Setup Instructions

i-PRO Active Guard for Video Insight

CONTENTS

1. Preface

1.1. Limitation of liability

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THE THIRD PARTY'S RIGHT.
THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE ADDED TO THE INFORMATION HEREIN, AT ANY TIME, FOR THE IMPROVEMENTS OF THIS PUBLICATION AND/OR THE CORRESPONDING PRODUCT (S).

1.2. Copyright

Distributing, copying, disassembling, reverse compiling and reverse engineering of the software provided with this product are all expressly prohibited. In addition, exporting any software provided with this product violating export laws is prohibited.

1.3. Trademarks and registered trademarks

- Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

- Intel, Intel Core and Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

- Other names of companies and products contained in these operating instructions may be trademarks or registered trademarks of their respective owners.

1.4. Abbreviations

These are descriptions of the basic terms used in these operating instructions.

Microsoft® Windows® are described as Windows.

1.5. Disclaimer of warranty

This product is designed to search/verify a specified face from database that stores face information and thumbnail images created based on faces captured by network cameras, and display statistical information by operation using a client terminal or system compatible with this product. This product by itself is not designed for crime prevention. Our company accepts no responsibility for the following under any circumstances.

(1) ANY DAMAGE AND LOSS, INCLUDING WITHOUT LIMITATION, DIRECT OR INDIRECT, SPECIAL,CONSEQUENTIAL OR EXEMPLARY, ARISING OUT OF OR RELATING TO THE PRODUCT;
(2) ANY INCONVENIENCE, LOSS, OR DAMAGE CAUSED BY INAPPROPRIATE USE OR NEGLIGENT OPERATION OF THE USER;
(3) UNAUTHORIZED DISASSEMBLE, REPAIR OR MODIFICATION OF THE PRODUCT BY THE USER;
(4) ANY PROBLEM, CONSEQUENTIAL INCONVENIENCE, OR LOSS OR DAMAGE, ARISING OUT OF THE SYSTEM COMBINED BY THE DEVICES OF THIRD PARTY;
(5) ANY CLAIM OR ACTION FOR DAMAGES BROUGHT BY ANY PERSON OR ORGANIZATION AS A PHOTOGRAPHED SUBJECT DUE TO VIOLATION OF PRIVACY CONCERNING A SURVEILLANCE CAMERA'S PICTURE OR SAVED DATA, FOR SOME REASON (INCLUDING USE WHEN USER AUTHENTICATION ON THE AUTHENTICATION SETTING SCREEN IS SET TO OFF), BECOMING PUBLIC OR BEING USED FOR ANY PURPOSE;
(6) LOSS OF REGISTERED DATA CAUSED BY ANY FAILURE (INCLUDING INITIALIZATION OF THE PRODUCT DUE TO FORGOTTEN AUTHENTICATION INFORMATION SUCH AS A USER NAME AND PASSWORD).
(7) ANY PROBLEM, DAMAGE OR COMPLAINT CAUSED BY THE OPERATION BY A MALICIOUS THIRD PARTY.

1.6. Collection of Usage Data

This software may collect data about utilization of this software and send it to i-PRO Co., Ltd. In particular, we use this data to improve our products and services. You can stop this data collection by unchecking “Send anonymous data to improve software and user experience,” checkbox.
The following is an example of the data collected by this software. We do not collect data about your personal information.

- Company name, Country and Purpose of use entered by user.
- The number of camera and camera’s extension software.

1.7. Network security

As you will use this product connected to a network, your attention is called to the following security risks.

1. Leakage or theft of information through this product

2. Use of this product for illegal operations by persons with malicious intent

3. Interference with or stoppage of this product by persons with malicious intent

It is your responsibility to take precautions such as those described below to protect yourself against the above network security risks.

- Use this product in a network secured by a firewall, etc.

- If this product is connected to a network that includes PCs, make sure that the system is not infected by computer viruses or other malicious entities (using a regularly updated anti-virus program, anti-spyware program, etc.).

- Protect your network against unauthorized access by restricting users to those who log in with an authorized user name and password set by using user authentication.

- After the product is accessed by the administrator, make sure to close the web browser.

- Change the administrator password periodically. Keep the authentication information (your user name and password) in a safe place free from public view.

- Apply measures such as user authentication to protect your network against leakage or theft of information, including image data, authentication information (user names and passwords), alarm mail information and FTP server information.

- Use a password that has never been used to protect your network from information leakage or theft.

1.8. Precaution for use

- The administrator should properly manage authentication information such as cameras, recorders, client software, Windows, databases, etc. so as not to leak to third parties.
- Always change passwords for cameras, recorders, client software, etc. from the default values, and perform appropriate management.
- Apply authentication information for each user, and do not share.
- Set the access privileges of the user appropriately.
- Make sure to manage login properly using auto logout function etc. so that third parties do not operate unintentionally by leaving it logged in.
- When downloading the application, please download from the official site.
- The administrator should properly manage exported data using export function so that there is no leakage to third parties.
- When repairing, disposing of, or transferring PC, there is a possibility that information may be left on the HDD etc. Therefore, please manage by an appropriate method such as physically destroying the HDD. Also, if using external media, remove them in advance and manage them so that they do not leak to third parties.
- If the authentication information is lost, system needs to be initialized. Store the authentication information properly in a place where only authorized persons can view it.
- It is recommended to back up and manage system configuration data regularly.
- Set the time for devices in the system, such as cameras, recorders, and PCs, using an NTP server, etc.
- Please properly manage the expiration date of the server certificate prepared by the customer.
- For Windows, apply the latest security patch. Also, please set up Windows properly according to your environment.

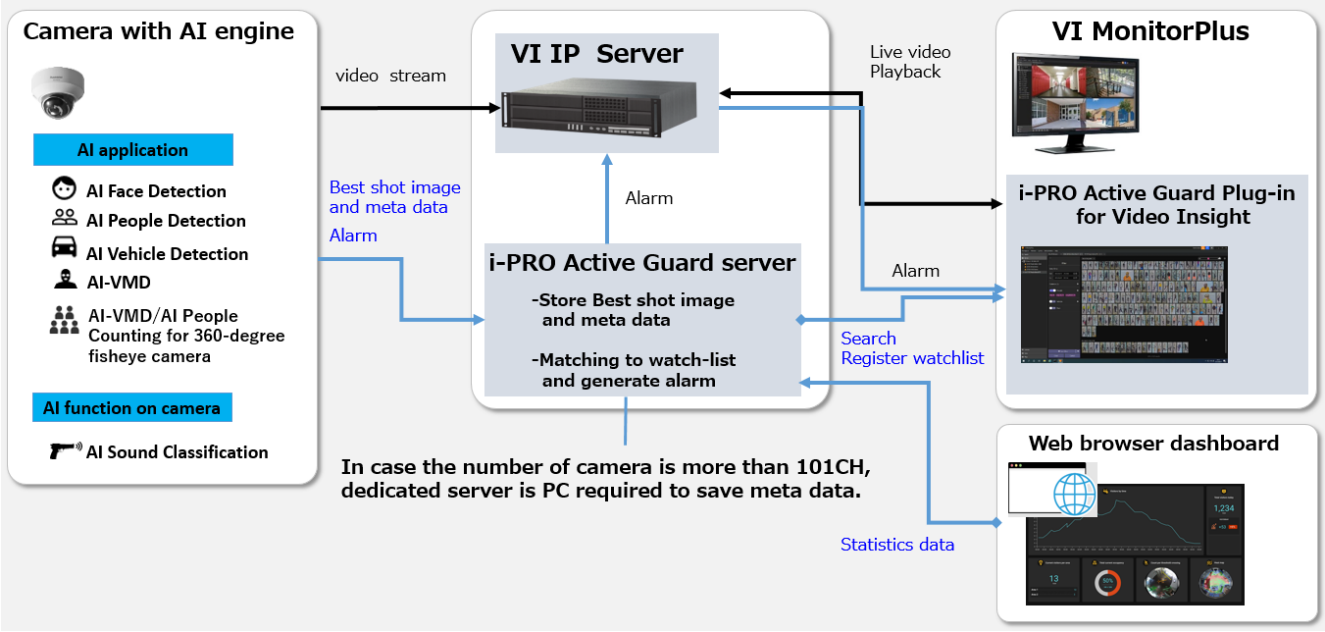
- Databases can be corrupted by forced shutdowns / power outages or system outages / system crashes due to power interruptions.

In that case, following phenomenon may occur. i-PRO Active Guard server software will not start, functions such as search, alarm notification, or watch registration will not be worked.

Damaged data cannot be recovered, so it is highly recommended to install a UPS in case of power failure.

2. Introduction to i-PRO Active Guard

2.1. System overview



AI application or AI function on cameras transmit video stream to VI IP server and transmit Best shot images and meta data to i-PRO Active Guard server.

i-PRO Active Guard server stores those data and also generate alarm when face or people is matched to watchlist.

i-PRO Active Guard Plug-in for Video Insight (hereinafter referred to as “Plug-in”) which is the plug-in software for VI MonitorPlus can search best shot images, register watchlist, show live video, recorded video, and alarm.

By visualizing statistics data from AI application on the web browser, it can also be used for business intelligence.

2.2. Software components and supported version

Camera's AI function

- AI Face Detection: Camera's extension software. V1.00 or later is supported.
  V1.10 or later is required for age and gender statistics dashboard.
- AI People Detection: Camera's extension software. V1.00 or later is supported.
- AI Vehicle Detection: Camera's extension software. V1.00 or later is supported.
  AI-VMD: Camera's extension software. V2.00 or later is supported.
  V3.00 or later is required for people or vehicle counting dashboard.
- AI Sound Classification: Camera's firmware function.
- AI-VMD/AI People Counting for 360-degree fisheye camera: Camera's extension software. V1.20 or later is supported.

Please see https://i-pro.com/global/en/surveillance/products/i-pro-ai-application/ for more information.

Cameras firmware

Camera with AI engine (hereinafter referred to as "camera") are supported.

Please also check supported camera models on VMS.

camera model	Version
WV-S1136,WV-S2136,WV-S2136L,WV-S2236L	1.00 or later
WV-S1536L,WV-S1536LN, WV-S1536LTN,WV-S2536L,WV-S2536LN, ,WV-S2536LTN	1.11 or later
WV-X1571L,WV-X2571L,WV-X2271L,WV-X1551L,WV-X2551L	1.50 or later
WV-S4576L,WV-S4176,WV-S4576LM,WV-S4156,WV-S4556L,WV-S4556LM	1.01 or later
WV-S8543,WV-S8543G,WV-S8543L,WV-S8543LG, WV-S8544,WV-S8544G,WV-S8544L,WV-S8544LG, WV-S8563L,WV-S8563LG,WV-S8564L,WV-S8564LG, WV-S8573L,WV-S8573LG,WV-S8574L,WV-S8574LG	1.01 or later
WV-S15500-V3L, WV-S15500-V3LN, WV-S15500-V3LN1, WV-S15500-V3LK,WV-S15600-V2L, WV-S15600-V2LN,WV-S15700-V2L, WV-S15700-V2LN, WV-S15700-V2LK,WV-S22500-V3L, WV-S22500-V3LG, WV-S22500-V3L1, WV-S22600-V2L, WV-S22600-V2LG,WV-S22700-V2L, WV-S22700-V2LG, WV-S22700-V2L1, WV-S25500-V3L,WV-S25500-V3LN, WV-S25500-V3LG, WV-S25500-V3LN1,WV-S25600-V2L, WV-S25600-V2LN, WV-S25600-V2LG,WV-S25700-V2L, WV-S25700-V2LN, WV-S25700-V2LG,WV-S25700-V2LN1,	1.00 or later
WV-S71300-F3	1.10 or later

VMS and i-PRO Active Guard server / Plug-in

Software	Version
VI IP server (Recording server) VI MonitorPlus (Client software) *VI Enterprise is supported, VI Express is not supported.	V7.8.3 or later
i-PRO Active Guard server / i-PRO Active Guard Plug-in for Video Insight	V1.0.0 or later

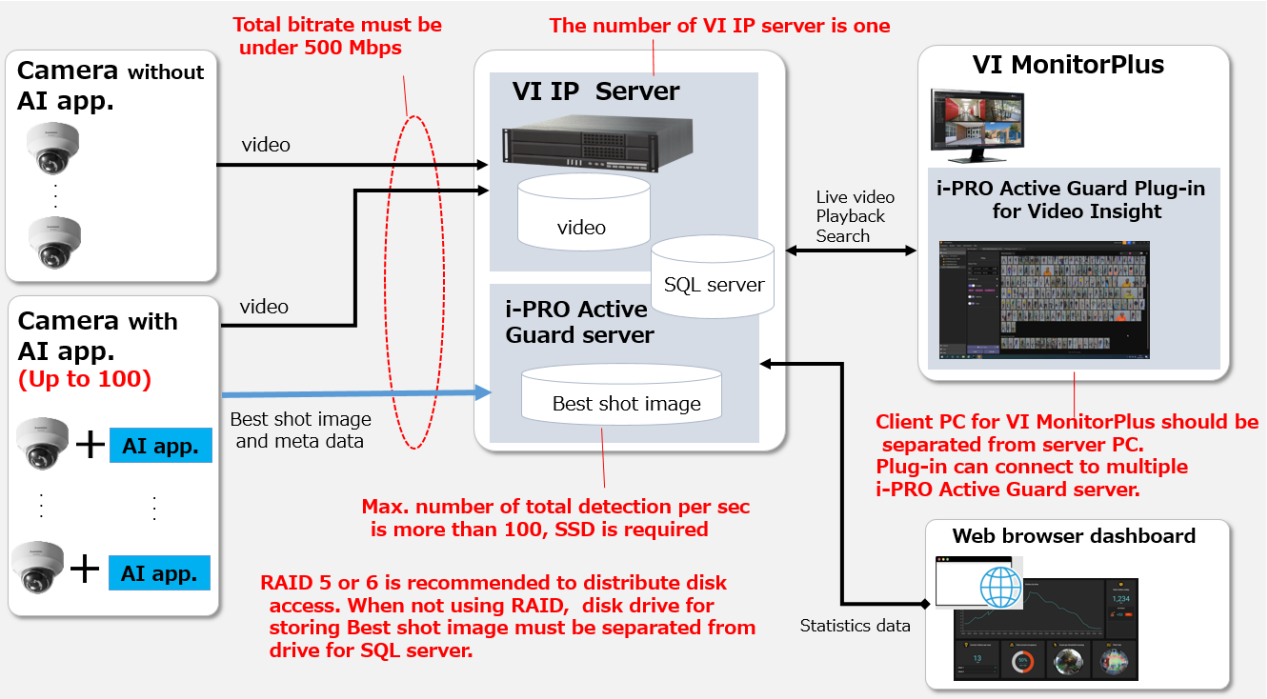
3. System design

3.1. System architecture

Two system architecture is selectable depending on the number of cameras, the number of VI IP server, the frequency that camera detects objects or storage size and so on.

	i-PRO Active Guard server installed with VI IP server	i-PRO Active Guard server installed In dedicated server
The number of cameras	100 (AI Face Detection is up to 20)	300 (AI Face Detection is up to 60)
The number of VI IP server	1	12
Total bitrate	500Mbps for video and Best shot images	500Mbps for Best shot images

3.1.A i-PRO Active Guard server installed to PC with VI IP server



There are some conditions for installing i-PRO Active Guard server to the server PC with VI IP server.

(1) The number of cameras with AI engine is up to 100
Camera with AI Face Detection is up to 20.

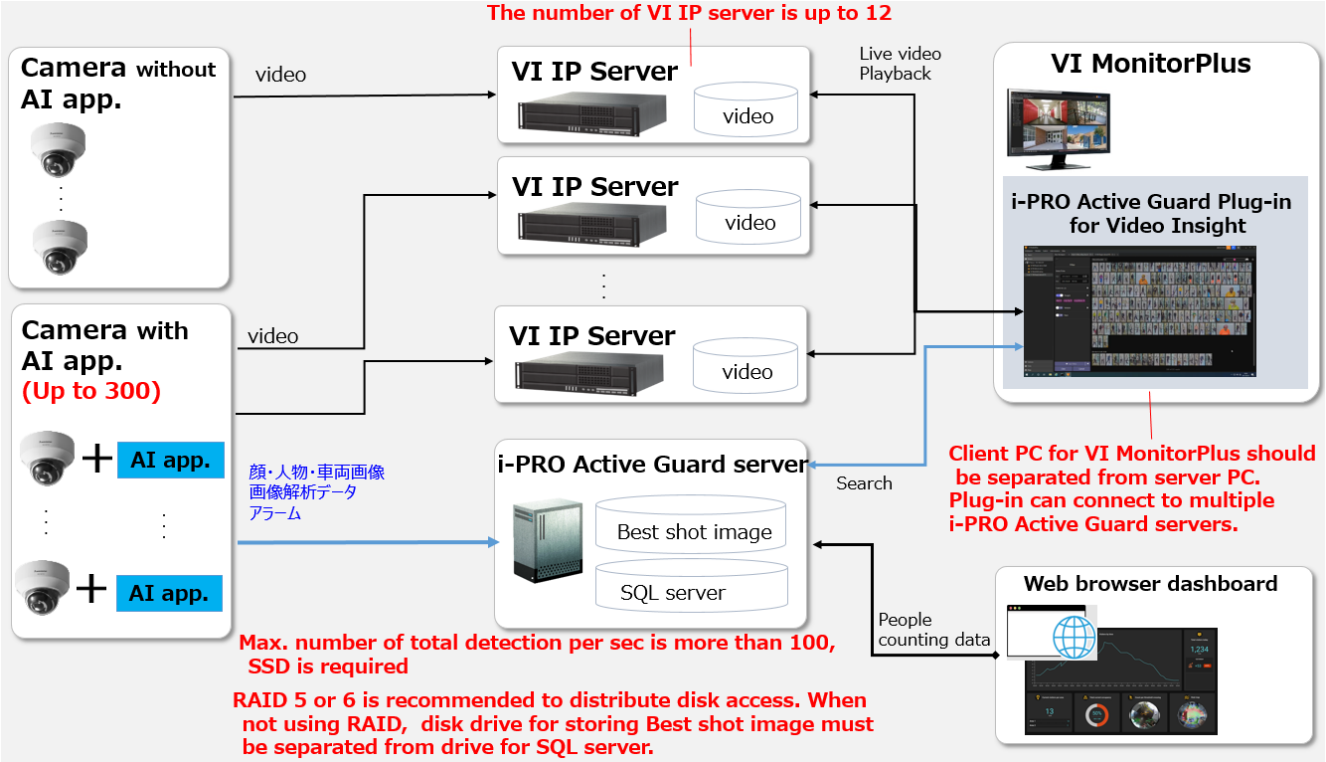
(2) Total bitrate that server PC receives must be under 500Mbps. Both bitrate of video data and Best shot images should be calculated. For video, the Storage and Bandwidth calculator is available on http://www.video-insight.com/storage- and-bandwidth-calculator.
Bitrate of Best shot images can be calculated in 3.3.

(3) The number of VI IP server is one. When multiple VI IP servers exist in system, dedicated server PC is required for i-PRO Active Guard server. Dedicated server PC is also required when using failover server for VI IP server.

(4) RAID 5 or 6 is recommended to distribute disk access. When not using RAID, disk drive for storing Best shot image must be separate from drive for storing video and SQL server.

(5) Client PC should be separated from server PC. Plug-in can connect to one i-PRO Active Guard server.

3.1.B i-PRO Active Guard server installed to dedicated server PC



When i-PRO Active Guard server is installed in dedicated server,

(1) The number of cameras with AI engine is up to 300.
Camera with AI Face Detection is up to 60.

(2) Up to 12 VI IP server can be registered to i-PRO Active Guard server.
Each camera should be registered to one VI IP Server.

(3) RAID 5 or 6 is recommended to distribute disk access. When not using RAID, disk drive for storing Best shot image must be separate from drive for SQL server.

(4) Client PC should be separated from server PC. Plug-in can connect to multiple i-PRO Active Guard server.

3.2. System requirement

3.2.1 System requirement for i-PRO Active Guard server

Hardware requirement

	Requirement
Up to 100 cameras i-PRO Active Guard server installed with VI IP server	• Intel® Xeon® Silver 4208 2.1 GHz(8 core 16 thread) or better • 32 GB of RAM or more • 64 bit operating system Microsoft® Windows Server 2016/2019 Standard Edition • GbE network interface card
Up to 100 cameras i-PRO Active Guard server installed in dedicated server	• Intel® Core™ i7-9700 (4.9 GHz, 8 core 8 thread) or better • 32 GB of RAM or more • 64 bit operating system Microsoft® Windows 10 Pro version 2004,21H1 or later , Microsoft® Windows 11 Pro, Microsoft® Windows Server 2016/2019 Standard Edition • GbE network interface card
Up to 300 cameras i-PRO Active Guard server installed in dedicated server	• Intel® Xeon® Silver 4208 2.1 GHz(8 core 16 thread) or better • 32 GB of RAM or more • 64 bit operating system Microsoft® Windows Server 2016/2019 Standard Edition • GbE network interface card

Common software requirement

Category	Supported software
Database Engines	• SQL server 2014/2016 Express/Standard Edition SQL server 2016 Express Edition is installed when installing i-PRO Active Guard server. Upgrade procedure is shown in 5.10.
Web browser for Configuration Tool	•Microsoft Edge 85 or later •Chrome 83 or later •Firefox 95 or later

Disk drive considerations

When the maximum number of detection exceeds 100 objects per second for all cameras, SSD is required for storing data. See 3.3 in detail. If using HDD, data will not be stored and system become unstable.

RAID 5 or 6 is recommended to distribute disk access. When not using RAID, disk drive for storing Best shot image must be separate from drive for SQL server.

Database considerations

The SQL server Express Edition has limitation that the maximum size for database is 10GB, so estimated used disk size for database of face, people and vehicle should be under 8GB.” Check 3.3 to see if the Express edition is sufficient.

3.2.2 System requirement for Plug-in

Component	Requirement
Processor	6th Generation or better Intel Core processor(3.1 GHz quad-core+)
Memory	8 GB or more
Video	1GB
Network	1 Gb/s+
OS	Microsoft® Windows 10 Pro (64 bit) Microsoft® Windows 11 Pro (64 bit)

3.3. How to determine the system architecture

STEP1: The number of camera

When the numbers of cameras with AI People detection, AI Vehicle detection, AI-VMD, Sound or AI-VMD/AI People Counting for 360-degree fisheye camera is no more than 100(AI Face detection is no more than 20), it may be possible that AI server is installed to PC with VI IP server. Please continue to check STEP2.

When over 100 (or over 20 for AI Face detection), i-PRO Active Guard server should be installed in dedicated server PC. Please see 3.1.B i-PRO Active Guard server installed to dedicated server PC".

In case of multi-sensor camera, extension software can be installed for each camera and the each camera needs to be registered to i-PRO Active Guard server.

STEP2: The number of extension software

To calculate the bitrate of Best shot, the number of extension software (Face, People, Vehicle and People Counting for for 360-degree fisheye camera) should be considered. Since the amount of counting data by AI-VMD is small, it is not necessary to consider it. Multiple extension software can be installed to each camera.
(ex, When People and Vehicle are installed to a camera, add 1 for People and Vehicle, respectively.)

		Face	People	Vehicle	People counting for 360-degree fisheye camera
The number of extension software					
# of people/vehicle	Max.	1,000	1,000	1,000	
[per camera, per hour]	Average.	1,000	1,000	1,000	

Maximum number of detection in total [per sec]	0

When "Maximum number of detection in total" is less than 100, HDD or SSD is available for disk drive.
When "Maximum number of detection in total" is over 100, SSD is required.

STEP3 : Total bitrate server receives

Maximum bitrate of Best shot image [Mbps]	0.00
Maximum bitrate of People counting data [Mbps]	0.00
Total bitrate of video recording for all cameras(*) [Mbps]	
Total bitrate that server PC receives [Mbps]	0.00

If the “Total bitrate that server PC receives” exceeds 500Mbps, i-PRO Active Guard server should be installed in dedicated server PC.

* Storage and Bandwidth calculator for video is available on
http://www.video-insight.com/storage-and-bandwidth-calculator

STEP4: Retention period and storage

	Face	People	Vehicle	People counting for 360-degree fisheye camera
Retention period (day) *Face, People, Vehicle(14-31), People counting(14-92)	31	31	31	92
Operating time (hours per day)	8	8	8	8

Estimated used disk size for Best shot images[GB]	0.00
Estimated used disk size for People counting[GB]	0.00
Estimated used disk size for database[GB]	0.00

When "Estimated used disk size for database" is under 8 GB, SQL Server Express Edition or Standard Edition can be used. When more than 8GB, SQL Server Express Edition cannot to be used due to the limitation of Express Edition. Standard Edition is must. (Refer to 5.10)

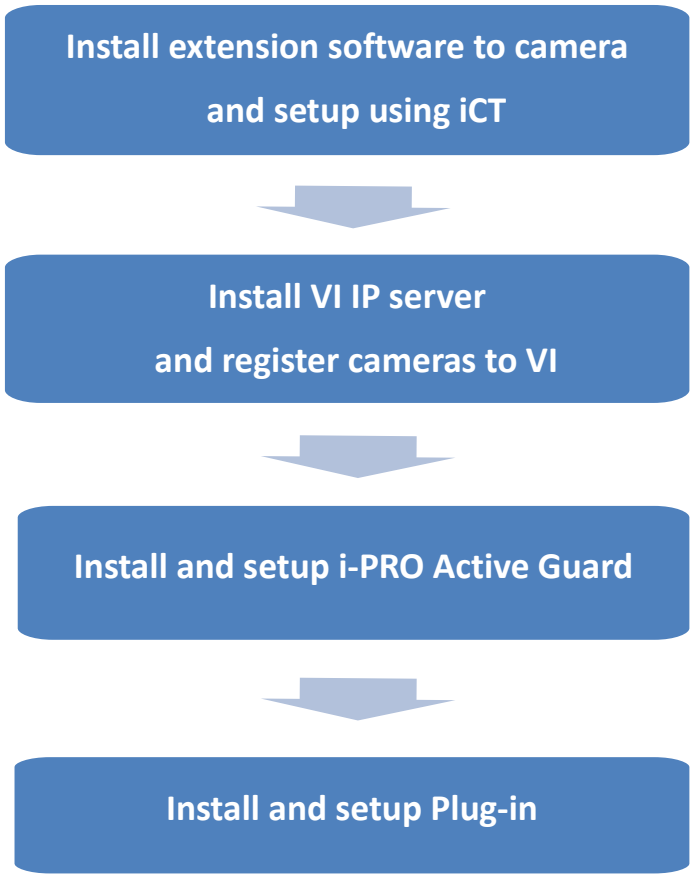
3.4. Ports used in i-PRO Active Guard server

The following table lists the default network ports used by i-PRO Active Guard server.
These ports need to be allowed from firewall configurations.

Port number	Protocol	Port usage
1435	TCP	Connection to SQL server
8090	HTTP	Client plugin connection
8091	HTTPS	Client plugin connection
8092	HTTPS	Web configuration tool connection
50000	TCP	Internal process communication
50002	TCP	Internal process communication

4. Installation and setup

Procedure overview



4.1. Install extension software to camera and setup using iCT

Download the extension software and refer manual from https://i-pro.com/global/en/surveillance/training-support/documentation-database-list/

4.2. Install and setup VI IP server

Install the VMS server software and register the AI camera with the VMS client.

Install Plug-in to VI IP server and configure alarm port.

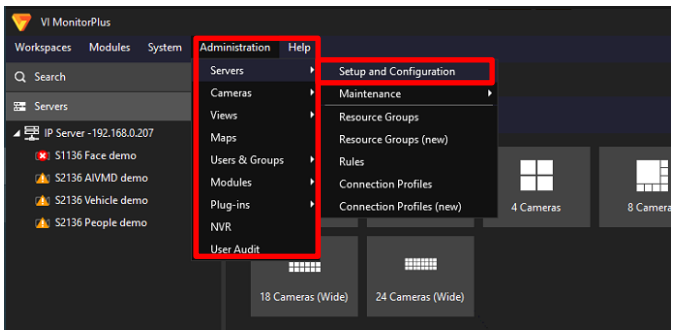
Register the camera in MAP as an Option setting

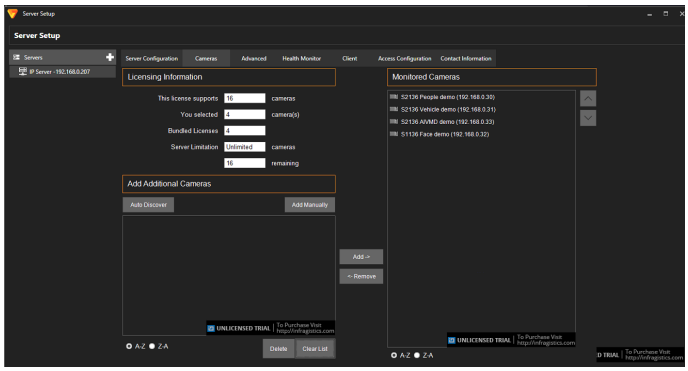
4.2.1. Install and register cameras to VI

Detail procedure about VI installation and basic setup are shown on VI's manual.

After installation, register AI cameras to VI IP server using VI MonitorPlus.

([Administration] – [Servers] – [Setup and Configuration] – [Cameras])



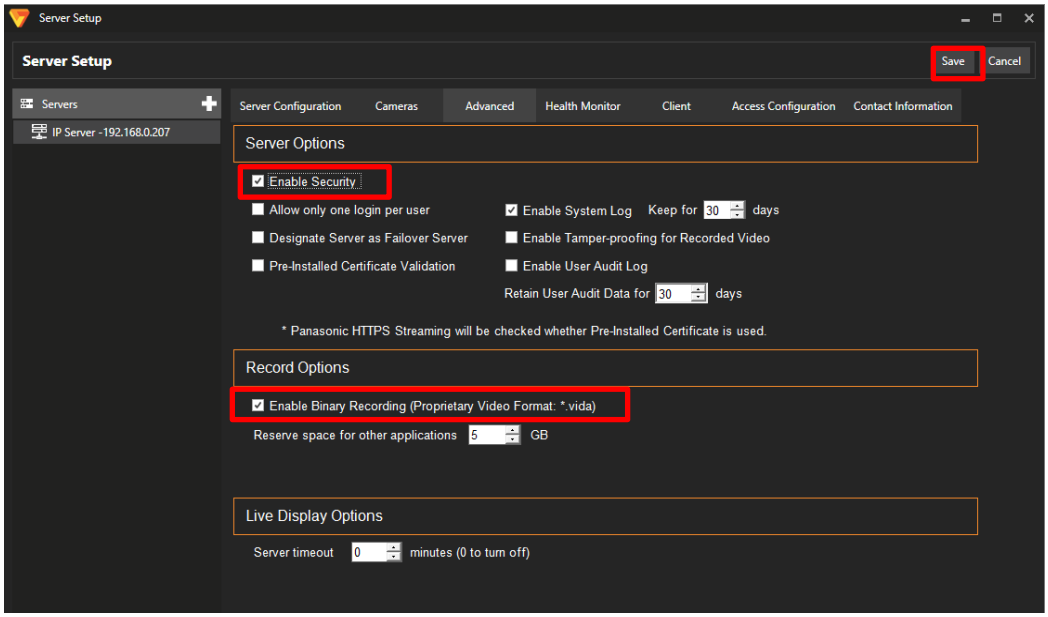


4.2.2. Setup VI IP server

4.2.2.1. Configure general settings

([Administration] - [Servers] - [Setup and Configuration] - [Advanced] tab)

Check [Enable Security] and [Enable Binary Recording] and [Save].

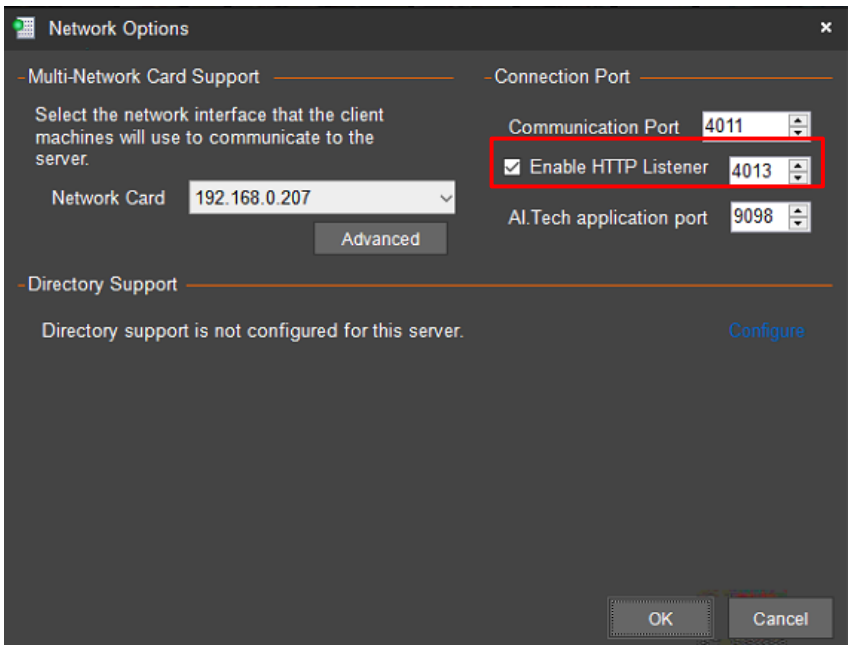


4.2.2.2. Configure the port to receive alarm

([IP Server Manager] – [Network Options])

Check [Enable HTTP Listener] and [OK].

[Restart] from Service Controls.



4.2.2.3. Register cameras to Map (optional)

Using maps, operator can easily found the location of each Best shot image on plugin screen.
See operation manual of VI in details.
([Administration] – [Maps])

4.2.3. Install Plug-in to VI IP server

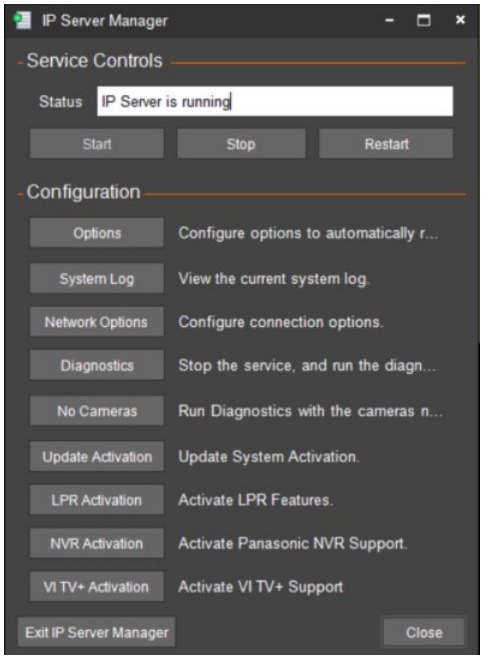
Install “i-PRO Active Guard Plug-in for Video Insight” software to VI IP server’s PC.

STEP1

Click [Run as administrator] in the right click menu of the [Server Manager] icon on the desktop.

STEP2

Click [Stop] button.



STEP3

Launch the executable installer as Administrator.
Click the [Next] button, then check mark [I accept the terms in the License Agreement], and then click the [Install]
When the installation complete window is displayed, click the [Finish] button.

STEP4

Restart the IP Server by click [Start] button.

4.3. Install and setup i-PRO Active Guard server

Download the installer from https://i-pro.com/global/en/surveillance/training-support/documentation-database-list/

Install i-PRO Active Guard server software. Configuration after installation can be done from web browser.

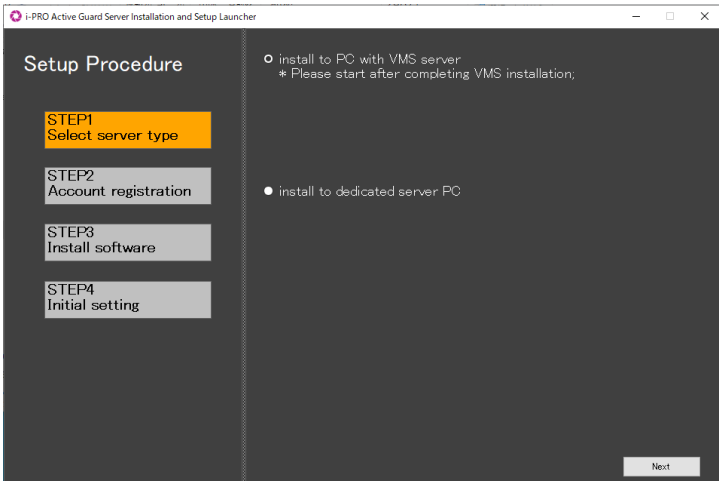
4.3.1. Install

Execute "MultiAIStartup.exe" as administrator (file path length must be less than 120).

When .NET Framework 4.8 is not installed on the PC, it will automatically be installed and the main screen of the setup tool will be displayed after the installation.

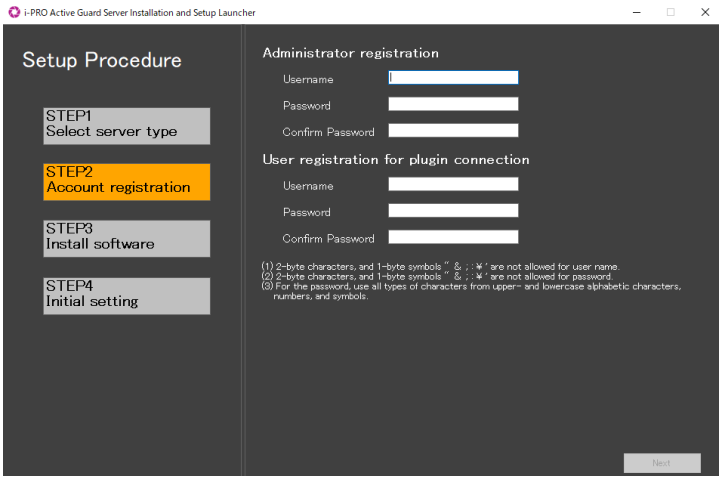
Also, when you use Windows 10 version 20H2, Windows Update message. Execute "Windows Update" according to the message.

Check for [Agree] for License terms and [OK].



Select [install to PC with VMS server] or [install to dedicated server PC] and click [Next].

Note)
When you install i-PRO Active Guard server to PC with VMS server, you need to install VMS server software in advance.

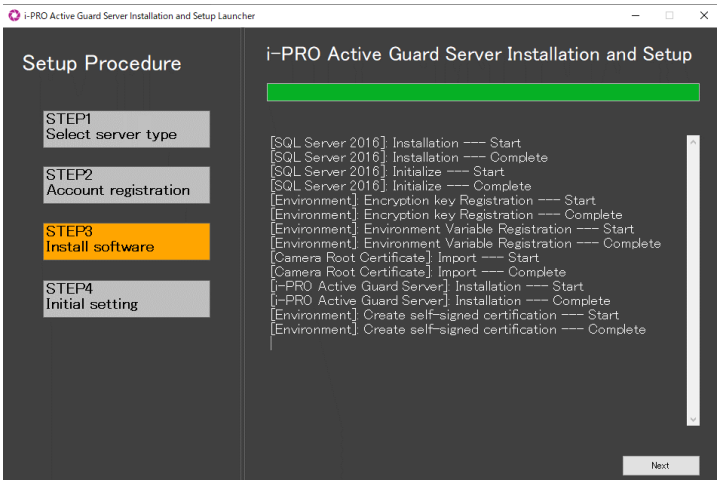


Register credentials and click [Next].

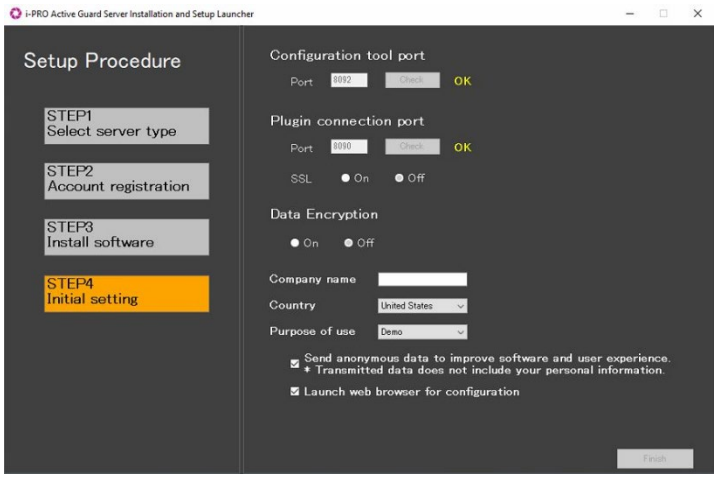
Note)
Make a note of the password you entered and keep it in a safe place.

When you forget the Administrator account, you can reset (Refer to 5.9).

When you forget the User account, you can reset (Refer to 4.3.7.2).



Installation starts and [Next] button will be appeared when finished. Click [Next].



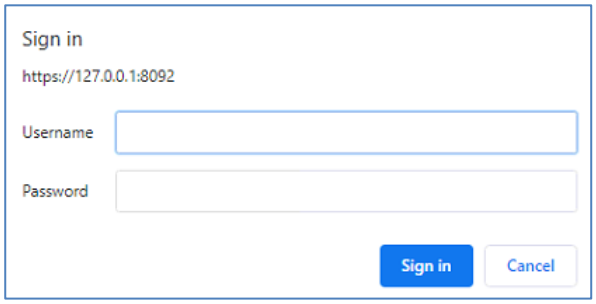
Configure port number, SSL and Data encryption, Company name, Country and Purpose of use and click [Finish].

Note) When On is selected for Data Encryption, Image data will be encrypt. This setting cannot be changed after installation. Re-installation is required when you want to change after completing installation.

4.3.2. Setup i-PRO Active Guard server

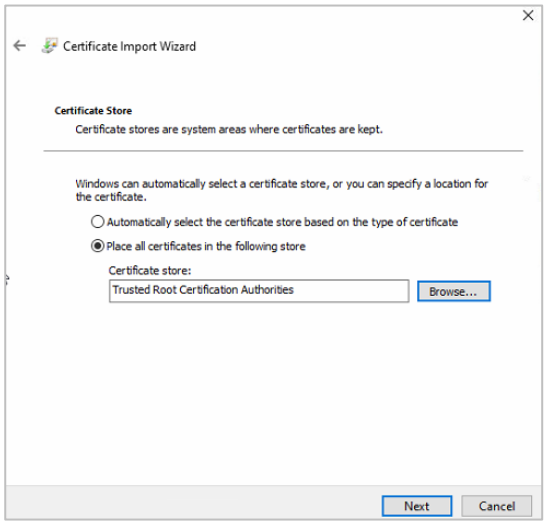
4.3.2.1. Login

Access https://<ip>:8092 using Google chrome, Microsoft Edge or Firefox.
Input credentials.

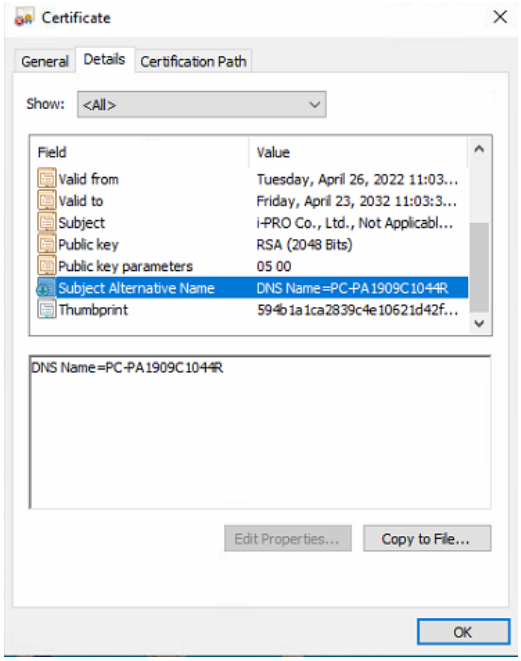


Note)
Credentials and port number configured by install tool 4.3.1 are used.
i-PRO Active Guard server uses self-signed certificate for web access.
When the security alert window is displayed, click [advanced] and [Proceed to <ip> (unsafe)].

It is possible to prevent the warning display by performing the following procedure for each client PC to be accessed.
1) Copy “C:¥MultiAI¥apache24¥conf¥server.crt” in i-PRO Active Guard server PC to client PC.
2) Double click the file and click “Install Certificate”.
3) Select “Local Machine” for Store Location
4) Select “Place all certificates in the following store and “Trusted Root Certification Authorities”.



5) Confirm “Subject Alternative Name” from “Details”. DNS Name=xxxx is shown.

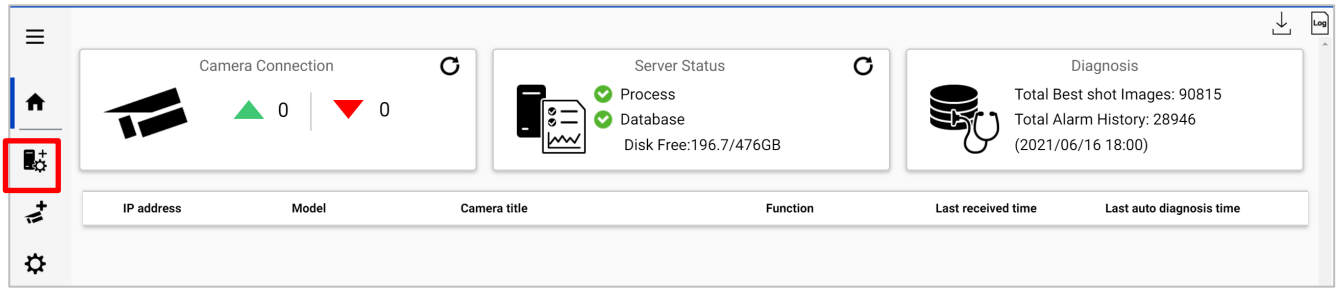


6) Open “C:¥Windows¥System32¥drivers¥etc¥hosts” and add IP address of i-PRO Active Guard server and xxxx(DNS Name).
ex. 192.168.0.125 PC-PA1909C1044R

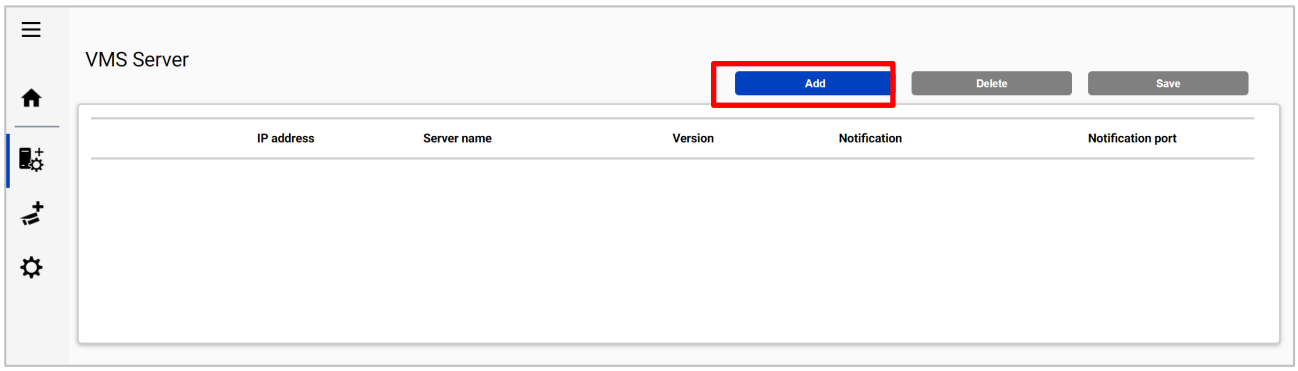
7) Access https://xxxx:8092 using web browser.

4.3.2.2. Register VMS

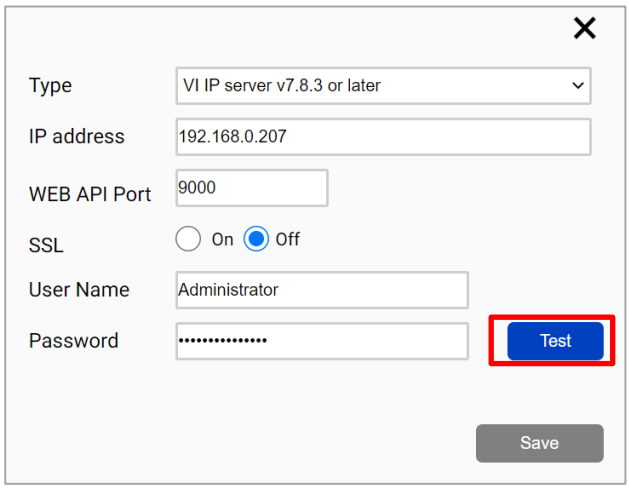
Click  (Register VMS)



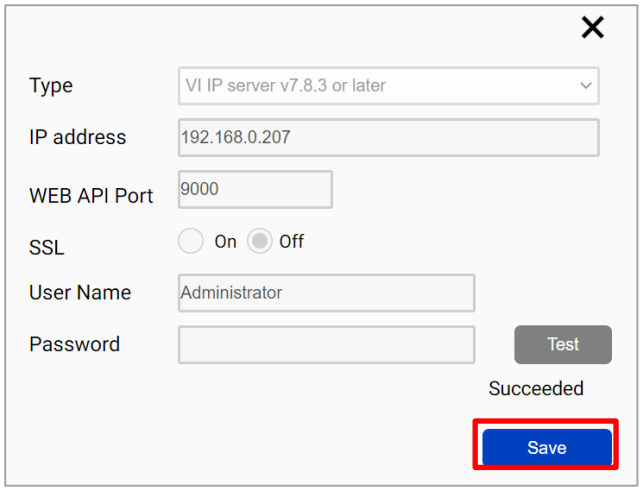
Click [Add]



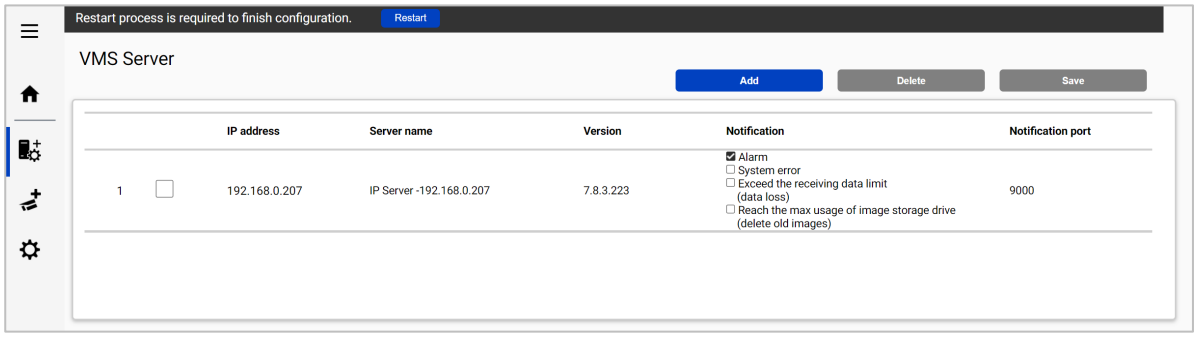
Input VI IP server's information and click [Test]



When Succeeded is shown, click [Save]



Confirm VMS server is registered

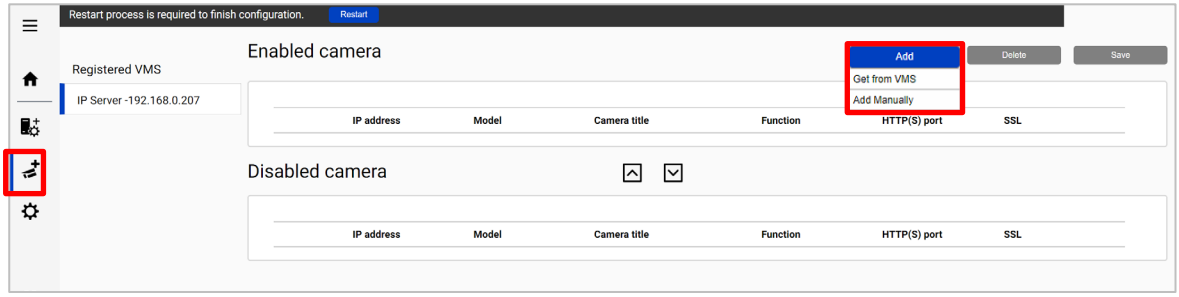


Note) Restart button will be appeared on the top of screen, but you do not need click now.
You need to click Restart after completing all other configuration.

4.3.2.3. Register Cameras

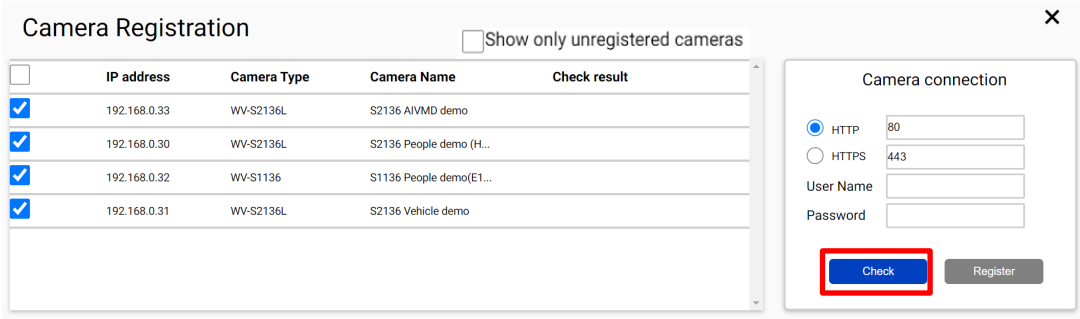
Click  (Register Cameras)

Select [Add] - [Get from VMS]



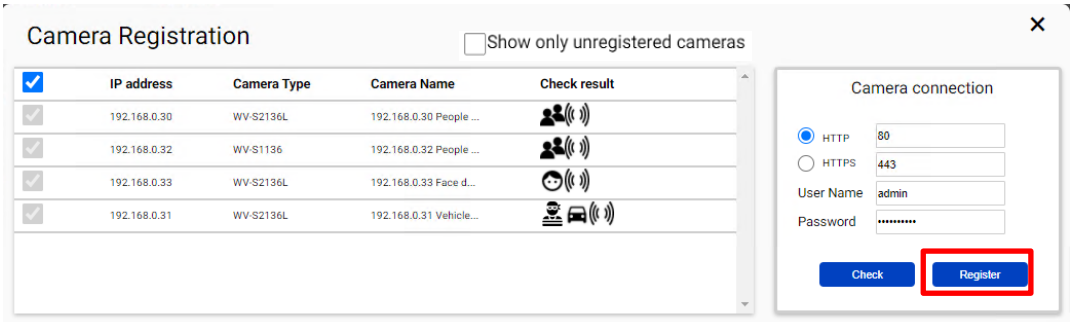
Note) When camera is registered from [Add manually], only dashboard function can be used. Plug-in cannot use the camera. Enter IP address of the camera, credentials, [Check] and [Register].

All i-PRO cameras (including not supported cameras) are shown.
Input camera's credentials and click [Check].



Note)
Camera can be sorted by [IP address], [Camera Type] or [Camera Name].
Unregistered cameras can be filtered by checking [Show only unregistered cameras].

Icon related to AI function is shown for supported AI cameras.
Click [Register].



(AI People detection)

(AI Vehicle detection)

(AI Face detection)

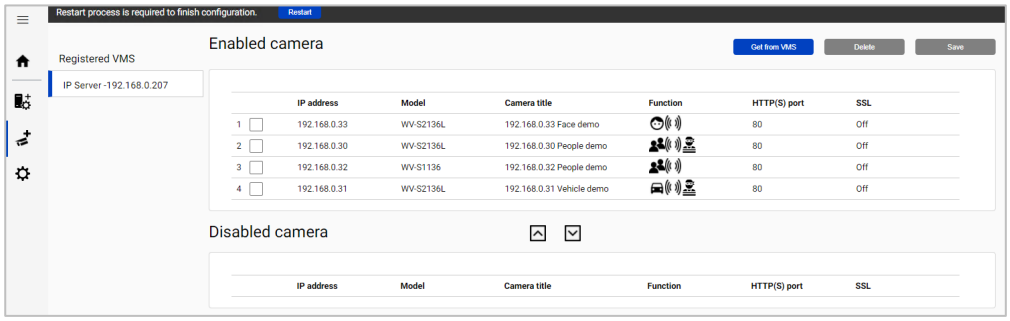
(AI-VMD)

(AI Sound classification)

(AI People Counting)

(AI Vehicle Counting)

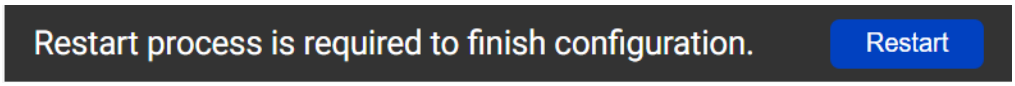
Confirm cameras are registered



4.3.3. Restart process to apply changes

*To apply any configuration changes, restart process is required.

When you finish all configuration. Click “Restart” from display bar above or Home screen.



4.3.4. Check

Click (Home)

- Check camera connection

Check all registered cameras are connected.

means the number of camera connected. (meta data session between camera and i-PRO Active Guard server).

means the number of camera disconnected. When disconnection detected, confirm network connection to camera.

- Check Server status

Check Process and Database shows status green.

4.3.5. System configuration (optional)

Click ⚙ (Configure system) and change settings if needed.

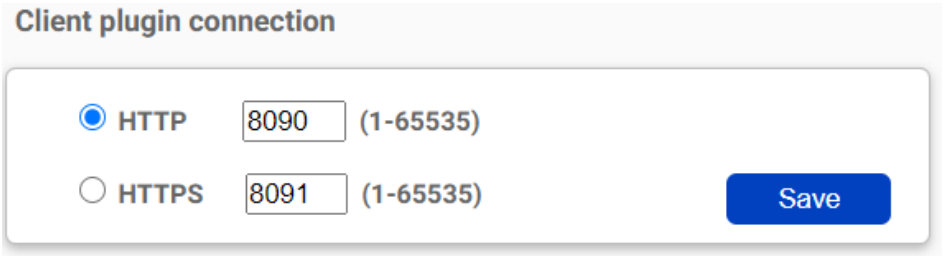
4.3.5.1. General

Select [Auto], [English] or [Japanese] for [Language]. (Default: Auto).
Check or uncheck for [Send anonymous data to improve software and user experience].

Note) When the language configuration for web browser is other than English or Japanese, English is shown.

4.3.5.2. Client plugin connection

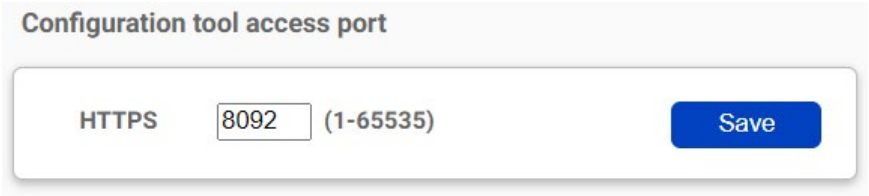
Select [HTTP] or [HTTPS] and port number (Default: Set by install tool at 4.3.1)



Note) For secure communication, HTTPS is recommended.

4.3.5.3. Configuration page access

Set port number for configuration tool (Default: Set by install tool at 4.3.1)



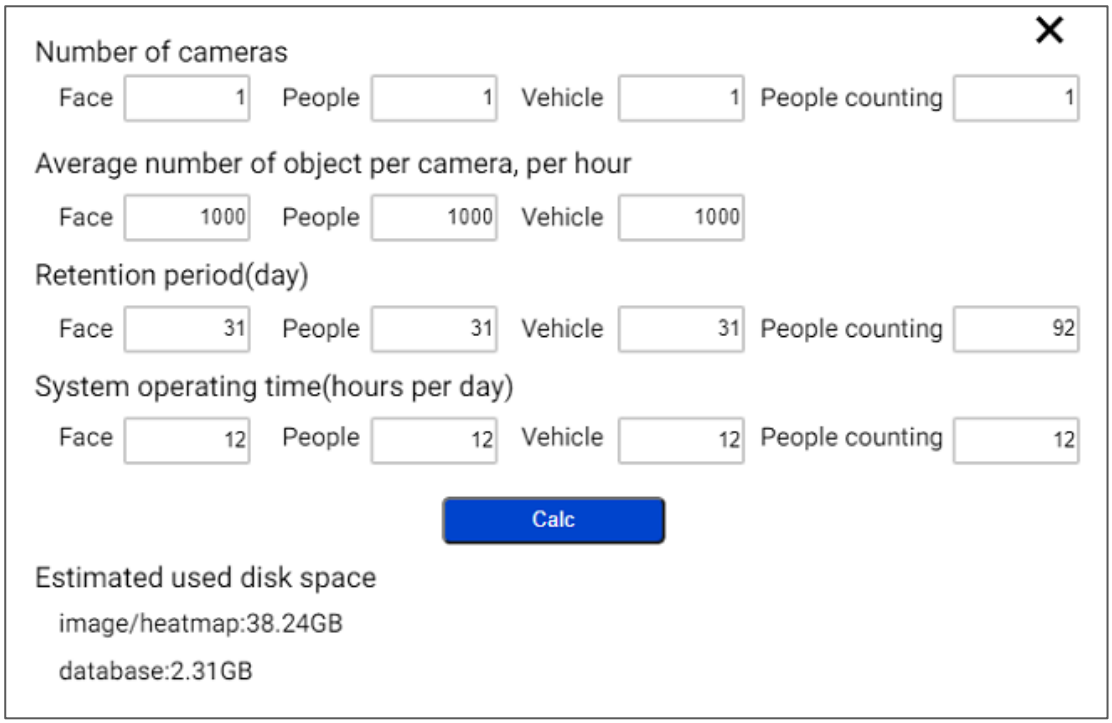
Note) When you change and restart software at 4.3.2, you need to access https://<ip>:<port> using new port number. Make a note not to forget.

4.3.5.4. Database

Configuration item	Comment
Storing images in database	On(default): Store Best shot images from camera Off: does not store images from camera.
Retention period	14 – 31 days (Default: 31) can be set for face image/statistics, people image/statistics, vehicle image/statistics and alarm history, respectively. 14 – 92 days (Default: 92) can be set for people/vehicle count including heat map statistics. Note) Data after retention period will be deleted at night (0:00am ~ 3:30 am). If the server is shut down, data cannot be deleted, so new data may not be stored due to lack of storage space.
CSV backup	Enable/Disable can be configured. (Default: Disable) When enable and the retention period for people counting data expires, the data will be deleted from SQL server but automatically backed up as CSV file. Data in CSV file cannot be shown on dashboard. Note) When enable, [Max usage of image storage drive] will be also enabled automatically.
Max usage of image storage drive(*)	Enable/Disable and data size 10- 2000 (GB) can be configured. (Default: Disable) Note) When enable, and the used disk space of drive for storing Best shot images exceed the setting value, old image will be deleted automatically. This works every hour. You can manage data size using this configuration that i-PRO Active Guard server stores. Used disk space equals total volume minus free space.
Image data save path	Save path for images (Default: C:¥MultiAI¥Image) Note) When you change save path, all existing image data cannot be used from Plug-in.
Max frequency of receiving object data (per sec)	50 -300 (Default: 100) Note: If the number of object data from all cameras exceed the value, those object data will be discarded to reduce disk access so that system is stable. SSD is required in case of 100 or more. When you set over 100 using HDD, system will be unstable.
Data encryption	On/Off is shown set by install tool at 4.3.1. You cannot change this after installation.

* Simple calculator can be used by clicking 

Input parameters of your system and click Calc. Estimate used disk space is shown.



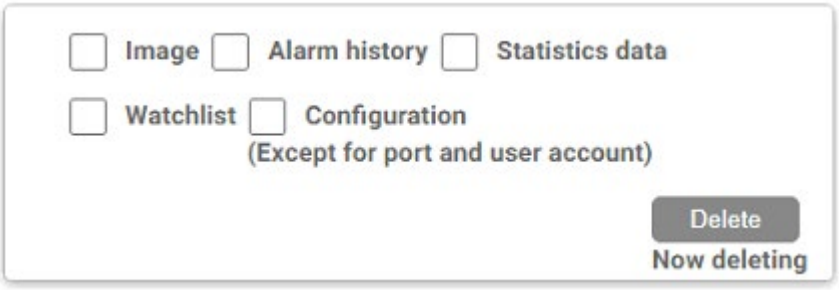
Note)

Estimated used disk space is just a reference. Actual data size highly depends on actual environment.

4.3.5.5. Initialization

Image: delete all Best shot images.
Alarm history: delete all alarm history
Statistics data: delete statistics data.
Watchlist: delete all face watchlist and people watchlist. See operation manual about watchlist.
Configuration: delete all registration data (VMS, Camera and logs) except for port and user account.

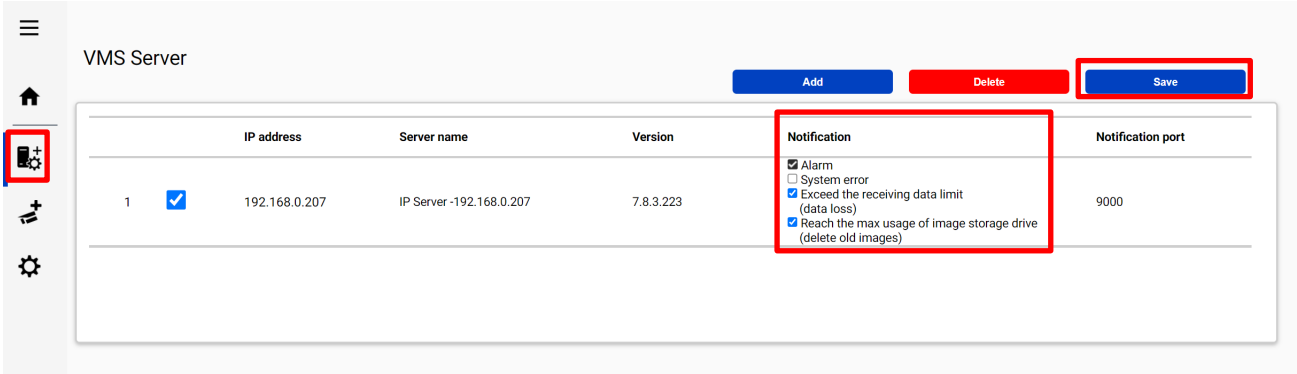
Note)
It may take time to delete image depending on the number of images. When deleting, button will be as follows. Please update page to confirm the latest status.



4.3.6. Notification to VMS Server (optional)

Some alarms related to i-PRO Active Guard server's system failure can be enabled.
Actions on VMS side also can be configured (4.5.1.E System alarm of i-PRO Active Guard server)

Click  (Register VMS)



Check following items that you want and [Save].

System error

Error that i-PRO Active Guard server detects. (ex. camera connection error between camera and i-PRO Active Guard server.)

Exceed the receiving data limit (data loss)

When the data exceeds the setting value for "Max frequency of receiving object data (per sec)" configured at 4.3.5.4.

Reach the max usage of image storage drive (delete old images)

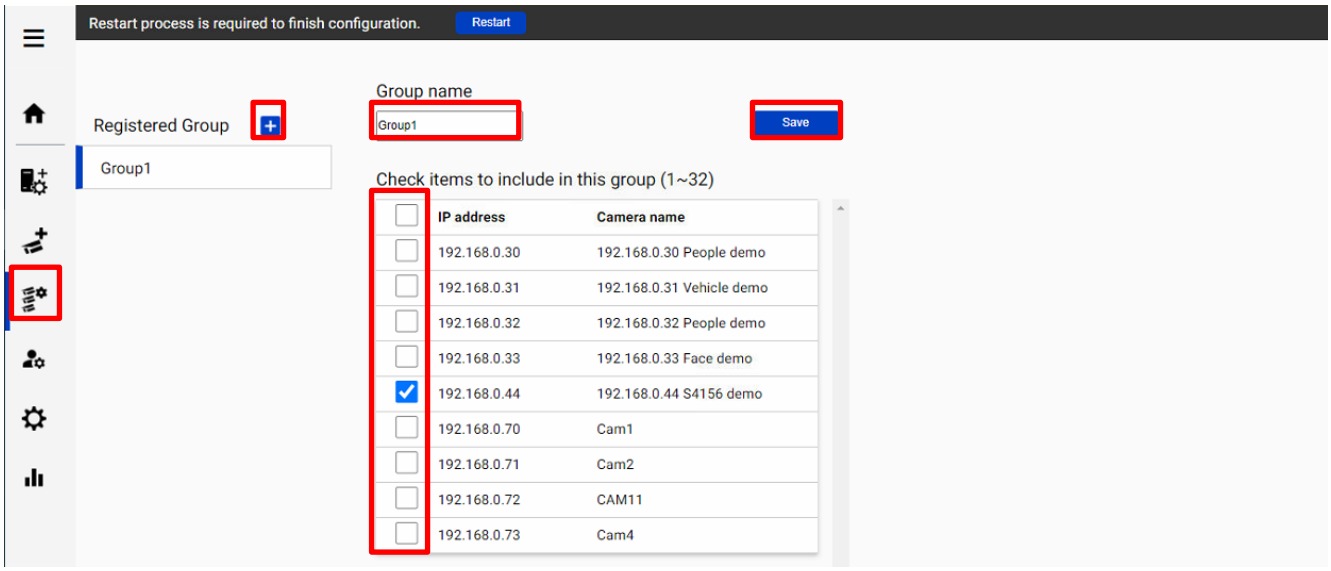
When the usage of image storage drive exceeds the setting value for "Max usage of image storage drive (GB)" configured at 4.3.5.4.

4.3.7. Dashboard configuration (optional)

4.3.7.1. Camera group configuration

When displaying the chart on the dashboard, it is possible to display it as statistical information for each group consisting of multiple cameras instead of statistical information for each camera.

Click  (Camera Group).



Click [+] button, input Group name, check for cameras and [Save].

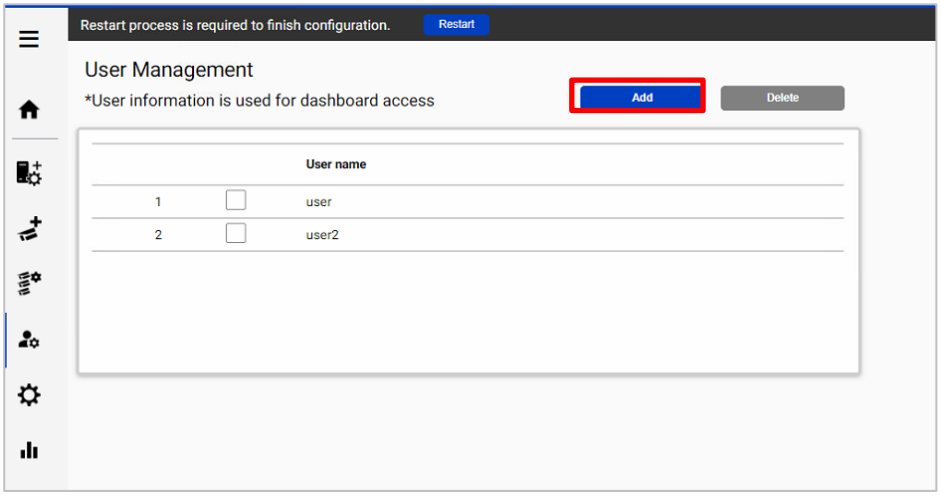
Note) Up to 16 groups can be configured.

To delete camera group, right click the group and select [Delete Camera Group].

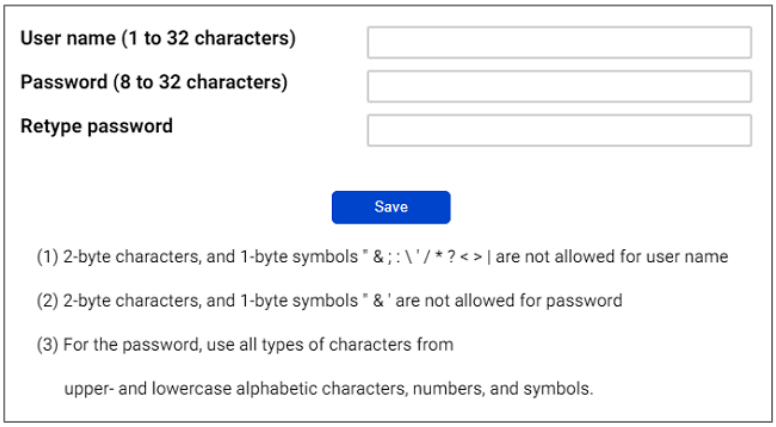
4.3.7.2. User Management

By registering multiple users, it is possible to customize the dashboard display for each user.

Click  (User Management) and [Add].



Enter [User name], [Password] and [Retype password] and then [Save]



Note) User information can also be used for plugin connection.

[User name] set by install tool at 4.3.1 is shown as default. [Password] is not shown.

If you forget password, delete the user and register again.

4.3.8. More information about status (optional)

4.3.8.1. Camera Connection

: Camera is connected.

: Camera is not connected.

: Camera is connected, but last auto diagnosis result error.

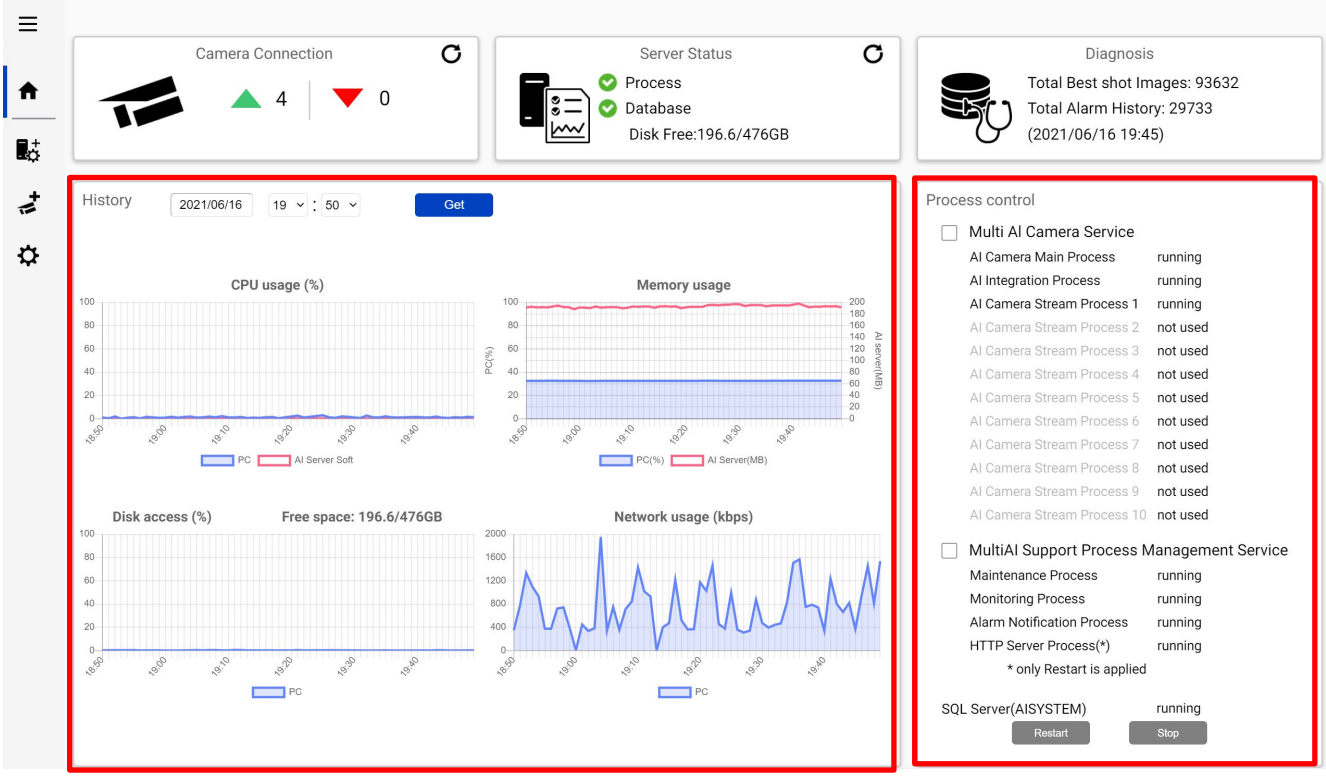
Metadata session is connected, but AI application on camera side may not work well. Check AI application on camera side is installed, schedule setting is on and also check whether “Last received time”.

“**Last received time**” shows the last detection time that the camera detected face, people, vehicle or alarm. If this time is older than when camera captured actually objects, AI application on camera side may not work well.

“**Last auto diagnosis time**” is the latest time when i-PRO Active Guard server tested connection to camera and database. The test executes every 5 minutes for a camera in order. When error occurs, the time is shown in red color. In that case, check Log and confirm the status of camera or database.

Note)
When schedule setting for the AI application is off, last auto diagnosis will be failed. If it is intended, please ignore this indicator.

4.3.8.2. Server Status



History

History shows CPU usage, Memory usage, Disk access and Network usage of the i-PRO Active Guard server. CPU usage and Memory usage show the total value in the PC and i-PRO Active Guard server. Data for one hour from specified date is shown. Select date and [Get] for previous date (within 31 days can be shown).

These data can be used to check whether PC performance is stable after installation or investigation of the system trouble.

Note) Data may not be shown correctly when PC is power off or i-PRO Active Guard server software is stopped for some duration.

Process Control

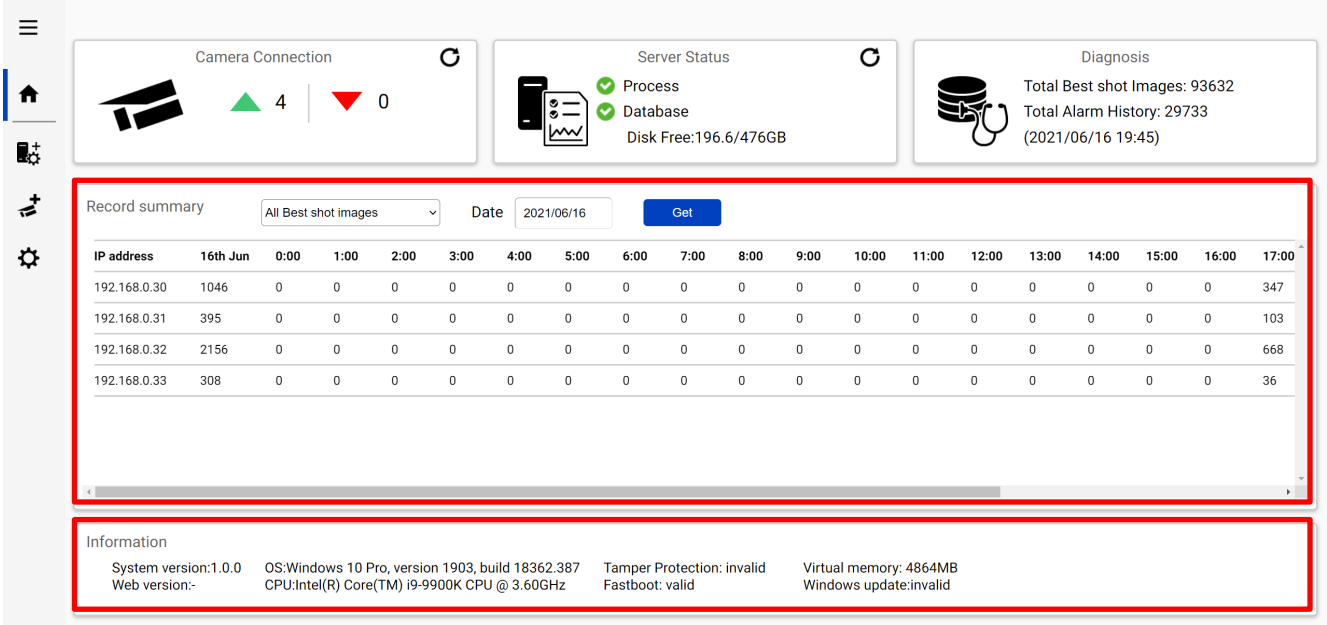
Processes related to i-PRO Active Guard server can be restarted or stopped. When the system is running, please check all processes show “running” or “not used”.

(The number of used “AI Camera Stream Process x” depends on the number of registered cameras.)

When it is required to restart PC, check [Multi AI Camera Service] and [MultiAI Support Process Management Service] are stopped (also see 5.8).

When investigation to system trouble is required, please check status and try to [Restart].

4.3.8.3. Diagnosis



Record summary

Record summary shows the number of received data from each camera on the specified date.

Selectable items depend on the registered camera and AI application.

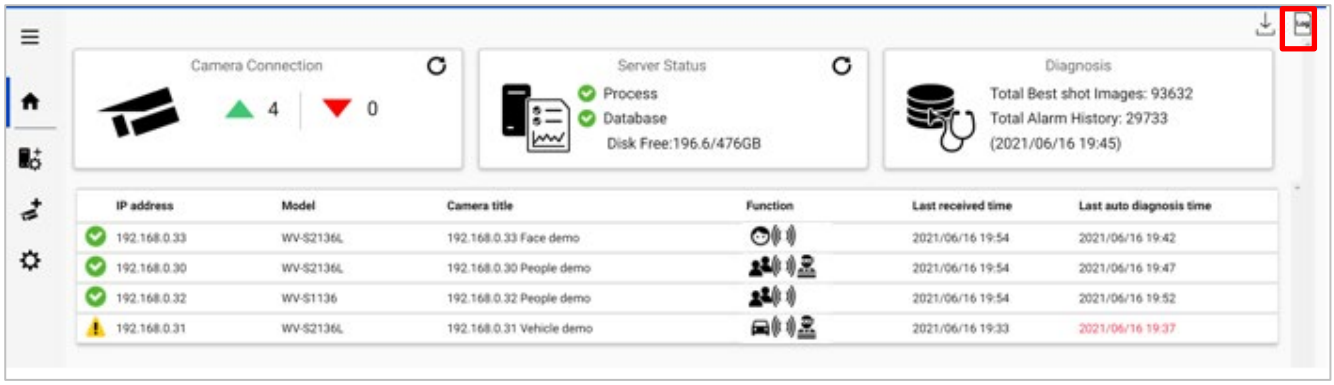
*Selectable items

- All Best shot images
- Face Best shot images
- People Best shot images
- Vehicle Best shot images
- All alarm
- Registered face detection
- Registered people detection
- AI-VMD
- Sound detection
- AI Occupancy detection

Information

Software version, OS, windows configuration are shown.

4.3.8.4. Display log

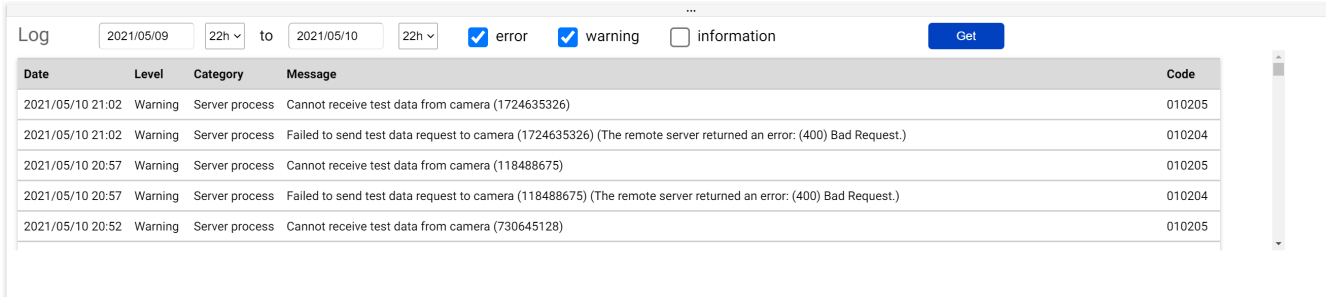


Click 

to show logs.

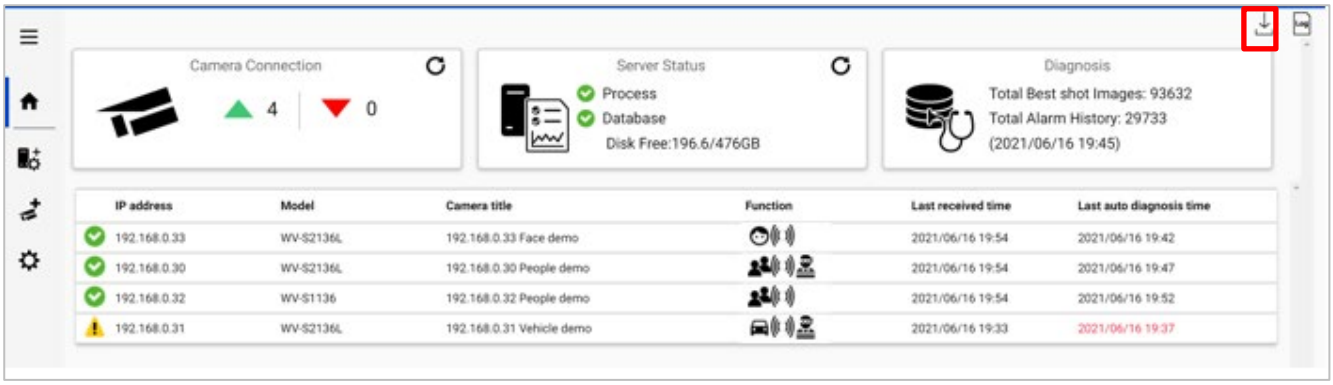
Overview of system error can be displayed. Select date and error level ([error], [warning] and [information]) and click [Get].

Detail for each message and troubleshoot for Code is shown on 6 Troubleshooting.

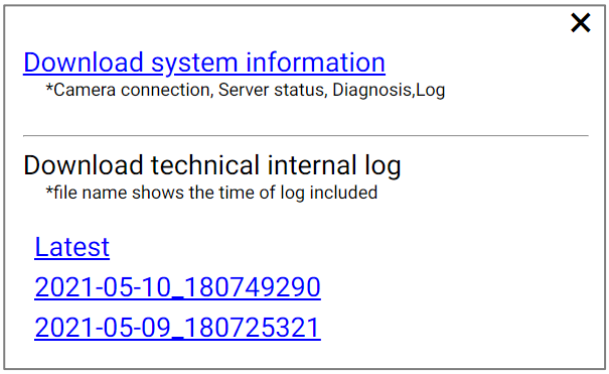


Note) Maximum 1000 logs can be shown at the same time.

4.3.8.5. Download log



Click ⬇ to download log.



Download system information

Download Camera Connection, Server Status, Diagnosis and Log loaded on screen as json format.

Download technical internal log

Download detail log. File name “yyyy-mm-dd_hhmmssfff” shows the time of log included. Log files are zipped automatically depending on the duration or size and the filename shows the time zipped.

Ex. “2021-05-10_180749290” includes logs from 2021-05-09 18:07:25.321 to 2021-05-10 18:07:49.290 on this example.

4.3.9. Windows setting

Following Windows configuration is required for i-PRO Active Guard server's work to be stable.
Location of configuration may differ depending on OS.

4.3.9.1. Disable Real-time protection and Tamper protection

This is required for i-PRO Active Guard server to keep the basic performance.

In case of Windows 10,
(Start – Settings – System – Update & Security – Windows Security – Virus & threat protection – Virus & threat protection - Virus & threat protection settings – Manage settings)
Off the "Real-time protection" and "Tamper protection".
Windows server OS does not have Tamper protection feature.

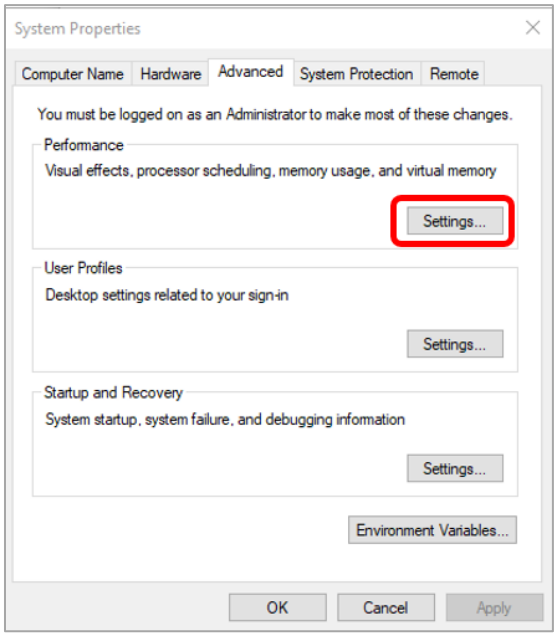
4.3.9.2. Disable Windows Update service

Windows updates are important to keep the system up to date, but auto update may require unplanned restart and some new Windows feature may influence the i-PRO Active Guard server. To avoid unplanned restarts or influences, disable Windows update service.

In case of Windows 10,
Start – Windows Administrative Tools – Services – right click "Windows Update" – Properties – select "Disabled" for "Startup type" and click OK.

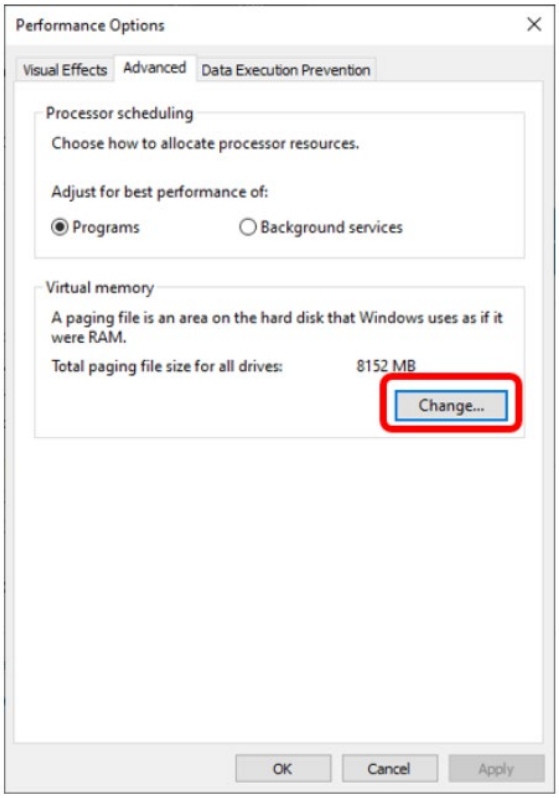
4.3.9.3. Virtual memory setting

If the virtual memory is insufficient, the database may stop.
Follow the procedures below to check the virtual memory setting



In case of Windows 10,
Start – Windows System – Control Panel – System and Security – System – Advanced system setting

Select Settings



Select “Advanced” tab on “Performance Options” screen and click “Change...” button of Virtual memory.

Confirm that “Automatically manage paging file size for all drives” is checked on “Virtual Memory” screen. Check it and click “OK” button.

4.4. Install and setup Plug-in for VI MonitorPlus

Section 4.2.3 should be completed in advance to install Plug-in to VI MonitorPlus.

4.4.1. Install Plug-in to VI MonitorPlus

STEP1

Click the [Modules] tab, then select [Plugins] - [Manage Plugins].

The [Plugin Manager] window will be displayed.

STEP2

Click the [i-PRO Active Guard Plug-in] in the [Plugin Manager] window. Then click the [Install] button.

STEP3

Follow the instructions on the screen to proceed with the installation.

STEP4

When the installation complete window is displayed, click the [Finish] button.

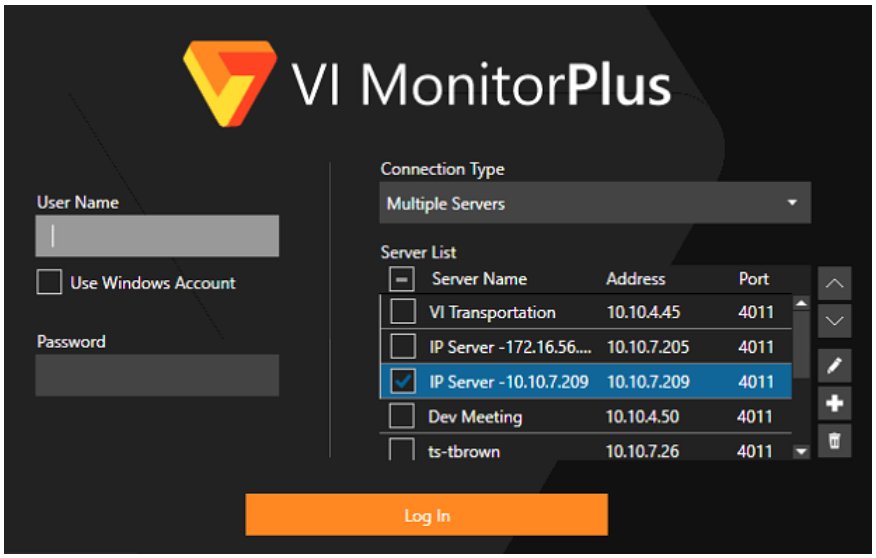
Click the [Yes] button to restart VI MonitorPlus.

STEP5

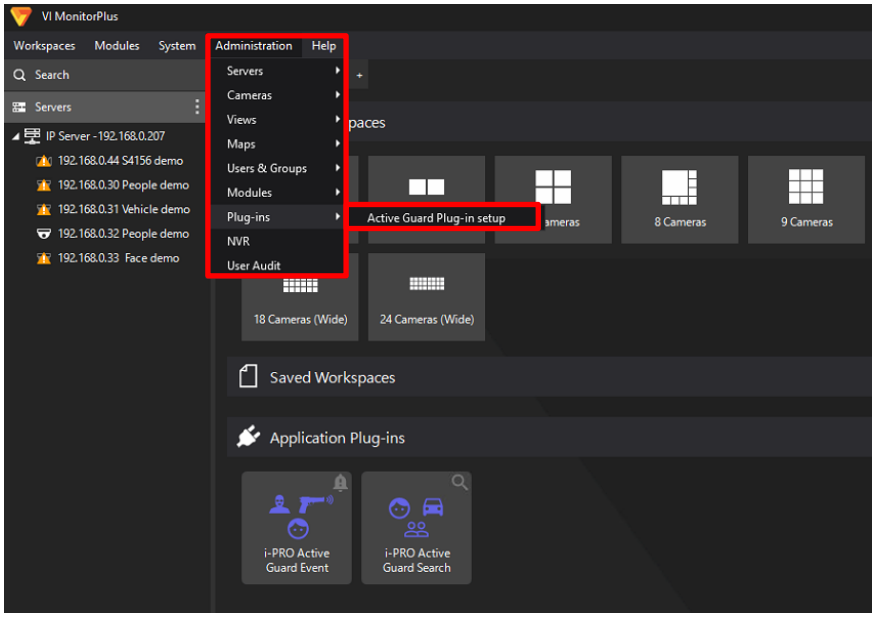
Log in again, and confirm that [i-PRO Active Guard Search] and [i-PRO Active Guard Event] is normally displayed in the [Application Plug-ins] area.

4.4.2. Connection to i-PRO Active Guard server

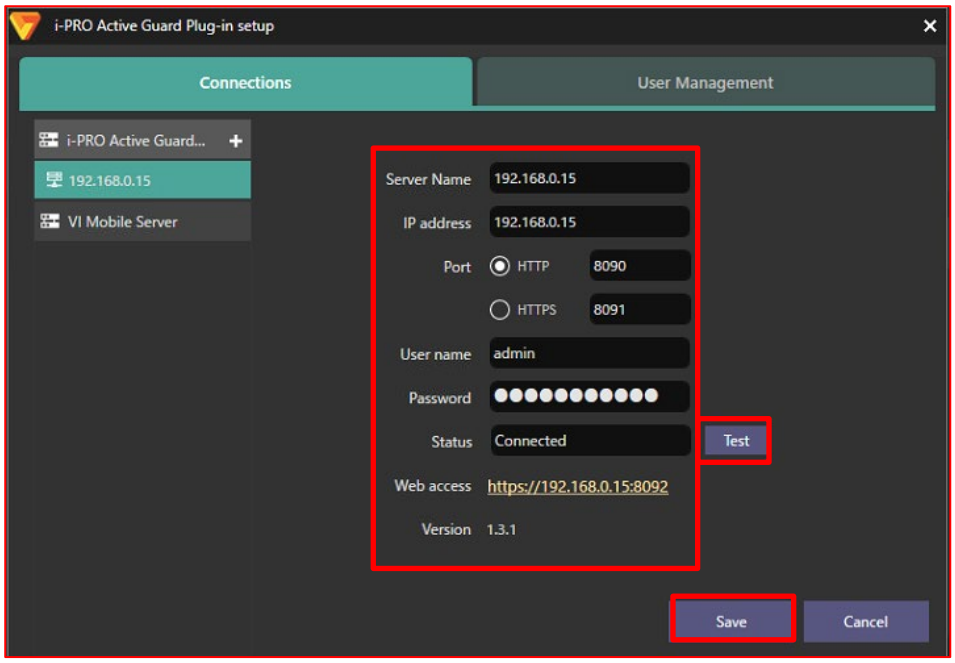
Login to VI VIMonitorPlus as a user who has admin credential.



Then select [Administration] – [Plug-ins] – [Active Guard Plug-in setup]



Input i-PRO Active Guard server information and Click [Test] and then click [Save].

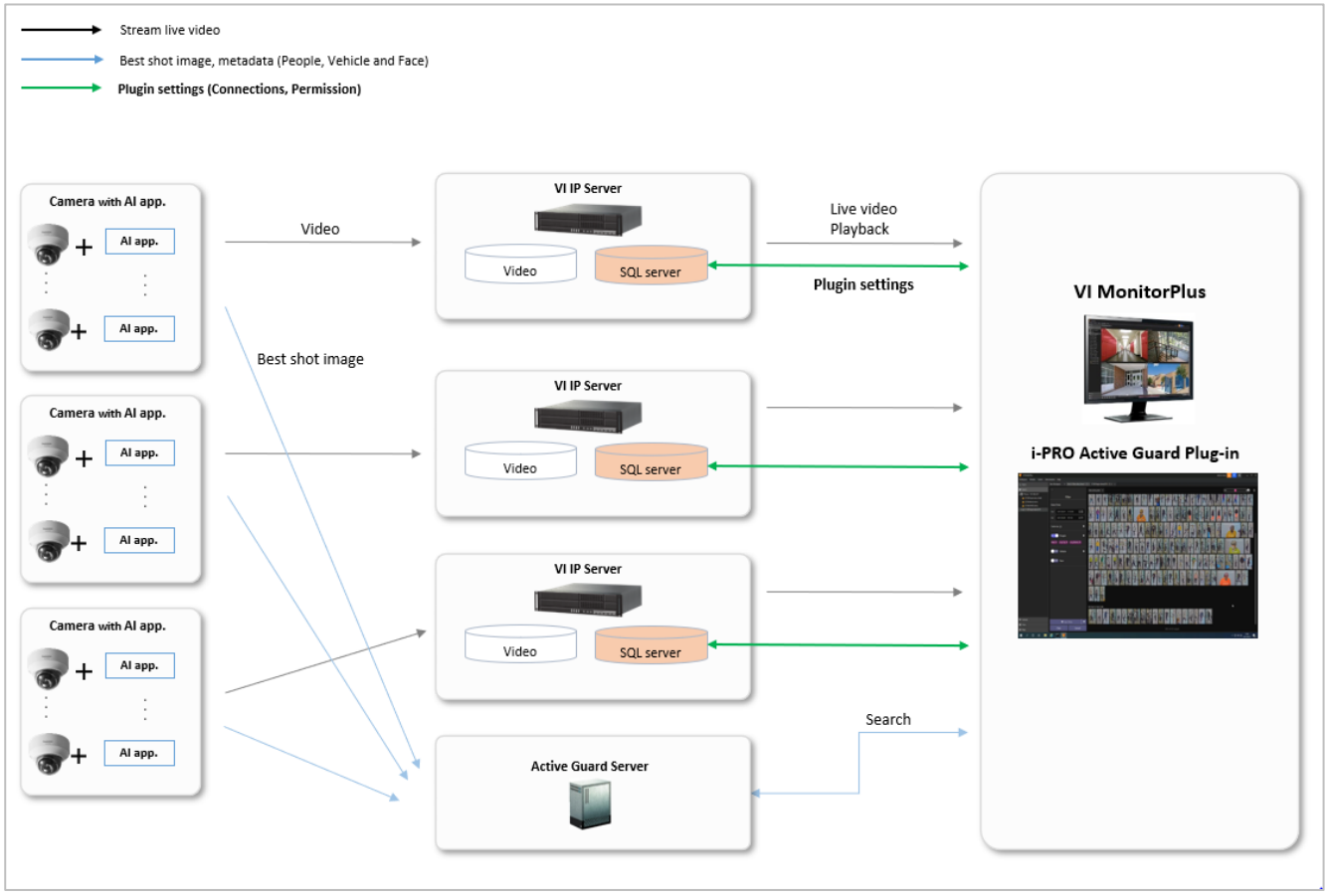


Note)

If Test failed, please check if credential is correct.

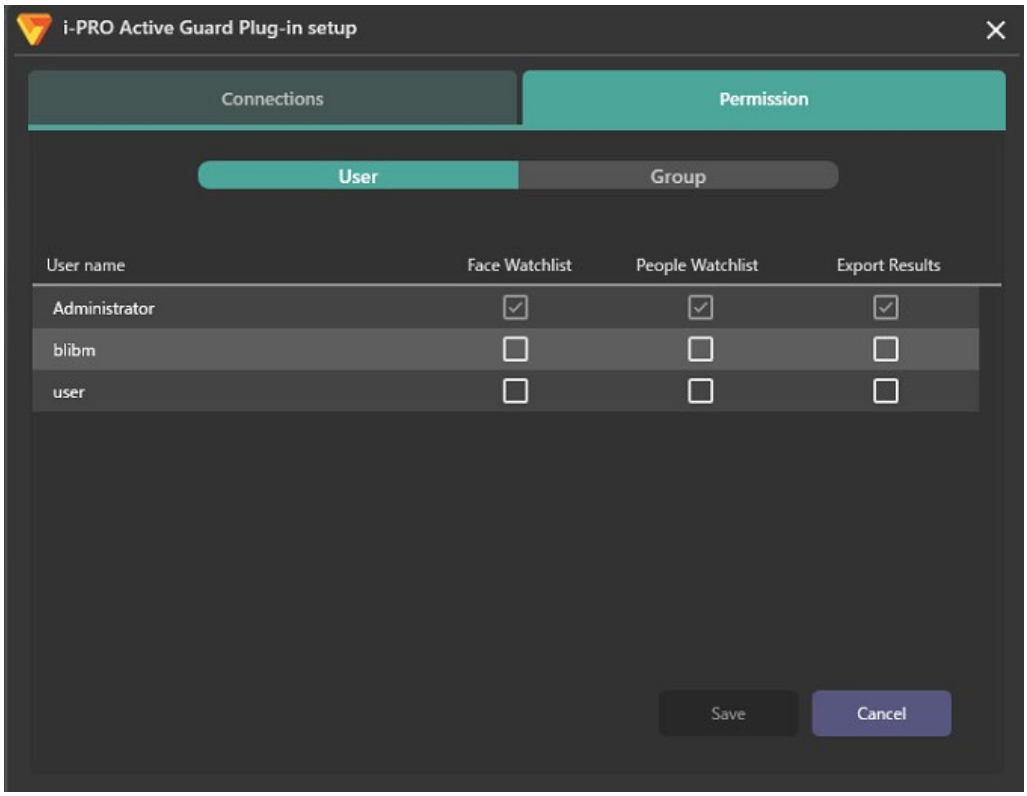
Note)

Connections and User Management settings in Plug-in setup is saved to all SQL databases of VI IP Servers which are connected to VI MonitorPlus.



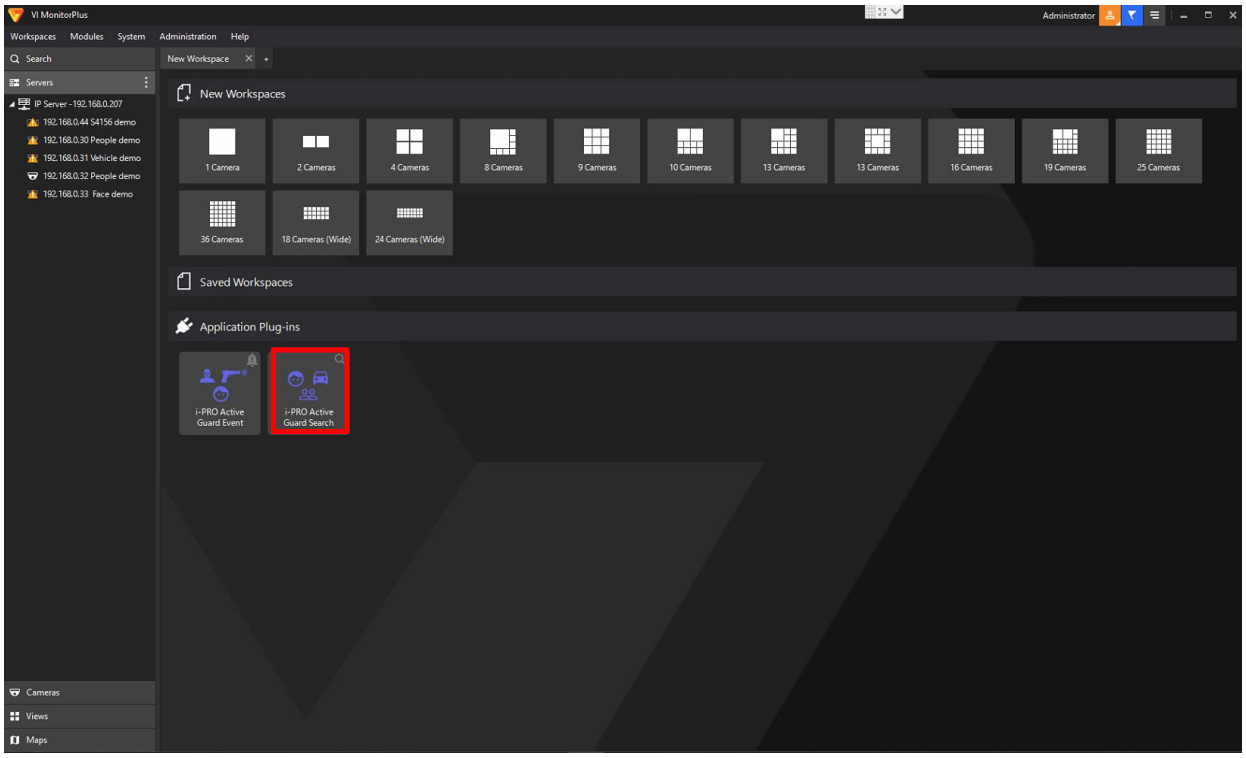
4.4.3. User Management (Optional)

Configure [User Management] for [Face Watch list] and [People Watchlist] access and [Export Results] for each user or group registered in VI IP server.



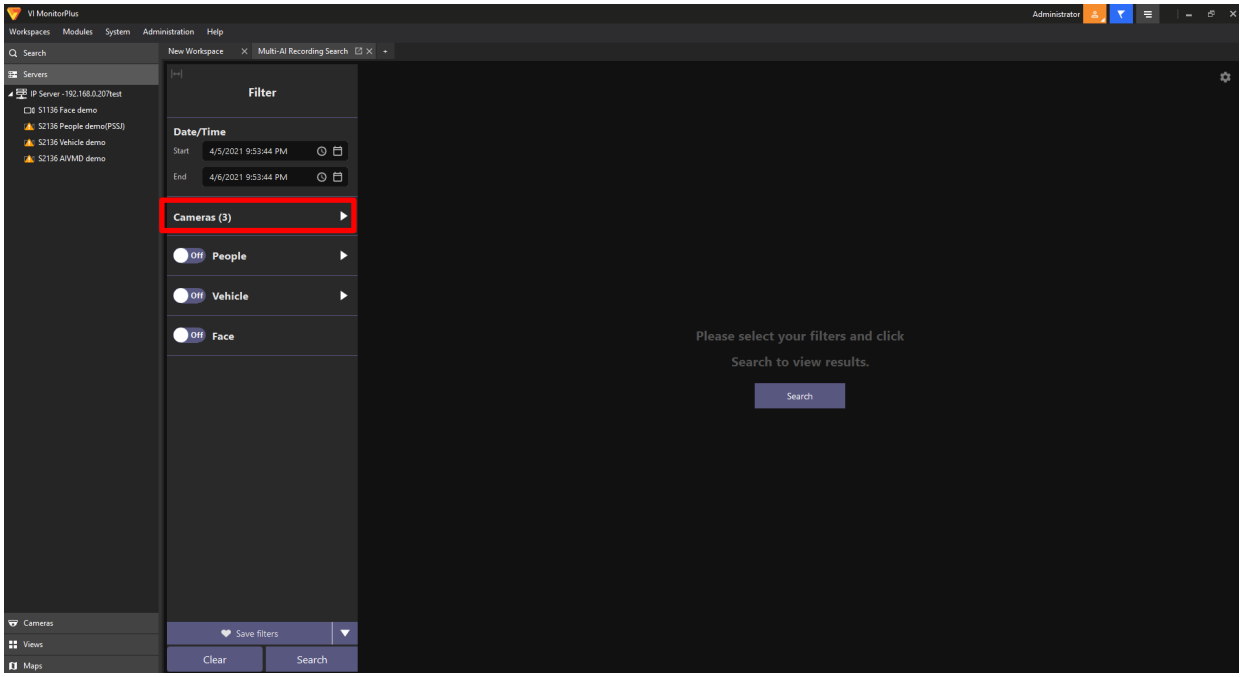
4.4.4. Check

Start [i-PRO Active Guard Search] from New Workspace



When the number is shown for “Cameras (x)”, Connection succeeded.

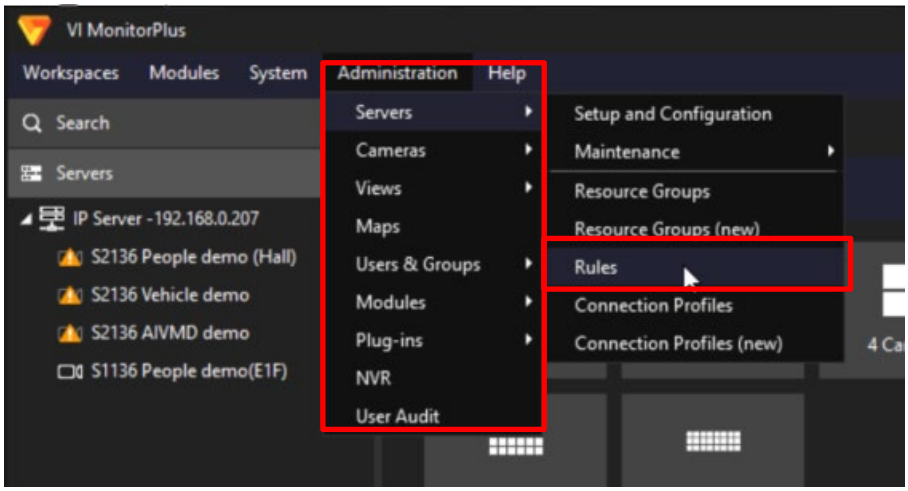
* x means the number of camera that Face, People or Vehicle extension software is installed.



When some camera has detected object, you can search Best shot images by clicking Search.

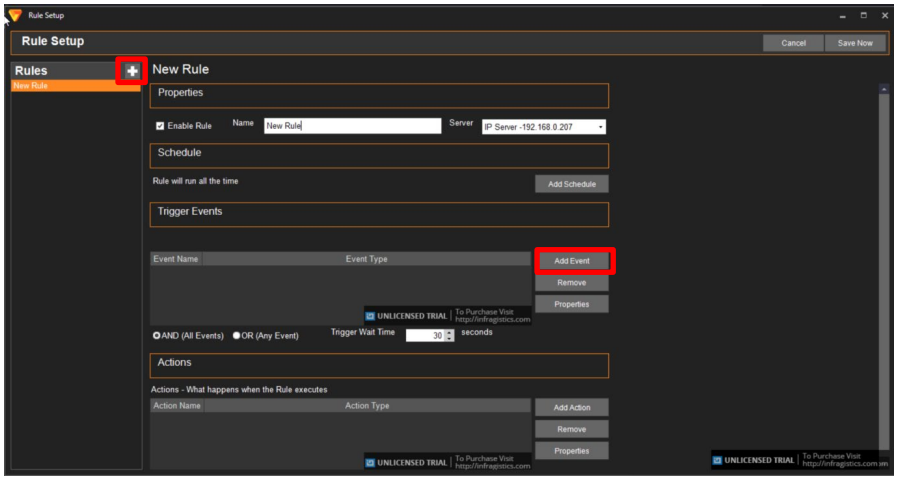
4.5. Rules setup for alarm notification (optional)

Basic alarm function can be used on Plug-in without Rules setup. Rules setup enables more advanced operation. ([Administration] – [Servers] – [Rules])

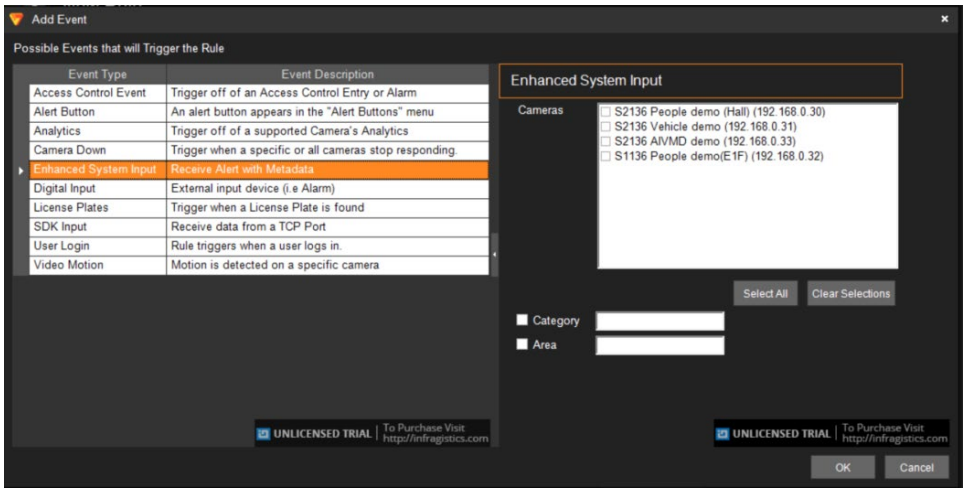


4.5.1. Add event

Create new Rules and click [Add event]

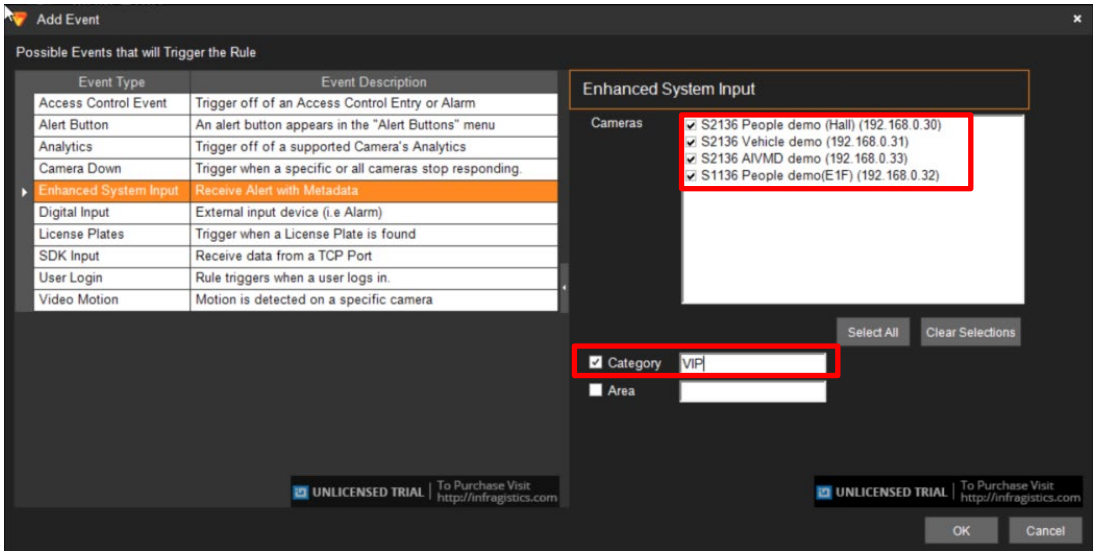


Select [Enhanced System Input]



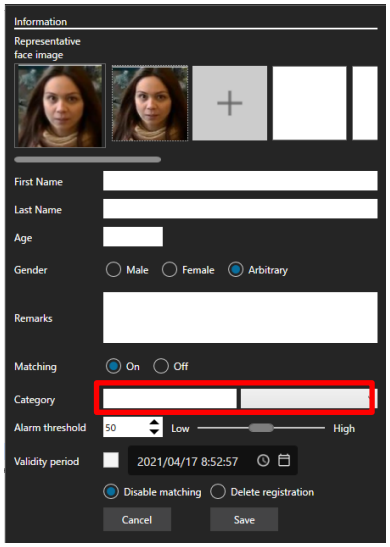
4.5.1.A Registered face detection

To use Registered face detection as Rules, check cameras with AI Face detection, Category (ex. VIP, Student, Employee and so on.) and input category strings registered as face watch list in advance. Actions can be set for specific category.



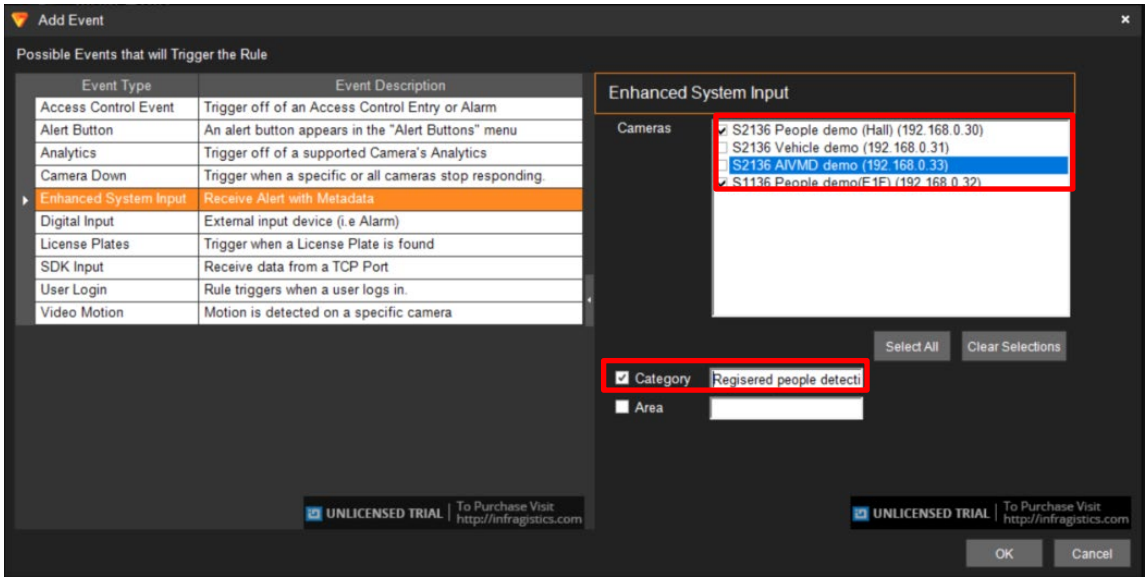
Category can be set from Face registration window. See operation manual in detail.

Area setting is invalid.



4.5.1.B Registered people detection

To use Registered people detection as Rules, check cameras with AI People detection and input “Registered people detection” for Category.

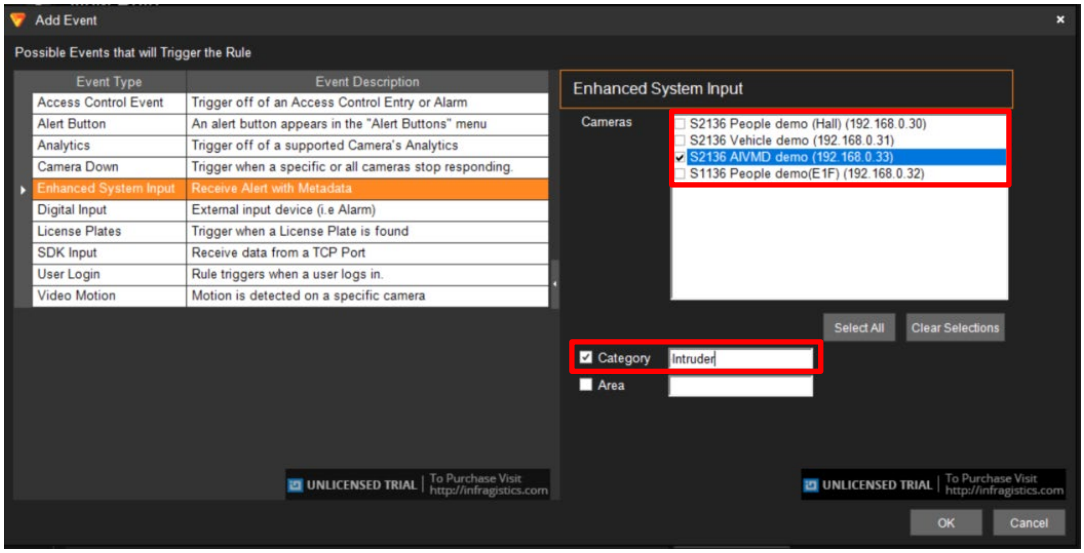


Area setting is invalid.

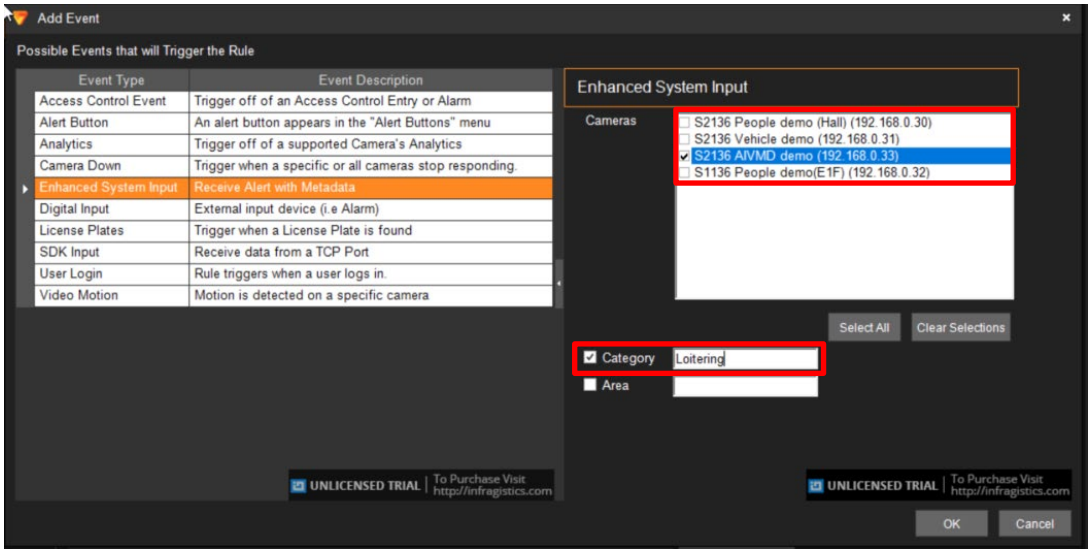
4.5.1.C AI-VMD

To use AI-VMD to trigger the Rule, check cameras with AI-VMD input Category and area as follows. Area means area number 1 to 8 configured by camera side.

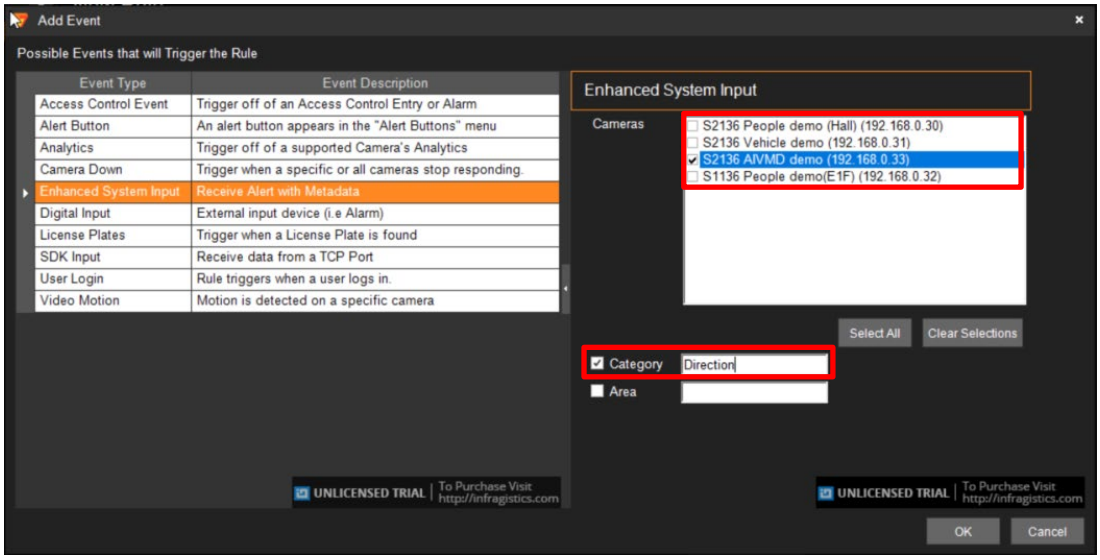
Intruder for all areas



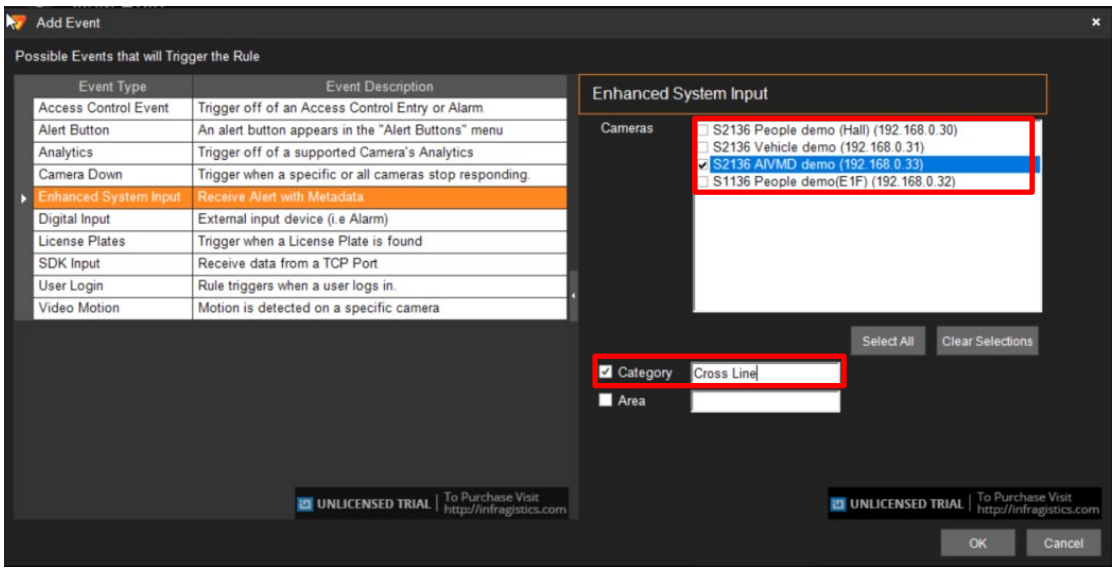
Loitering for all areas



Direction for all areas



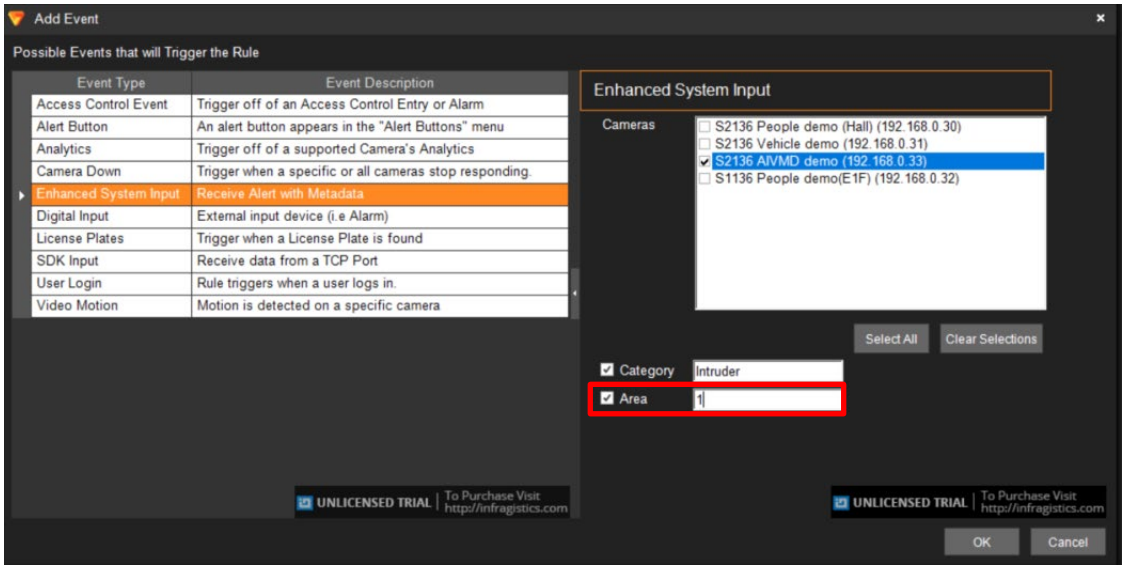
Cross Line for all areas



Area field enables that another actions for each area can be set.

Example of use case using Area field.
Area 1 is an exclusion zone and area 2 is around the area 1.
Popup live window and start recording when someone intrudes into area 2, and e-mail notification when the person intrude into area 1.These can be set by Rules setup using Area field.

Intruder for area 1 (example of using Area field)
Check Area and input area number.

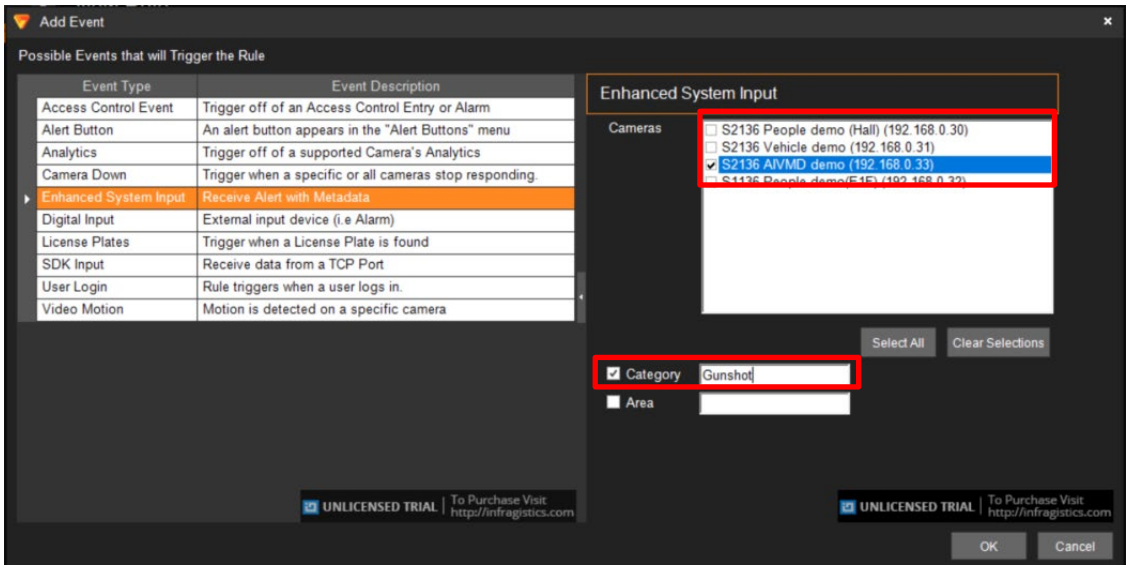


4.5.1.D AI Sound classification

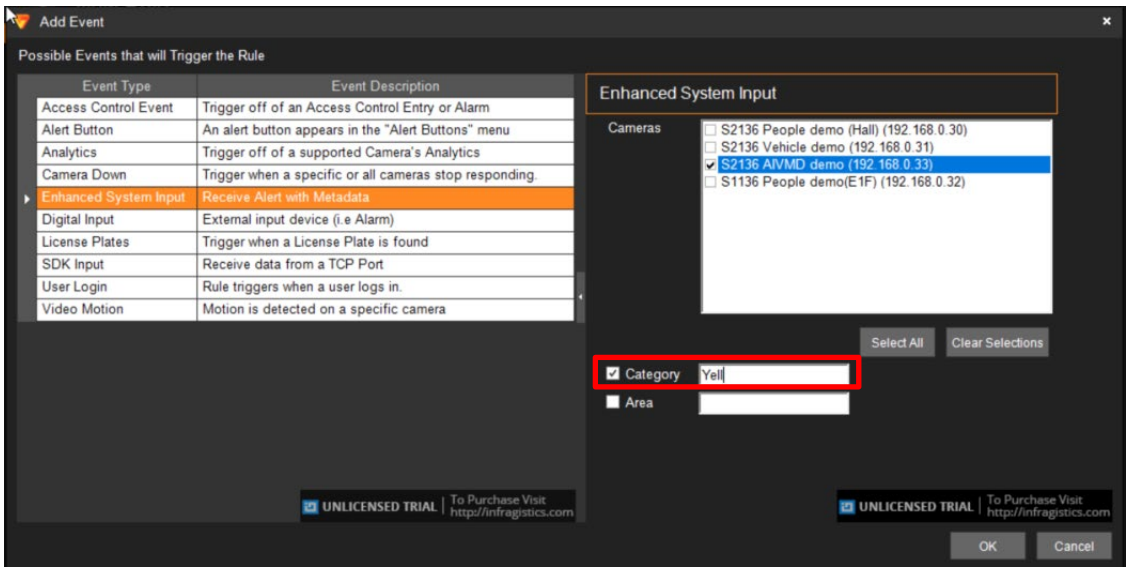
Category for AI Sound classification (Gunshot, Yell, Glass break, Vehicle horn and Audio detection) can be distinguished and Actions can be set for specific category.

Check cameras with AI Sound classification, Category and input category strings.
Area setting has no relation.

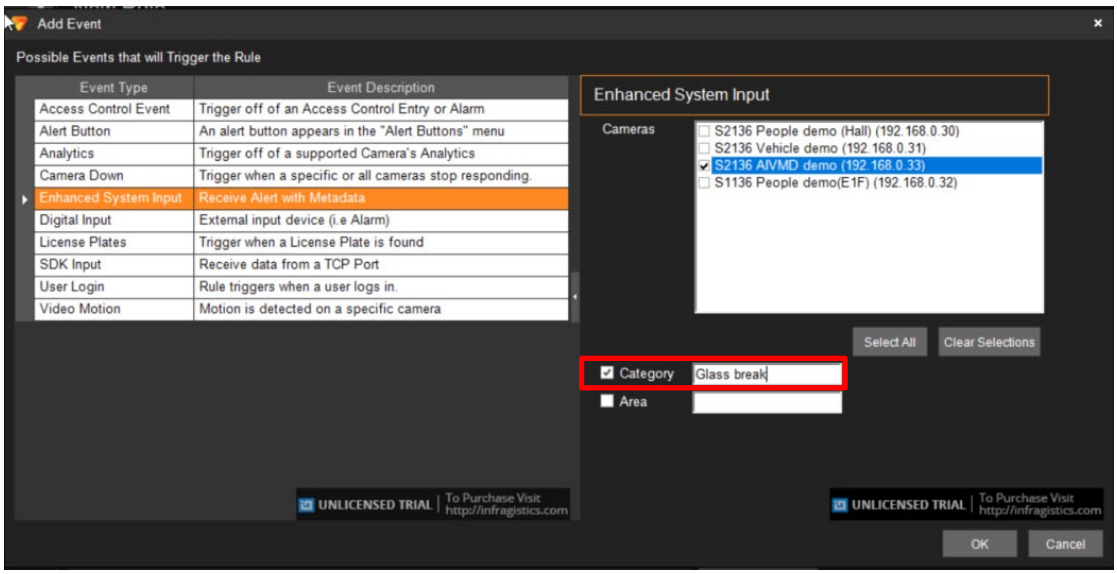
Gunshot



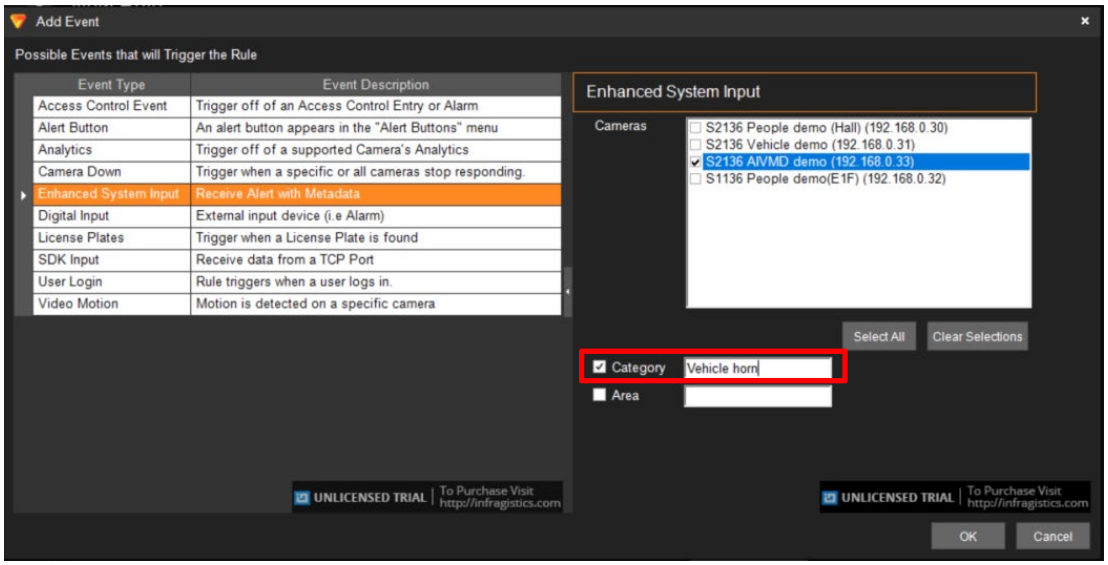
Yell



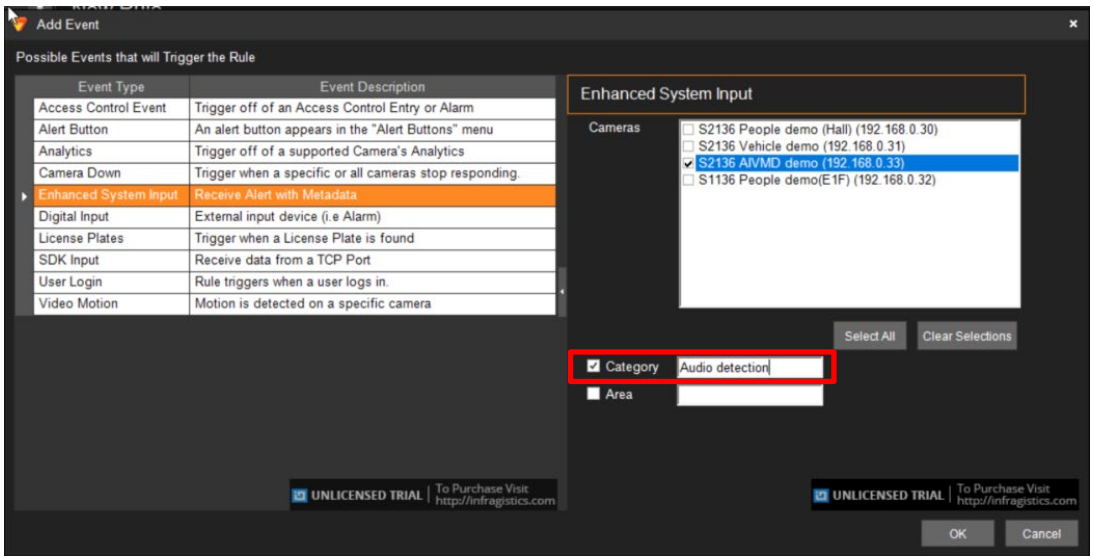
Glass break



Vehicle horn



Audio detection

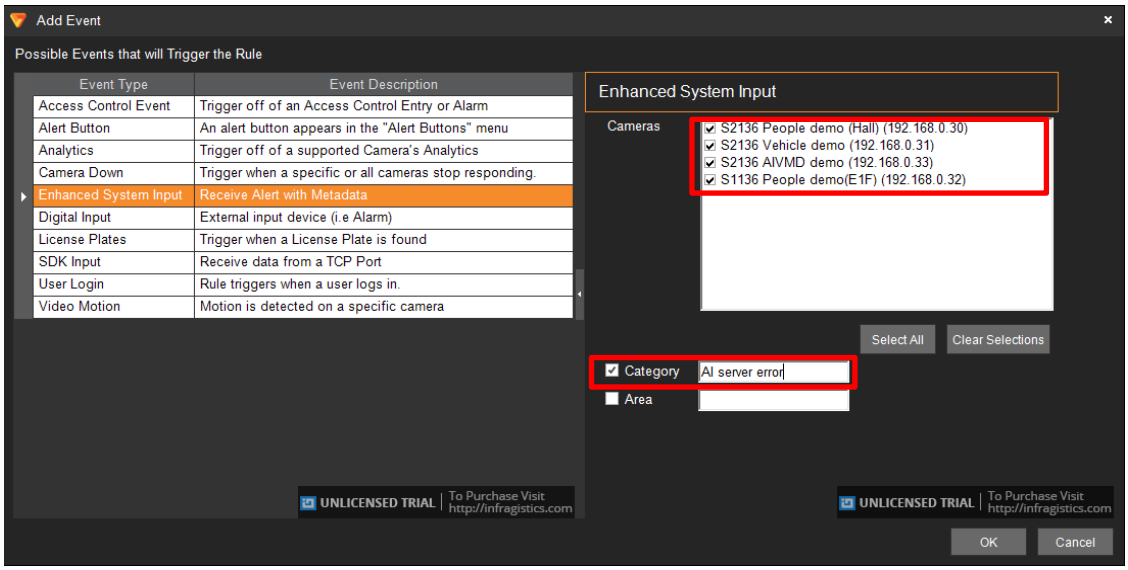


4.5.1.E System alarm of i-PRO Active Guard server

Some alarms related to i-PRO Active Guard server failure can be enabled.

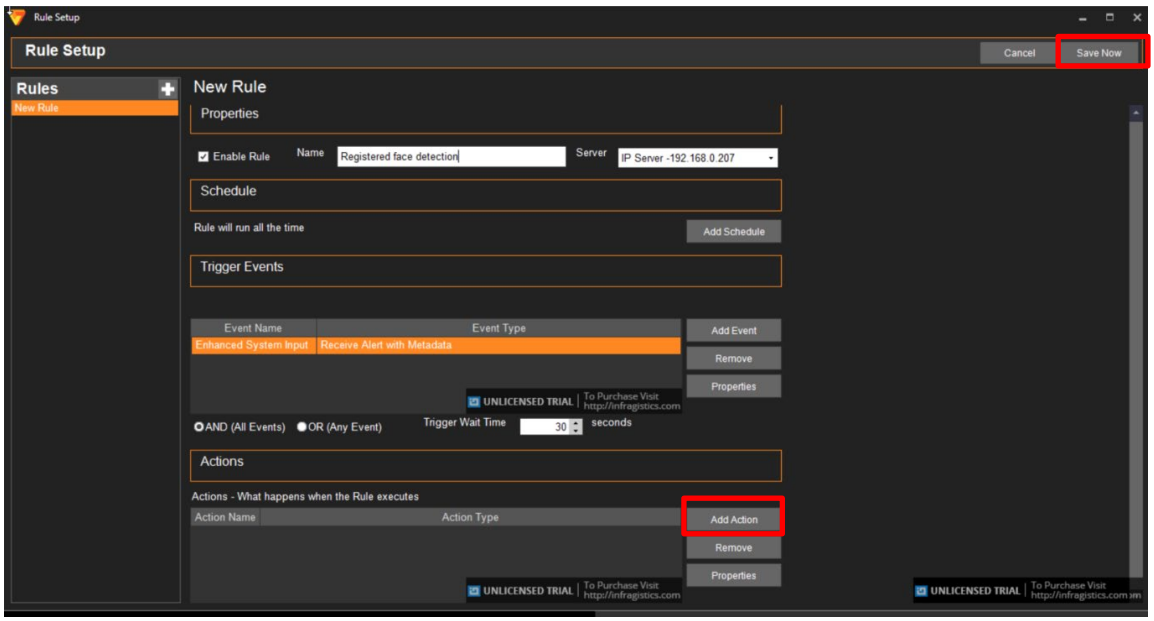
Configuration on i-PRO Active Guard server side is required in advance (Refer to 4.3.6)

Check for all cameras and input “AI server error” for Category.



4.5.2. Add Actions

Click [Add Action] and select any actions, and then [Save Now]

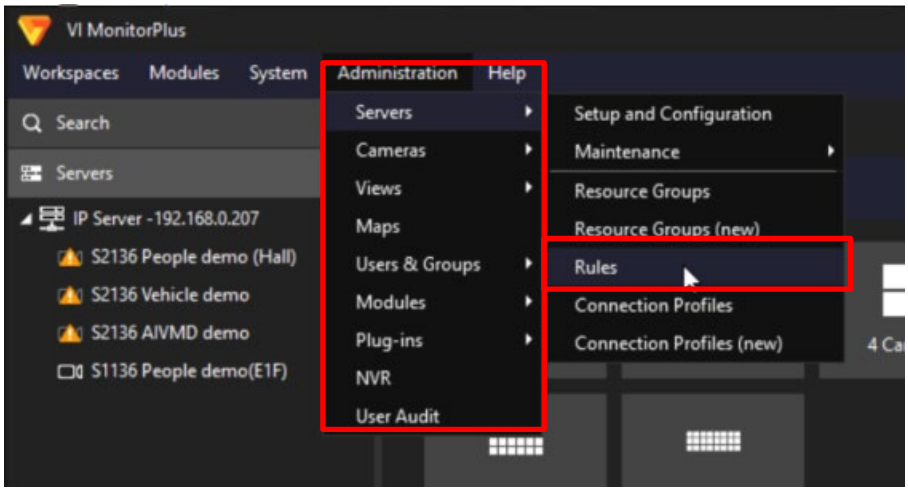


4.6. Setup for LPR monitoring function (optional)

License Plate Recognition (LPR) is available in Plug-in if Video Insight LPR is integrated into the IP Server. LPR Plugin must be configured in VI MonitorPlus (See *VI LPR Administrative Guide*). Once camera is setup with the LPR Plug-in, the camera is ready for use with Plug-in.

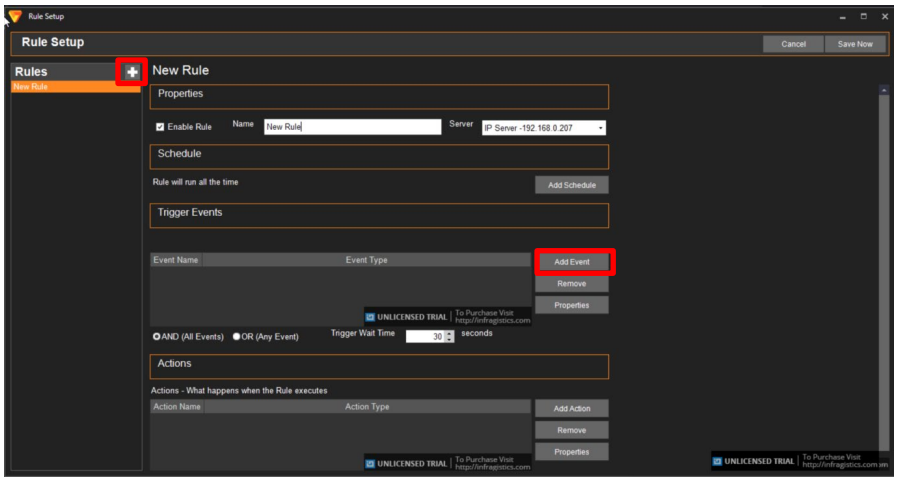
4.7. Setup for VCA monitoring function (optional)

Video Control Analytics (VCA) is available in Plug-in if a camera is equipped with Analytic functionality. This feature must be enabled in the individual camera's properties (See *Video Insight Administrative Guide*). Navigate to ([Administration] – [Servers] – [Rules])

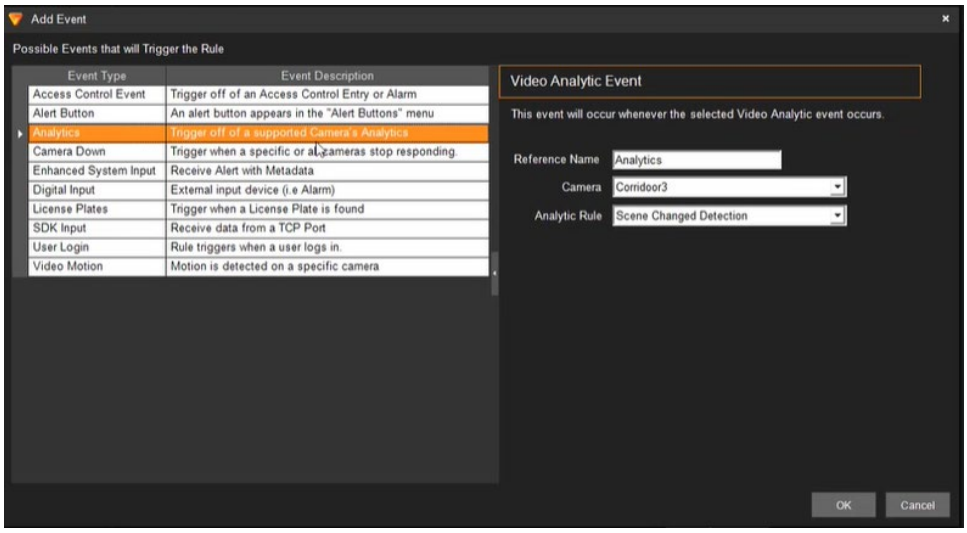


4.7.1. Add event

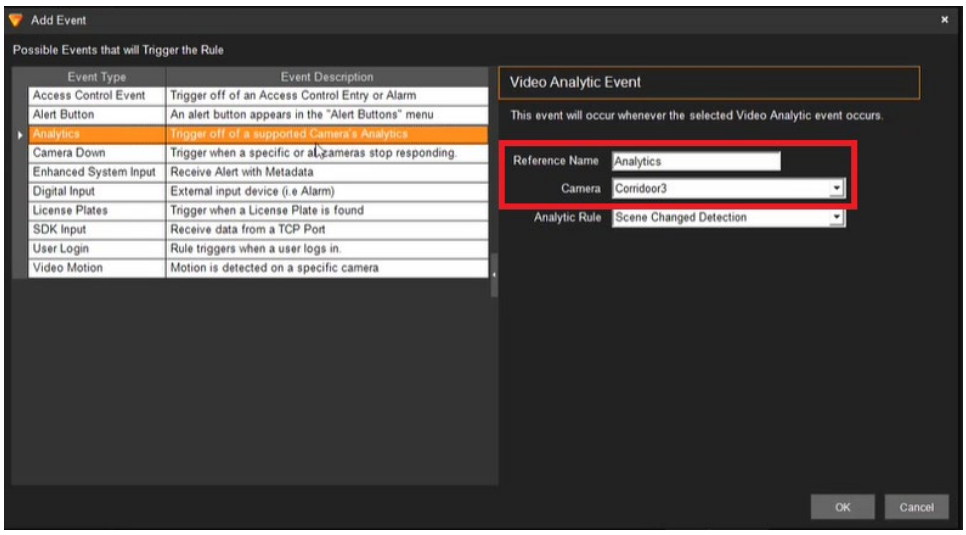
Create new Rules and click [Add event]



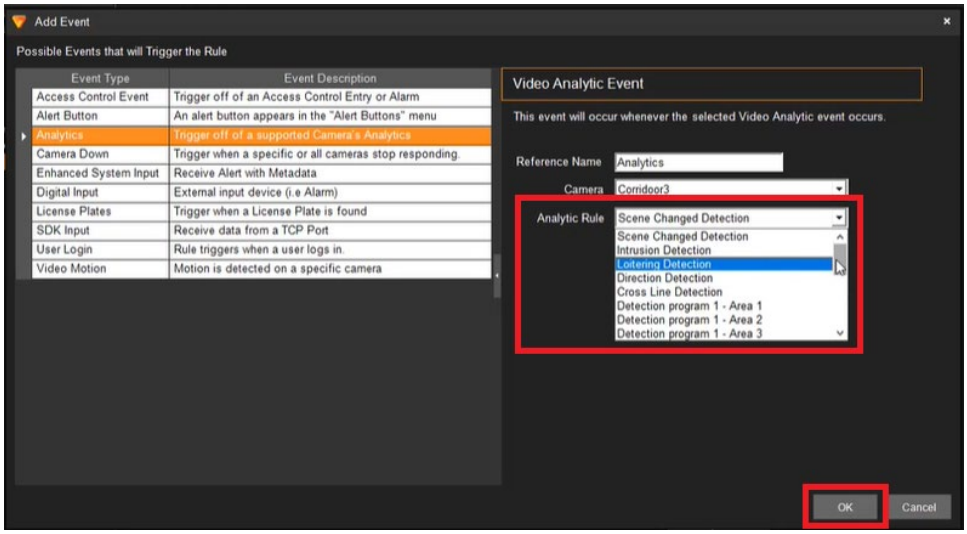
Select [Analytics]



Enter a [Reference Name], then select a [Camera] (camera must be enabled with analytics).

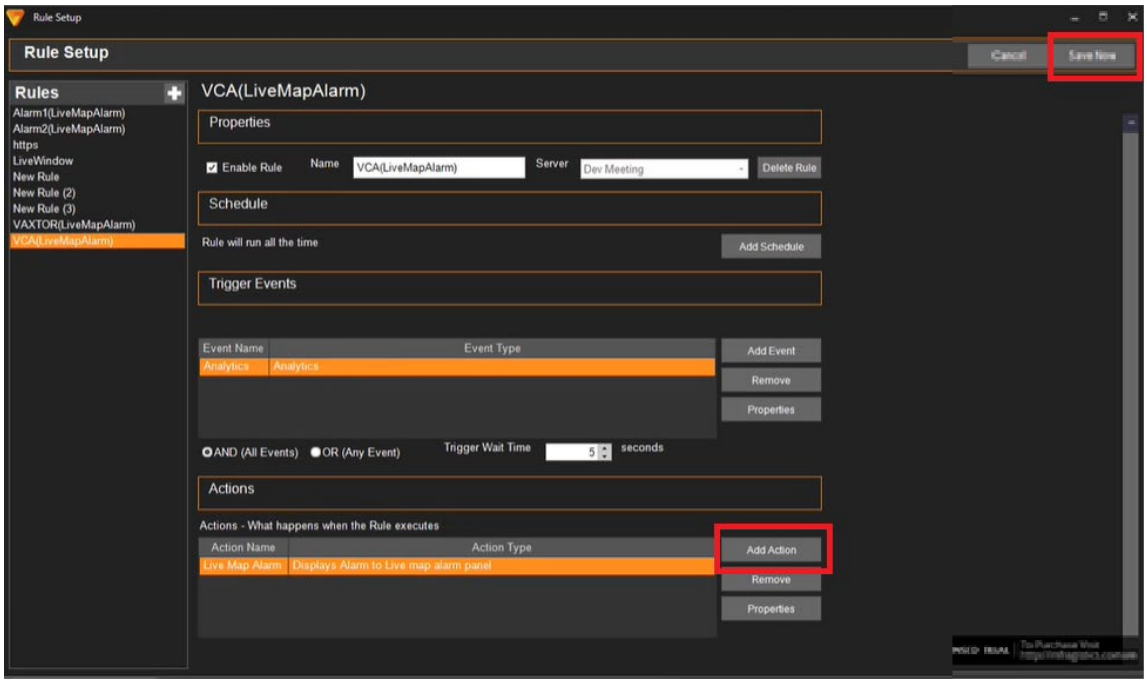


Select an [Analytic Rule] (available rules vary according to the functionality of each individual camera) and click OK.



4.7.2. Add Actions

Click [Add Action] and select [Live Map Alarm], and then [Save Now]



4.8. Setup for Access Control monitoring function (optional)

Access Control monitoring is available in Plug-in if IP Server is integrated with an Access Control server. Access Control must be configured in VI MonitorPlus (See *Video Insight Administrative Guide, section 4.8.A*). It is required to assign cameras to specific doors.

5. When changing system component

5.1. Add system device

5.1.1. Add camera

STEP1

Register AI cameras to VI IP server using VI MonitorPlus (Refer to 4.2.1).

STEP2

Register AI cameras to i-PRO Active Guard server (Refer to 4.3.2.3)

STEP3

Restart process (Refer to 4.3.3)

5.1.2. Add IP server

STEP1

Register AI cameras to new VI IP server using VI MonitorPlus. (Refer to 4.2.1).

STEP2

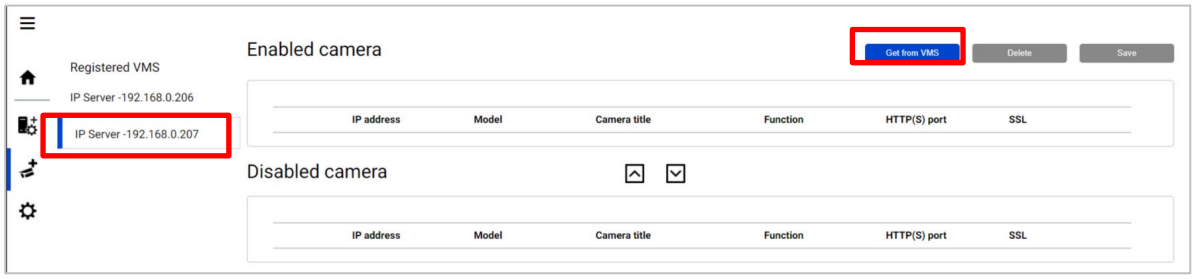
Register new VI IP server to i-PRO Active Guard server (Refer to 4.3.2.2)

STEP3

Register AI cameras associated with new VI IP server to i-PRO Active Guard server.

Select new VI IP server and click [Get from VMS].

Following procedure is the same as 4.3.2.3



STEP4

Restart process (Refer to 4.3.3)

5.2. Delete system device

5.2.1. Delete camera

STEP1

Check camera and [Delete] from Register Cameras screen.

Existing data of the selected camera will be unavailable.

STEP2

Restart process (Refer to 4.3.3)

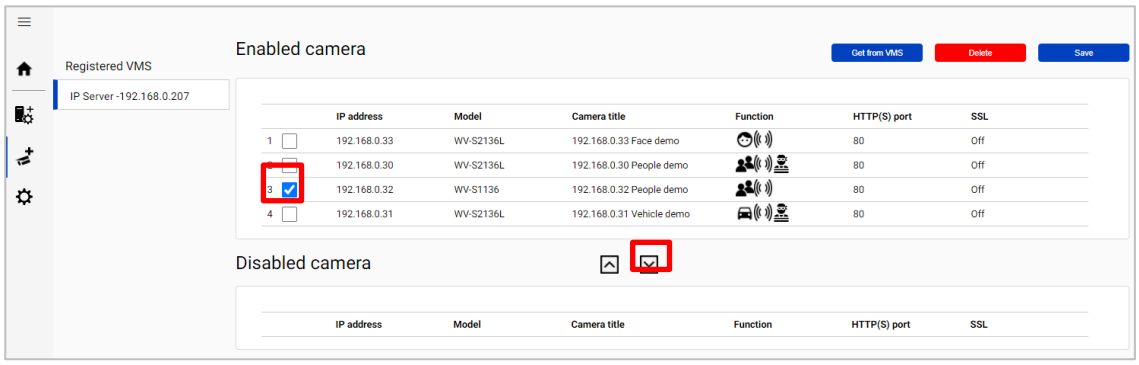
5.2.2. Disable camera

When you want disable specific cameras temporarily, which means there is a possibility you want to search existing data of the camera later, configure the camera as Disabled camera.

STEP1

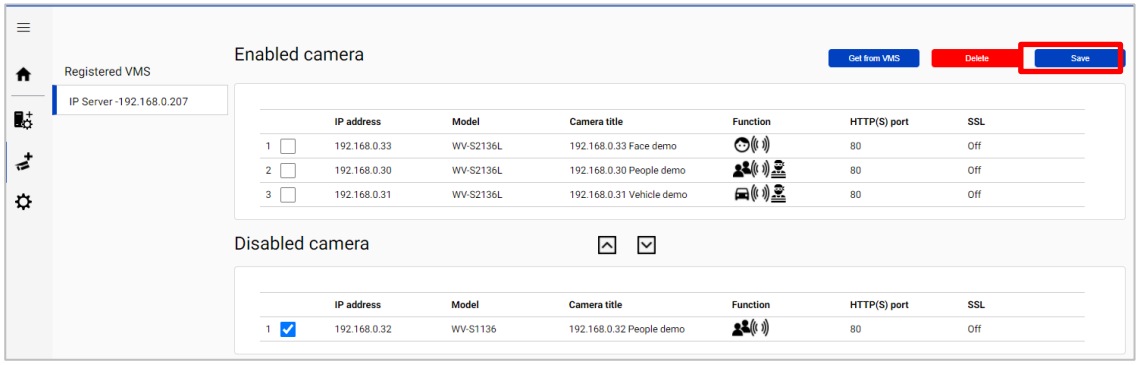
Check camera and move to Disabled camera from Register Cameras screen.

Existing data of the selected camera will be unavailable as long as the camera is disabled camera.



STEP2

[Save]



STEP3

Restart process (Refer to 4.3.3)

When you want to use the camera and existing data of the camera again, move to Enabled camera and [Save].

Existing data of the camera will be available as long as retention period is not exceeded from plugin.

5.2.3. Delete IP server

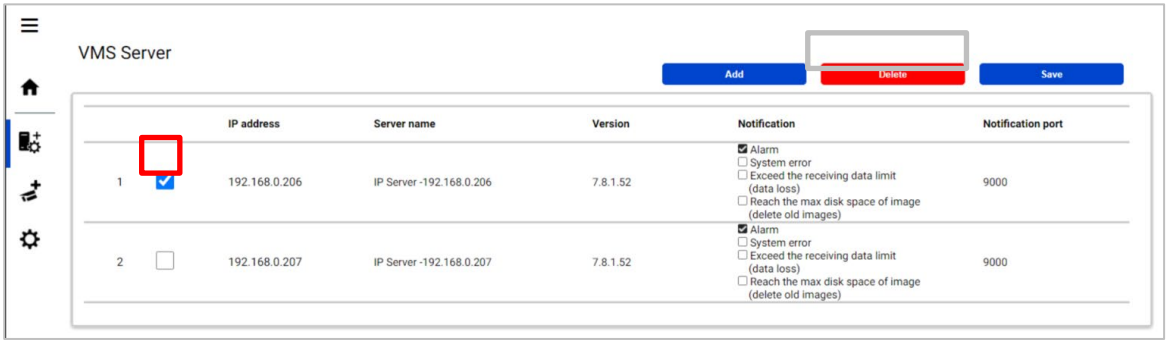
STEP1

Check server and [Delete] from Register VMS screen.

Cameras belonged to the selected server are also deleted and exiting data will not be searched from plugin.

When the same VMS server are registered again, existing data becomes available.

Best shot images and related database will be delete when retention period exceed.



STEP2

Restart process (Refer to 4.3.3)

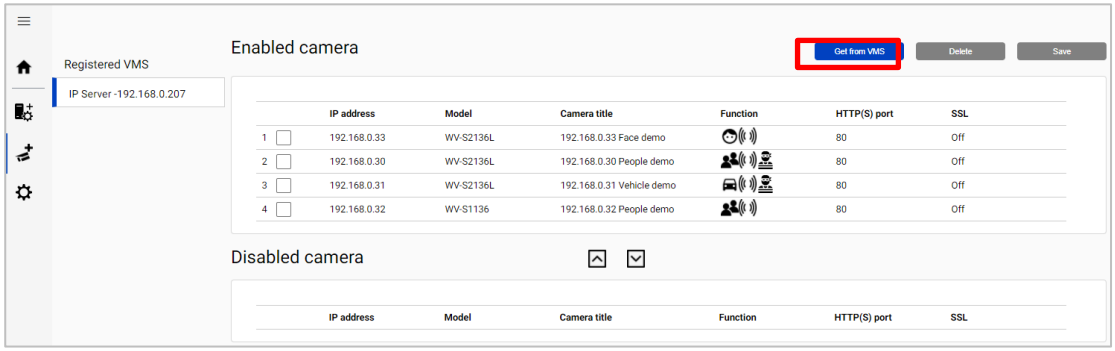
5.3. Add or Change camera's extension software

STEP1

Install or change extension software using iCT. (Refer to 4.1)

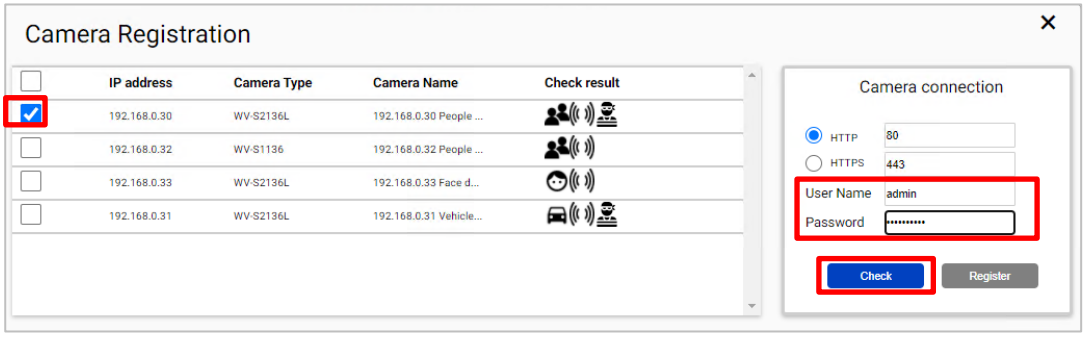
STEP2

Click [Get from VMS] on Register Cameras screen.



STEP3

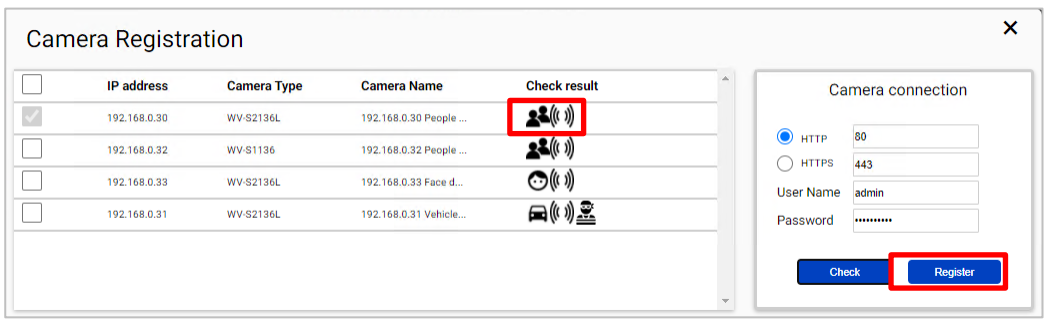
Select the camera and input credentials and [Check].



STEP4

Confirm the icons for Check result is changed and [Register].

In this example, AI-VMD is uninstalled (see 4.3.2.3 about the meaning of icons).



STEP5

Restart process (Refer to 4.3.3)

5.4. Uninstall the system

5.4.1. Uninstall Plug-in from client PC

STEP1

Open the Programs and Features window (from the Control Panel).

STEP2

Find [Multi AI Plugins] and [Uninstall].

Note)

Do not use the [Remove] button on Plugin Manager window.

5.4.2. Uninstall i-PRO Active Guard server

STEP1

Open the Programs and Features window (from the Control Panel).

STEP2

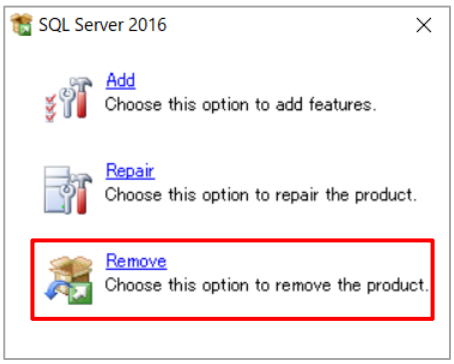
Find [Multi AI Plugins – Server] and [Uninstall].

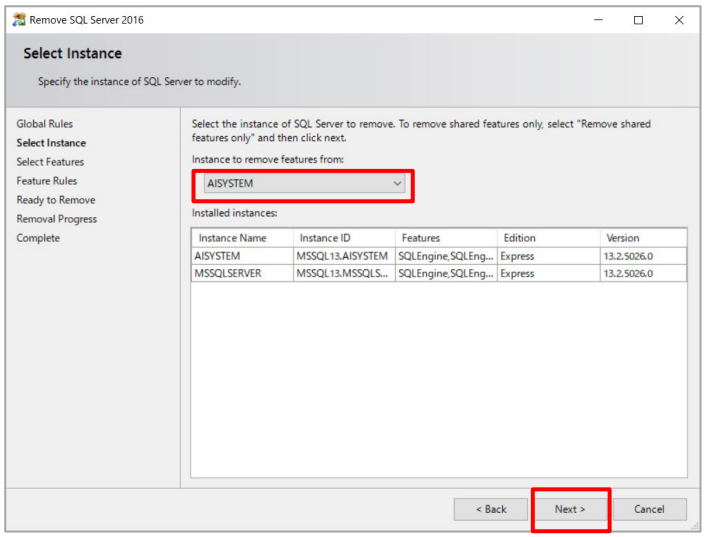
Delete “C:¥MultiAI” folder if exist.

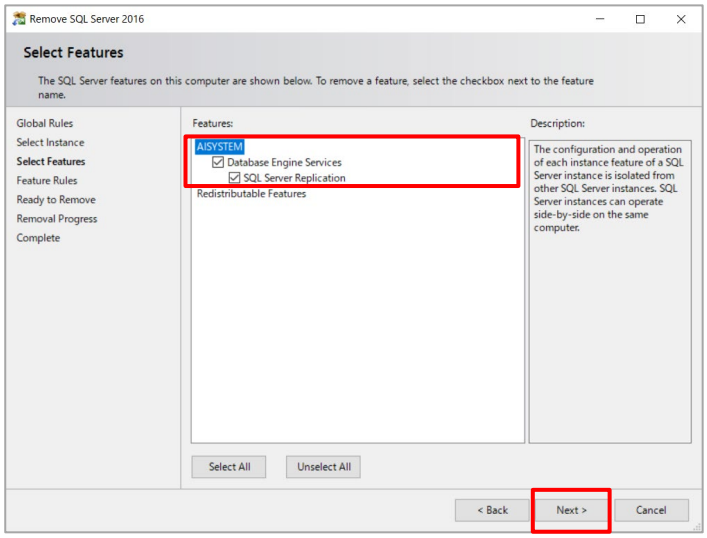
STEP3

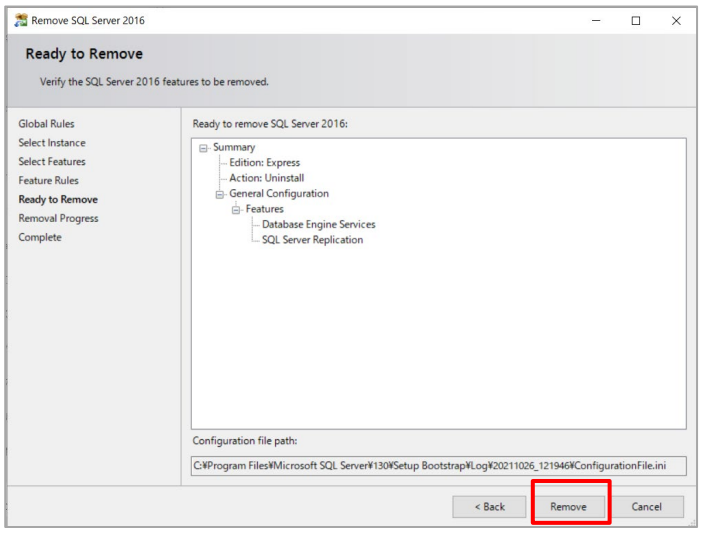
Find [Microsoft SQL Server 2016 (64 bit)] and [Uninstall].

Select [Remove] and delete “AISYSTEM” instance.









Note) SQL server instance that VMS uses is not deleted. Only instance for i-PRO Active Guard server is deleted.

STEP4

Delete “C:¥Program Files¥Microsoft SQL Server¥MSSQL13.AYSYSTEM” folder.

5.5. Change IP address

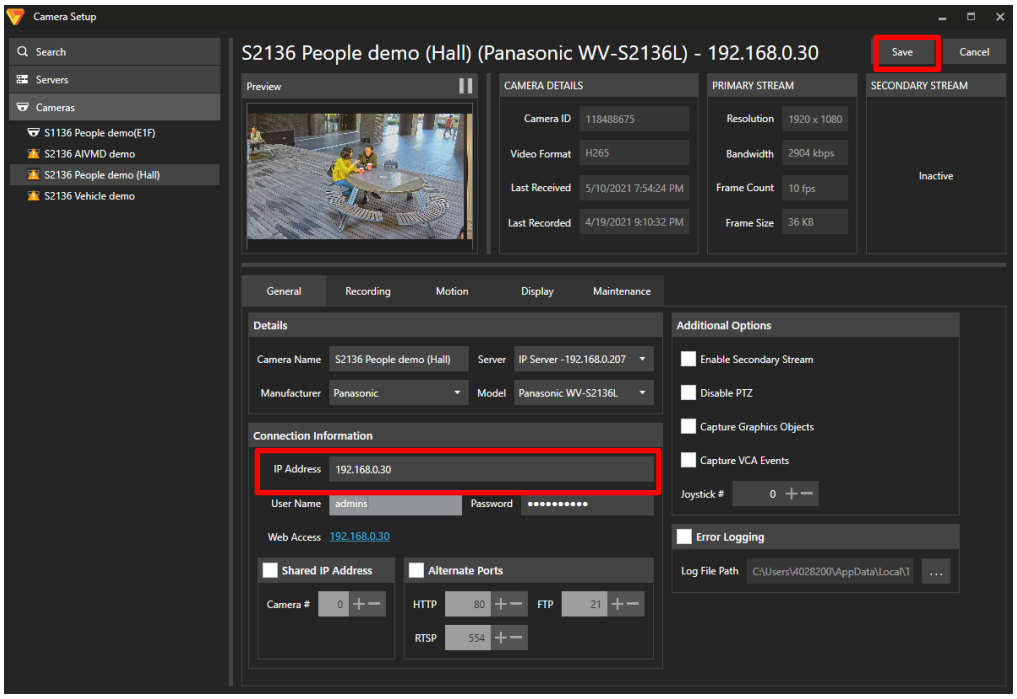
5.5.1. Change camera’s IP address

STEP1

Change camera’s IP address

STEP2

When you want to maintain existing recorded data and Best shot images of the camera, update [IP Address] and [Save] from VI MonitorPlus ([Administration] – [Cameras] – [Configure Properties])



Once deleting cameras from VI Monitor Plus and re-register the camera using new IP address, existing data will be unavailable.

STEP3

Delete the camera from i-PRO Active Guard server (Refer to 5.2.1)

STEP4

Register the camera again (Refer to 4.3.2.3).

STEP5

Restart process (Refer to 4.3.3).

5.5.2. Change IP server’s IP address

Existing recorded data and Best shot images are available after changing IP address.

STEP1

Change IP server’s IP address.

STEP2

Delete the IP server from i-PRO Active Guard server (Refer to 5.2.3)

STEP3

Register the IP server again (Refer to 4.3.2.2).

STEP4

Restart process (Refer to 4.3.3).

5.5.3. Change i-PRO Active Guard server’s IP address

Existing recorded data and Best shot images are available after changing IP address.

STEP1

Change i-PRO Active Guard server’s IP address.

STEP2

Update configuration for Connection to i-PRO Active Guard server from Plug-in (4.4.2).

5.6. Data backup and restore

Image data and related database can be backed-up manually. It is important to note that the reinstallation of i-PRO Active Guard server requires the same version of software for reinstallation from backup due to differences in each database version.

5.6.1. Backup process

STEP1

Start – Windows Administrative Tools – Task Scheduler. Right click and disable “AliveMonitoringProcess”

STEP2

Start – Windows Administrative Tools – Services.
Right click and stop for “MultiAICameraService”, “MultiAISupportProcessManagementService” and “SQL Server(AISYSTEM)”, respectively.

STEP3

Browse to “C:¥Program Files¥Microsoft SQL Server¥MSSQL13.AISYSTEM¥MSSQL¥DATA”.
Copy “ai_db.mdf”, “aicam.mdf”, “support_db.mdf”, ai_db_log.ldf”, “aicam_log.ldf”, “support_db_log.ldf”, “bi.mdf” and “bi_log.ldf” to safe location (i.e.: a USB drive, a NAS device, another server, etc.).

STEP4

Copy “C:¥MultiAI¥Image” folder to safe location.If you changed image data save path, copy the folder.
Copy “C:¥MultiAI¥Backup¥WebConfig” folder to safe location.

STEP5

Type “regedit” to Start menu and run. Right click two folder and export to safe location, respectively.
“¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Panasonic¥AiSystem”.
“¥HKEY_LOCAL_MACHINE¥SOFTWARE¥WOW6432Node¥Panasonic¥AiSystem”.

STEP6

Start – Windows Administrative Tools – Services.
Right click and run for “MultiAICameraService”, “MultiAISupportProcessManagementService” and “SQL Server(AISYSTEM)”, respectively.

STEP7

Start – Windows Administrative Tools – Task Scheduler. Right click and enable “AliveMonitoringProcess”

5.6.2. Restore process

STEP1

Start – Windows Administrative Tools – Task Scheduler. Right click and disable “AliveMonitoringProcess”

STEP2

Start – Windows Administrative Tools – Services.

Right click and stop for “MultiAICameraService”, “MultiAISupportProcessManagementService” and “SQL Server(AISYSTEM)”, respectively.

STEP3

Copy saved files “ai_db.mdf”, “aicam.mdf”, “support_db.mdf”, ai_db_log.ldf”, “aicam_log.ldf”, “support_db_log.ldf”, “bi.mdf” and “bi_log.ldf” to “C:¥Program Files¥Microsoft SQL Server¥MSSQL13.AISYSTEM¥MSSQL¥DATA” and replace existing files.

STEP4

Copy saved folder “Image” to “C:¥MultiAI” and replace existing files.

Copy saved folder “WebConfig” to “C:¥MultiAI¥Backup” and replace existing files.

STEP5

Double-click the saved registry export file. This will re-install the registry keys.

STEP6

Start – Windows Administrative Tools – Services.

Right click and run for “SQL Server(AISYSTEM)”.

STEP7

Execute “C:¥MultiAI¥tools¥restore_user¥restore_user.bat” as administrator.

STEP8

Right click and run for “MultiAICameraService”, “MultiAISupportProcessManagementService”, respectively.

STEP9

Start – Windows Administrative Tools – Task Scheduler. Right click and enable “AliveMonitoringProcess”.

5.7. Procedure to move i-PRO Active Guard server location from IP Server’s PC to dedicated server’s PC

i-PRO Active Guard server location can be moved from VI IP server’s PC to dedicated server’s PC, for example, when the number of cameras are increased or when distributing processing load is required.

5.7.1. Preparation of data and account information

STEP1

Prepare administrator account information of existing i-PRO Active Guard server when install.
If you forget administrator account, reset it (Refer to 5.9).

STEP2

Backup data (Refer to 5.6.1)

5.7.2. Install i-PRO Active Guard server to new PC and restore data

STEP1

Install i-PRO Active Guard server to new PC as dedicated server PC (Refer to 4.3.1).

Note) Account information you set when installing will be overwritten in restore process (Refer to step 2).

STEP2

Restore data (Refer to 5.6.2)

STEP3

Execute “C:¥MultiAI¥tools¥init_dedicated_server.bat” as administrator.

STEP4

Start – Windows Administrative Tools – Services.
Right click and Restart for “MultiAICameraService”, “MultiAISupportProcessManagementService”.

5.8. Procedure to restart/shut down i-PRO Active Guard server PC

As a safety precaution, it is recommended to stop the services before rebooting the computer.

STEP1

Stop i-PRO Active Guard server’s process (4.3.7.2).

STEP2

Restart or shutdown.

5.9. Reset administrator account

When you forget credential of administrator to access configuration, you need to reset on PC that i-PRO Active Guard server is installed.

Execute “C:¥MultiAI¥tools¥ChangeAdminPassword¥ChangeAdminPassword.exe” as administrator and set credentials.

5.10. Upgrade SQL server to Standard Edition

You can determine if you need Standard Edition from 3.3.

If you need it, please follow the steps below to upgrade after purchasing the license.

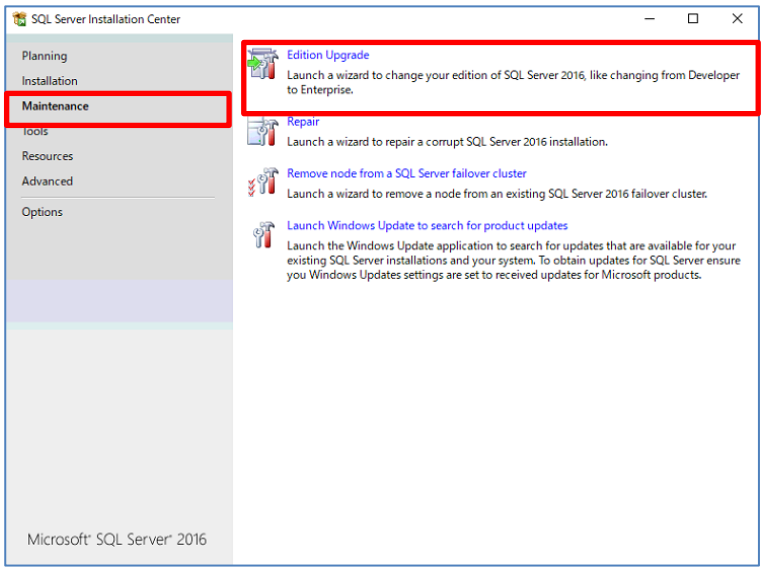
i-PRO Active Guard server software need to be installed in advance.

STEP1

Start [setup.exe] from install media of SQL server Standard Edition.

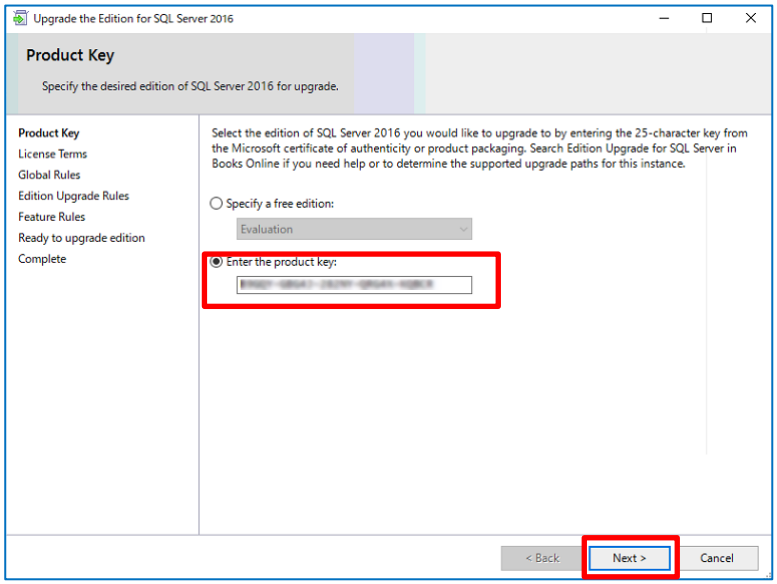
STEP2

Select [Edition Upgrade] from Maintenance.



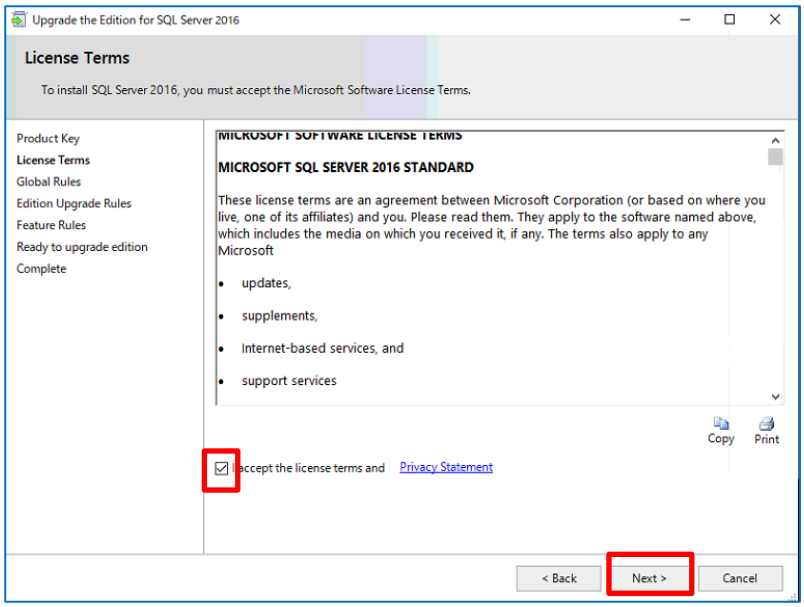
STEP3

Confirm product key is shown and click [Next].



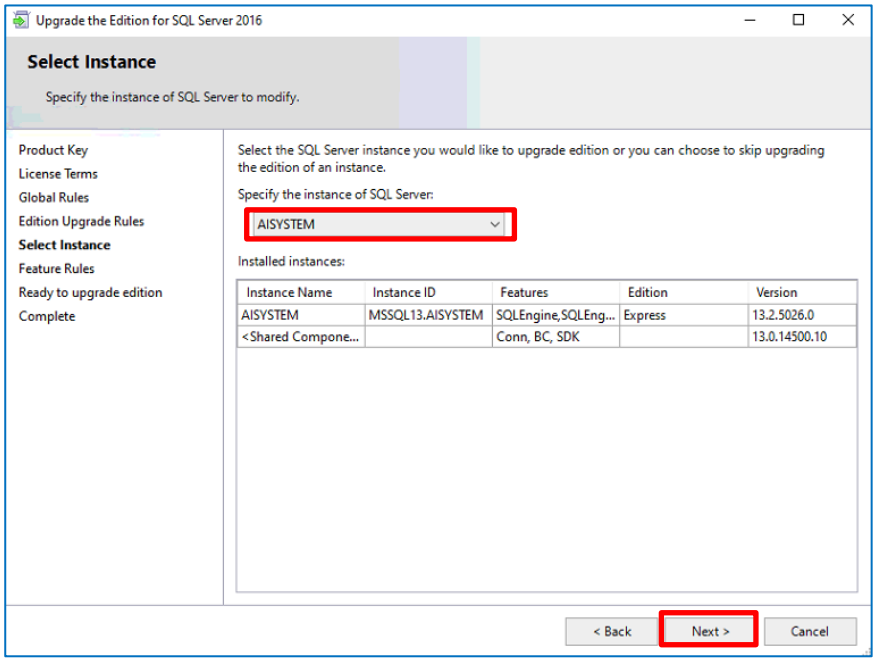
STEP4

Check for license term and click [Next].



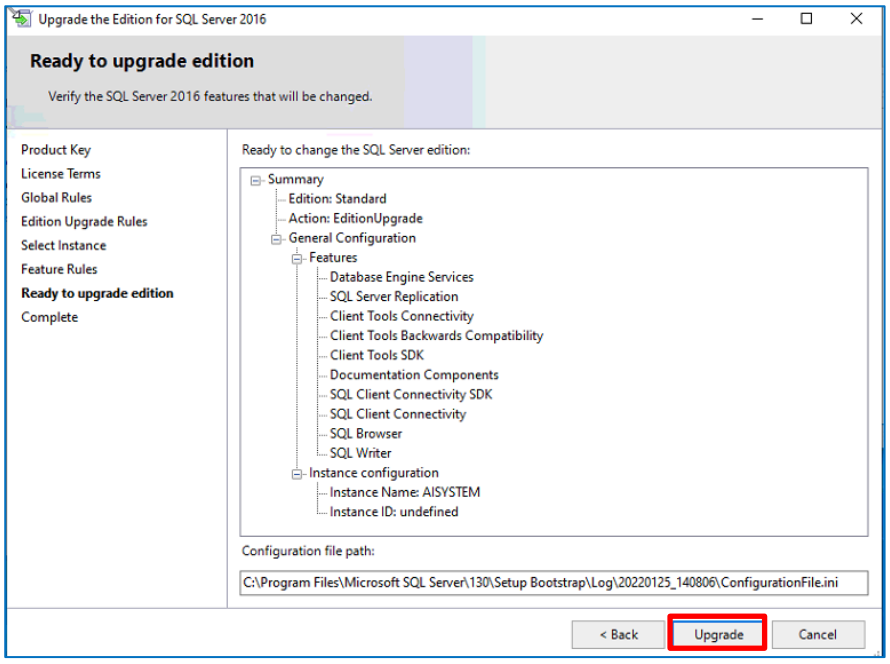
STEP5

Select [AISYSTEM] for instance and click [Next].



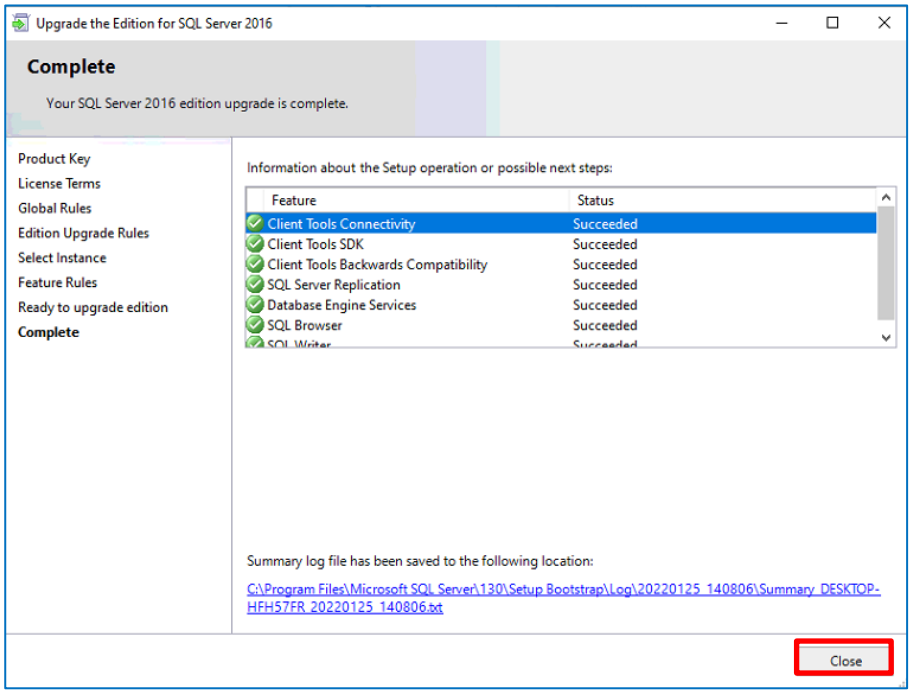
STEP6

Click [Upgrade]



STEP7

Click [Close]



6. Troubleshooting

6.1. Trouble shooting for Installation and Setup

Symptom	Cause and solution	Refer
Failed to install SQL server	There may be some data that was used in the past. Uninstall program related to SQL server 2016, delete folder C:¥Program Files¥Microsoft SQL Server¥MSSQL13.AISYSTEM and delete folder C:¥MultiAI if you installed before.	5.4.2
	Check if the file path length of file path of install package is less than 120 and launch installer as administrator.	4.3.1
	When you use Window 10, version 20H2 and the Microsoft Edge browser of any version from 84.0.522.52 through 86.0.622.55, execute “Windows update”. Ref.https://docs.microsoft.com/en-us/troubleshoot/sql/install/error-set-up-update-instances	-
Cannot install VMS server software after i-PRO Active Guard server installation	When you install i-PRO Active Guard server to PC with VMS server, you need to install VMS server software in advance. If i-PRO Active Guard server is installed before that, uninstall i-PRO Active Guard server and SQL server and then, install VMS server.	4.3.1 5.4.2
Cannot access i-PRO Active Guard configuration.	Did you access http://<ip>:8092 ? “https://<ip>:8092” is correct. When you set another port number when installation or you changed after installation, enter the port number.	4.3.2.1
	Supported browser is Microsoft Edge 85(or later), Chrome 83(or later) and Firefox 95(or later.)	3.2
	Please confirm related service is running on PC that i-PRO Active Guard server is installed. Start – Windows Administrative Tools – Services. “MultiAICameraService”, “MultiAISupportProcessManagementService” and “SQL Server(AISYSTEM)”	5.6.1

	If stopped, right click and run.	
Cannot log in to i-PRO Active Guard configuration	If you forget administrator account, reset account from PC that i-PRO Active Guard server is installed.	5.9
Cannot register VMS.	Check if IP address, port, protocol and credentials are correct.	4.3.2.2 4.2.3
	Supported version of VI IP server is 7.8.3 or later. If you use VI IP server is 7.8.3 or later and “Not supported version” or “Invalid response” is shown, please restart Insight API from Insight API config tool.	2.2
Cannot register cameras	Check if IP address, port, protocol and credentials are correct.	-
	Check if extension software is installed to camera in advance.	4.1
	Check if cameras are registered to VI IP server in advance.	4.2.1
	Check if PC time of i-PRO Active Guard server is synchronized to that of VMS server. When the difference is larger than about 1hour, camera list cannot be got from [Get from VMS]	-
	Check if “Digest” is used for authentication on camera side. ([Settings] - [User mng.] - [User auth.])	-
Face, People or Vehicle images cannot be searched from Plug-in (camera is not shown for camera list).	Camera registration to i-PRO Active Guard server should be done after registering camera to VI IP server. When you re-register the camera to VI IP server after registration to i-PRO Active Guard server, you need to also re-register the camera to i-PRO Active Guard server (delete and then register again.)	5.2.1 5.1.1
Face, People or Vehicle images cannot be searched from Plug-in (the number of search result is 0).	Receiving status from each cameras can be confirmed from i-PRO Active Guard configuration. Check network connection between camera and i-PRO Active Guard server, last received time, last diagnosis time. If the result is not expected, check if schedule setting on camera side for extension software is on.	4.3.8.1
	Check process status of i-PRO Active Guard server. If some process is stopped, restart the process.	4.3.8.2

	Check if schedule setting on camera side for extension software is on.	-
	Configuration issues in a multiple network environment Check if the camera is connected to a network that is not local to the server.	-
	Firewall configuration issues. Check if i-PRO Active Guard server's program are listed on "Allowed apps and features" for firewall settings.	-
Cannot connect from Plug-in to i-PRO Active Guard server.	Check if IP address, port, protocol and credentials are correct. Port and credentials can be changed from i-PRO Active Guard configuration.	4.3.5.2 4.4.2
Playback time is incorrect.	Check if PC time of i-PRO Active Guard server and VMS server are synchronized when i-PRO Active Guard server is installed to dedicated server. Also check if time zone setting of VMS server and VMS client are the same.	-
Registered face detection or registered people detection cannot be shown	Check if i-PRO Active Guard server detect alarm from diagnosis on i-PRO Active Guard configuration. If alarm exists, check the process status of i-PRO Active Guard server.	4.3.8.3
	Check the configuration VMS to receive alarm from IP server manager.	4.2.2.2
	Check the insight API status from Insight API config tool.	-
System alarm cannot be shown	Check the configuration for alarm notification.	4.3.6

6.2. Trouble shooting after staring operation

When trouble occurs after starting operation, you can confirm error code on i-PRO Active Guard configuration (Refer to 4.3.7.4)

Symptom	Error code	Cause and solution
Server process is stopped on i-PRO Active Guard configuration	514 - 517	Services related to i-PRO Active Guard server does not exist. Please install i-PRO Active Guard server again
	1025 – 1028 4097 – 4100 4354,4357, 4610,4611	Process related to i-PRO Active Guard server failed to start. Restart i-PRO Active Guard server manually (Refer to 4.3.8.2). When process stops again, download logs (Refer to 4.3.8.5) and contact the system administrator.
Camera disconnect	4355,4356,4358	Check network connection between camera and i-PRO Active Guard server. Check if video recording to VMS and live monitoring works well or not. If recording or live monitoring also has problem, check camera's status. If problem continues after restarting camera and i-PRO Active Guard server manually (Refer to 4.3.8.2), download logs (Refer to 4.3.8.5) and contact the system administrator.
Face, People or Vehicle Images cannot be searched from Plug-in (the number of search result is 0).	66052,66053	Receiving status from each cameras can be confirmed from i-PRO Active Guard configuration. Check network connection between camera and i-PRO Active Guard server, last received time and last diagnosis time. If the result is not expected, check if schedule setting on camera side for extension software is on.
False detection (Not face, people or vehicle is searched)	-	To avoid false detection, configure mask area using iCT (Refer to 4.1).

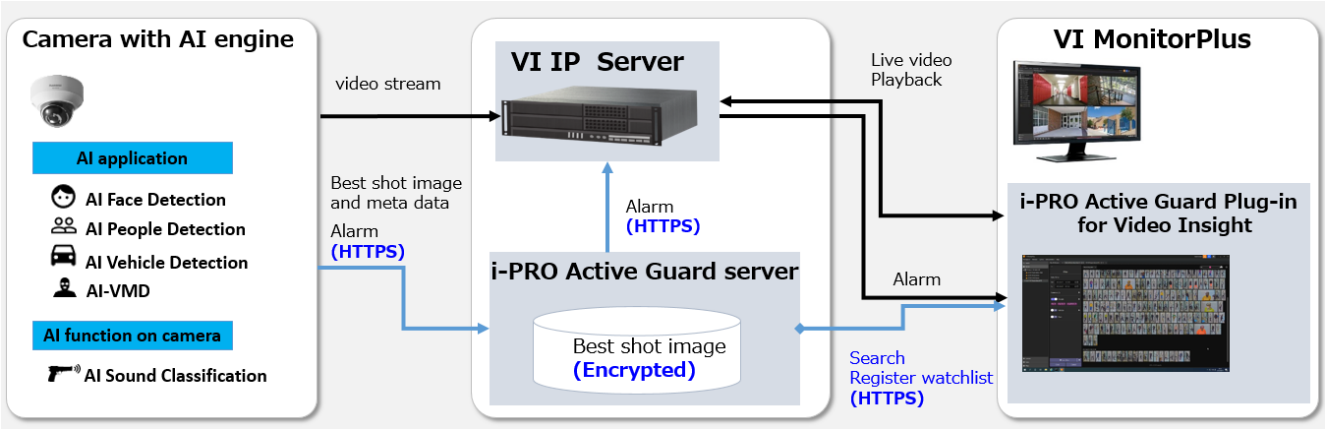
High CPU usage, memory usage or disk access	65793,65794 65796,65797	Check CPU or memory status (Refer to 4.3.8.2) and confirm whether the usage by i-PRO Active Guard server software is high. If the usage of i-PRO Active Guard server is high, to reduce load, configure mask area on camera side using iCT (Refer to 4.1) or “Max frequency of receiving object data (per sec)” (Refer to 4.3.5.4) If the usage of i-PRO Active Guard server is low and those of whole PC is high, check the influence of other software. When i-PRO Active Guard server is installed with VMS software, check the VMS software status.
Reach the max disk space of image (delete old images)	65795	Old images has been deleted by exceeding the settings for “Max usage of image storage drive”. If you need to store data for “Retention period”, configure mask area on camera side using iCT (Refer to 4.1) to reduce the number of detection.

7. Appendices

7.1. Secure system guideline

To ensure encrypted communications within critical environments, the secure system has been created as an additional security layer for the application. This document describes how to enable and configure secure system.

The communication between the cameras and i-PRO Active Guard server can be encrypted over HTTPS protocol.
The communication between the VI IP Server and i-PRO Active Guard server can be encrypted over HTTPS protocol.
The communication between i-PRO Active Guard server and Plug-in can be encrypted over HTTPS protocol.
Recorded Best shot images on i-PRO Active Guard server can be encrypted. Data encryption can be configured only when you install i-PRO Active Guard server.



7.1.1. HTTPS between camera and i-PRO Active Guard server

STEP1

Open the camera's web browser (*see instructions for each made and model*).
[Setup] – [Network] – [Advanced] – [HTTPS], select [HTTPS] from the Connections list box.

STEP2

When you register camera to i-PRO Active Guard server, select HTTPS (Refer to 4.3.2.3).

7.1.2. HTTPS between i-PRO Active Guard server and Plug-in

STEP1

Configure HTTPS for [Client plugin connection] on i-PRO Active Guard server's setting (Refer to 4.3.5.2) and Restart process.

STEP2

Configure HTTPS connection on Plug-in's setting (Refer to 4.4.2)

7.1.3. HTTPS between VMS and i-PRO Active Guard server

STEP1

Run Insight API Configuration Tool on VI IP server (Start – VI Enterprise – Insight API Config).
Click [SSL Config] and check [Enable SSL], and select Certificate.
[Stop] and [Start] Insight API Service.

STEP2

When you register VMS to i-PRO Active Guard server, select HTTPS (Refer to 4.3.2.2).

7.1.4. Encryption of Best shot images

Encryption on/off can be configured only when installing i-PRO Active Guard server (Refer to 4.3.1).
When data is encrypted, image can be seen from Plug-in software. Other software cannot open the file.

7.2. Open source software

This product uses open source software.
For details concerning licensing, read license.txt included in install package.