The app will remember your last login and if not deactivated in settings, repeated logins are automatic.

The camera system network names or IP addresses are maintained in your login history which can be displayed and a camera system can be selected easily.

TIP

All history items can be renamed to some user-friendly names to make your history more readable.

14.3. Camera list and live video



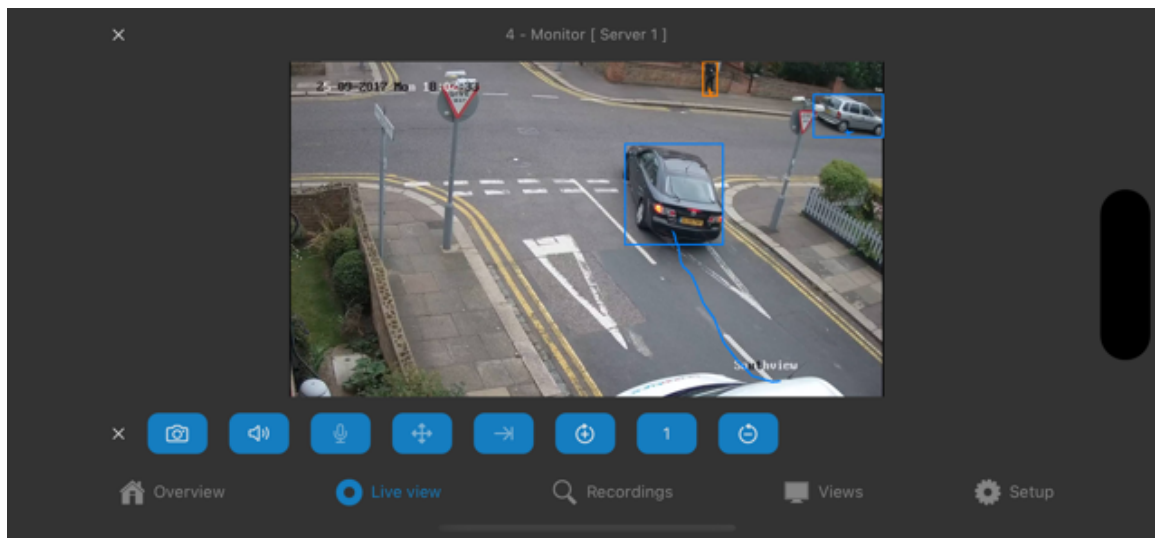
After a successful login, the app creates a connection to all camera servers available. Tapping a server displays all cameras available. Using the search field above the server list, you can easily search for cameras. The search is limited to the selected camera server.

TIP

Tapping an already selected camera server deselects the server so that searching will include all camera servers.

Selecting a camera activates the live mode.





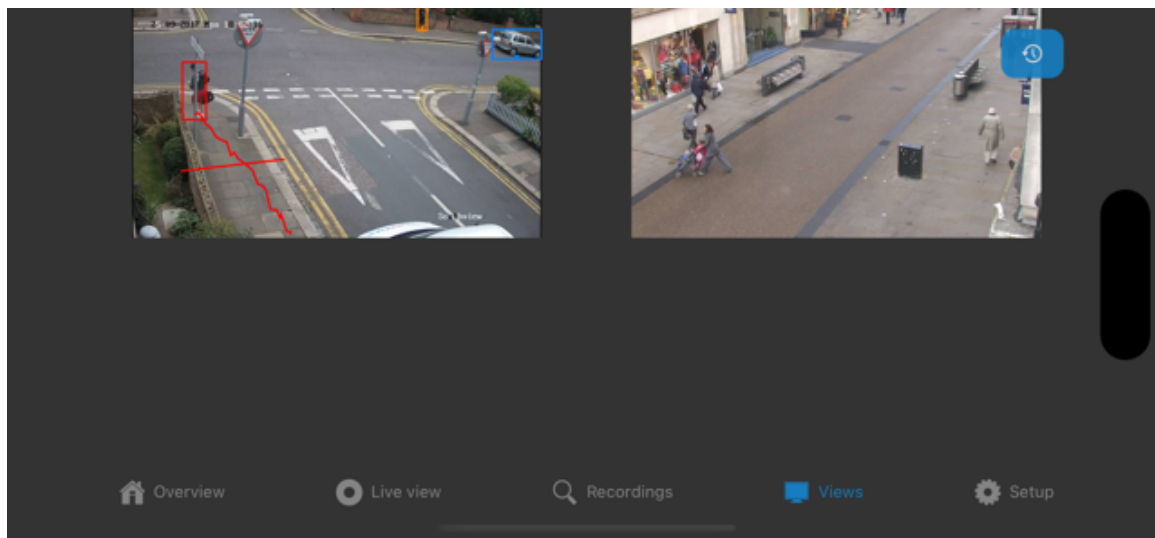
In live mode, the following buttons are available:

- button for taking a snapshot,
- button for connecting or disconnecting audio,
- button for activating or deactivating audio transmission to the device,
- button for activating PTZ control,
- button for displaying the list of presets,
- button for activating the output,
- button for changing the output number,
- button for deactivating the output.

In live mode, a swipe gesture can be used to switch between cameras. If you have selected a camera from the list, switching cameras will guide you through the list of cameras in that list. If the camera has been selected from a view, all cameras in the view will be presented one after the other.

14.4. Views of multiple cameras

In Views, it is possible to display the list of all views an administrator has shared and placed in the Mobile views group. These might be views consisting of 4, 9 or 16 cameras. Selecting a view opens the corresponding layout in live mode. The views reflect the secondary streams if configured.

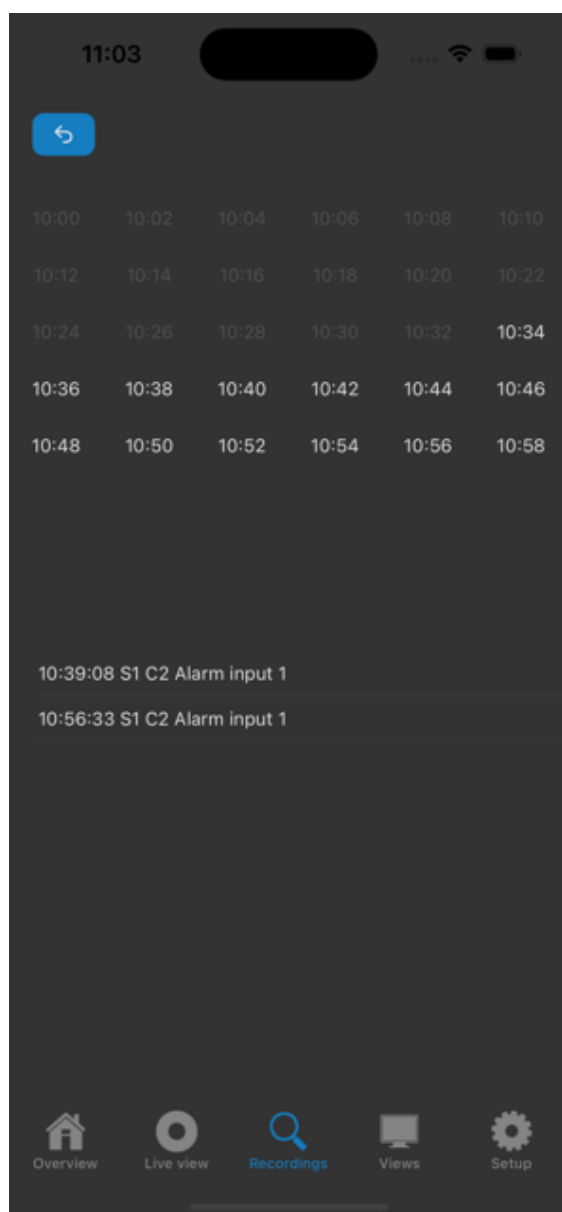


14.5. Replaying recordings

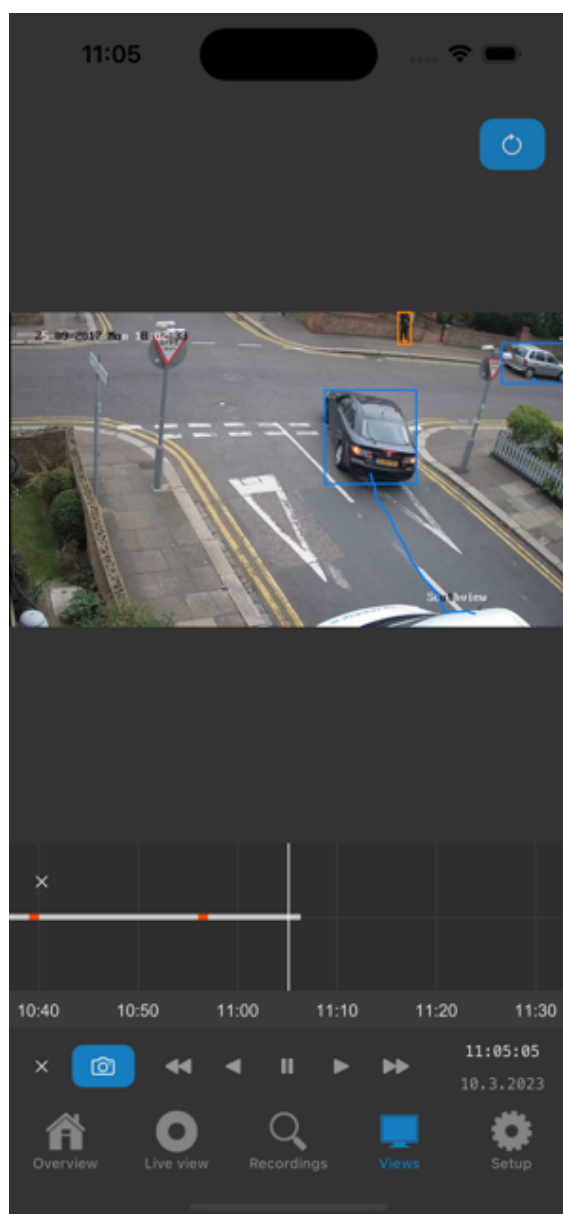
To enter the replay recordings app section, you can use the corresponding item in the main menu or you can switch an active view to replay mode. If the former option applies, a time overview will be displayed first for the selected camera, where, by successive selections, it is possible to reach a detailed hour overview with a list of events.

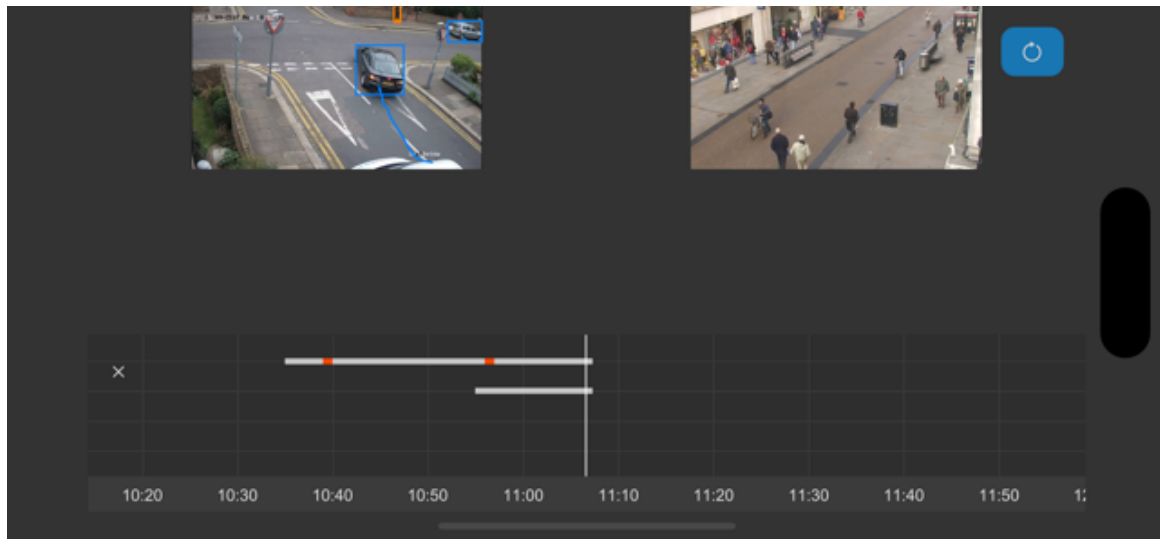
NOTE

In the overview, days or hours containing any events are visually marked for easy orientation.



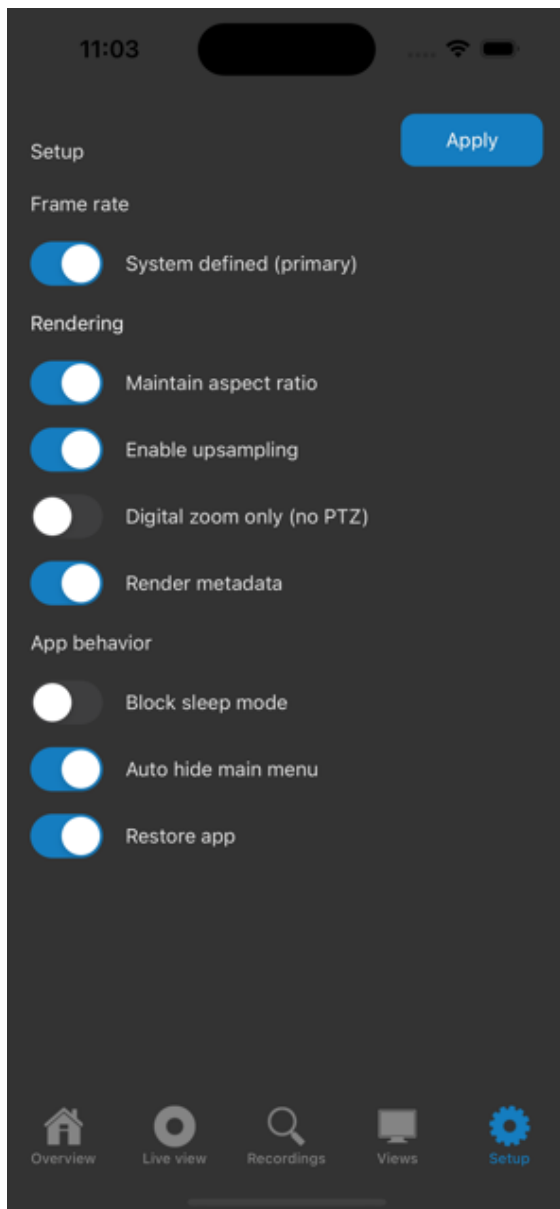
During the replay, two control panels are displayed. The time axis and the replay control which can be used to change the replay direction or speed.





14.6. Setup

The Setup section contains options for customizing the rendering or app behavior as shown in the following picture.



The Auto hide main menu option maximizes the video area if no screen touch is registered for a short amount of time. A double-tap can be used to display the menu again. The same principle is used for other control panels or menus (live video features, replay control, time axis). A double-tap always displays the main menu first followed by any specific control panels. After that, the default double-tap handler like switching a camera to detail mode will be called.

14.7. Using the integrated camera

NOTE

Video streaming from the mobile camera is available starting from the ATEAS Security PROFESSIONAL edition.

The app offers the unique feature of streaming video, audio and GPS coordinates of your device directly to ATEAS servers, where your camera behaves like a regular surveillance camera. In order to use the camera from your mobile device, an administrator must add a camera of type user to a camera server. This user is required to log in on the respective mobile device.

In order to stream audio, you have to activate audio in the basic setup of the camera. Likewise, in order to stream GPS coordinates (and locate the mobile device in a coordinate map live or during replay) your camera must be first placed at some default location in the map by the administrator.

The streaming can be initiated by tapping the camera symbol button on the main camera overview screen, the same button can be used to stop the streaming.

NOTE

An event can be coupled with this action so that operators are notified when devices start streaming.

If LP detection or face recognition are activated for the camera, you will be able to get an immediate feedback on the display of your device. This applies to faces saved in your face recognition database and for all system and user defined LP lists.



Chapter 15 - Access from Android devices

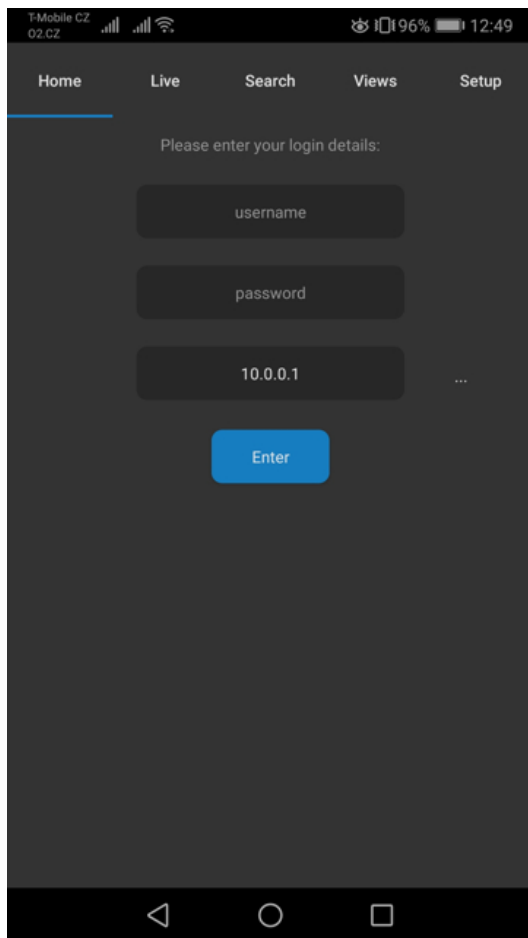
15.1. Supported features

The application for Android targets phone, TV and display devices and is equipped with features as follows:

- highly effective displaying of video (supported codecs are MJPEG, H264, H265 or AV1),
- hardware video acceleration,
- displaying mobile views of up to 16 cameras simultaneously,
- secondary stream support in shared views,
- simultaneous replay of all cameras in the view with timeline preview,
- playing audio (supported audio codec is G711),
- transmitting audio to the camera,
- digital zoom and digital PTZ for all cameras including recorded video,
- highly sensitive PTZ camera control based on PTZ priority configuration and permissions,
- sending cameras into preset positions,
- camera output activation based on the permissions,
- intuitive viewing and replaying of recorded video including audio,
- event preview and replay,
- local video display settings,
- exporting of snapshots,
- live video (and audio) transmission from the camera of the mobile device including GPS,
- live displaying and replay of neural networks metadata,
- push-video notifications upon system events,
- LP detection directly on the device display,
- face recognition directly on the device display,
- receiving and handling multi-factor authentication confirmations.

15.2. Launching and login

Valid user credentials must be provided to enter a camera system.

**NOTE**

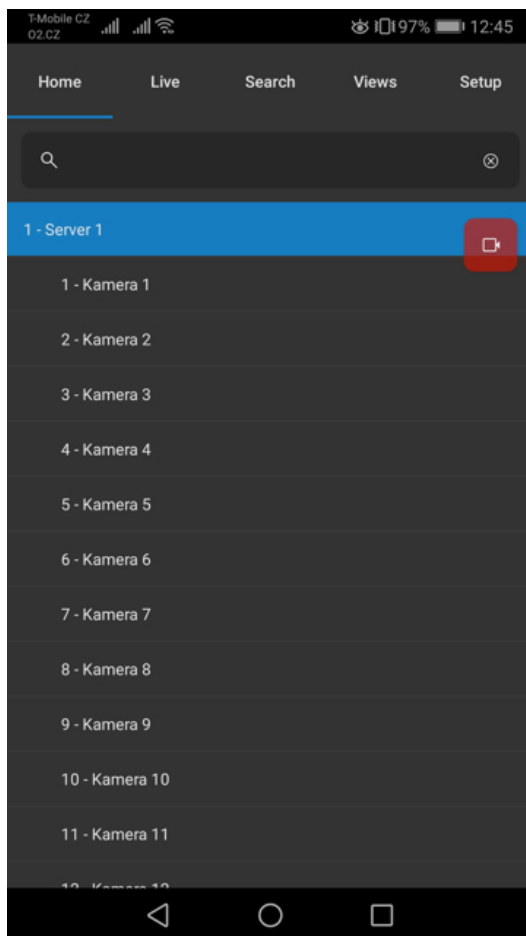
The app will remember your last login and if not deactivated in settings, repeated logins are automatic.

The camera system network names or IP addresses are maintained in your login history which can be displayed and a camera system can be selected easily.

TIP

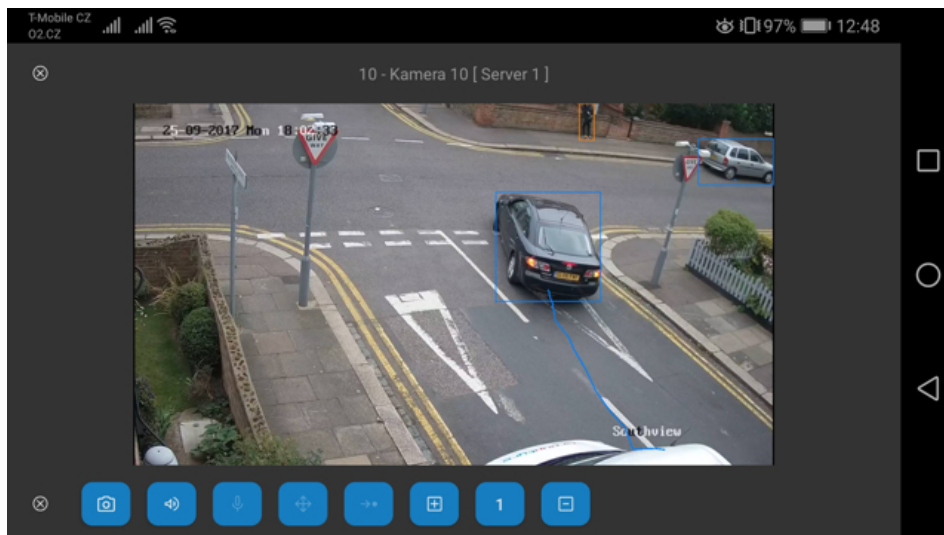
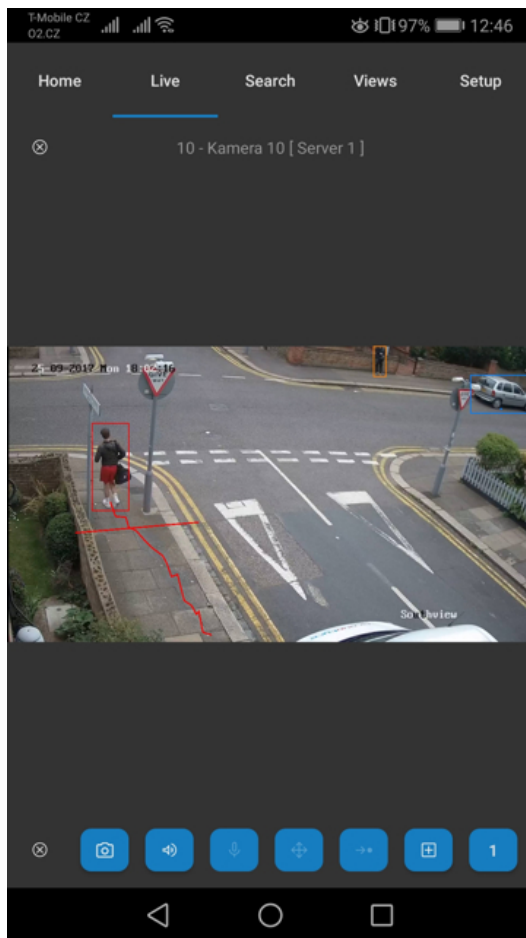
All history items can be renamed to some user-friendly names to make your history more readable.

15.3. Camera list and live video



After a successful login, the app creates a connection to all camera servers available. Tapping a server displays all cameras available. Using the search field above the server list, you can easily search for cameras. Searching is performed across all camera servers.

Selecting a camera activates the live mode.



In live mode, the following buttons are available:

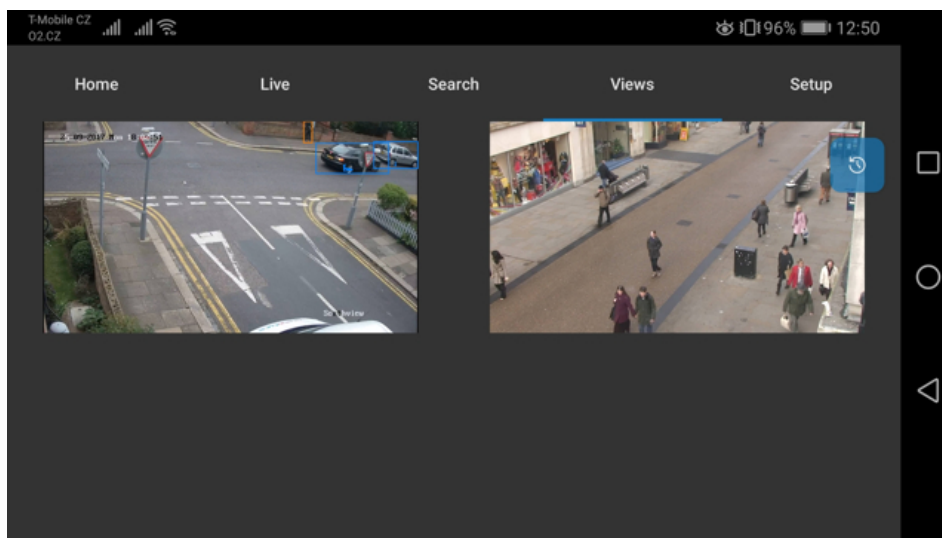
- button for taking a snapshot,
- button for connecting or disconnecting audio,

- button for activating or deactivating audio transmission to the device,
- button for activating PTZ control,
- button for displaying the list of presets,
- button for activating the output,
- button for changing the output number,
- button for deactivating the output.

In live mode, a swipe gesture can be used to switch between cameras. If you have selected a camera from the list, switching cameras will guide you through the list of cameras in that list. If the camera has been selected from a view, all cameras in the view will be presented one after the other.

15.4. Views of multiple cameras

In Views, it is possible to display the list of all views an administrator has shared and placed in the Mobile views group. These might be views consisting of 4, 9 or 16 cameras. Selecting a view opens the corresponding layout in live mode. The views reflect the secondary streams if configured.

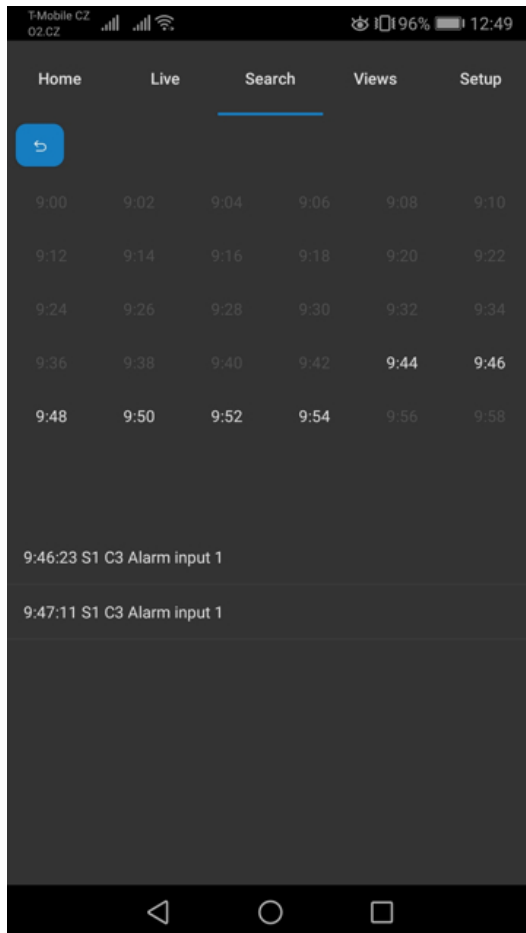


15.5. Replaying recordings

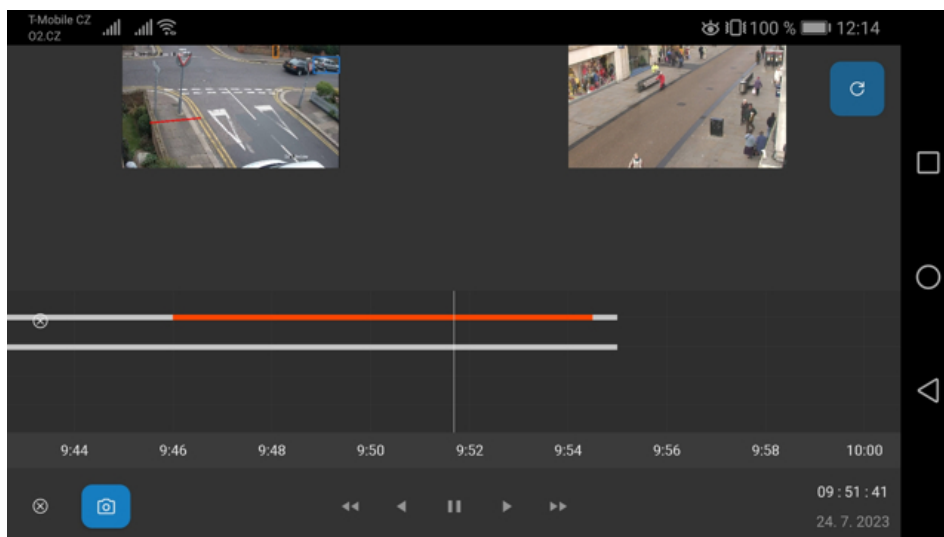
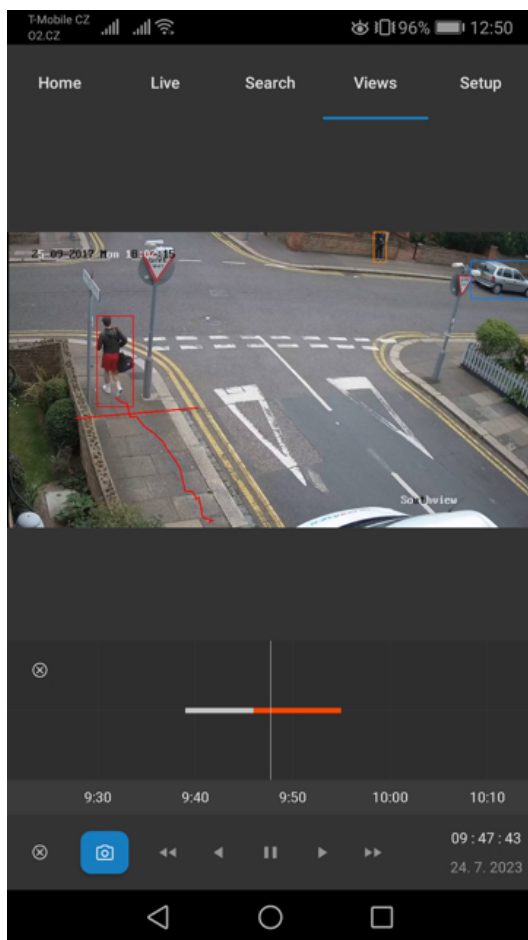
To enter the replay recordings app section, you can use the corresponding item in the main menu or you can switch an active view to replay mode. If the former option applies, a time overview will be displayed first for the selected camera, where, by successive selections, it is possible to reach a detailed hour overview with a list of events.

NOTE

In the overview, days or hours containing any events are visually marked for easy orientation.

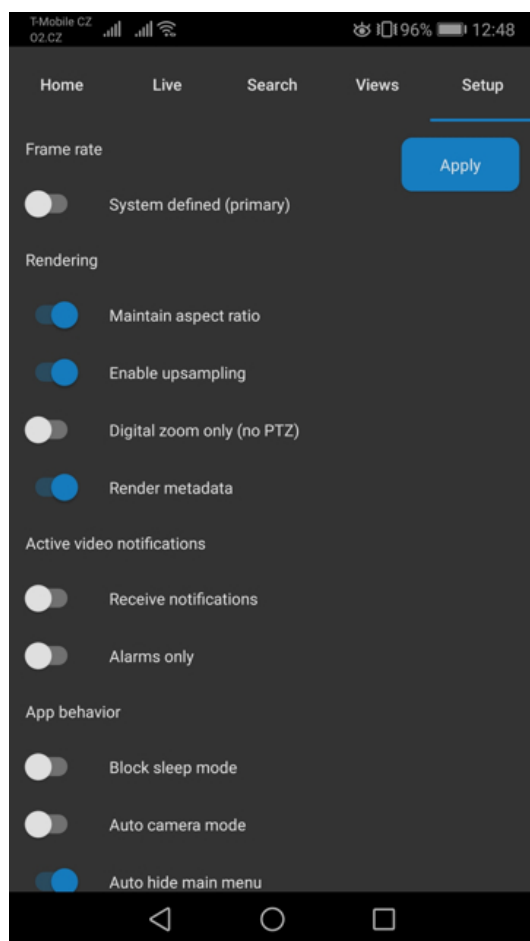


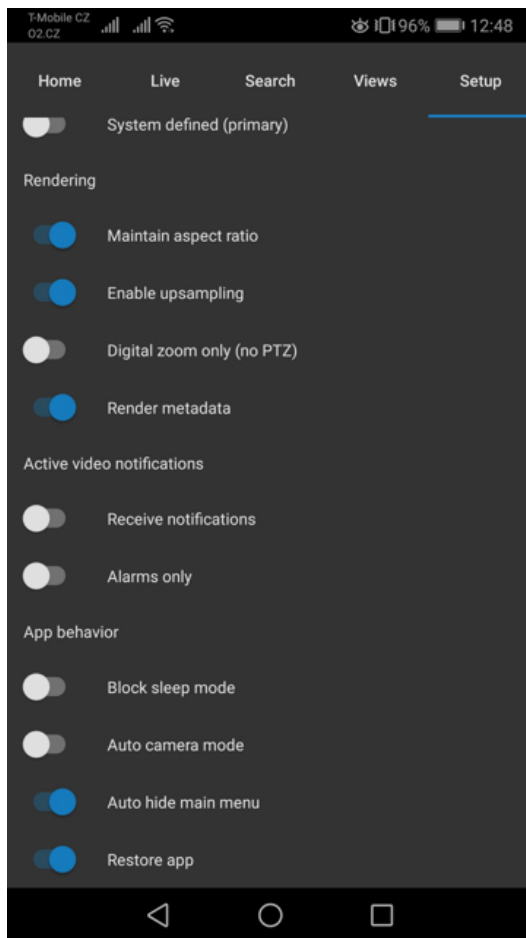
During the replay, two control panels are displayed. The time axis and the replay control which can be used to change the replay direction or speed.



15.6. Setup

The Setup section contains options for customizing the rendering or app behavior as shown in the following picture.

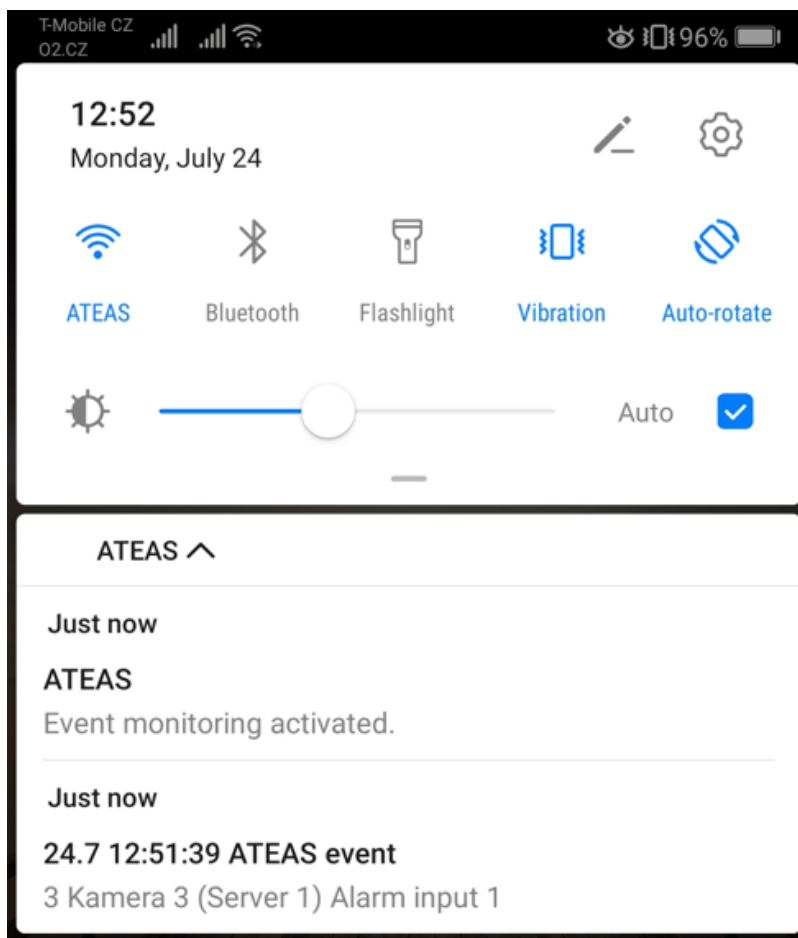




The Auto hide main menu option maximizes the video area if no screen touch is registered for a short amount of time. A double-tap can be used to display the menu again. The same principle is used for other control panels or menus (live video features, replay control, time axis). A double-tap always displays the main menu first followed by any specific control panels. After that, the default double-tap handler like switching a camera to detail mode will be called.

15.7. Notifications

In the Setup section, the push-video feature can be activated. After activation, the device will receive system events with a simple one-tap replay option. This feature maintains a data connection directly to the administration server and does not involve any operating system push services. It has been highly optimized for minimal power consumption.



If your device temporarily loses data connection, notifications will be delivered once the connection has been reestablished.

TIP

To limit the number of delivered notifications, you can activate the Alarms only option or you can restrict the user account in its permissions to receive events from specific cameras only.

15.8. Using the integrated camera

NOTE

Video streaming from the mobile camera is available starting from the ATEAS Security PROFESSIONAL edition.

The app offers the unique feature of streaming video, audio and GPS coordinates of your device directly to ATEAS servers, where your camera behaves like a regular surveillance camera. In order to use the camera from your mobile device, an administrator must add a camera of type user to a camera server. This user is required to log in on the respective mobile device.

In order to stream audio, you have to activate audio in the basic setup of the camera. Likewise, in order to stream GPS coordinates (and locate the mobile device in a coordinate map live or during replay) your camera must be first placed at some default location in the map by the administrator.

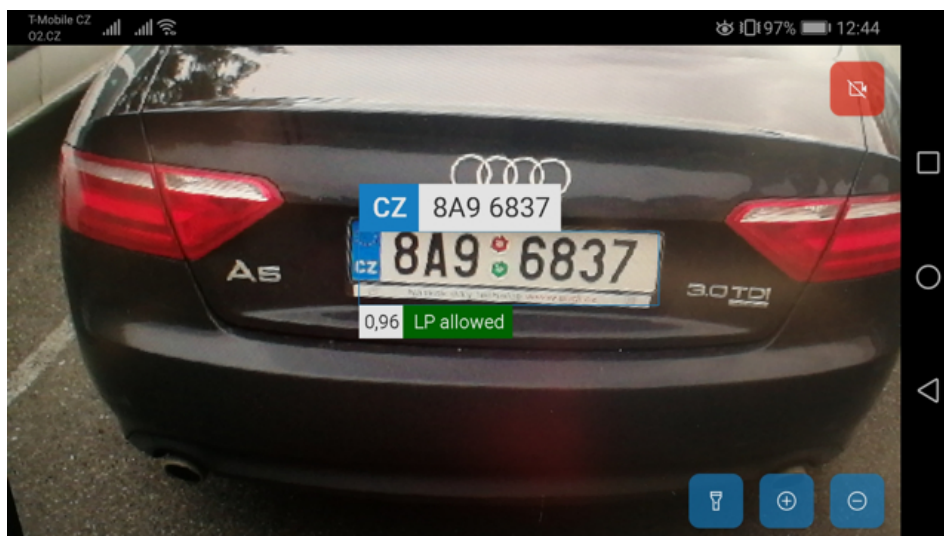
The streaming can be initiated by tapping the camera symbol button on the main camera overview screen, the same button can be used to stop the streaming.

NOTE

An event can be coupled with this action so that operators are notified when devices start streaming.

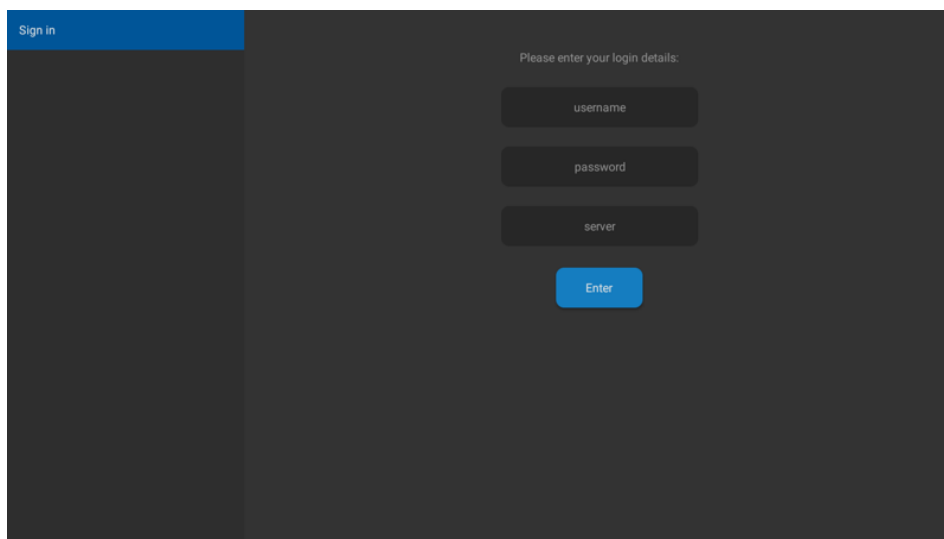
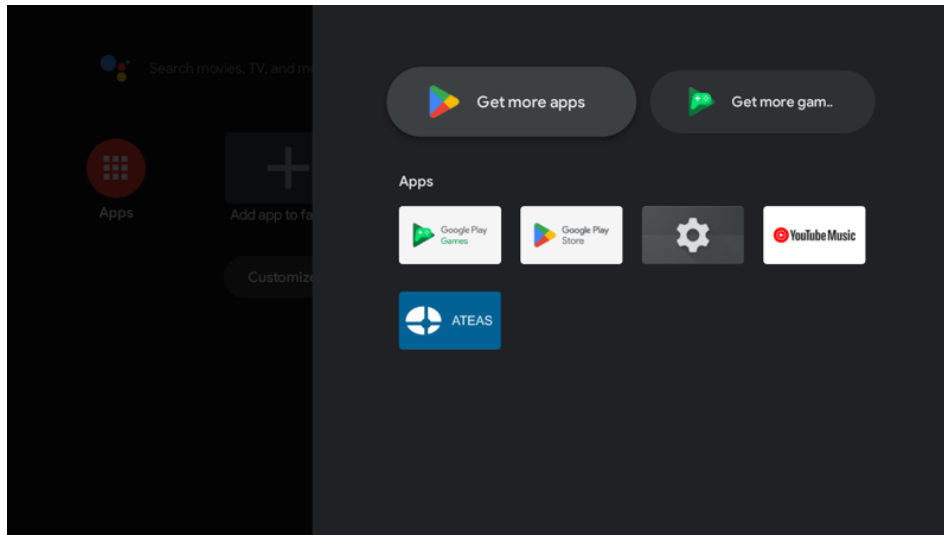
If supported by the device, you can use the zoom buttons to perform linear zooming or use a pinch-to-zoom feature in video area. During video transmission, the device torch can be activated.

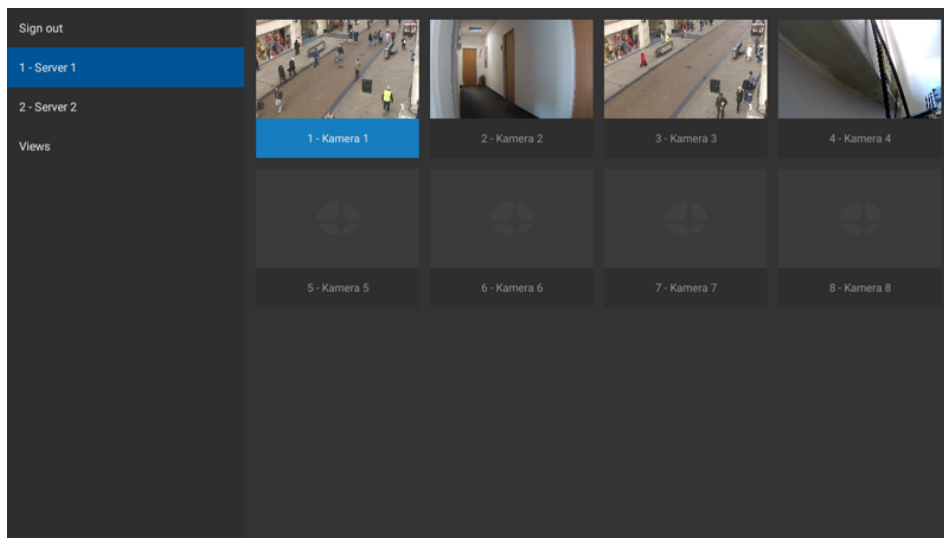
If LP detection or face recognition are activated for the camera, you will be able to get an immediate feedback on the display of your device. This applies to faces saved in your face recognition database and for all system and user defined LP lists.



15.9. Android TV

Running on a TV or display device, the app features and updated interface to comply with standard remote control.





The TV app can be used to display individual cameras or views. The views reflect the secondary streams if configured.

TIP

The camera preview image can be uploaded to the server after saving a camera snapshot.

15.9.1. Video wall

TV and display devices can be part of an ATEAS video wall and it is possible to manage and remotely control them just like regular PC stations with client in slave mode installed (for remote control from other computers),

Chapter 16 - Application for monitoring the screen

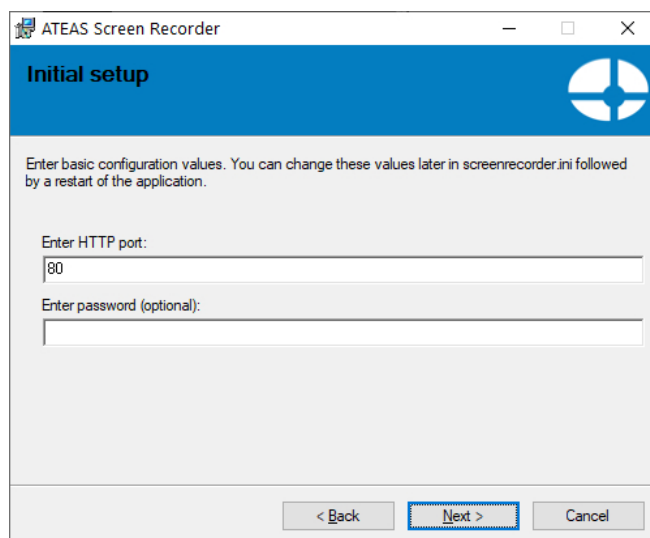
16.1. Installation and start-up

Security systems usually include the demand for monitoring the computer screens (or any particular window) of certain users by providing a live view and recording of user actions. ATEAS Security includes the ATEAS Screen Recorder application which can turn the computer, on which it is installed, into a camera. Authorized users can therefore watch live video, the camera can make recordings including motion detection etc. The data stored from the computer screen can be processed further as with any other camera including the option of synchronous playback with other cameras, searching and playback, exporting snapshots or videos etc.

CAUTION

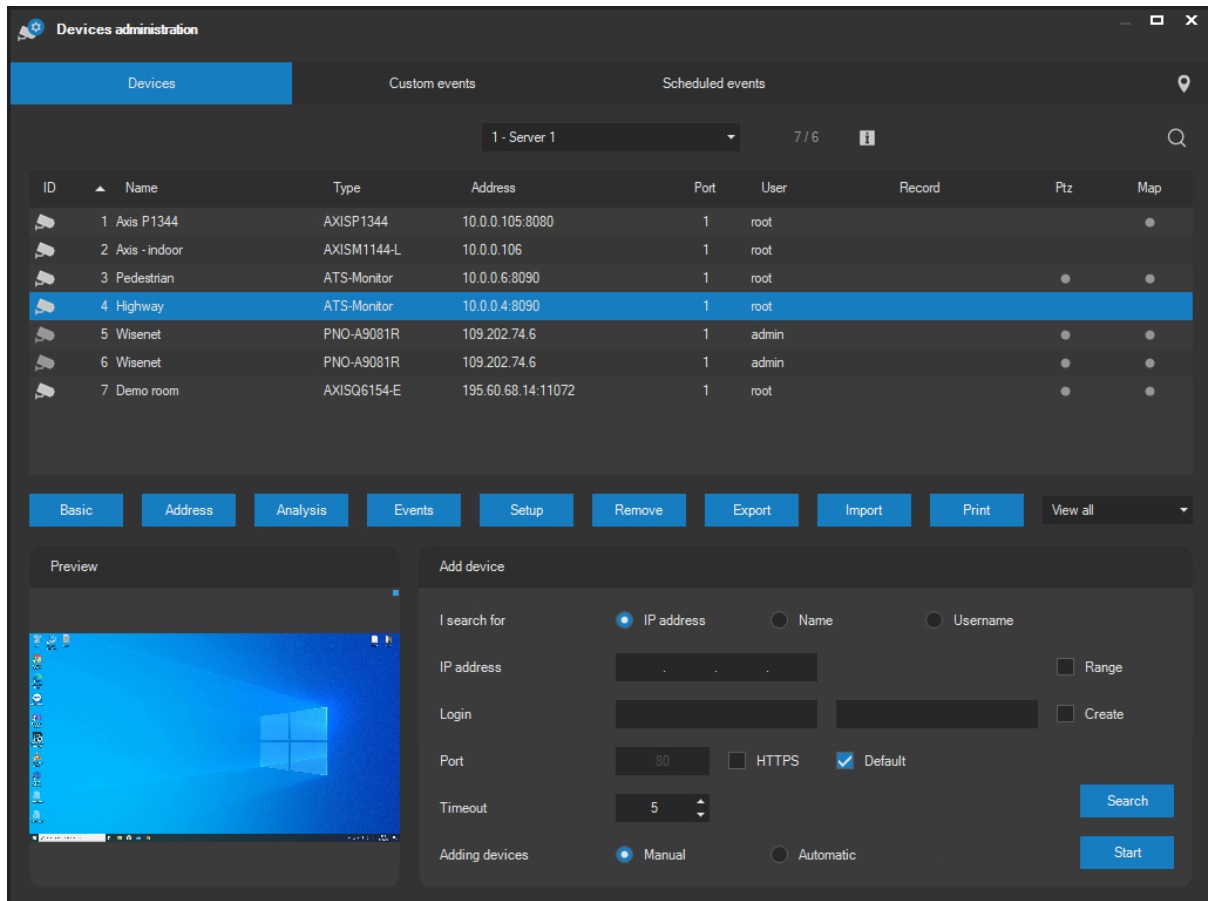
A computer screen can be added to the server as an ATEAS Monitor camera from version ATEAS Security PROFESSIONAL or higher.

The link for installing the application for computer screen monitoring is available on the installation media home page and on the system administration server web site. The installation uses the same wizard as does the installation of other applications. The only dialog specific to this installation is the option to enter basic settings parameters - HTTP port and password.



The screenshot shows the 'Initial setup' window for the ATEAS Screen Recorder application. The window has a blue header bar with the title 'ATEAS Screen Recorder' and a close button. Below the header, the text 'Initial setup' is displayed. A message states: 'Enter basic configuration values. You can change these values later in screenrecorder.ini followed by a restart of the application.' There are two input fields: 'Enter HTTP port:' with the value '80' entered, and 'Enter password (optional):' which is empty. At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

You can leave the default value of 80 in the Enter port text field or change it to a different network port number. You can optionally enter a password that will be requested when adding a camera to the system (for any user name). These parameters can be configured later using the screenrecorder.ini configuration file located in the folder in which the application is installed.



NOTE

Due to the option of accessing the computer screen and for security reasons, ATEAS Screen Recorder is started only after the user has logged into the system.

CAUTION

ATEAS Screen Recorder does not support multiple users logged in simultaneously and therefore the simultaneous adding of multiple cameras on different ports of one computer (e.g. two users logged in to one Windows station at the same time).

After the application is installed, it is automatically started and its automatic start-up is also ensured with each computer restart and user login. By default, the application start-up is indicated by the ATEAS icon in the Windows system tray. Right-clicking on this icon will open a context menu with one available option, Exit, which is used to close the application.

NOTE

To hide ATEAS Screen Recorder on the computer, the ATEAS icon can be hidden in the system tray by configuration in the INI file. See next subchapter.

16.2. Configuration

Video settings are configured directly by adjusting the camera settings in the client application. Frame rate settings (within 1 - 25 FPS) and video compression level settings (supported format is MJPEG) are supported.

The application is configured using the screenrecorder.ini configuration file located in the folder in which the application is installed. Changing any of the keys in this file requires restarting ATEAS Screen Recorder for changes to take effect. The following keys are available:

HTTPPORT - indicates the number of the port on which the camera will be available,

SHOWICON - indicates whether the icon in the system tray will be displayed (1) or hidden (0),

PASSWORDHASH - indicates the hashing of the password used for accessing the camera. The password will not be required if the value is deleted. Since the password hash is written to this key during the installation, a new password cannot be directly entered here.

NOTE

To set a new password for the camera - screen - on this computer, you must reinstall ATEAS Screen Recorder.

PROCID – empty by default. This item may contain the process ID. If the process ID is filled in, ATEAS Screen Recorder will not use the entire desktop to create the video stream, but only the main window associated with the specified process.

NOTE

Monitoring a selected window can be used, for example, for an offline testing of images or videos from a future vehicle license plate detection and recognition module installation sites.

MUTEXLEVEL – if the value is set to 1, the application cannot be started multiple times. By changing the value to 0 and installing the application into separate user folders, it is possible to launch the recorder multiple times, which may be useful for thin clients (terminal services).

CAPTUREMOUSE – the value is set to 0 by default, if changed to 1, the mouse cursor will become part of the video stream.

ACTIVESCREEN – the value is set to 0 by default, if changed to 1, an ATEAS client will be able to control this computer remotely. To be able to control all windows on the computer including privileged windows with computer settings etc., it is necessary to launch the recorder as an administrator. The computer can be controlled with all mouse and keyboard input events.

NOTE

To get the best look and smooth image for remote control, it is recommended to activate GPU acceleration for video rendering on the client.

Chapter 17 - Appendix 1 – Network configuration

In order to run ATEAS Security applications, you might need to configure certain network devices (for example, network routers, especially when the camera system is located within the local network) so that server applications will be able to operate on their specified ports. The table below shows a general overview of the network ports. The system client is always the party establishing connections. Therefore, no special settings have to be performed on the client side.

NOTE

Basic system operation requires verifying that port 8501 for the administration server and port 8502 for the camera server are open. Other ports are used for advanced functionality and integration.

17.1. Administration server

Port	Transport protocol	Application protocol	Communication
8501	TCP	ATEAS	Basic communication port
8503	TCP	ATEAS	Cloud based connection
8504	TCP	ATEAS	Receiving external events
9001 - N	TCP	WebSocket / TLS	Cloud based connection for web clients
80	TCP	HTTP	System home page, web client, automatic updates
443	TCP	HTTPS / TLS	System home page, web client, automatic updates
162	UDP	SNMP	Receiving traps for event activation

17.2. Camera server

Port	Transport protocol	Application protocol	Communication
8502	TCP	ATEAS	Basic communication port

8505	TCP	ATEAS	Custom camera events
8506	TCP	HTTP	Access to the web page of all cameras
8507	TCP	WebSocket	Unsecured web streaming
8508	TCP	WebSocket / TLS	Secured web streaming
8509	TCP	HTTP	Video streaming using DLNA
3702 - 3	UDP	SOAP	Searching Onvif devices (WS Discovery)
8080	TCP	HTTP	Body Worn System

CAUTION

If the RTP/UDP scheme is used for transmitting camera data, UDP ports are dynamically allocated and an exception for the entire camera server shall be set, not just for specific ports. This also applies for the client, provided its profile is set to LOCAL and therefore connects to multicast addresses and receives data via the UDP protocol.

Chapter 18 - Appendix 2 – ATEAS API

18.1. Communication basics

It is possible to use a TCP or HTTP protocol based channel. Using the TCP protocol may be easier and may be supported by a wider range of external devices. The transmission, however, cannot be secured, nor is it possible to require authentication. Using the HTTP protocol, TLS can be enforced for maximum security and it is also possible to require authentication.

Using this API, the administration and camera servers are listening on the specified ports, whereas external devices are responsible for creating and maintaining connections.

The administration server listens on the API ports 8504 (TCP channel) and 80 (HTTP) which is default HTTP port of the administration server and may be changed in the configuration file. The camera server listens on the API ports 8505 (TCP channel) and 8080 (HTTP) which is default HTTP port of the camera server and may be changed in the configuration file.

The HTTP protocol uses standard HTTP response codes. Sending data must be performed with the HTTP POST method. The HTTP protocol may return data in JSON format.

Using the TCP protocol, unsolicited messages may be sent (e.g. system events). For this purpose, WebSocket protocol is used on HTTP protocol level. Data can have the JSON or XML format.

Text encoding can be configured for TCP protocol when opening the channel. HTTP protocol defaults to UTF8 encoding.

TIP

You can find some useful links to TCP and HTTP implementation examples on the homepage of your administration server.

18.2. ATEAS API of the administration server

18.2.1. External events

Receiving an external event

Protocol	API
TCP	[ATEAS EVENT (status) (objectid) (elementid)]
HTTP	POST /api-base/event DATA: status=(status)&objectid=(objectid)&elementid=(elementid)

Parameters:

Parameter	Value	Default	Description
status	START, STOP		Start or stop
objectid	1 – 10 000		Object number
elementid	1 – 99 999		Element number

Example:

Protocol	API
TCP	[ATEAS EVENT START 1 1]
HTTP	DATA: status=START&objectid=1&elementid=1

18.2.2. Video wall

Switch content to video wall

Protocol	API
TCP	[ATEAS VIDEOWALL (monitor) (submonitor) (serverid) (deviceid) (wallid) (meta)]
HTTP	POST /api-base/videowall DATA: monitor=(monitor)&submonitor=(submonitor)& serverid=(serverid)&deviceid=(deviceid)&wallid=(wallid)&meta=(meta)

Parameters:

Parameter	Value	Default	Description
-----------	-------	---------	-------------

monitor	1 – 192		Monitor number
submonitor	0 – 16	0	Submonitor number
serverid	1 – 9 999		Server number
deviceid	1 – 999		Device number
wallid	1 – 1000	1	Video wall number
meta	0 – 1	0	Metadata yes or no

Example:

Protocol	API
TCP	[ATEAS VIDEOWALL 1 1 1 10 1 0]
HTTP	DATA: monitor=1&submonitor=1&serverid=1&deviceid=10&wallid=1&meta=0

NOTE

For monitors of type 4, 9 or 16, a submonitor value must be passed.

NOTE

If both serverid and deviceid values are zero, the monitor will be turned off (video disappears and the default ATEAS logo shows up).

NOTE

If serverid is zero, a positive deviceid will be interpreted as a URL number of a web content link created by the administrator).

NOTE

For TCP protocol, if using the optional wallid parameter, the submonitor parameter must be passed as well to enable the server to parse the message.

18.2.3. License plates

LP list assignment

Protocol	API
TCP	
HTTP	POST /api-base/plate DATA: plate=(plate)&list=(list)

Parameters:

Parameter	Value	Default	Description
plate	(plate)		License plate
list	none, white, black, user1, user2, custom		List assignment

Example:

Protocol	API
TCP	
HTTP	DATA: plate=2A56217&plate=white

JSON response:

```
{
  "Plate": "2A56217",
  "List": "white"
}
```

NOTE

License plates can be provided in both decorative and normalized form.

NOTE

The list parameter is optional. If omitted, the current list of the LP will be returned.

18.2.4. Face database

Adding a group of people

Protocol	API
TCP	
HTTP	POST /api-base/face/group/add DATA: name=(name)

Parameters:

Parameter	Value	Default	Description
name	(name)		Group name

Example:

Protocol	API
TCP	
HTTP	DATA: name=group

JSON response:

```
{  
  "result": "ok",
```

```
{  
  "id": 2,  
  "name": "group"  
}
```

NOTE

Groups with duplicate names disregarding any case differences cannot be created.

Removing a group of people

Protocol	API
TCP	
HTTP	POST /api-base/face/group/remove DATA: id=(id)

Parameters:

Parameter	Value	Default	Description
id	(id)		Group number

Example:

Protocol	API
TCP	
HTTP	DATA: id=2

JSON response:

```
{  
  "result": "ok"  
}
```

Renaming a group of people

Protocol	API
TCP	
HTTP	POST /api-base/face/group/name DATA: id=(id)&name=(name)

Parameters:

Parameter	Value	Default	Description
id	(id)		Group number
name	(name)		New group name

Example:

Protocol	API
TCP	
HTTP	DATA: id=2&name=group

JSON response:

```
{  
  "result": "ok"  
}
```

Adding a person

Protocol	API
TCP	

HTTP	POST /api-base/face/person/add DATA: name=(name)&group=(group)&uuid=(uuid)
-------------	--

Parameters:

Parameter	Value	Default	Description
name	(name)		Person name
group	(id)	1	Group number
uuid	(uuid)		Custom identifier

Example:

Protocol	API
TCP	
HTTP	DATA: name=person&group=&uuid=

JSON response:

```
{
  "result": "ok",
  "id": 1,
  "name": "person",
  "uuid": ""
}
```

NOTE

The uuid parameter can be used as an external identifier e.g. in an access system. It will also be part of the face recognition event.

Removing a person

Protocol	API
TCP	
HTTP	POST /api-base/face/person/remove DATA: id=(id)

Parameters:

Parameter	Value	Default	Description
id	(id)		Person number

Example:

Protocol	API
TCP	
HTTP	DATA: id=1

JSON response:

```
{
  "result": "ok"
}
```

Edit a person

Protocol	API
TCP	
HTTP	POST /api-base/face/person/update DATA: id=(id)&name=(name)&group=(group)&uuid=(uuid)

Parameters:

Parameter	Value	Default	Description
id	(id)		Person number
name	(name)		New person name
group	(id)		Group number
uuid	(uuid)		Custom identifier

Example:

Protocol	API
TCP	
HTTP	DATA: id=1&name=person&group=2&uuid=

JSON response:

```
{
  "result": "ok",
  "name": "person",
  "uuid": ""
}
```

Adding a face

Protocol	API
TCP	
HTTP	POST /api-base/face/person/image DATA: person=(person)&serverid=(serverid)&index=(index)&data=(data)

Parameters:

Parameter	Value	Default	Description
-----------	-------	---------	-------------

person	(id)		Person number
serverid	(id)		Server number for analytics
index	0 – 9	0	Image index
data	(uuid)		Image data

Example:

Protocol	API
TCP	
HTTP	DATA: person=1&serverid=1&index=0&data=

JSON response:

```
{
  "result": "ok",
  "image": "/9j/4AA..."
}
```

NOTE

The data parameter is expected to contain a base64 encoded jpeg or bmp image with a 24 or 32-bit pixel color. If the data parameter is empty, the image will be removed.

NOTE

After a face image has been successfully saved in the database, the response contains the canonical face representation as a base64 encoded jpeg image data blob.

18.2.5. User and group management

Adding a user

Protocol	API
TCP	
HTTP	POST /api-base/user/add DATA: name=(name)&group=(name)&slave=(slave)

Parameters:

Parameter	Value	Default	Description
name	(name)		User name
group	(name)	USER	Group name
slave	(slave)	0	Video wall slave account

Example:

Protocol	API
TCP	
HTTP	DATA: name=operator

JSON response:

```
{
  "result": "ok",
  "userid": 2,
  "group": "USER"
}
```

NOTE

Apart the system defined user groups USER and ADMINISTRATOR, any existing group name can be used.

Deleting a user

Protocol	API
TCP	
HTTP	POST /api-base/user/delete DATA: userid=(id)

Parameters:

Parameter	Value	Default	Description
userid	(id)		User identification

Example:

Protocol	API
TCP	
HTTP	DATA: userid=2

JSON response:

```
{
  "result": "ok",
  "userid": 2
}
```

Profiling a user

Protocol	API
TCP	
HTTP	POST /api-base/user/profile DATA: userid=(id)&serverid=(id)&profile=(profile)

Parameters:

Parameter	Value	Default	Description
userid	(id)		User identification
serverid	(id)		Server identification
profile	(profile)		Server profile (no, default, local, remote)

Example:

Protocol	API
TCP	
HTTP	DATA: userid=1&serverid=1&profile=default

JSON response:

```
{
  "result": "ok",
  "userid": 1,
  "profile": "default"
}
```

Adding a group

Protocol	API
TCP	
HTTP	POST /api-base/group/add DATA: name=(name)

Parameters:

Parameter	Value	Default	Description
name	(name)		Group name
group	(name)	USER	Group base name

Example:

Protocol	API
TCP	
HTTP	DATA: name=operators

JSON response:

```
{
  "result": "ok",
  "groupid": 1,
  "group": "USER",
}
```

NOTE

Group parameter must be one of the system predefined base groups USER or ADMINISTRATOR.

Deleting a group

Protocol	API
TCP	
HTTP	POST /api-base/group/delete DATA: groupid=(id)

Parameters:

Parameter	Value	Default	Description
groupid	(id)		Group identification

Example:

Protocol	API
TCP	
HTTP	DATA: groupid=1

JSON response:

```
{
  "result": "ok",
  "groupid": 1
}
```

Profiling a group

Protocol	API
TCP	
HTTP	POST /api-base/group/profile DATA: groupid=(id)&serverid=(id)&profile=(profile)

Parameters:

Parameter	Value	Default	Description
groupid	(id)		Group identification
serverid	(id)		Server identification
profile	(profile)		Server profile (no, default, local, remote)

Example:

Protocol	API
TCP	
HTTP	DATA: groupid=1&serverid=1&profile=default

JSON response:

```
{
  "result": "ok",
  "groupid": 1,
  "profile": "default"
}
```

18.2.6. Device management

Adding a device

Protocol	API
TCP	
HTTP	POST /api-base/device/add DATA: serverid=(serverid)&host=(host) &user=(user)&password=(password) &deviceid=(deviceid)

Parameters:

Parameter	Value	Default	Description
serverid	(id)		Server identification
host	(host)		Host name or IP endpoint
user	(user)		User name
password	(password)		User password
deviceid	(id)	0	Device identification

index	(index)	1	Device index
-------	---------	---	--------------

Example:

Protocol	API
TCP	
HTTP	DATA: name=10.0.0.100&serverid=1&user=root&password=pass&deviceid=&index=

JSON response:

```
{
  "result": "ok",
  "serverid": 1,
  "deviceid": 1,
  "model": "Axis P1346",
  "format": "mjpg",
  "profile": "",
  "ptz": "no",
  "audio": "full"
}
```

NOTE

The deviceid parameter may be omitted or set to zero to assign a device number automatically.

NOTE

The index parameter may be set to a higher value to address devices with multiple sources on a single IP address.

Deleting a device

Protocol	API
TCP	
HTTP	POST /api-base/device/delete DATA: serverid=(serverid)&deviceid=(deviceid)

Parameters:

Parameter	Value	Default	Description
serverid	(id)		Server identification
deviceid	(id)		Device identification

Example:

Protocol	API
TCP	
HTTP	DATA: serverid=1&deviceid=1

JSON response:

```
{
  "result": "ok",
  "serverid": 1,
  "deviceid": 1
}
```

Configuring a device

Protocol	API
TCP	
HTTP	POST /api-base/device/setup DATA: serverid=(serverid)&deviceid=(deviceid)&format=(format)&profile=(profile) &ptz=(ptz)&audio=(audio)&rule=(rule)

Parameters:

Parameter	Value	Default	Description
serverid	(id)		Server identification
deviceid	(id)		Device identification
name	(name)	""	Device name
format	(format)	""	Video format (mjpg, mpg4, h264, h265)
profile	(profile)	""	Video profile
ptz	(ptz)	""	PTZ support (yes, no)
audio	(audio)	""	Audio support (yes, no)
rule	(rule)	""	Name of the recording rule or none.

Example:

Protocol	API
TCP	
HTTP	DATA: serverid=1&deviceid=1&format=h264&rule="base"

JSON response:

```
{
  "result": "ok",
  "serverid": 1,
  "deviceid": 1
}
```

NOTE

Natively integrated devices may use the format value to change the video format. Onvif compatible devices use the profile parameter to select an existing media profile instead.

NOTE

Rule can be set to none to remove a recording rule from the camera.

18.2.7. Event notifications

Subscription

Protocol	API
TCP	automatic
HTTP	GET /api-base/events/subscribe&filter=all

The HTTP version of this API uses SSE (Server-Sent Events) protocol for maximum and straight-forward interoperability with both desktop and web applications.

TCP event start XML

```
<?xml version="1.0" encoding="utf-8"?>
<ateas>
  <event>
    <id>1-464646</id>
    <level>1</level>
    <server>
      <id>1</id>
      <name>Server 1</name>
    </server>
    <camera>
      <id>1</id>
      <name>Camera 1</name>
    </camera>
    <source>
```

```
<id>1</id>
</source>
<datetime>
  <utcstamp>128989433710312500</utcstamp>
  <localvalue>1.7.2023 9:05:51</localvalue>
</datetime>
<data></data>
<dataex></dataex>
<uuid></uuid>
</event>
</ateas>
```

TCP event stop XML

```
<?xml version="1.0" encoding="utf-8"?>
<ateas>
  <eventstop>
    <id>1-464646</id>
    <datetime>
      <utcstamp>128989433710312500</utcstamp>
      <localvalue>1.7.2023 9:05:51</localvalue>
    </datetime>
    <data></data>
  </eventstop>
</ateas>
```

HTTP event start JSON

```
{
  "Action": "START",
  "ID": "1-464646",
  "Time": {
    "Timestamp": 133758779641144365,
    "LocalValue": "12.11.2024 10:39:24"
  },
  "Type": "EVENT",
  "Server": {
    "ID": 1,
    "Name": "Server 1"
  }
}
```

```
{
  "Device": {
    "ID": 1,
    "Name": "Device 1"
  },
  "Source": 1,
  "Input": {
    "Number": 1
  },
  "LicensePlate": {
    "RawText": "001ATEAS",
    "NiceText": "001 ATEAS",
    "Country": "CZ",
    "Direction": ""
  },
  "WagonNumber": {
    "RawText": "218124712173",
    "NiceText": "2181 2471 217-3",
    "Direction": "LEFT"
  },
  "Face": {
    "UUID": "1",
    "Name": "Test face",
    "Group": "Main"
  },
  "Image": {
    "Detail": "base64",
    "Image": "base64"
  }
}
```

The image object, if it exists, contains JPEG data encoded using the Base64 encoding scheme.

HTTP event stop JSON

```
{
  "Action": "STOP",
  "ID": "1-464646",
  "Time": {
    "Timestamp": 133758780524709309,
```

```
"LocalValue": "12.11.2024 10:40:52"  
}  
}
```

NOTE

Events are centralized and collected from all camera servers.

NOTE

The source number uniquely identifies the event type, which can be observed using the test tool.

Source ID examples:

- 1 – camera motion detection
- 2 – device unavailable
- 3 – alarm input, data contains the input number
- 10 – 14 – vehicle LP detection, data contains the LP in decorative form
- 32 – video quality loss, data contains the required frame rate level
- 40 – server based motion detection
- 51 – 100 – custom events
- 110 – manual recording event
- 111 – 130 – Onvif events, data may contain additional information
- 131 – 150 – complex events
- 151 – 200 – custom events
- 201 – 250 – analytical events

NOTE

The UTC timestamp indicates the absolute time not affected by the time zone or daylight time changes. It is expressed as the number of 100-nanosecond intervals elapsed since 1.1.1601 UTC.

18.2.8. User notifications

Subscription

Protocol	API
TCP	automatic
HTTP	

User login XML

```
<?xml version="1.0" encoding="utf-8"?>
<ateas>
  <user>
    <id>10</id>
    <name>tester</name>
    <action>login</action>
    <datetime>
      <utcstamp>128989433710312500</utcstamp>
      <localvalue>22.7.2023 15:05:23</localvalue>
    </datetime>
  </user>
</ateas>
```

NOTE

During logout, the action parameter has the value of logout.

NOTE

The UTC timestamp indicates the absolute time not affected by the time zone or daylight time changes. It is expressed as the number of 100-nanosecond intervals elapsed since 1.1.1601 UTC.

18.3. ATEAS API of the camera server

18.3.1. External events

Receiving an external event

Protocol	API
TCP	[ATEAS EVENT (status) (deviceid) (code) (data)]
HTTP	

Parameters:

Parameter	Value	Default	Description
status	START, STOP		Start or stop
deviceid	1 – 999		Device number
code	(as configured)		Custom event name
data	(max. 1000 characters)		Additional data

Příklad:

Protocol	API
TCP	[ATEAS EVENT START 1 TEMPERATURE 76]
HTTP	

NOTE

The event code must correspond with an existing name in the camera administration section.

NOTE

The event can be ended explicitly or by configuring a maximum event duration interval.

18.3.2. Metadata

Inserting metadata

Protocol	API
TCP	[ATEAS META (deviceid) (timestamp) (code) (data)]
HTTP	

Parameters:

Parameter	Value	Default	Description
deviceid	1 – 999		Device number
timestamp	0 – N		UTC timestamp
code	(as configured)		Custom event name
data	(max. 1000 characters)		Metadata

Example:

Protocol	API
TCP	[ATEAS META 1 0 SCAN AB512459]
HTTP	

NOTE

The UTC timestamp indicates the absolute time not affected by the time zone or daylight time changes. It is expressed as the number of 100-nanosecond intervals elapsed since 1.1.1601 UTC.

NOTE

The timestamp may have the value of 0. In such a case the timestamp will be determined by the server. Using user defined timestamps helps for offline data uploads. Timestamps earlier than 30 days in the past or later than 1 minute in the future are not accepted, based on server time.

NOTE

The event code must correspond with an existing name in the camera administration section.

18.4. Parameterized application launch

ATEAS Security applications can be launched with additional parameters that are passed to the application executable while starting. In Windows these parameters can be added under the service settings. All existing parameters are described below.

18.4.1. Administration server

Parameter	Values	Meaning	Note
-ssl	password	Certificate password	Necessary to use when the PFX certificate is password protected.

18.4.2. Camera server

Parameter	Values	Meaning	Note
-ssl	password	Certificate password	Necessary to use when the PFX certificate is password protected.
-loglevel	0 - 1	Log level setting	Using a positive value activates logging of the record buffer level in the log subfolder.

18.4.3. Camera client

Parameter	Values	Meaning	Note
-l, -login	complex	Login details	Automatic user login.
-v, -view	complex	View definition	Automatic view opening.

The **login** option:

Parameter	Values	Meaning	Note
u:, user:	string	User name	Part of the login details.
p:, password:	string	Password	Part of the login details.
a:, administrator:	string	Administration server	Address or name of the server.

The **view** option:

Parameter	Values	Meaning	Note
c:, camera:	complex	List of cameras	Camera numbers to be opened.
s:, screen:	1 – 16	Screen	Screen identification for the view.
p:, position:	complex	Window position	Windows position for the view.
t:, timestamp:	numeric	Timestamp	Number of seconds since 1.1.2010 0:00:00 UTC.
f:, full:	empty	Maximized view	A view with no control panels.
a:, autoplay:	empty	Auto play	Auto play recorded material.

The **camera** option (server-camera-extra):

Parameter	Values	Meaning	Note
server	1-9999	Server number	Server identification.
camera	1-999	Camera number	Camera identification.

extra	string	Additional parameters	m – attach metadata.
--------------	--------	-----------------------	----------------------

NOTE

If the server part is omitted, a server number 1 is assumed. The extra part is optional.

The **position** option (x,y,w,h):

Parameter	Values	Meaning	Note
x	0-100	X coordinate	Relative window position.
y	0-100	Y coordinate	Relative window position.
w	10-100	Width	Relative window position.
h	10-100	Height	Relative window position.

Examples:

Logging to a system and opening a view with two cameras in live mode placing the view on the second screen without control panels in its default size:

```
observer -l u:admin p:12345 a:10.0.0.1 -v c:1-1 c:1-2-m s:2 f:
```

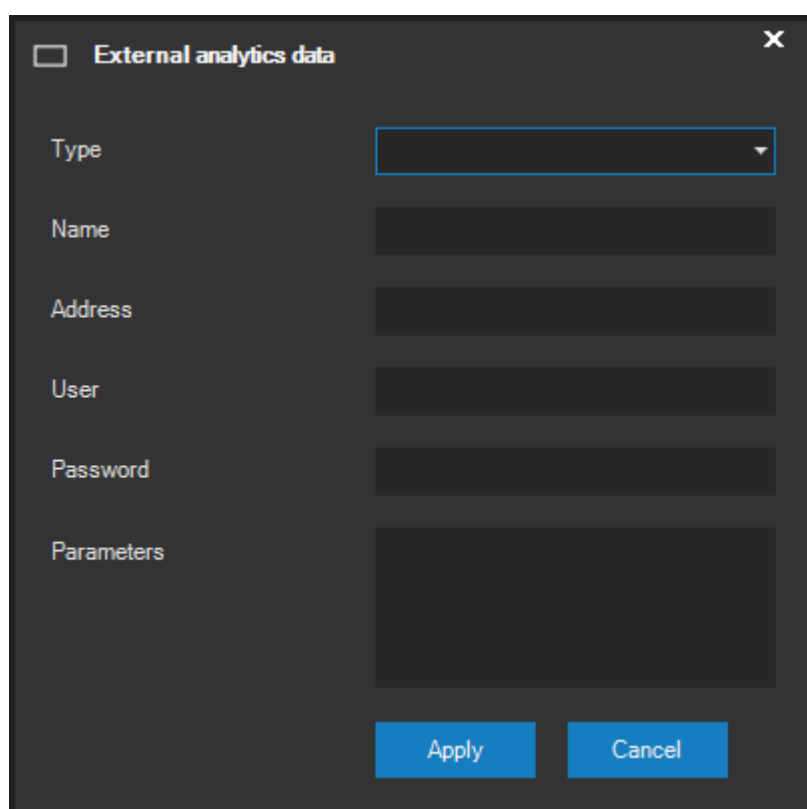
NOTE

Up to 16 views can be defined.

Chapter 19 - Appendix 3 – External analytics data

19.1. Prerequisites

In order to connect an external analytical data source, one or more external analytical data sources must be added to the respective cameras by following the instructions provided in chapter Basic camera setup, section External analytics data. The following dialog must be filled in.



☐ External analytics data

Type

Name

Address

User

Password

Parameters

Apply Cancel

19.2. Integration with the VTrack system

19.2.1. Connecting metadata from server

The following values are required to connect the VTrack analysis as an external data source executed directly on a VTrack server:

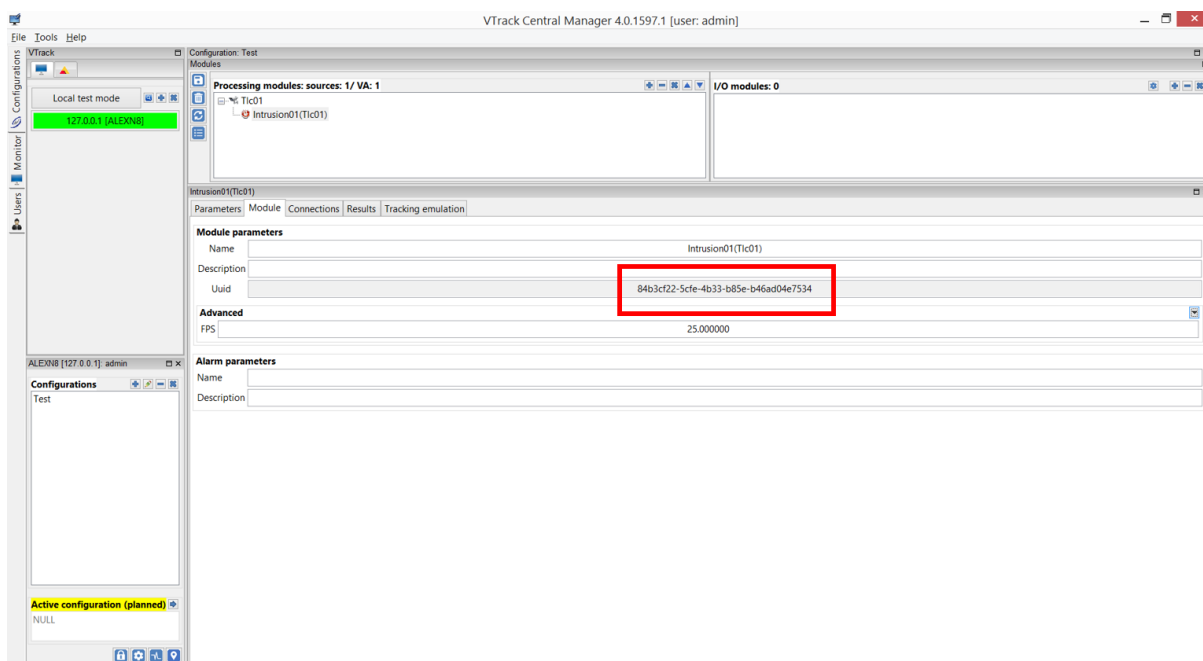
Type: VTRACK (selection from the list).

Name: A user defined name for the external analytical data source.

Address: VTrack server address (IP address or name). E.g. 10.0.0.1:30002.

User name and password: Enter the user name and password in cases where authentication is required to connect to the source.

Parameters: The unambiguous identifier of the specific analysis shall be entered, see the following image.



19.2.2. Connecting metadata from camera

The following values are required to connect the VTrack analysis as an external data source executed directly in the camera:

Type: VTRACK (selection from the list).

Name: A user defined name for the external analytical data source.

Address: The metadata source address, which contains the camera address, application name and other parameters. The provided example is for the Intrusion application running inside an Axis camera with the address 10.0.0.1:

10.0.0.1/local/vtIntrusion/results.cgi?tags=metadata

User name and password: Enter the user name and password in cases where authentication is required to connect to the source.

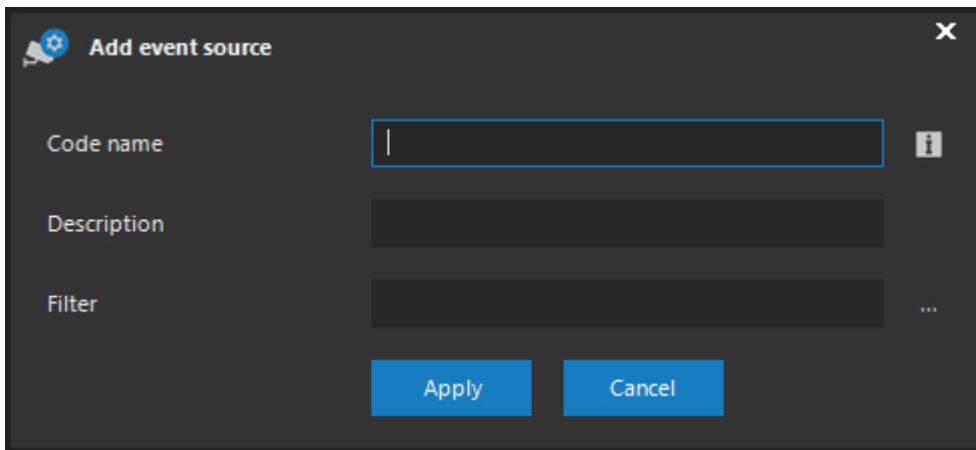
Parameters: No value required.

NOTE

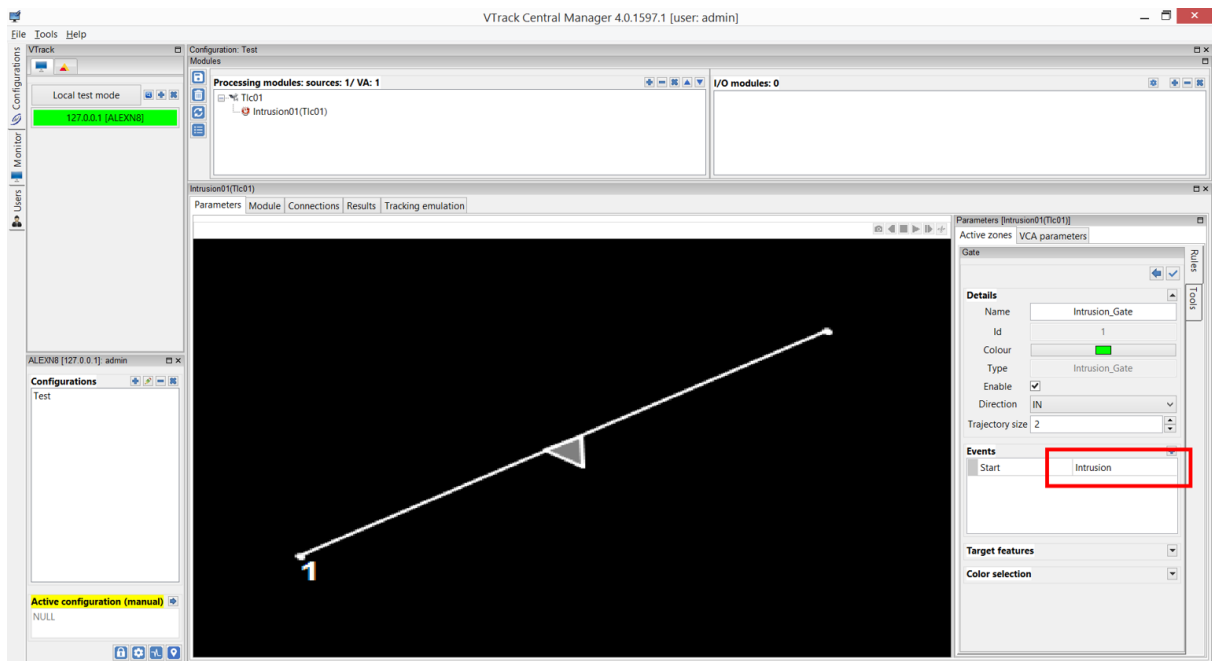
Currently, this can only be used for selected camera devices. The VTrack system tools and documentation must be checked for the proper address configuration for other applications or camera manufacturers.

19.2.3. Linking events

In order to automatically detect alarm situations from external analytical data sources, custom camera events must be created in ATEAS. These events must have identical names to the event names in the VTrack system. More information about creating custom events can be found in the relevant chapter of the documentation. When creating a custom event in ATEAS, you must enter the name of the event (code name) and a description.



The code name must correspond to the value entered in the VTrack system as shown in the following image.



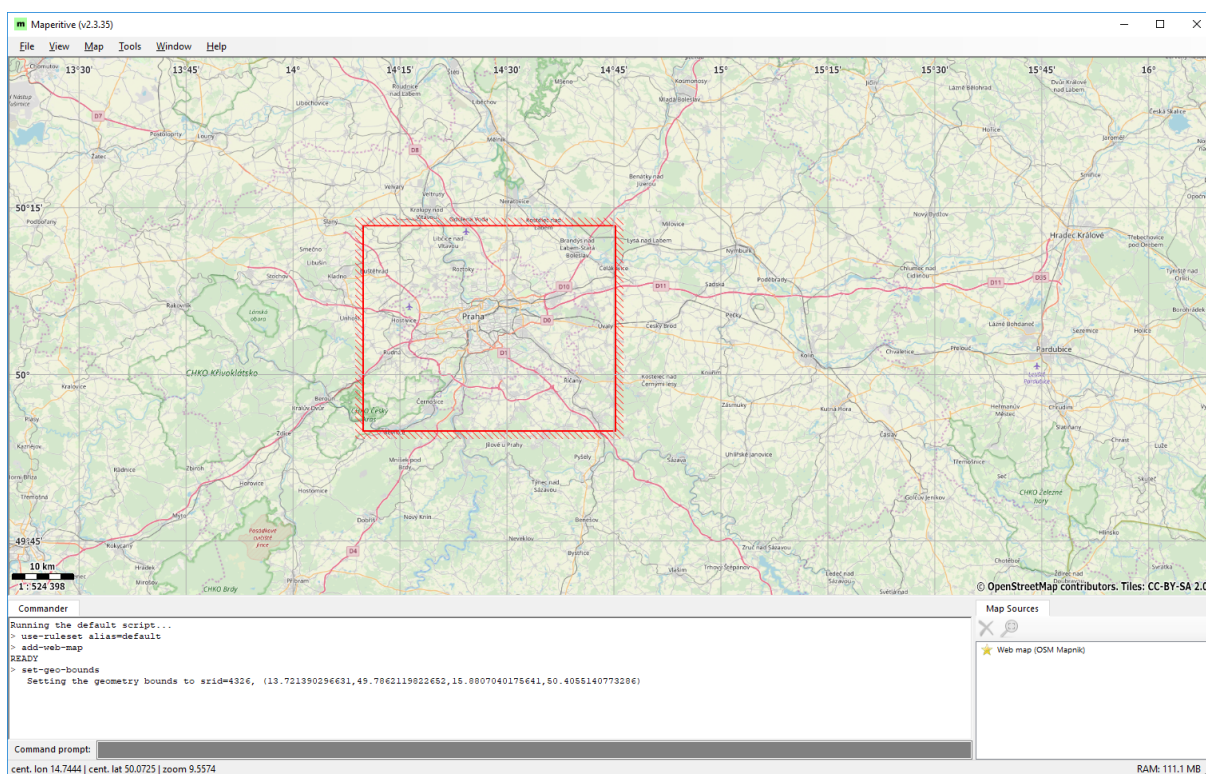
Chapter 20 - Appendix 4 – OpenStreetMap sources

20.1. Creating maps from free map sources

The OpenStreetMap (OSM) map model is a free to use vector map model. Data for any given area in the world can easily be converted and used as a map interface in ATEAS. Conversion to the so called hybrid model is necessary because handling vector formats for larger areas is slow. Any tool can be used to convert to hybrid format (OSM tiles). The following is the conversion procedure using Maperitive.

20.1.1. Area selection and data download

After launching the Maperitive application, find the area of interest and use the Map - Set Geometry Bounds command to specify the target rectangle.



Use the Map - Download OSM Data (Overpass API) command to download the data to the local computer.

Turn off the Web map display in the bottom right corner of the window and leave the downloaded map displayed. The map does not need to be saved, nevertheless, this is possible by using the following command:

```
save-source index=n file="path"
```

whereby index must be set to the value of the downloaded map (can be determined by hiding and showing the map- the index will be displayed in the application console) and the file must be set to a valid path to the new file, e.g. d:\savedmap.osm. Commands are entered into the application command line.

A map saved in this way can be opened at any time again.

NOTE

If the server refuses to send all data (the extent of downloaded data is too large), you can either download and convert one segment at a time, or convert directly from the web map, which, however, will be very slow.

20.1.2. Data conversion

Downloaded data can be converted using the following command:

```
generate-tiles minzoom=m maxzoom=n
```

whereby m is the minimum zoom (usually 12) and n is the maximum zoom (19 at most).

After the conversion is complete, data is located in the Tiles folder of the Maperitive application folder. A file with a json suffix is also created, but is not needed and can be deleted. Because the data contains a large number of files, you can, for example, create a .zip archive to make the data management easier. Data from the Tiles folder can then be deleted.

20.1.3. Using the data

The created data can be placed into a folder with a custom name (e.g. OSM-Prague) which can be placed, for example, directly into the maps folder or into any other folder in the map data structure on the administration server, which is subject to distribution.

If the map is too small, upon opening in the map window, it indicates the minimum zoom in the generate-tiles command was too low. This can be resolved by deleting the folder corresponding to the minimum zoom number. This process can be repeated. After a new map distribution, the result of this operation and the size of the first map layer can be validated.

20.1.4. Support for various levels of detail

An advantage of the OSM map model, implemented by ATEAS, is the unambiguous conversion of terrain to an areal map model in the form of converted map files. This feature can be used when we need to combine multiple areas. For example, if we require an overview map of the entire Czech Republic and detailed maps of several cities in a single map scene, we will use the following command for the overview map:

```
generate-tiles minzoom=10 maxzoom=13
```

and the following command for cities:

```
generate-tiles minzoom=13 maxzoom=19
```

The generated converted maps are then to be copied into one of single folder. File collisions occur only if the same data is included in multiple conversions, however, you do not have to pay any attention to them.

20.2. Generating maps from raster bitmaps and plans

A very similar approach can be taken when you need to convert bitmaps into the OSM model.

NOTE

Bitmaps can be used directly as a simple map, however, for performance reasons, the conversion of an image with a width or height in multiple thousands of pixels (CAD drawing export) will be necessary.

In order to open a bitmap in Maperitive, you need its georeference in georef (world file) format, e.g. for a file named cadexport.jpg, you will need cadexport.jpg.georef. The conversion procedure is then identical to the procedure in the previous sub-chapter.

If the converted bitmap is not georeferenced and the georeference is not required, we can select an area wherever on the map of approximately the same size and use the export-bitmap command to create a georef file.

At a minimum, the following two functions will not work if the bitmap is not georeferenced:

- the position of the mobile device transmitting video cannot be correctly displayed when the map is shown,
- you will not be able to zoom-in from the city map level, for example, directly onto a premises or building. In order to access the premises, you will have to use the map location function (door symbol) and enter a different map by clicking on this symbol.

Georeferenced tiff files can be converted using available tools for creating georef files from this type of files.

Chapter 21 - Appendix 5 – JSON data integration

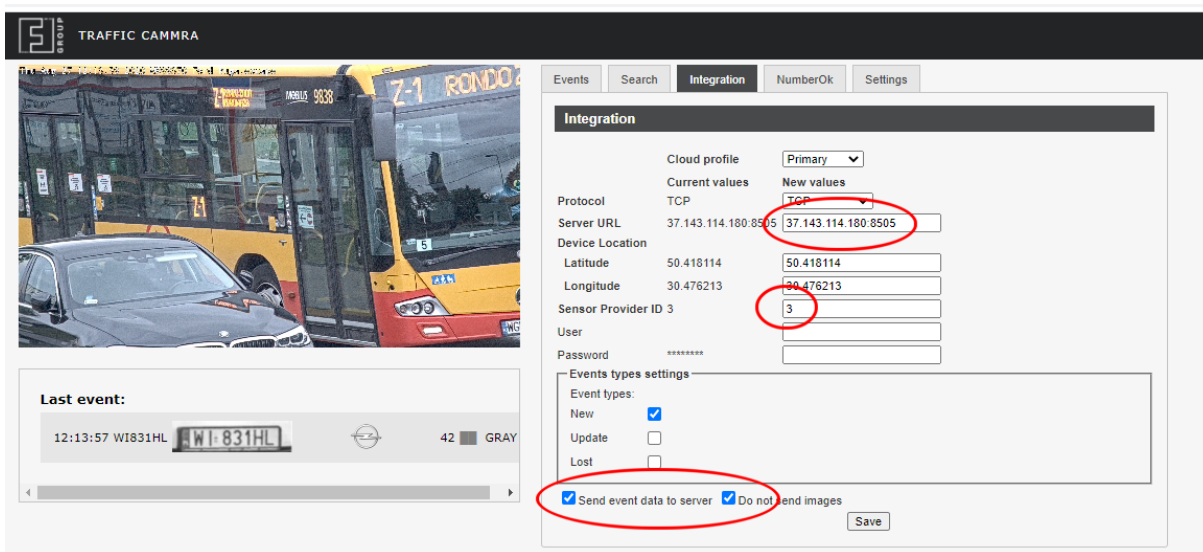
21.1. Prerequisites

Apart from the ATEAS API interface, a JSON (JavaScript Object Notation) data format is also supported on the ATEAS event integration ports.

21.2. Cammra application integration

21.2.1. Receiving metadata over TCP

The Cammra app can be easily configured to transmit LP metadata, country, brand, model or the vehicle color data directly to an ATEAS camera server. On the app website, the JSON based integration must be chosen and the camera server event port must be set as the communication target. Other options should be set according to the image below.



The screenshot displays the 'TRAFFIC CAMMRA' application interface. On the left, there is a live video feed showing a yellow bus and a black car. Below the feed, a 'Last event' section shows a timestamp of 12:13:57, a license plate 'WI831HL', a car icon, and the text '42 GRAY'. On the right, the 'Integration' settings page is open. It features a 'Cloud profile' dropdown set to 'Primary'. Below this is a table with 'Current values' and 'New values' columns. The 'Protocol' is set to 'TCP'. The 'Server URL' is '37.143.114.180:8505'. The 'Device Location' section includes 'Latitude' (50.418114) and 'Longitude' (30.476213). The 'Sensor Provider ID' is set to '3'. The 'User' and 'Password' fields are empty. The 'Events types settings' section has checkboxes for 'New' (checked), 'Update' (unchecked), and 'Lost' (unchecked). At the bottom, there are two checked checkboxes: 'Send event data to server' and 'Do not send images'. A 'Save' button is located at the bottom right of the settings form.

An important point is to modify the Sensor Provider ID to hold the number of the camera on the target ATEAS camera server. It is also recommended to turn off sending image data using the Do not send images option.

NOTE

In order for the system to raise an event, the event source must be given a standard schedule like any other event source.

21.2.2. Receiving metadata over HTTP

Alternatively, the HTTP protocol can be used as well. In this case, data must be sent using the HTTP communication integration channel of the administration server. To be able to infer not only the camera identification but also the server identification, the Sensor Provider ID item can have the form S-C, where S stands for server and C for camera, so for example 1-5.

NOTE

If omitted, the server identification is presumed to be 1.

To be able to receive the data, the Road endpoint must be selected when opening the HTTP communication channel which is bound to this application. The address will look as follows:

`http(s)://administrator/api-base/road`

21.2.3. Metadata and events

The external application then sends its metadata for the selected camera, which are automatically assigned to the vehicle LP event sources. Moreover, any additional data is also stored and can be searched for in the Recordings window. The search basics are described in the searching metadata chapter. Basically, a search phrase may contain words in any particular order being subject to a natural language interpretation. E.g.:

2A CZ skoda – searches for all Skoda vehicles with a Czech LP containing 2A.

rapid green – searches for all green Skoda Rapid vehicles.

NOTE

In order for the system to raise an event, the event source must be given a standard schedule like any other event source.

21.2.4. Charts

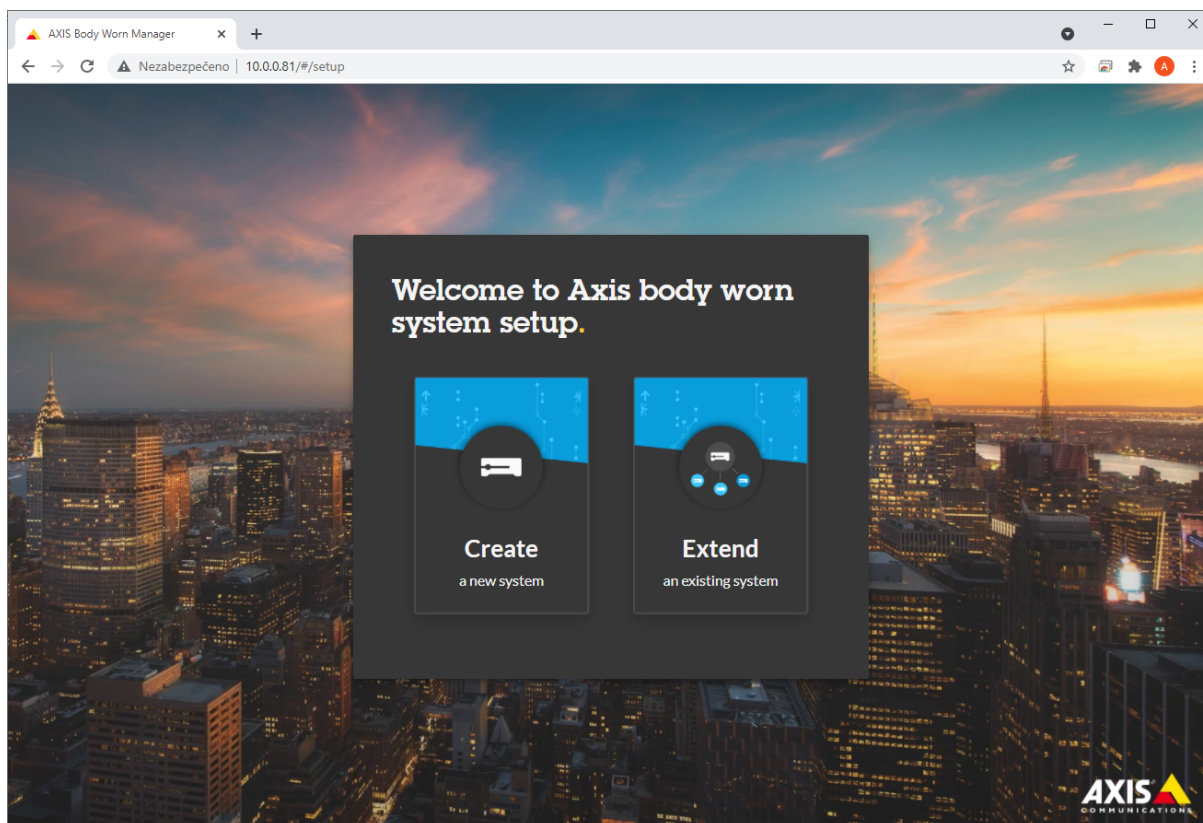
The ATEAS chart feature comes with an advanced chart creation support even for external metadata. The basic charts include some daily or hourly based vehicle frequency charts, some more advanced charts may include further data subdivisions according to any additional data items on certain positions – charts according to LP countries, vehicle brand or model etc. are possible.

If we need to generate statistical outputs for a subset of the data (e.g. a chart of all Czech cars according to their model), it is easily possible to combine the search tool with the chart creation to achieve this goal.

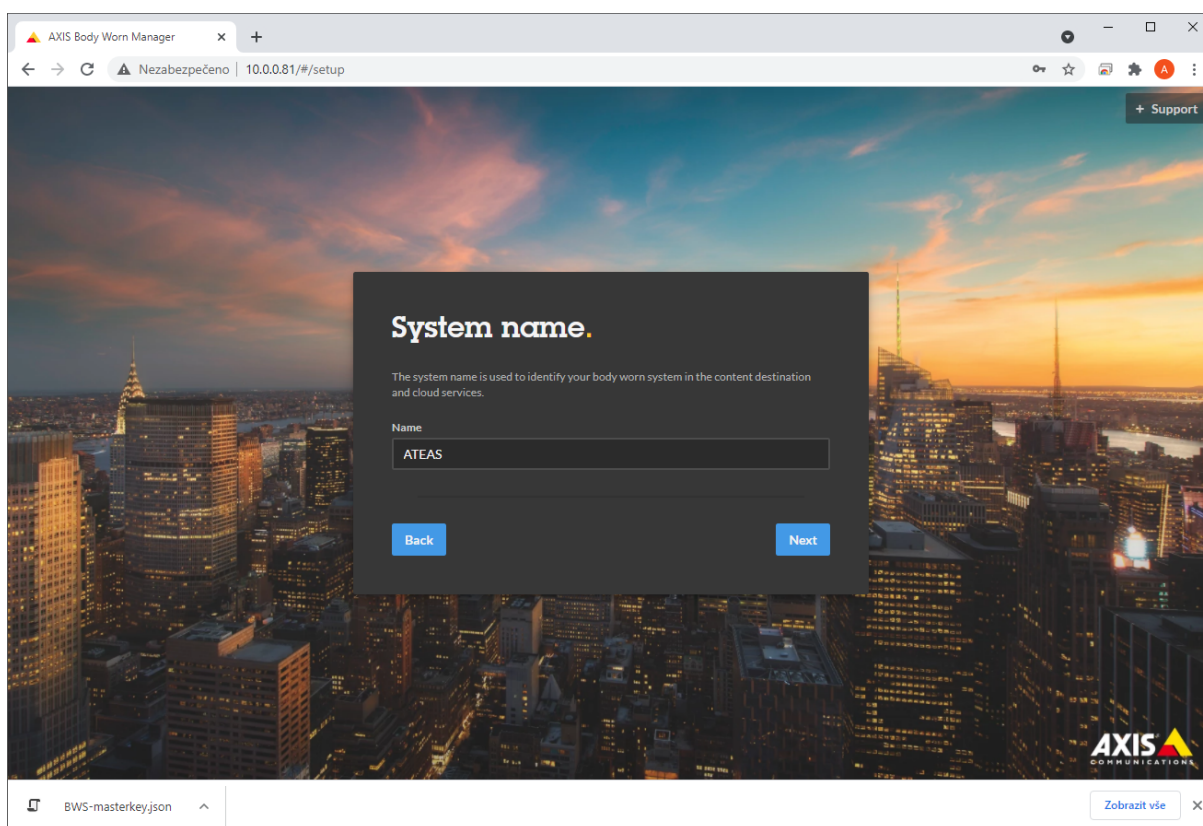
Chapter 22 - Appendix 6 – Axis Body Worn integration

22.1. Connecting to ATEAS

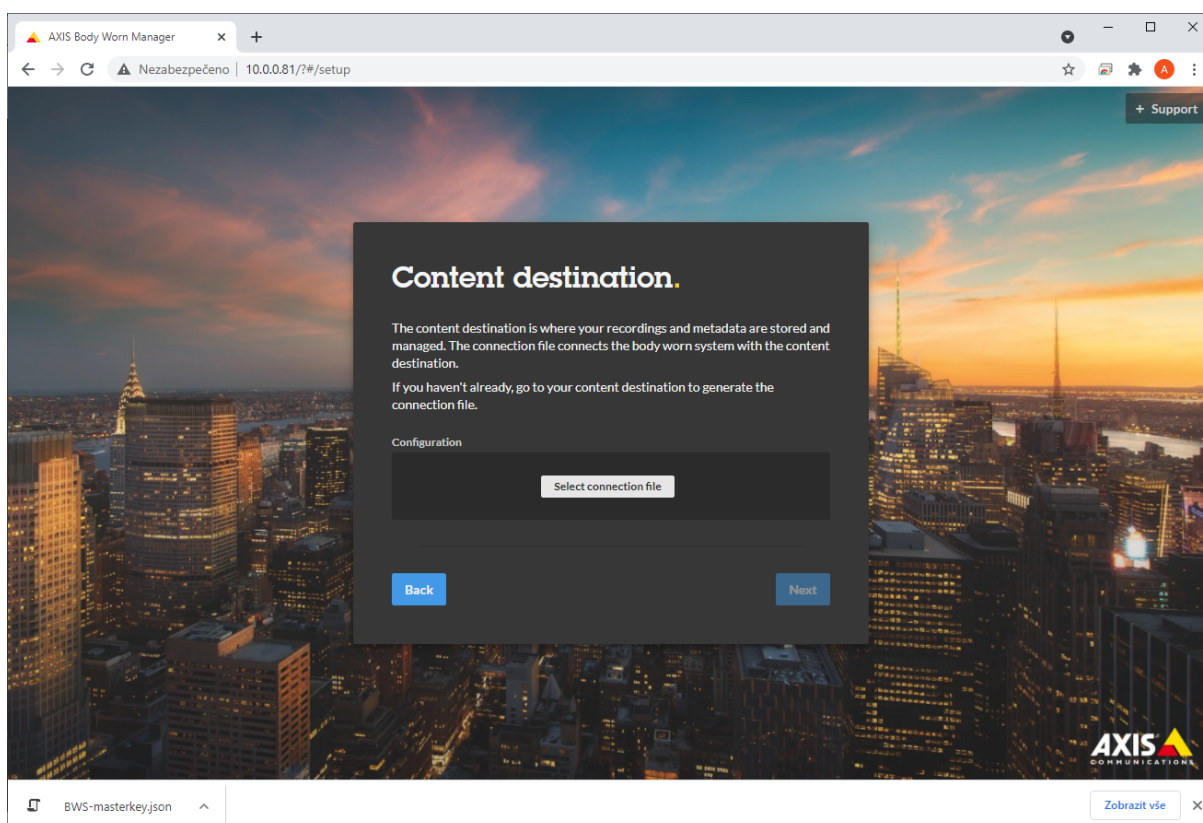
The Axis Body Worn System (BWS) consists of several components, from which the BWS controller unit is crucial for integration purposes. During the initial setup the controller requires a connection to the so called content destination, where all video, audio and metadata will be stored during operation. The initial setup process goes as follows.



After the initial screen you will have to choose a system name.



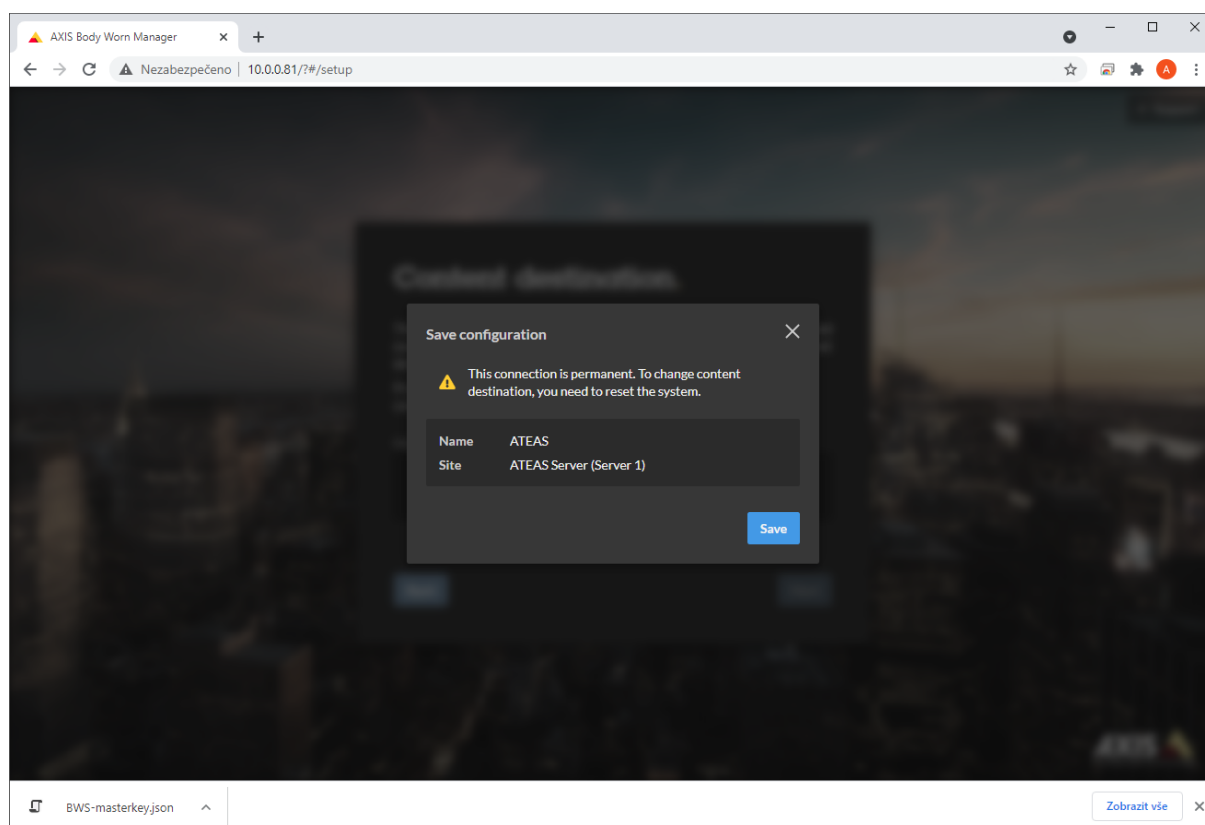
The next step is crucial for creating the connection to the target camera server.



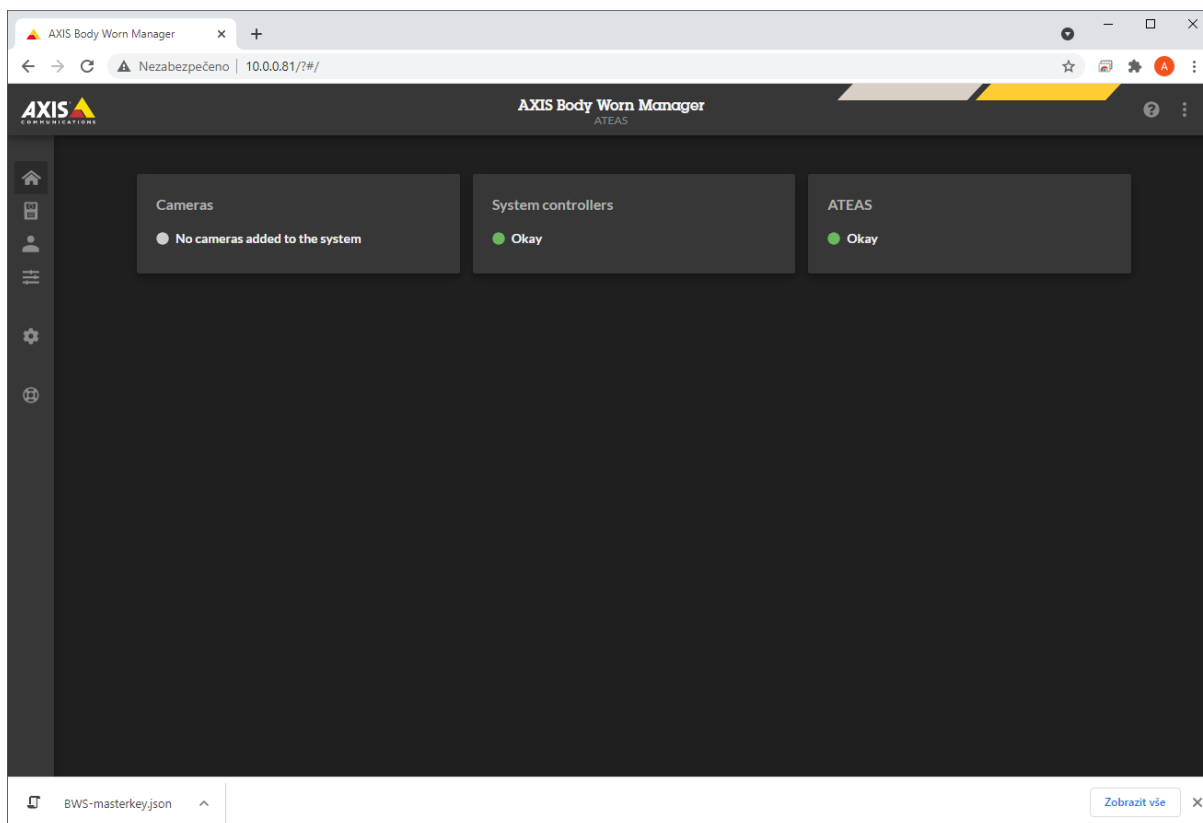
The required JSON formatted connection file containing the BWS connection parameters is automatically created in the connect subfolder in the installation folder of all camera servers. This folder serves also as a temporary folder for any data exchange with the BWS.

An URL address and credentials are maybe the most important parameters in the file. The camera server derives these parameters from the IP address used for camera sever identification in the system and from values in the server.ini file (HTTPPORT, HTTPUSER and HTTPPASS – local port and credentials of the http server running in the context of the ATEAS camera server).

After uploading the JSON configuration file, the connection parameters cannot be changed unless a full system reset is performed, which is indicated by the following BWS message.



A successful BWS connection to the ATEAS server is indicated by the controller's main switch turning green as well as on the controller's website.



22.2. Adding cameras and users

Adding cameras and users must be performed directly using the controller's website. The BWS can be configured in such a way that multiple users share the same camera. For this reason, BWS users are the actual cameras in ATEAS instead of the cameras themselves.

When adding a user, a camera with the same name is also automatically added to the ATEAS camera server, unless:

- there is no free camera license on the server,
- a duplicate camera number is detected.

The BWS users are assigned a user symbol in contrast to the more common camera symbol for other type of cameras. The same symbol is used for mobile users who stream media from their mobile devices with Android or iOS operating systems to an ATEAS server.

CAUTION

The BWS uploads data to ATEAS servers with historical timestamps. Before adding a BWS camera with a specific ID, the server requires that there are no recordings left on the server for this ID. Therefore, deleting a camera might not be sufficient to free a specific ID for the BWS.

NOTE

Since a BWS camera can be successively assigned to multiple users, a 4 : 1 ratio is applied for the BWS camera (i.e. user) license. This means that one ATEAS camera license can be used for up to four BWS users.

22.3. System operation

During operation, BWS data are automatically uploaded to the ATEAS server without further interaction necessary. After uploading, all common replay features can be used to view the data as usual starting from the moment, when a specific time interval from a camera appears on the time axis or in the interval preview.

Chapter 23 - Appendix 7 – Certificates

23.1. Introduction

In this section, we will show how to deploy a certificate to secure the communication between the web browser and the ATEAS servers. This is especially important for web client operation. The procedure is not specific to the ATEAS system, but assumes a general knowledge of the functioning of communication using the HTTP and HTTPS protocols (i.e. TLS).

The entire process of deploying certificates takes a few minutes, and in this description we will show both the use of an existing certificate, including ensuring trustworthiness in the Internet environment, and the creation of your own certificate, e.g. for operation only within the intranet.

Unlike web applications normally delivered including implementation into the customer's infrastructure, ATEAS naturally does not have the ability to know in advance in which domain the customer will operate it, therefore it is not possible to include some "universal" certificate that would enable immediate trusted operation of HTTPS in the customer's network.

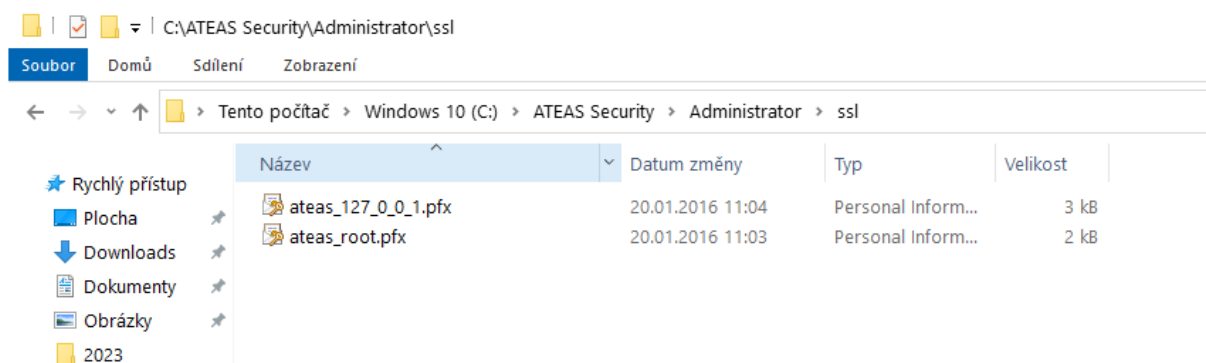
23.2. Prerequisites

Although the process of deploying the certificate is very simple, basic knowledge at the level of ATEAS system management and the functioning of certificates in communication between clients and servers using the HTTP protocol is assumed. For clarity, we summarize these basic assumptions here.

NOTE

For further details, please refer to the ATEAS user manual.

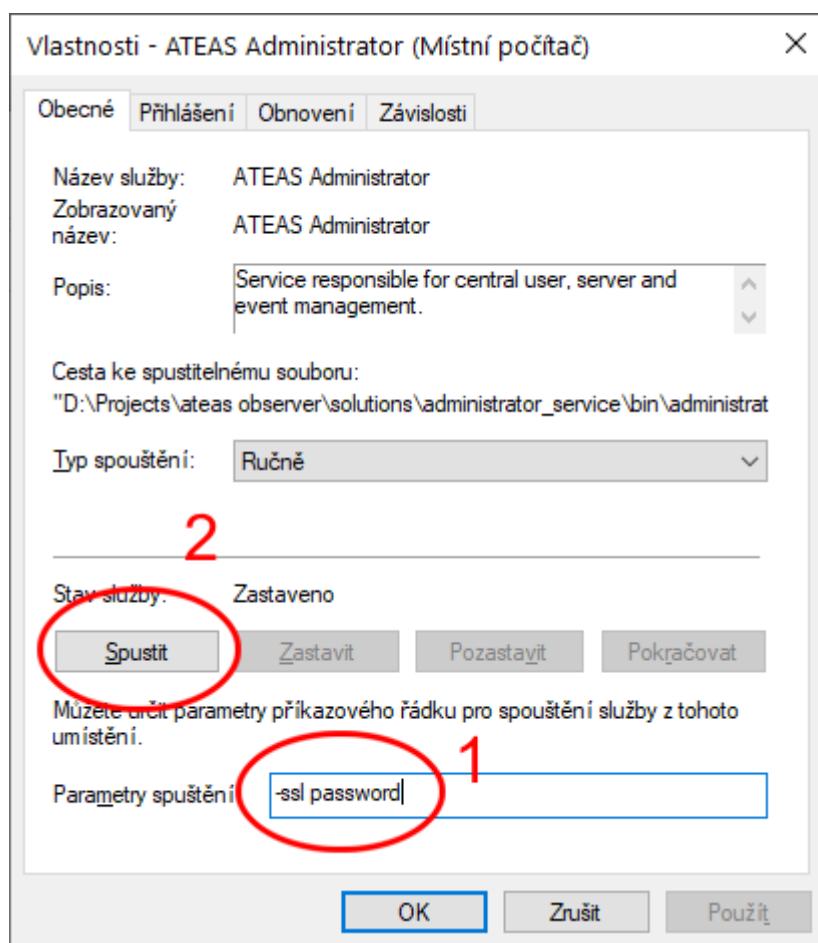
- The certificate for both the ATEAS administration server and the camera server is expected in PFX format, must contain a private key (otherwise it would not be possible to implement the cryptography part where the server proves its origin) and is usually secured with a password to open.
- The certificate is placed in the ssl folder in the installation folder of the administration or camera server.



NOTE

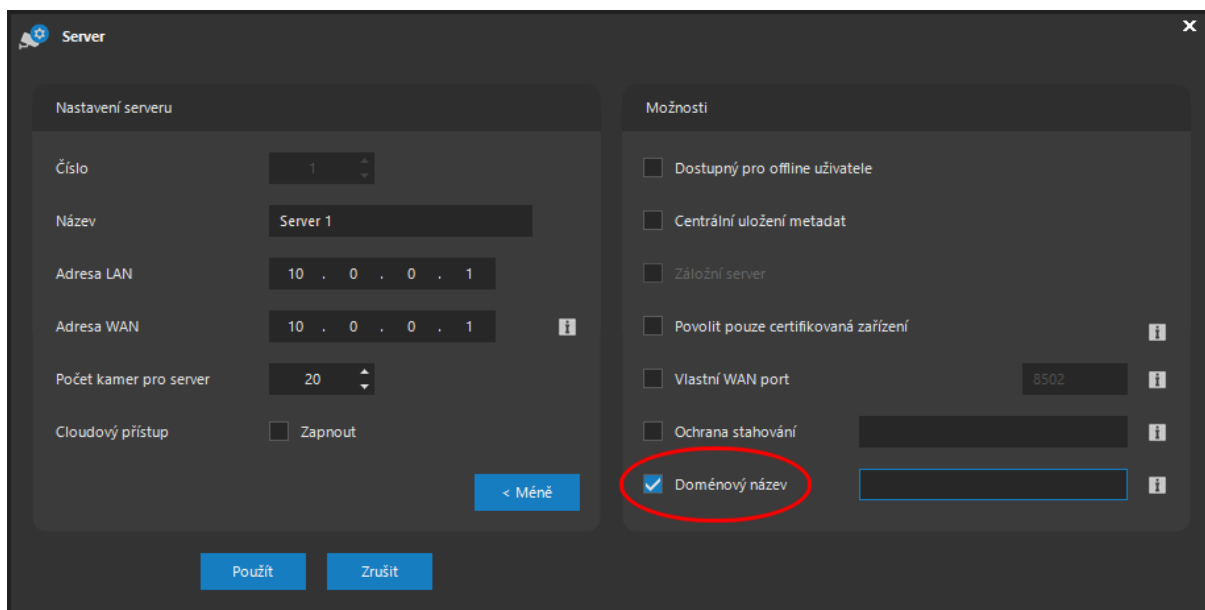
The certificates already placed in this folder are intended for testing purposes to be accessed directly from the computer where the server is installed. There is no need to delete them, the newly added certificate will take precedence.

- The password for opening the certificate file is passed to the administration or camera server service in the `-ssl` parameter when the service starts.



The password for the certificate will not remain visible here, as the service startup parameters are not persistent. ATEAS therefore saves the password to the file in an encrypted form so that the certificate file can be used again when the service or server is restarted.

- Certificates can be issued to an IP address or to a domain name. Certificates for IP addresses are not common and in practice can only be used within the intranet. Certificates issued by certification authorities, including free ones (e.g. Let's Encrypt), will always be issued to a domain name. In this case, domains need to be assigned to ATEAS camera servers.



Server

Nastavení serveru

Číslo: 1

Název: Server 1

Adresa LAN: 10 . 0 . 0 . 1

Adresa WAN: 10 . 0 . 0 . 1

Počet kamer pro server: 20

Cloudový přístup: ☐ Zapnout

Možnosti

☐ Dostupný pro offline uživatele

☐ Centrální uložení metadat

☐ Záložní server

☐ Povolit pouze certifikovaná zařízení

☐ Vlastní WAN port: 8502

☐ Ochrana stahování

☒ Doménový název

Použit **Zrušit**

NOTE

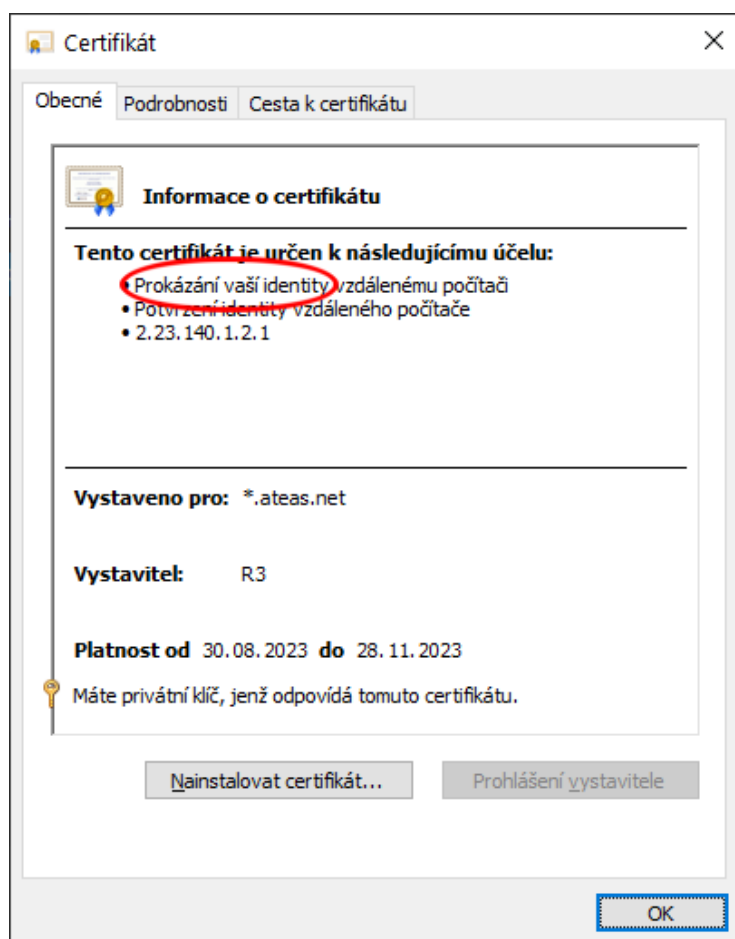
There is no need to assign the domain to the system's administration server, as it is given by entering it in the web browser.

23.3. Certificates

More detailed information on certificates is beyond the scope of this text, however, here we present some relevant information for their deployment within the ATEAS system.

ATEAS will accept all certificates in PFX format. The trustworthiness of the HTTPS connection is determined by the certificate itself and the settings in the client environment (trusted root certification authorities, etc.). ATEAS and the web browser will negotiate the version of the TLS protocol and (if we consider new versions of ATEAS and .NET) and agree to use the highest possible and acceptable version for both parties (most often TLS 1.3).

In order for the certificate to be used to prove the origin of the server, it must have this fact listed in the list of use cases (purposes for which it was issued). When using already existing certificates of the organization, this is automatic, it should be remembered when generating your own certificate.



23.3.1. ACME protocol

Due to the popularity of services such as Let's Encrypt, but also in view of the extreme increase in the number of issued certificates for the operation of web applications in particular, the ACME (Automatic Certificate Management Environment) protocol was standardized within RFC 8555, which serves to automate the process of issuing and renewing certificates. This protocol is commonly used by companies offering web hosting services or directly by end customers who run their own infrastructure for web services.

At first glance, it might seem appropriate for the ACME protocol to be implemented directly in the ATEAS system, so that obtaining and deploying the certificate could be fully automated. However, this solution does not seem practical for at least two reasons:

- Primarily, client access within ATEAS is realized by a proprietary protocol, not the HTTPS protocol, which is used only for a limited part of ATEAS functions – in particular, a web guide for downloading installers or documentation, automatic system updates, a new HTTP-based communication API, and the system's web client. Therefore, the involvement of automation to obtain certificates for HTTPS does not appear to be fully justified.

- The second and main reason is the very functioning of ACME. The management of certificates for certain domains is subordinated to ACME user accounts maintained directly by the provider of this service. Therefore, in order for the ATEAS camera system to manage a certificate for e.g. the cctv.mycompany.com domain on the already existing mycompany.com domain, it would have to gain access to the ACME credentials. In practice, this can be a bigger problem than the actual export of the certificate and its simple deployment within the ATEAS system.

23.3.2. Wildcard certificates

Certificates issued for a domain name can only be successfully used when communicating with a remote server at an address (URL) that exactly matches the domain name, including compliance with the order of the domain (second- or third-level domains). However, it is not very practical to manage different certificates for most third-level domains (e.g. www.mycompany.com, helpdesk.mycompany.com, webmail.mycompany.com etc.). This problem is solved by wildcard certificates, which enable the verification of all higher order domains.

NOTE

Wildcard certificates can also be obtained for free, e.g. within the Let's Encrypt service. However, obtaining it is more complicated within ACME because it is not enough to prove the ability to control the content on the given domain, but also the DNS records for the given domain.

The following is an example of an at eas.net wildcard certificate:

Obecné		Podrobnosti
Vydán pro		
Běžný název (CN)	*.ateas.net	
Organizace (O)	<Není součástí certifikátu>	
Organizační jednotka (OU)	<Není součástí certifikátu>	
Vydal:		
Běžný název (CN)	R3	
Organizace (O)	Let's Encrypt	
Organizační jednotka (OU)	<Není součástí certifikátu>	

One wildcard certificate can be used to secure all camera servers within the ATEAS UNLIMITED edition, as ATEAS supports these wildcard certificates.

TIP

If you use wildcard certificates, it will be possible to use the same certificate for the administration server and all camera servers in the system.

23.4. Using an existing certificate of an organization

In this procedure, we will show how easy it is to deploy an existing certificate for atead.net to run web content and the ATEAS web client, for example at cctv.ateas.net.

23.4.1. Obtaining the certificate

The first step is to obtain an existing certificate, ideally in PFX format, but any other format is possible.

NOTE

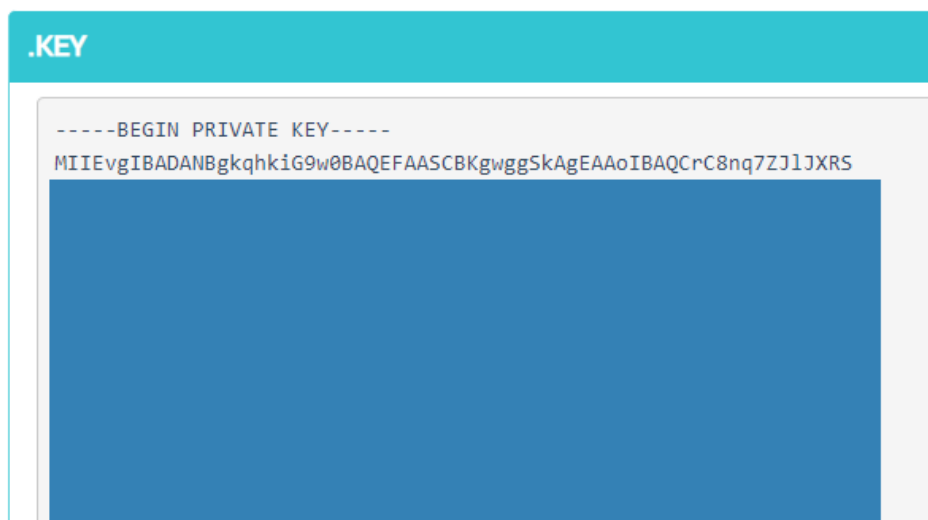
The procedure will vary depending on your web hosting service provider, in most quality services access to the certificate is immediately possible from the administration interface. If the web services are deployed on your own infrastructure, ask the administrator of this service to export the certificate.

From the administrative interface of the service provider for the operation of at eas.net, the public part of the Let's Encrypt wildcard certificate can be obtained in CRT format and the private key can also be saved separately.

+ Nový SSL certifikát			
Doména/Subdoména	Typ	Stav	Datum platnosti
ateas.net	bezplatný certifikát Let's Encrypt Wildcard	Aktivní	28.11.2023
			Detail

.CRT

```
-----BEGIN CERTIFICATE-----
MIIE7jCCA9agAwIBAgISA5/0l0CXEiCcYRA9fMqsuAjj4MA0GCSqGSIb3DQEBCwUA
MDIxSzA3BGNVBAZTA1VTMRyWfAYDVQKEw1MZXQncyBfbmNyeXB0MQswCQYDVQQL
EwJSMzAeFw0yMzA4MzAxMTE3NDdaFw0yMzExMjg0MTE3NDZaMBYxZDASBgNVBAMM
CyouYXRlYXN0bWV0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqwvJ
6u2SZ5V0Uoh/14N+xi4Ff/ou40UEmarEaze7yY0x3Ig8RjkAydUk0SvaSX0QUZjR
BNi8h10LcaIx0trcbF04/fjwVVMhsI2p00hSM/oh1FoAskCp3pavZY+zfqSuYrYG
TeqazN1Xh+2Lo21TGCzejs8dChRZMVnu0+d6EAFt5s2P5XdB4btKjM8uDMedKaH
+aRspXopG1CQqA8wIm+H1zMDaT8ic3eCe589lBoohw7sb0oiZgBpCokHdAwnFvF
oxRu97YIrnCRqoAzjZvXHEMAJhWPF1QUX521PNw4Mh5vNDZEMKKe4MvUm6UddNGm
/LVBsnPtyRkFujB7ewIDAQABo4ICGDCCAhQwDgYDVDR0PAQH/BAQDAgWgMB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBGNVHRMBAf8EAJAAMB0GA1UdDgQW
BBRhsNcMrcwz59gi0Mr09AFGqsb1uzAfBgNVHSMEGDAWgBQULrMXt1hWY65QCUDm
H6+dxTCxjBVBggrBgEFBQcBAQRJMEcwIQYIKwYBBQUHMAAGGFWwh0dHA6Ly9yMy5v
Lmx1bmNyLm9yZzA1BgggrBgEFBQcwoA0YwHR0cDovL3IzLmLmubGVuY3Iub3JnLzAh
BgNVHREEGjAYggqLmF0ZWZzLm51dIIjYXRlYXN0bWV0MBMGA1UdIAQMMAowCAYG
Z4EMAQIBMIIBBAYKKwYBAHWQIEAgSB9QSB8gDwAHUAejKMVN13LbYg6jjgUh7p
hBZwMhOFTTYSK8E6V6NS61IAAAGKRmDbeAAABAMARjBEAiBEJLyqXopHcwsCiAP1
YZmAzS2AG/Gp32tSLD2tSt9F1AIgbPKEmw8LC3aDWB+erS4+3Q16MSZsU4qQdRSf
ymZ41vsAdwC3Pvsk35xNunXyOcw6WPRsXfxc3qfNcSeHQMbjE20mQAAAYpGYntf
AAAEAwBIMEYCIQClG1Zf6sskYBUEb4IriN17DikLrrRwRUd8TLd8PCrYiwIhA0pC
euA/UTmeGPw74WmPYOgx45/SEVEAIk+L4DHGQq09MA0GCSqGSIb3DQEBCwUAA4IB
AQBekXTX50IU0hBZ1kd3J9yMaCyLSq90rFuSqeFR3icC8EbY4wDD5X2FOR50Uu5o
vwT8//wqGaPb/ucJRfMP2Pbc5+7M/Irbo+eFyatctAk+CN311ym5w+PoU+xsR4V9
JfFP5dxjEfts2spAoA2ihIW1tT4f32sRd8h81hi20y1KYRMF6hTJKPbckXEbNW1
eic9Zk9uuFaAm1J/1kpPn97YwYv8spuHAG5ONT98myU2trX70QtavV120Ew9rA6
ZSMfta9NyIQ+Mw9Pt1JpuOLpRbPeDyTpFqfBpQTJaMMqyEiMMGdd2GJTj3DBskVh
+iCUDCzrxCS05wQ6P3g/+gOQ
-----END CERTIFICATE-----
```



We will save the text files as `ateas.crt` and `ateas.key`.

23.4.2. Exporting the certificate

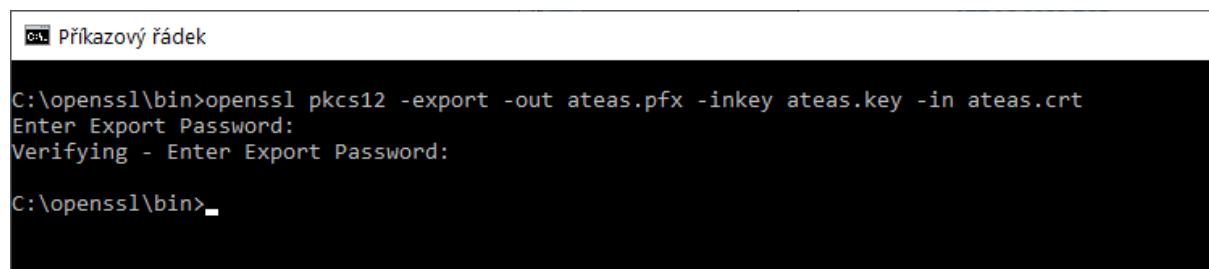
To create a file in PFX format, we can use, for example, `openssl`.

NOTE

If your supplier or system administrator allows you to export the certificate already in PFX format, this step can be omitted.

```
openssl pkcs12 -export -out ateas.pfx -inkey ateas.key -in ateas.crt
```

With this command, we obtain a certificate including a private key in PFX format. `Openssl` will ask for a password when saving the file to open the file later.



23.4.3. Installing the certificate

Deploying the resulting file in PFX format is already done in a completely standard way, which is described above in the Prerequisites section. The file is just placed in the appropriate folder and the server service is restarted using the password to open the file.

23.4.4. Updating DNS records

In order to be able to test the functionality of the exported certificate when used in the ATEAS system, we will also modify the DNS record for `cctv.ateas.net` so that it corresponds to the IP address on which the ATEAS administration server is running.

NOTE

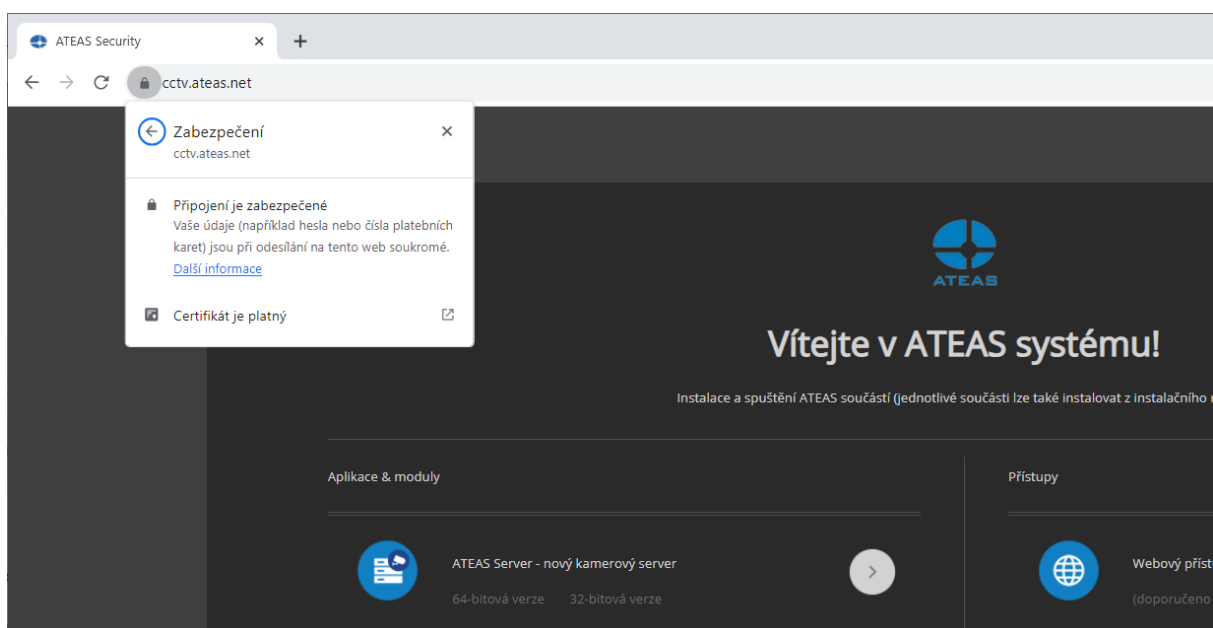
It will also be necessary to redirect the domains of individual camera servers.

If we use an IPv4 address, we add a new type A record to the DNS records, for example as follows.

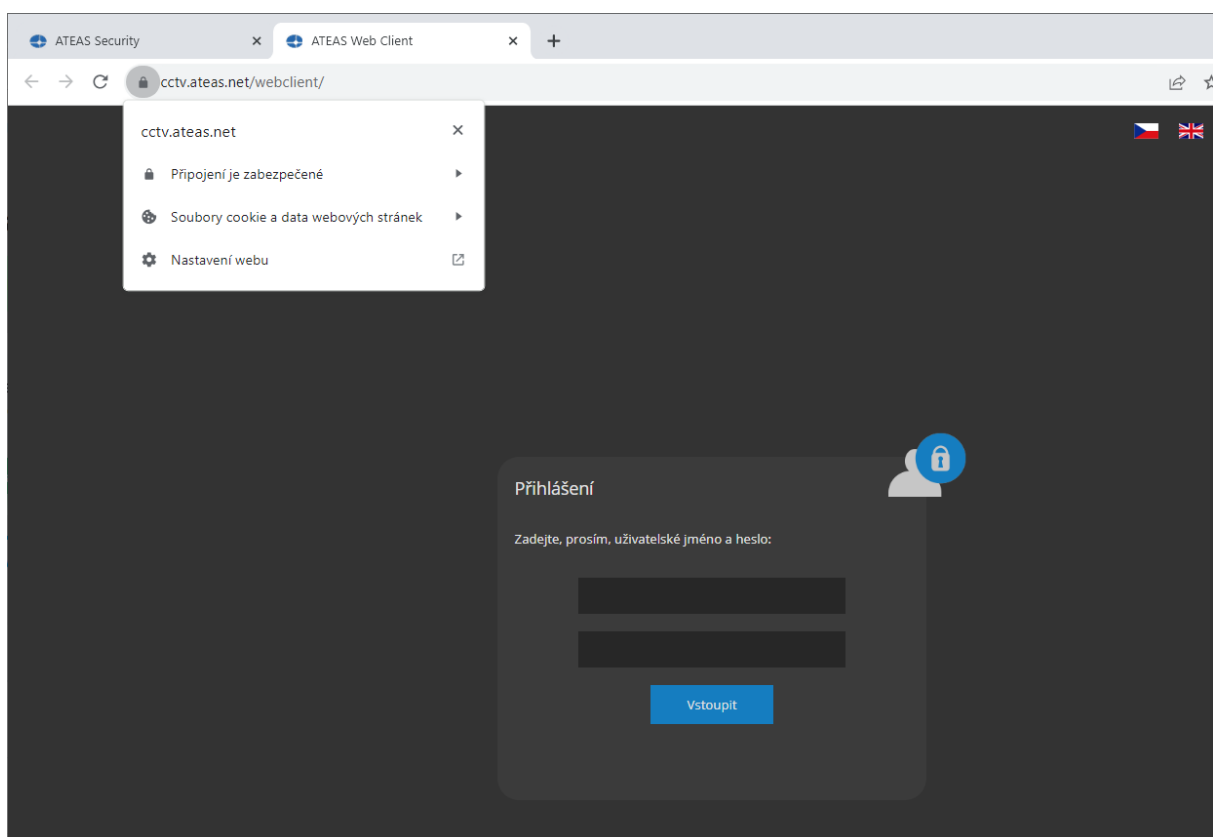
cctv	360	A	37.143.114.180	Upravit
------	-----	---	----------------	-------------------------

23.4.5. Testing the certificate

Now, if we access the address `cctv.ateas.net`, the Let's Encrypt wildcard certificate should ensure the correct verification of this domain, including the indication that it is a trusted connection, since the client environment considers Let's Encrypt as a trusted certificate authority.



In the same way, access to the server will be secured if we start the web client.



The architecture within the ATEAS system (if the cloud mode is not activated for some camera servers) always connects the client with the camera servers to which it has access, directly, i.e. not

through the administration server, which significantly optimizes data flows in the network, e.g. in a system with a central administration and local camera servers.

NOTE

In the background, additional connections using the WebSocket protocol (within HTTPS) will be created with the camera servers, when the certificates of the camera servers will also be gradually verified during video transmission from the cameras.

23.5. Using a new certificate

For HTTPS communication with ATEAS administration and camera servers, it is also possible to create your own certificate, either derived from an existing certificate of a root certification authority or a so-called self-signed certificate, where you create both a new root certificate and a certificate for the camera system yourself.

NOTE

It is obvious that such a type of certificate will ensure the highest level of communication encryption, but does not guarantee any trust whatsoever.

This means that the web browser will warn about untrustworthiness (not a missing encryption) of the connection. Within the intranet, this can of course be avoided by importing the relevant certificates among trusted certification authorities and thereby eliminating this problem. However, this will not be possible within the open Internet. It therefore depends on the environment in which the web interface of the ATEAS camera system is to be operated.

Any tool compatible with the x509 certificate format can be used to create a custom certificate that will be accepted by ATEAS. There are many of these tools, some of them are also equipped with a graphical user interface. We'll stick with the openssl reference tool here.

23.5.1. Creating a root certificate

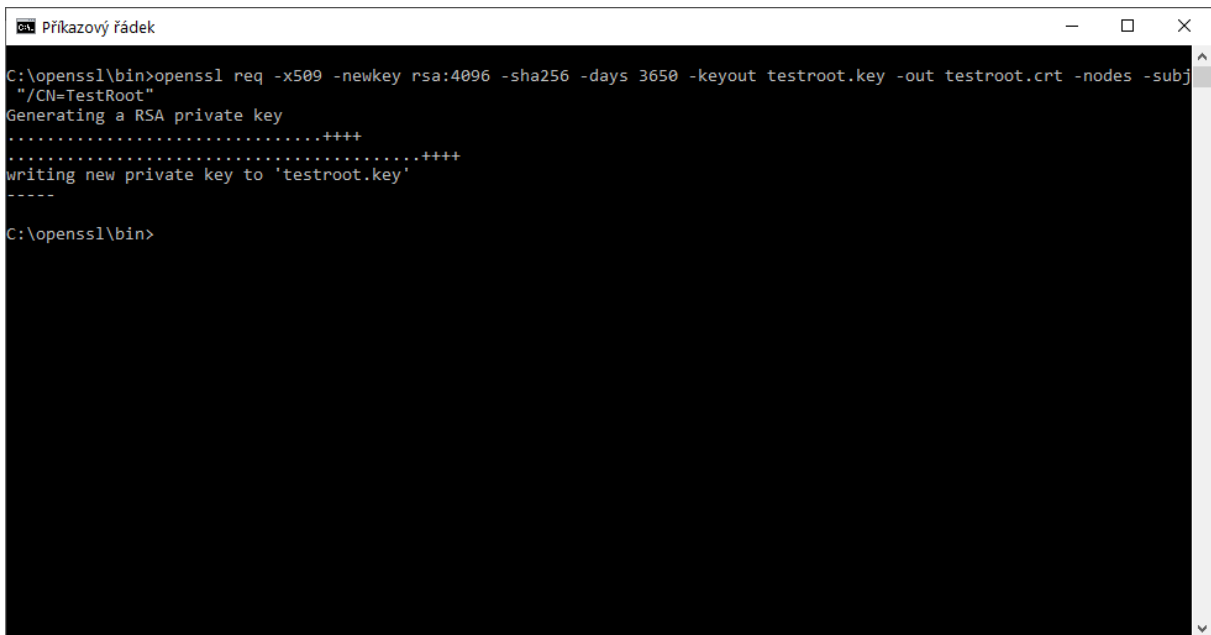
To create certificates of a new certification authority, we can use, for example, the following command:

```
openssl req -x509 -newkey rsa:4096 -sha256 -days 3650
```

```
-keyout testroot.key  
-out testroot.crt  
-nodes  
-subj "/CN=TestRoot"
```

This command creates a new TestRoot CA certificate in the testroot.crt file. The other parameters have the following meaning:

- -newkey specifies that a new RSA private key with a key length of 4 KB should be created,
- -days determines the ten-year validity of the certificate,
- -out and -keyout specify output file names.
- -nodes disables the use of a password to store the private key (here for simplicity),
- -subj specifies the name of the authority in the CN key, no other parameters are needed.



NOTE

If you do not specify the subj parameter, the openssl command will work interactively and it will be possible to specify other properties for the certificate one by one.

23.5.2. Creating the server certificate

Now we will create a certificate for the server that will be signed by our newly created certificate authority. Again we will use openssl and in the first step we will create a request for a certificate

authority in CSR format. You normally create this request in Windows or macOS operating systems using the built-in tools (certmgr.msc or Keychain on macOS).

```
openssl req -new -newkey rsa:2048  
-keyout 10.0.0.1.key  
-out 10.0.0.1.csr  
-nodes  
-subj "/CN=10.0.0.1"
```

The command is very similar to the previous case with these main differences:

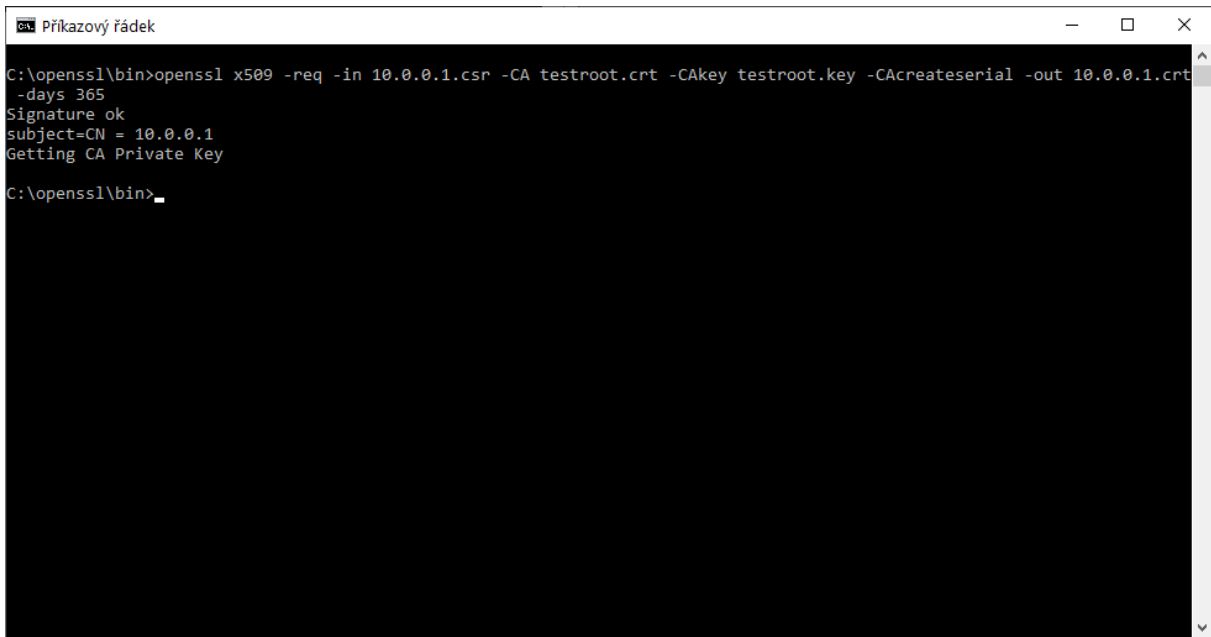
- -new will take care of creating a request for a certification authority,
- -subj must already contain the exact name of the server where the certificate will be deployed, i.e. the domain name or, as in this case, the IP address.

Now our certificate authority must process (approve) the request stored in the CSR file and create a certificate for our server.

```
openssl x509 -req -in 10.0.0.1.csr  
-CA testroot.crt  
-CAkey testroot.key  
-CAcreateserial  
-out 10.0.0.1.crt  
-days 365
```

In the command we can see that the CA processes our certificate request for server 10.0.0.1 and finally signs it with its root certificate (so we also need to provide the authority's private key to the command). Other parameters mean:

- -CA and -CAkey specify the public and private part of the authority's certificate,
- -CAcreateserial creates a number series for serial numbers of the issued certificates,
- -days specifies an annual validity of the certificate for our server.



```
C:\openssl\bin>openssl x509 -req -in 10.0.0.1.csr -CA testroot.crt -CAkey testroot.key -CAcreateserial -out 10.0.0.1.crt  
-days 365  
Signature ok  
subject=CN = 10.0.0.1  
Getting CA Private Key  
C:\openssl\bin>
```

Any number of additional servers can be certified by repeating the procedure in this subchapter.

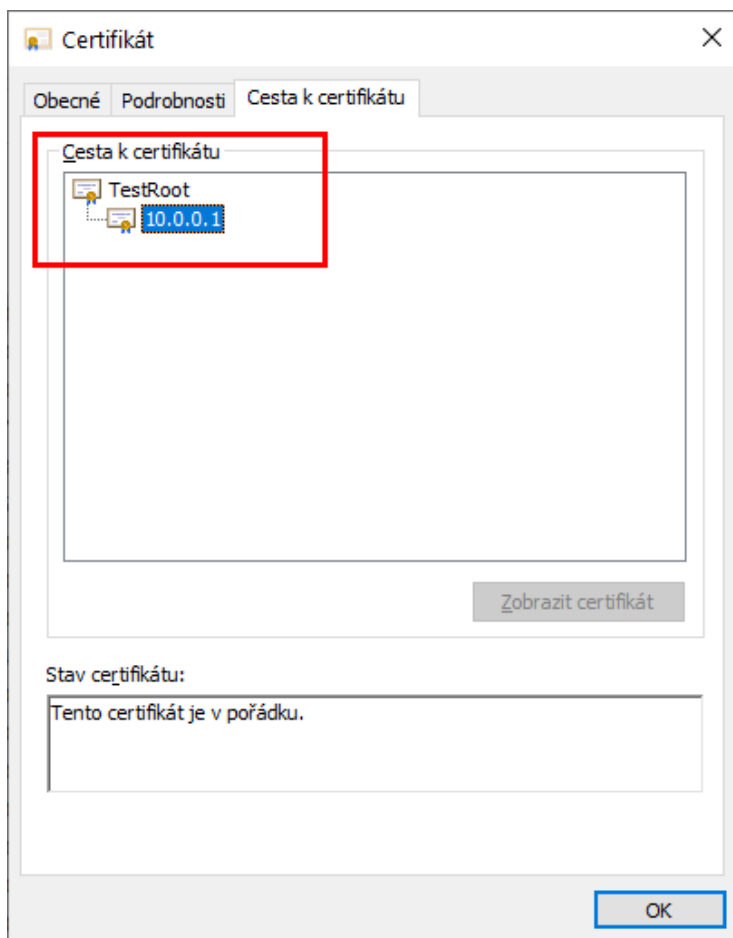
NOTE

However, from the second server, the `CAcreateserial` parameter should be replaced with the `CAserial` parameter and provide the path to the file in which the authority stores the serial numbers of the issued certificates.

The resulting certificate can be seen in the following image.

CAUTION

In order to load the full path to the certificate, it is necessary to import the certificate of our CA among the trusted root CAs in advance.



Now we have created our own certificate for the operation of the ATEAS server at the address 10.0.0.1. It remains to add that theoretically (and cryptographically validly) it would be possible to create a server certificate in the very first step using the server name (instead of our TestRoot name). However, the obvious defect of such an approach will be immediately apparent to readers with a basic certification knowledge. Each server would then be its own certificate issuer and it would be necessary to establish each server as a trusted root certificate authority. This goes against the principle of issuing certificates and at the same time makes their management more difficult.

NOTE

When creating your own certificates, respect the established principles shown here and avoid creating self-signed certificates directly at the level of individual ATEAS servers.

23.5.3. Installing the certificate

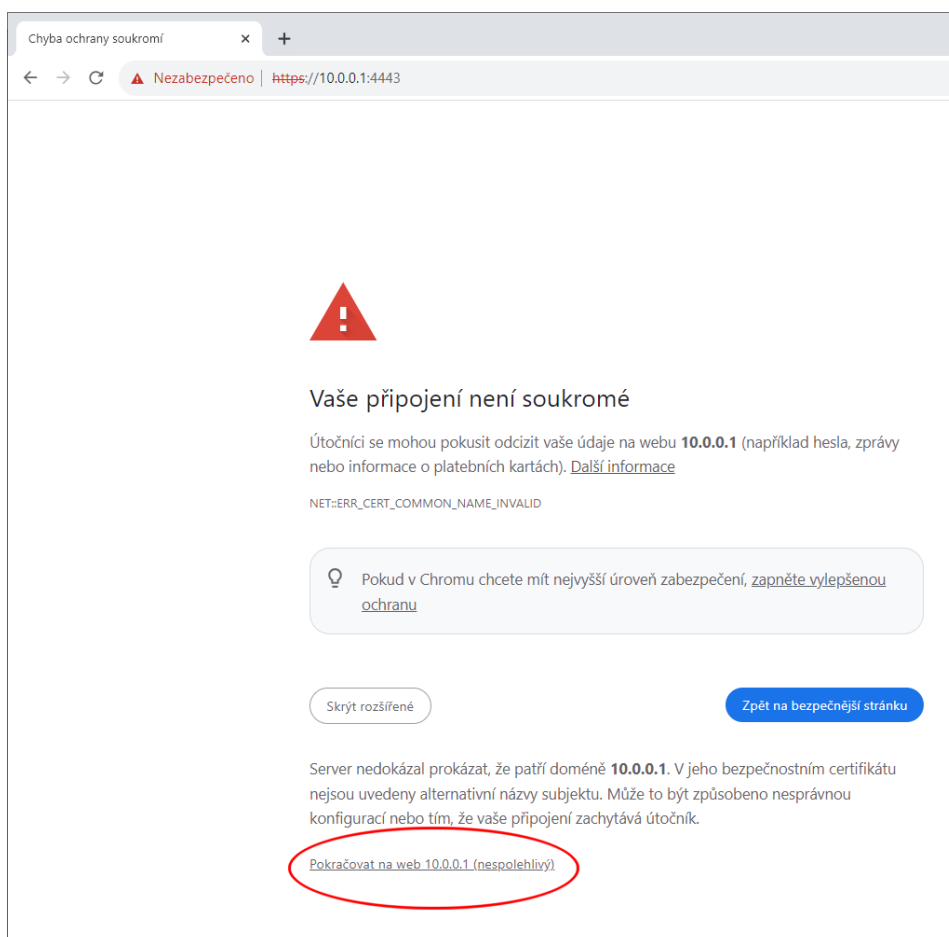
Now all that remains is to convert the issued certificate for the address 10.0.0.1 (signed and approved by our certification authority) into PFX format. During the export, openssl will ask for the password

again. You will deploy the resulting certificate in the PFX file in the usual way described in the Prerequisites section.

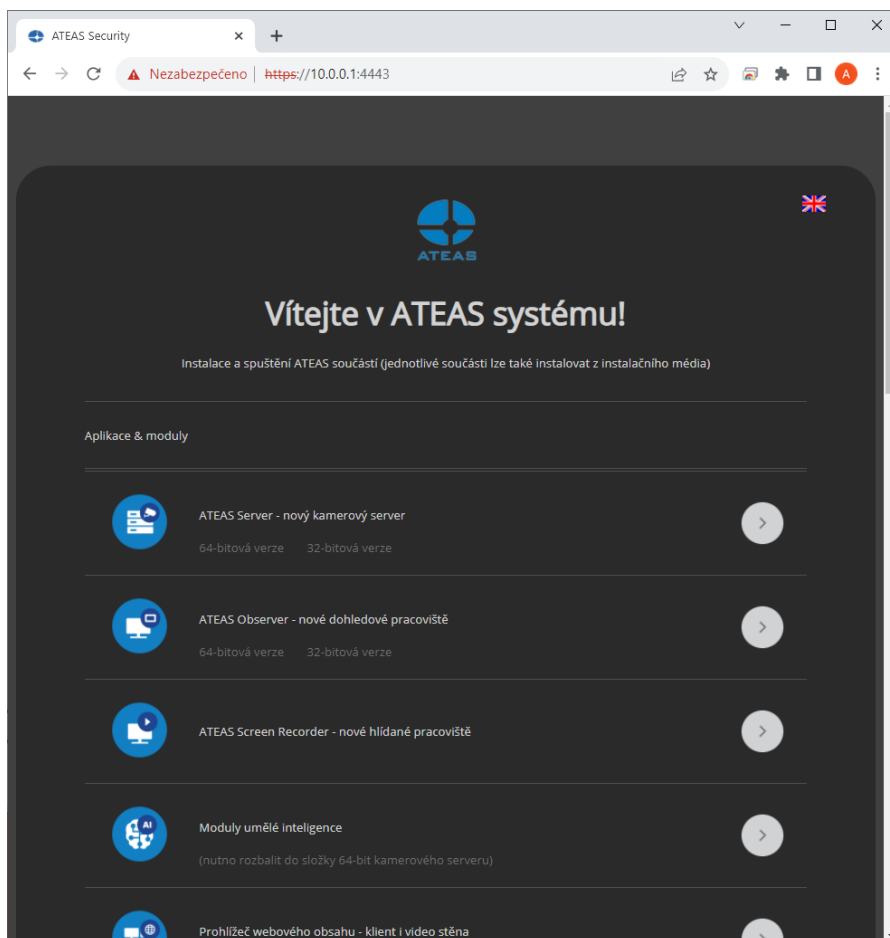
```
openssl pkcs12 -export -out 10.0.0.1.pfx -inkey 10.0.0.1.key -in 10.0.0.1.crt
```

23.5.4. Preliminary certificate test

When accessing the system via HTTPS, the browser (here Chrome) first displays a warning (we'll eliminate it in the next subsection) claiming that the server was unable to prove its origin. However, since we have already imported our CA among trusted CAs, it won't be a trust issue.



If we bypass the warning using the link above, the certificate will work, but the warning will remain active in the form of a red highlight and some warning message.



23.5.5. Proving the origin of the server

To eliminate this somewhat user-unfriendly step, we still need to make one final edit to our certificate. Our system already trusts the TestRoot CA, however the browser now keeps saying that the server was unable to prove its origin at 10.0.0.1. This is because modern versions of browsers require the inclusion of a so-called alternative name in the certificate. To do this, we will create a simple extension file 10.0.0.1.ext with the following minimum content:

```
[v3_ca]
extendedKeyUsage = serverAuth
subjectAltName = IP:10.0.0.1
```

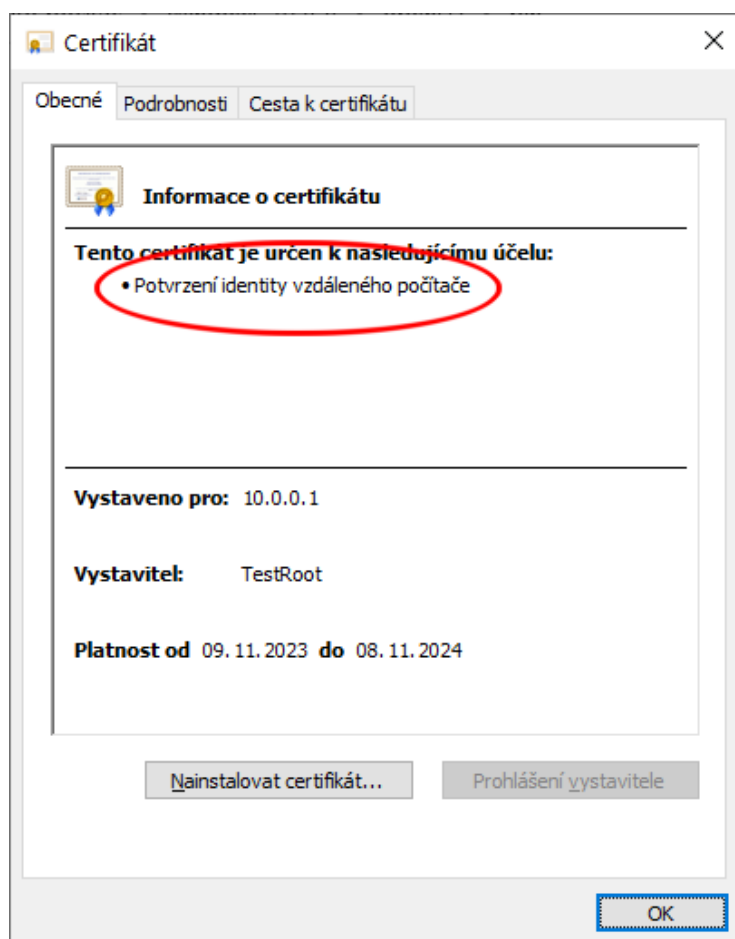
NOTE

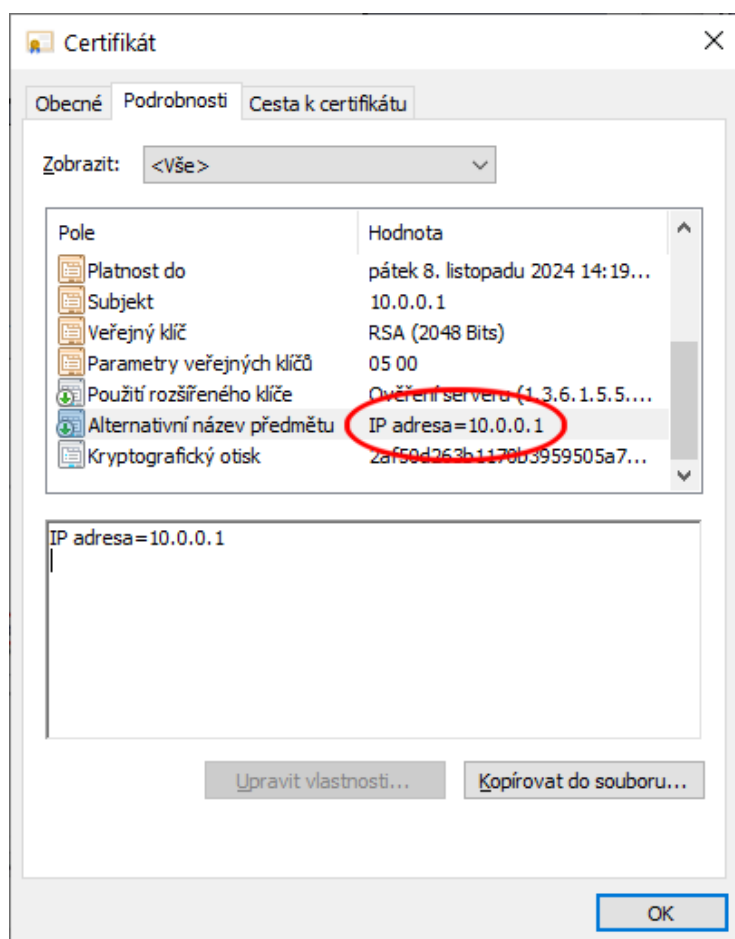
If we were to issue a certificate for a domain, we would change the IP text to DNS. In addition, the use of an IP address is only possible in version 3 of the X509 standard.

So, the authority expands the command to create the server certificate to the following form:

```
openssl x509 -req -in 10.0.0.1.csr  
-CA testroot.crt  
-CAkey testroot.key  
-CAcreateserial  
-out 10.0.0.1.crt  
-days 365  
-extfile 10.0.0.1.ext  
-extensions v3_ca
```

We have now defined an extended usage property for the certificate to prove the origin of the server, and have accommodated browsers' request to provide an alternative name. We can see these two changes in the following images.





23.5.6. Final certificate test

After exporting the certificate to PFX and deploying it in the manner shown above and ensuring its trustworthiness by importing our certificate authority among the trusted root certificate authorities, we will then be able to access the system without any warnings from the browser.

