Setup Instructions

i-PRO Active Guard for Genetec

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. This product must not be used for any purpose that is unlawful or prohibited by any law or regulation. We are not responsible for such unlawful or infringing use of our products. In addition, 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 USERNAME 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 username 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.

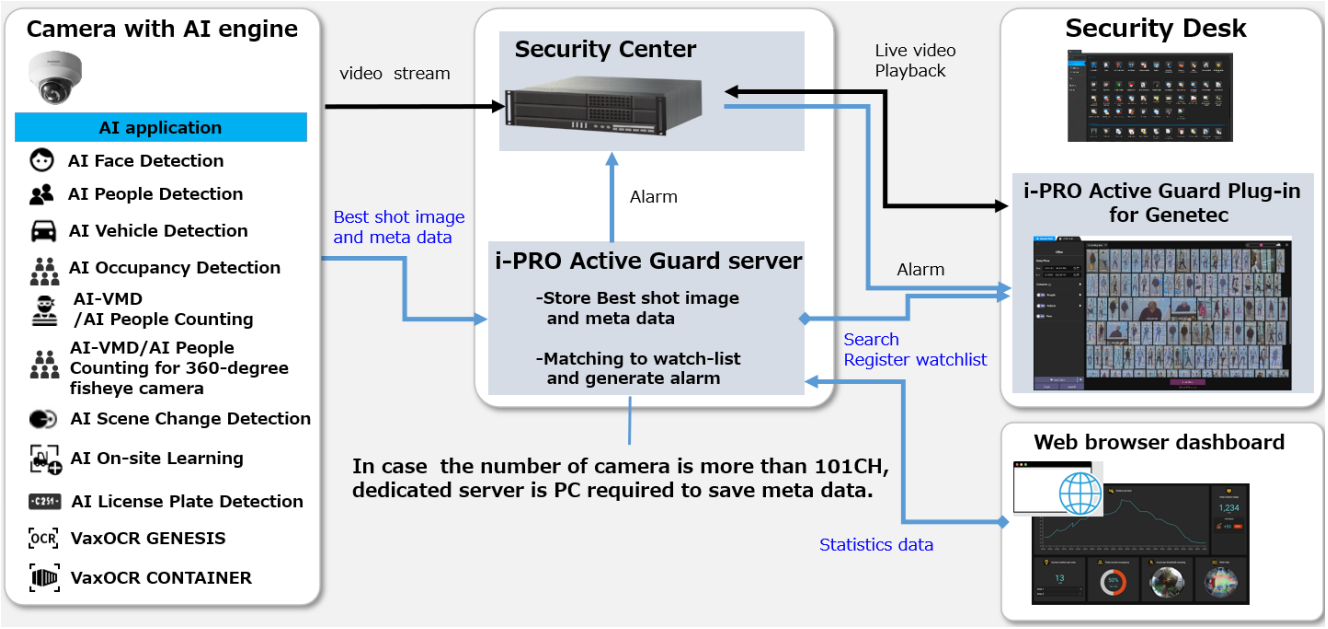
- Use a password that has never been used to protect your network from information leakage or theft.

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 work.
  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 Security Center 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, people, vehicle, LPR, code or container is matched to watchlist.

i-PRO Active Guard Plug-in for Genetec (hereinafter referred to as “Plug-in”) which is the plug-in software for Security Desk can search Best shot images, register watchlist, show live video, recorded video.

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. V1.11 or later is supported.
  - V2.10 or later is required for area-specific search (Region of interest) in Plug-in.
- AI People Detection: Camera's extension software. V1.11 or later is supported.
  - V1.40 or later is required for to use the automatic detection of people attributes from images.
  - V2.10 or later is required for area-specific search (Region of interest) in Plug-in.
- AI Vehicle Detection: Camera's extension software. V1.11 or later is supported.
  - V1.40 or later is required for to use the automatic detection of vehicle attributes from images.
  - V2.10 or later is required for area-specific search (Region of interest) in Plug-in.
- AI Occupancy Detection: Camera's extension software. V1.60 or later is supported.
- AI-VMD/AI People Counting: Camera's extension software. V2.00 or later is supported.
  - V3.00 or later is required for people or vehicle counting dashboard.
  - V3.20 or later is required for to show the line names set by the camera in dashboard.
  - V3.70 or later is required for heatmap in dashboard People counting.
- AI Sound Classification: Camera's firmware function.
- AI-VMD/AI People Counting for 360-degree fisheye camera: Camera's extension software. V1.21 or later is supported.
- V1.50 or later is required for to show the area/line names set by the camera in dashboard.
- AI Scene Change Detection: Camera's extension software. V1.00 or later is supported.
- AI On-site Learning: Camera's extension software. V1.00 or later is supported.
- AI Processing Relay: Camera's extension software. V1.00 or later is supported.
  - V2.10 or later is required for specify lines/area individually in dashboard.

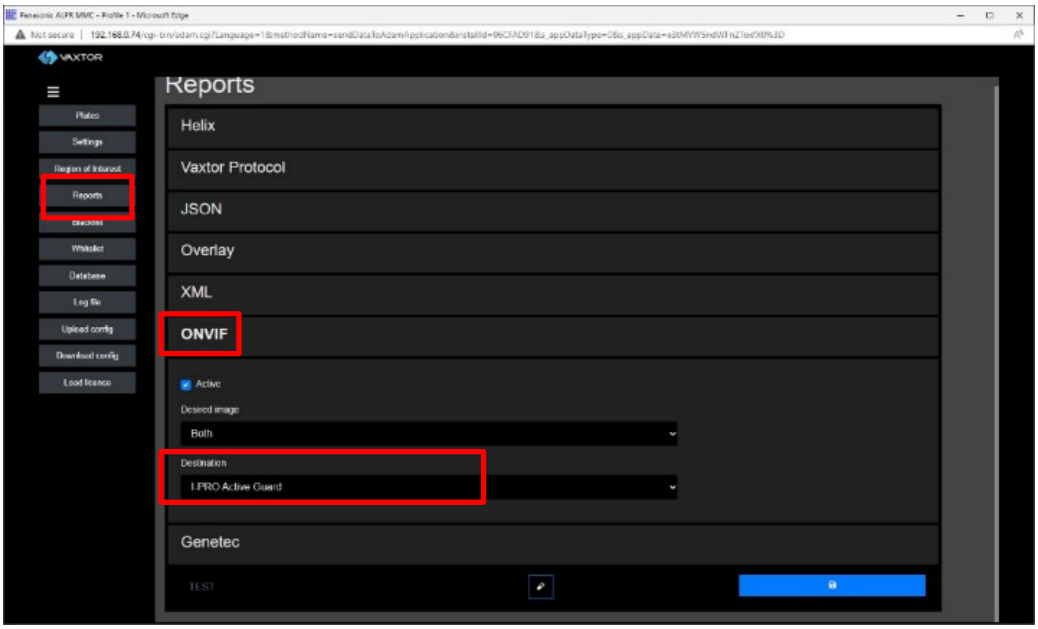
Please see https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/knowledge-base/product-tips/active-guard-links for more information.

[Partner's application: Vaxtor Technologies]

- VaxALPR Camera's extension software. V1.3.16 or later is supported.
- VaxOCR GENESIS Camera's extension software. V1.3.7 or later is supported.
- VaxOCR CONTAINER Camera's extension software. V1.0.5 or later is supported.

About Vaxtor's application (VaxALPR, VaxOCR GENESIS, VaxOCR CONTAINER)

- For Multi-Sensor Cameras, only 1ch is supported.
- Vaxtor's application does not work just by installing it on the camera.
  Set "Reports - ONVIF – Destination" to "i-PRO Active Guard" in Vaxtor's application settings.



For more information on Vaxtor's application, please see application list.

For integration with 3rd party extension software, excluding VaxALPR, VaxOCR GENESIS and VaxOCR CONTAINER, refer to 7.3.

Camera's 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	1.11 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

camera model	Version
WV-S71300-F3	1.10 or later
WV-S61301-Z2, WV-S61302-Z4, WV-S65340-Z2N, WV-S65340-Z2K, WV-S65340-Z4N, WV-S65340-Z4K	1.00 or later

Please see https://i-pro.com/global/en/surveillance/training-support/support/technical-information<Control No:C0103> for more information.

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

Software	Version
Genetec Security Center	SC 5.10.1.0 or later
i-PRO Active Guard server / i-PRO Active Guard Plug-in for Genetec	V1.0.0 or later

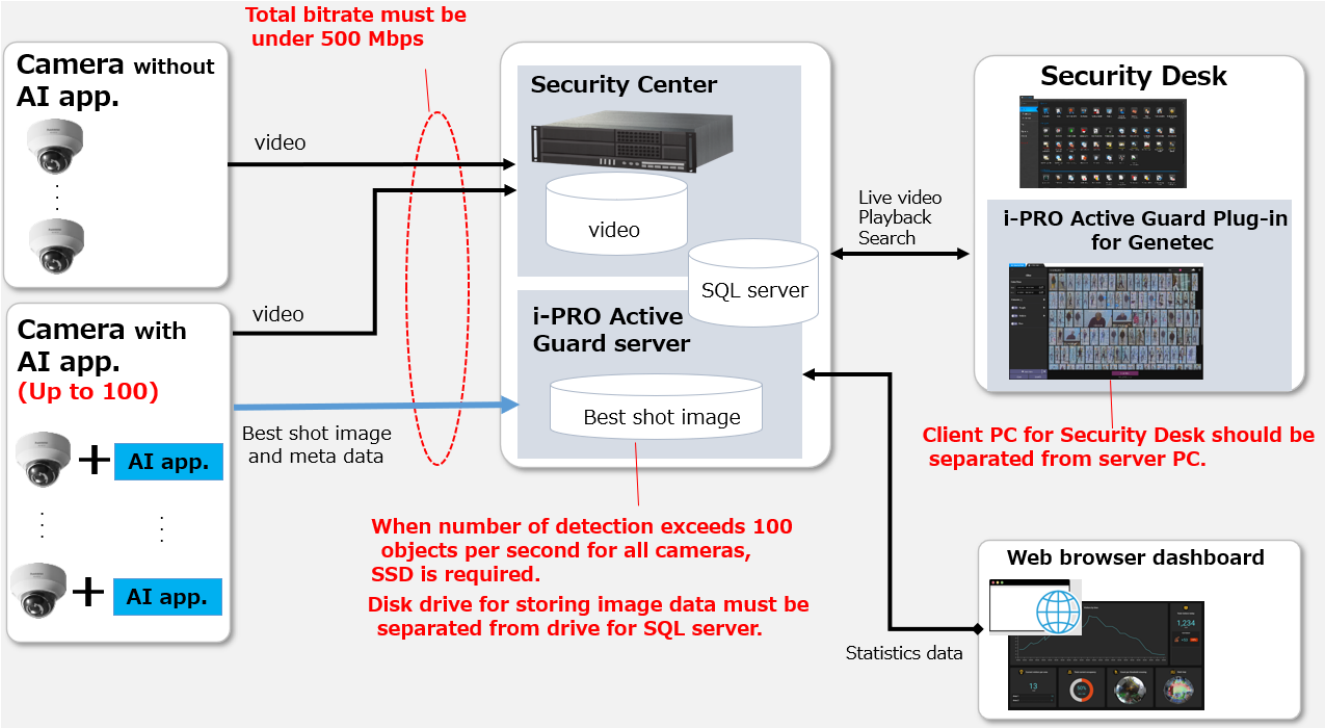
3. System design

3.1. System architecture

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

	i-PRO Active Guard server installed with Security Center	i-PRO Active Guard server installed In dedicated server
The number of cameras	Up to 100 (including up to 20 AI Face Detection cameras)	Up to 300 (including up to 100 AI Face Detection cameras)
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 Security Center



Important:

・Due to i-PRO Active Guard server maintenance, i-PRO Active Guard server and SQL Server must be kept running from 0:00-4:00.

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

(1) Up to 100 cameras with AI engine, including up to 20 cameras with AI Face Detection.

(2) Total bitrate that server PC receives must be under 500Mbps. Both bitrate of video data and best shot images should be calculated.

Bitrate of best shot images can be calculated in 3.3.

(3) Disk drive for storing Best shot image must be separate from drive for storing video and SQL server.

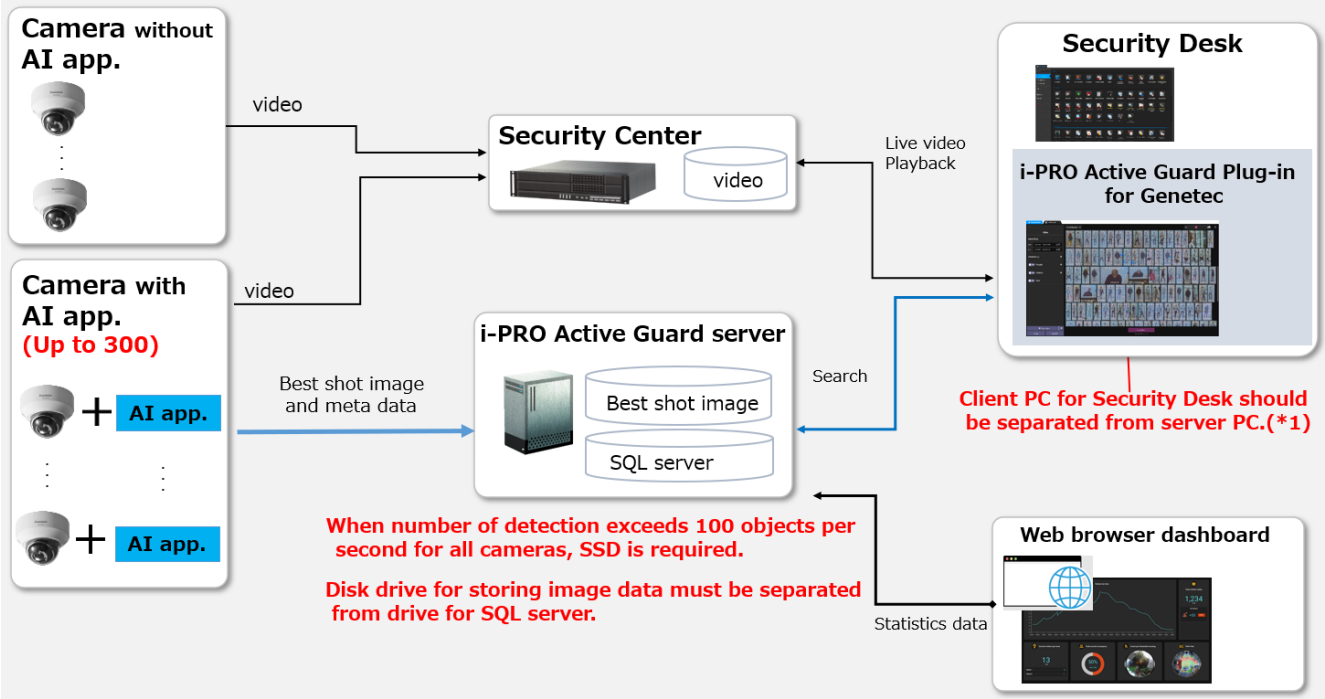
For the file path to store "SQL server", see 4.3.1.

For the file path to store “Best shot image”, see 4.3.1 or 4.3.5.4.

If you require reliable data management, please consider using RAID5/6.

(4) 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



*1 Plug-in can be connected to multiple i-PRO Active Guard servers. It supports bulk search and watchlist alarm.
Watchlist need to be set for each i-PRO Active Guard server and cannot be shared.

Important:

・Due to i-PRO Active Guard server maintenance, i-PRO Active Guard server and SQL Server must be kept running from 0:00-4:00.

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

(1) Up to 300 cameras with AI engine, including up to 100 cameras with AI Face Detection.

(2) Disk drive for storing Best shot image must be separate from drive for SQL server.
For the file path to store "SQL server", see 4.3.1.
For the file path to store “Best shot image”, see 4.3.1. or 4.3.5.4.
If you require reliable data management, please consider using RAID5/6.

(3) Client PC should be separated from server PC. Plug-in can connect to one 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 Security Center * Bandwidth limitations apply.	• Intel® Xeon® Silver 4210 (2.2 GHz, 10 core 20 thread) or better • 32 GB of RAM or more • 64 bit operating system Microsoft® Windows Server 2016 Standard Microsoft® Windows Server 2019 Standard Microsoft® Windows Server 2022 Standard Microsoft® Windows Server 2016 Datacenter Microsoft® Windows Server 2019 Datacenter Microsoft® Windows Server 2022 Datacenter • 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 Microsoft® Windows 10 Enterprise Microsoft® Windows 10 Education Microsoft® Windows 10 Pro Education Microsoft® Windows 10 IoT Enterprise * Version 2004 or later Microsoft® Windows 11 Pro Microsoft® Windows 11 Enterprise Microsoft® Windows 11 Education Microsoft® Windows 11 Pro Education Microsoft® Windows 11 IoT Enterprise Microsoft® Windows Server 2016 Standard Microsoft® Windows Server 2019 Standard Microsoft® Windows Server 2022 Standard Microsoft® Windows Server 2016 Datacenter Microsoft® Windows Server 2019 Datacenter Microsoft® Windows Server 2022 Datacenter • GbE network interface card

	Requirement
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 Standard Microsoft® Windows Server 2019 Standard Microsoft® Windows Server 2022 Standard Microsoft® Windows Server 2016 Datacenter Microsoft® Windows Server 2019 Datacenter Microsoft® Windows Server 2022 Datacenter • GbE network interface card

Note)

i-PRO Active Guard server can be run on Microsoft® Hyper-V with Windows Server 2022 and VMware® ESXi 7.0 Update 3.

When using virtual platform, CPU, memory, network adapters, and storage may become bottlenecks. Please consider in advance the allocation of sufficient CPU, memory, and network settings to meet the above hardware requirements.

Requirements for the number of cameras registered on Security Center

	Requirement
Number of cameras registered on Security Center	• Upper limit 10,000 cameras *The number of cameras includes cameras other than i-PRO cameras.

Common software requirement

Category	Supported software
Database Engines	• SQL server 2014/2016/2019/2022 The following SQL server is installed when new installing. - i-PRO Active Guard server version 1.0.0 to 1.6.2 SQL server 2016 Express Edition. - i-PRO Active Guard server version 1.7.0 or later SQL server 2019 Express Edition. For update i-PRO Active Guard server, SQL Server carries over the existing version. Upgrade procedure is shown in 5.11.
Web browser for Configuration Tool	•Microsoft Edge 85 or later •Chrome 83 or later •Firefox 95 or later * In Firefox, if the monitor resolution is higher than Full-HD (1920 x 1080), the display scaling may not work.

Disk drive considerations

When the maximum number of detections exceed 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.

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, vehicle, etc. should be under 8GB.” Check 3.3 to see if the Express edition is sufficient.

3.2.2. System requirement for Plug-in

Requirement (Recommended)
● Intel® Core™ i7-9700 (4.9 GHz, 8 core 8 thread) or better. ● 8 GB of RAM or better ● OS: Microsoft® Windows 10 Pro (64 bit), Microsoft® Windows 11 Pro (64bit) ● 120 GB Solid State Drive for OS and Security Center applications, with a minimum of 6 GB of free disk space to install the Security Center client application ● GbE network interface card ● NVIDIA® GTX 1660 video card

Please also see the Security Center‘s manual.

Language setting

Please set the language of Security Center and Windows to the same.

3.3. How to determine the system architecture

STEP1: The number of cameras

Confirm the number of cameras with following software to be registered on i-PRO Active Guard Server.

- AI Face detection
- AI People detection
- AI Vehicle detection
- AI Occupancy detection
- AI-VMD/AI People Counting
- AI Sound Classification
- AI-VMD/AI People Counting for 360-degree fisheye camera
- AI Scene Change detection
- License plate detection
- VaxOCR GENESIS
- VaxOCR CONTAINER

Note:

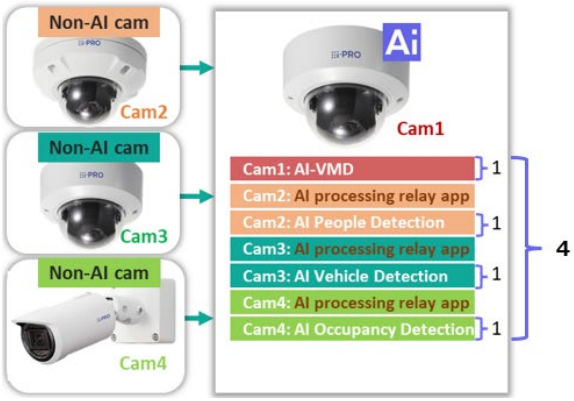
How to count when using multi-directional cameras and AI processing relay application.

- Multi-directional cameras: Count the number of sensors as the number of AI cameras.
- Using AI encoder application: Count the number of cameras including non-AI cameras.

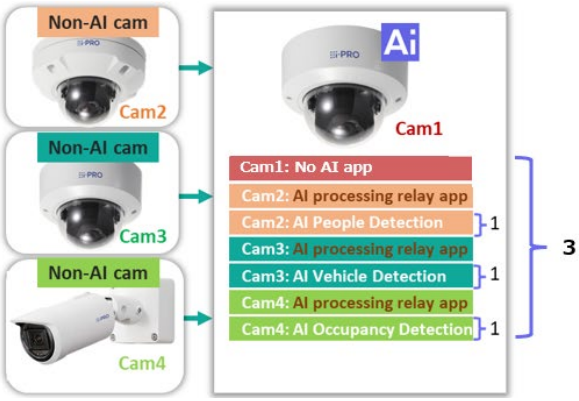
Ex) 1 AI camera + 3 non-AI cameras: counted as 4 cameras. (*1)

However, if AI camera does not use an AI application, only 3 non-AI are counted. (*2)

(*1)



(*2)



■ When there are fewer than 100 cameras and fewer than 20 AI face detection cameras.

i-PRO Active Guard server can be installed on the same PC as Security Center. Please see 3.1.A.

■ When there are 100 or more cameras or 20 or more AI face detection cameras.

i-PRO Active Guard server must be installed in dedicated server PC. Please see 3.1.B.

STEP2: The number of activated AI functions

To calculate the bitrate of images, it is necessary to count the number of the following AI functions installed on each camera.

AI functions to include in the calculation:

Face / People / Vehicle / License Plate / Code / Container / Heat map*

Count each AI functions individually per camera. For example, if both People and Vehicle are installed on a single camera, count 1 for each.

(Ex, When People and Vehicle are installed to a camera, add 1 for People and Vehicle, respectively.)

*Heat Map refers to the function in the AI-VMD app. For this item, please enter the number of cameras with the Heat Map function enabled in the AI-VMD app.

AI functions NOT to Include in the calculation:

AI Occupancy / AI Scene Change Detection / AI-VMD (Intruders, Loitering, Direction, Cross Line including Tailgating, People / Vehicle Counting). Since these AI functions are used for alarm purposes and generate minimal data. They do not need to be including the calculation.

		Face	People	Vehicle	License plate	Code	Container	Heat map
The number of activated AI functions		0	0	0	0	0	0	0
The Number of detections [per camera, per hour]	Max.	1,000	1,000	1,000	1,000	1,000	1,000	
	Avg.	1,000	1,000	1,000	1,000	1,000	1,000	

Estimated data points of detections [per sec]	0

*For people, 1 object is counted as 2 data points. For other objects, 1 object is counted as 1 data point.

■ When the number of “Estimated data points of detections” is less than 100

HDD or SSD is available for disk drive.

■ When the number of “Estimated data points of detections” is over 100

SSD is required.

If an HDD is used, excess data will not be saved, and the entire system may not function properly.

“Estimated data points of detections” can be limited by the settings, see 4.3.5.4

The default setting is 100. Set the calculated value plus a margin.

STEP3: Total bitrate server receives

Total bitrate of best shot image [Mbps]	0.00
Maximum bitrate of Heat map 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.

STEP4: Retention period and storage

	Face	People	Vehicle	License plate	Code	Container	Count/ heatmap/ Statistics
Retention period (day) (*1)	31	31	31	31	31	31	92
Operating time (hours per day)	8	8	8	8	8	8	8

*1: Up to 31 days (92 days for Count/heatmap/Statistics) when using SQL Server Express Edition.
Up to 397 days (732 days for Count/heatmap/Statistics) when using SQL Server Standard Edition or higher.

Estimated used disk size for best shot images [GB]	0.00
Estimated used disk size for Heat map data [GB]	0.00
Total Estimated used disk size [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 higher can be used. When more than 8GB, SQL Server Express Edition cannot to be used due to the limitation of Express Edition. Standard Edition or higher is must. (Refer to 5.11)

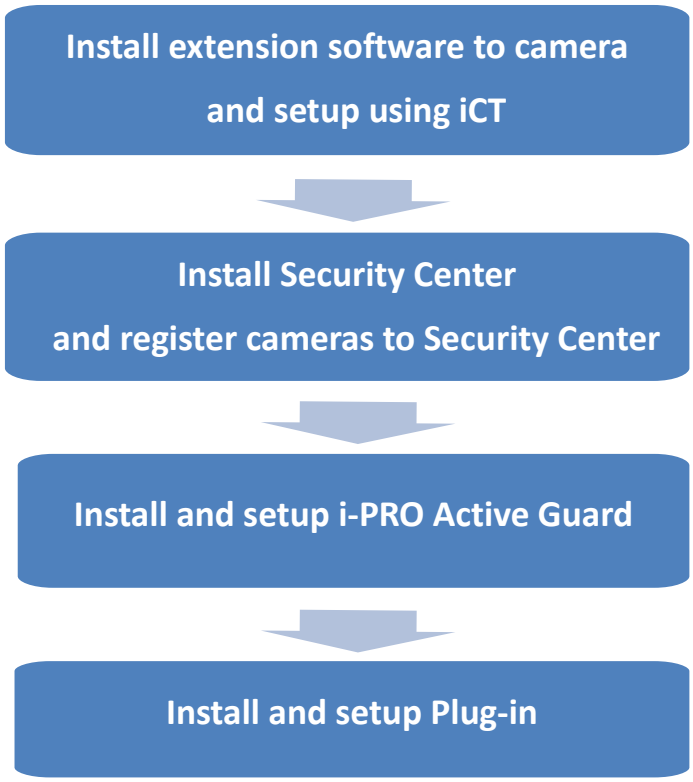
3.4. Ports used in i-PRO Active Guard server

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
1434	UDP	Connection to SQL Server Browser
1435	TCP	Connection to SQL Server
8090	HTTP	Client Plug-in connection
8091	HTTPS	Client Plug-in connection
8092	HTTPS	Web configuration tool connection
8888	TCP	Internal process communication
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

Extension software is installed and configured using i-PRO Configuration Tool (iCT).
Please refer to the URL below for downloading extension software and i-PRO Configuration Tool (iCT).

https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/knowledge-base/product-tips/active-guard-links

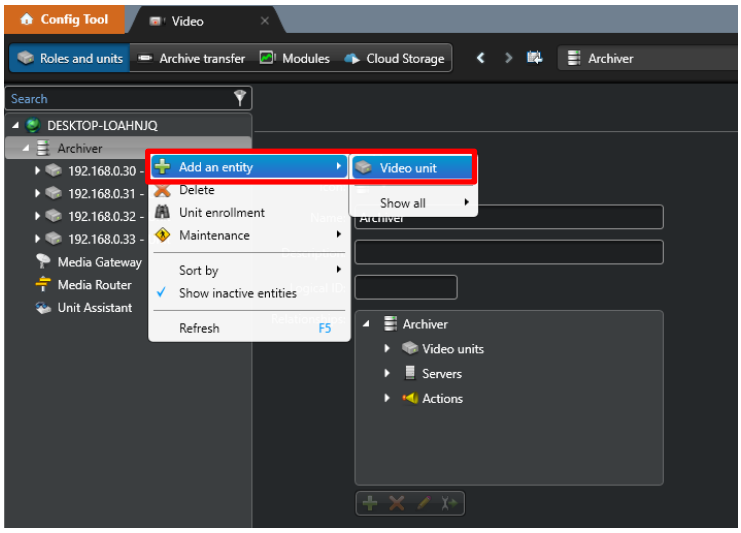
4.2. Install and setup Security Center

Install the VMS server software and register the AI camera with the VMS client.
Install Plug-in to Security Desk.
Register the camera in MAP as an Option setting.

4.2.1. Install and register cameras to Security Center

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

After installation, register AI cameras to Security Center using Config Tool.
(Genetec Security Center – [Config Tool] – [Video] – [Cameras])



4.2.2. Install Plug-in to Security Center

Download the installer from
https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/knowledge-base/product-tips/active-guard-links

Install “i-PRO Active Guard Plug-in for Genetec” software to PC that Genetec Security Center is installed.

4.2.2.1. Install

STEP1

Search for Services App in search box and run it.

Select “Genetec Server” and “Stop” in right-click menu.

STEP2

Launch the executable installer as Administrator.

Click the [Next] button, then check marks [I accept the terms in the License Agreement], and then click the [Install]

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

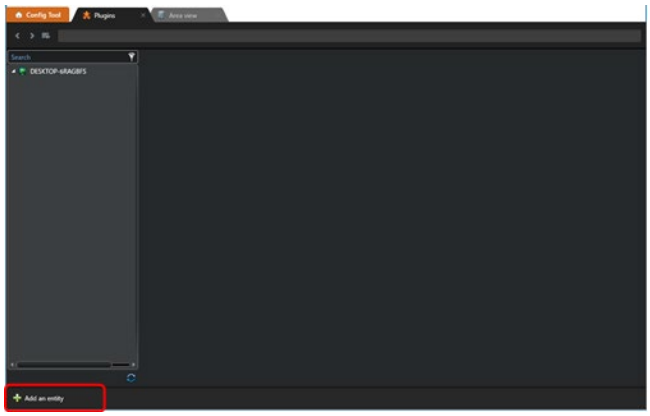
STEP3

In Services App, select “Genetec Server” and “Start” in right-click menu.

4.2.2.2. Configure Plug-in to Security Center

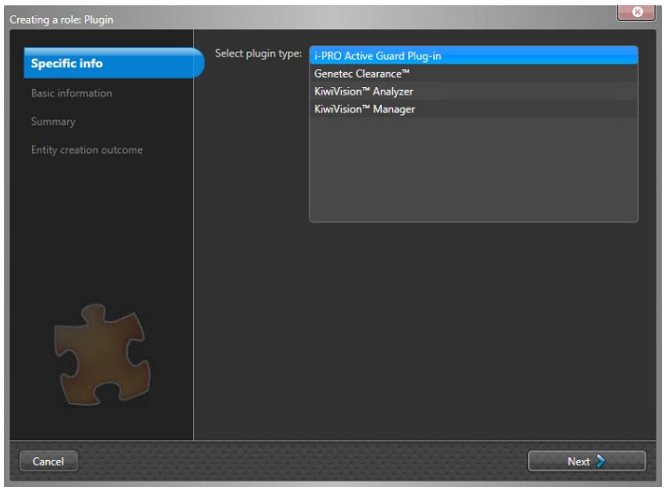
STEP1

Connect Config Tool with Security Center. In the Config Tool site, click the [Plugins] in the [Tasks] menu.



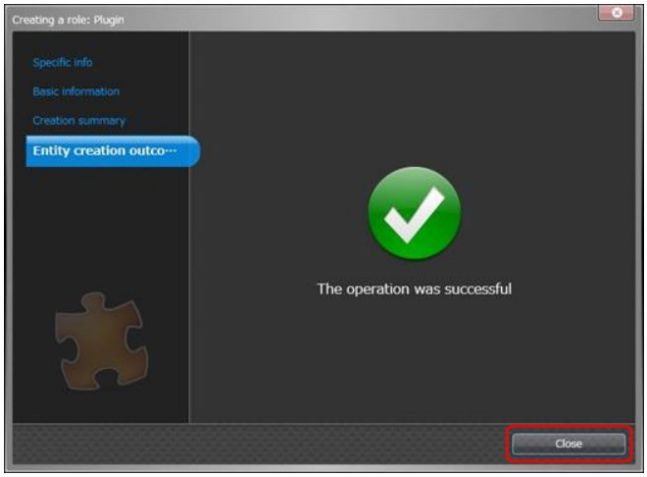
STEP2

Click the [Add an entity] button at the bottom left of the screen.



STEP3

Select [i-PRO Active Guard Plug-in] and [Next].



STEP4

Install following the screen and [Close] when finished.

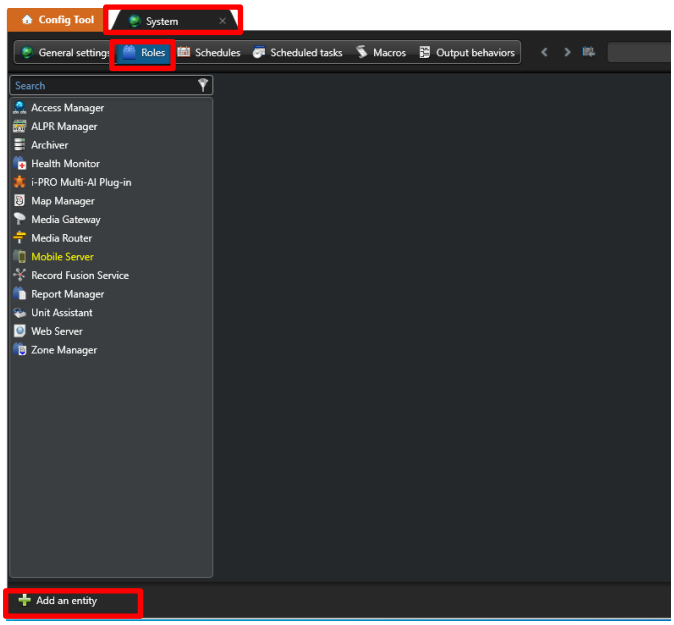
.

4.2.3. Configure the Web-SDK

STEP1

[Config tool] – [System] - [Roles] button.

Click the [Add an entity] button at the bottom left of the screen and select the [Web-based SDK].



Click the [Next] button in [Basic information], [Create] button in [Creation summary] and [Close] button in [Entity creation outcome].

STEP2

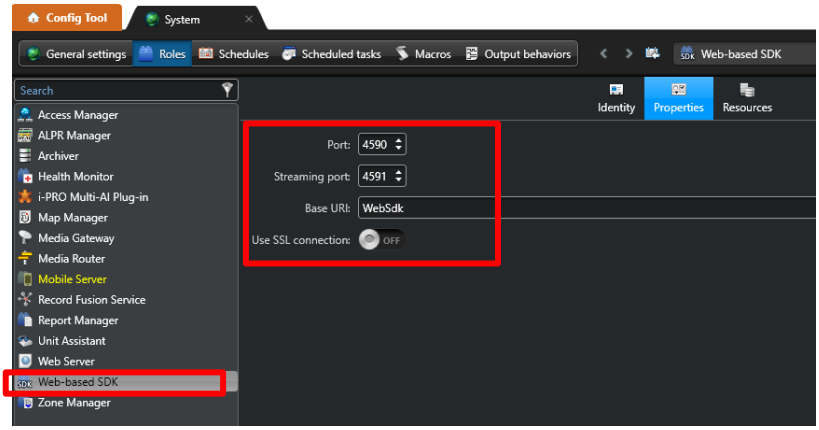
Confirm that [Web-based SDK] is displayed.

Click [Properties] in [Web-based SDK] and set as follows.

Port: 4590

Base URI: WebSdk

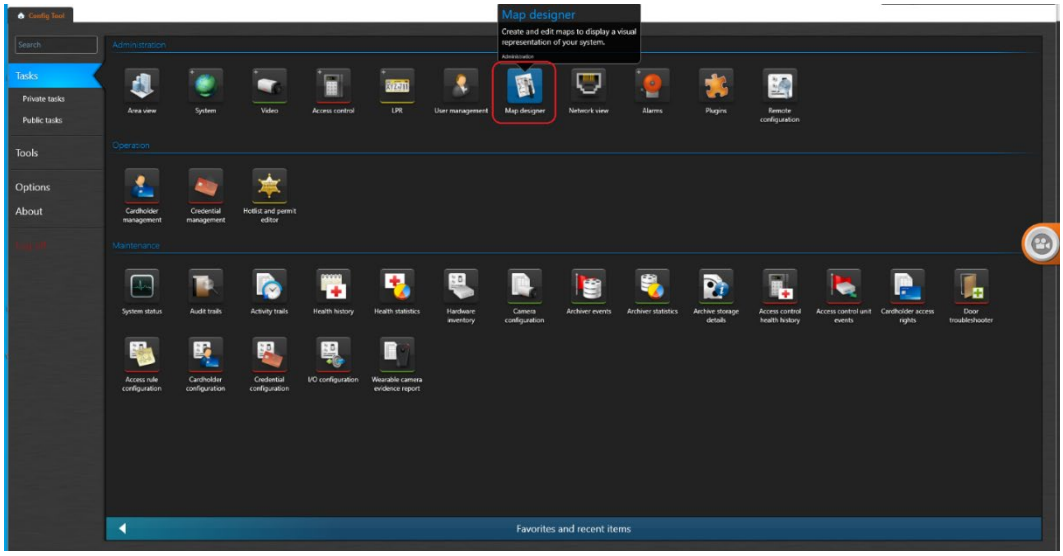
Use SSL connection can be used when using SSL connections.



4.2.4. Register cameras to Map (optional)

Using maps, operator can easily find the location of each Best shot image on Plug-in screen.
See operation manual of Security Center in details.
([Config Tool] – [Map designer])

When you register or change the map, terminate Security Desk and start again.



4.3. Install and setup i-PRO Active Guard server

Download the installer from

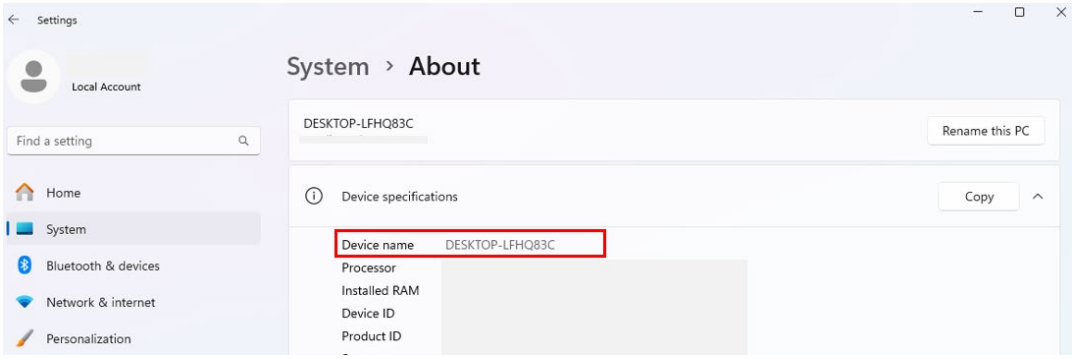
https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/knowledge-base/product-tips/active-guard-links

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

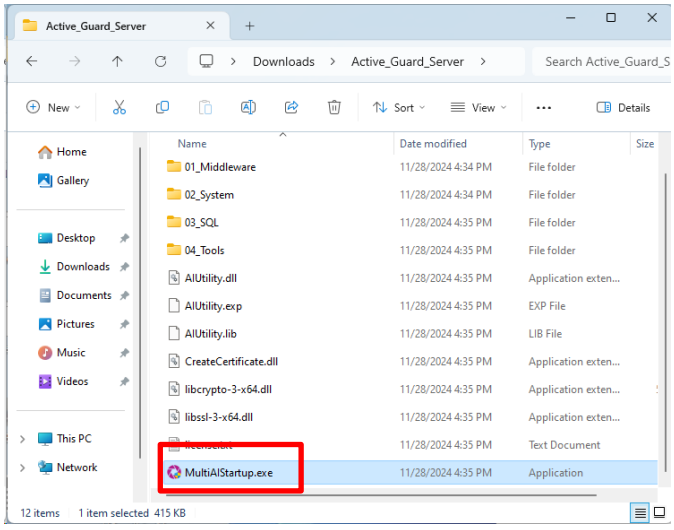
4.3.1. Install

Important:

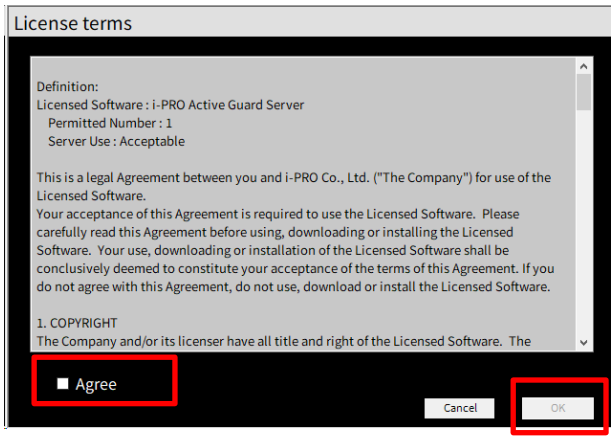
- Please temporarily turn off antivirus software before installing.
- File path length of ***MultiAIStartup.exe*** must be less than 119.
- Device name must be alphanumeric and hyphenated only.



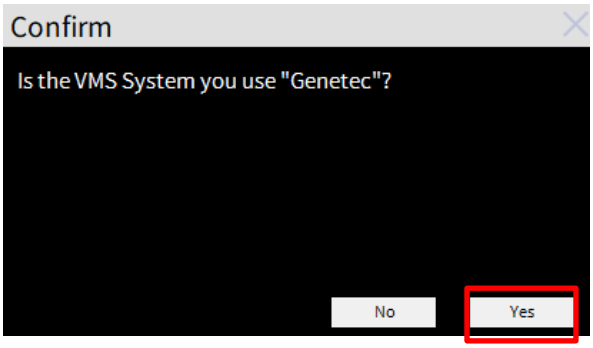
Execute ***"MultiAIStartup.exe"*** as administrator.



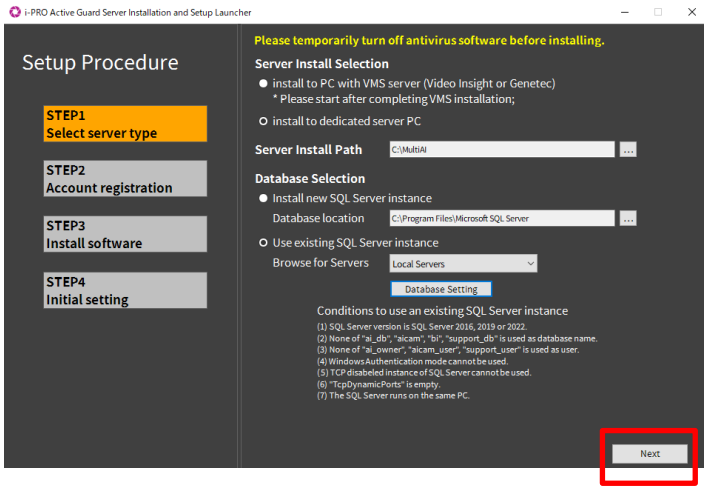
When .NET Framework 4.8 and Microsoft Visual C++ Redistributable are not installed on the PC, it will automatically be installed, and the main screen of the setup tool will be displayed after the installation. Also, when you use Windows 10 version 20H2, Windows Update message. Execute "Windows Update" according to the message.



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



Click [OK]. Genetec SDK installer will start.
Follow the instructions to install it.
If Genetec SDK (v5.12.2181.29 or later) is already installed, click [No].



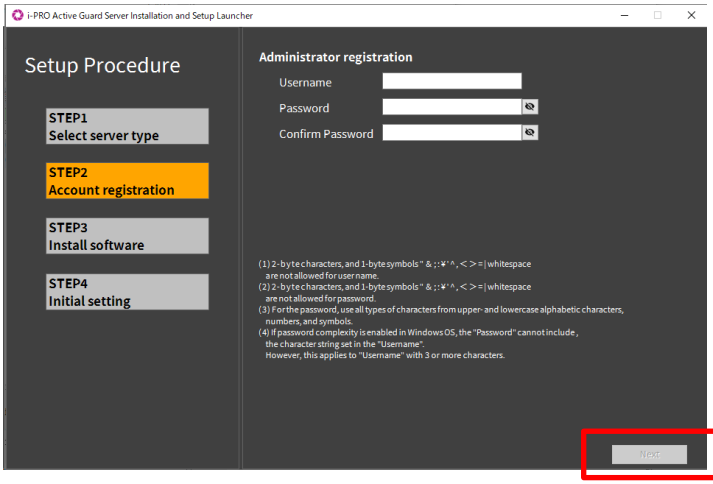
・Server Install Selection
Select [install to PC with VMS server] or [install to dedicated server PC].

・Server Install Path
Set install path for i-PRO Active Guard server.

・Database Selection
Select [Install new SQL Server instance] or [Use existing SQL Server instance].
For [Install new SQL Server instance], you need to set Database location.

For [Use existing SQL Server instance], you need to click [Database Setting] to set the existing SQL Server instance.
For details, please refer to 4.3.1.1

Click [Next].

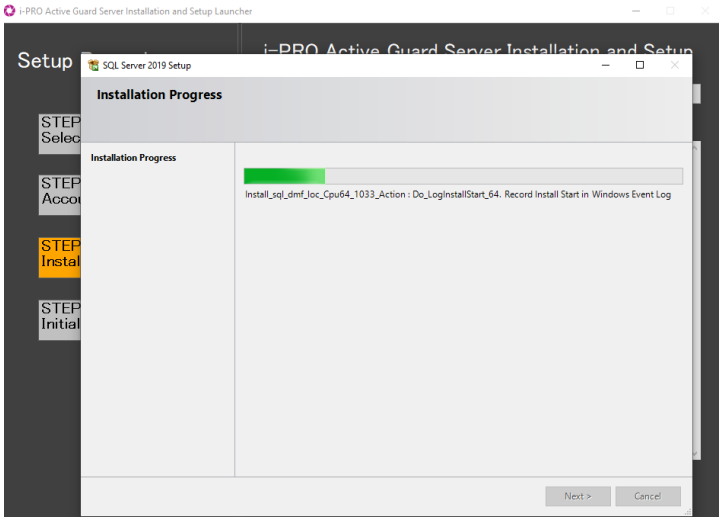


Register credentials and click [Next].

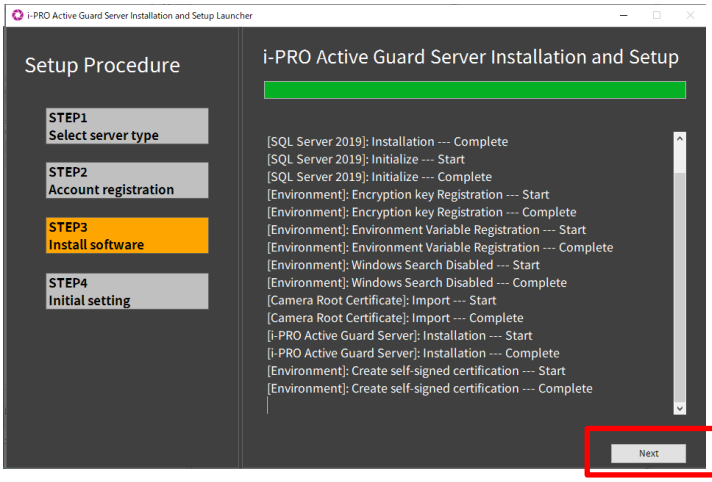
Note)

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

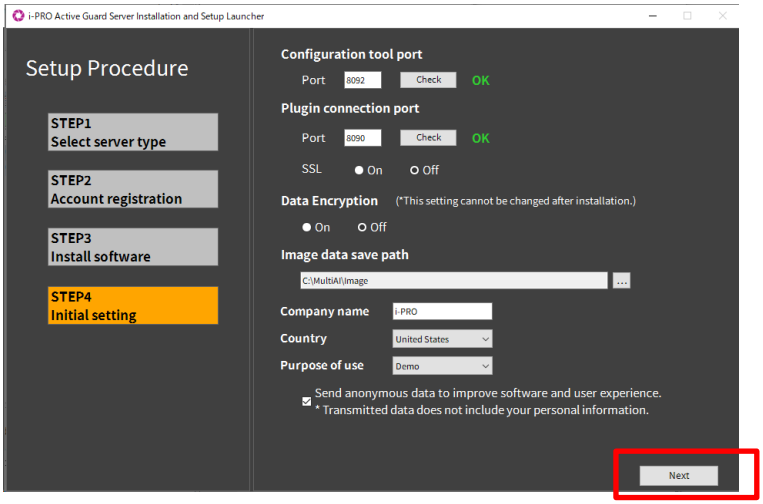
When you forget the Administrator account, you can reset (Refer to 5.9).



Installation starts.



[Next] button will be appeared when finished. Click [Next].

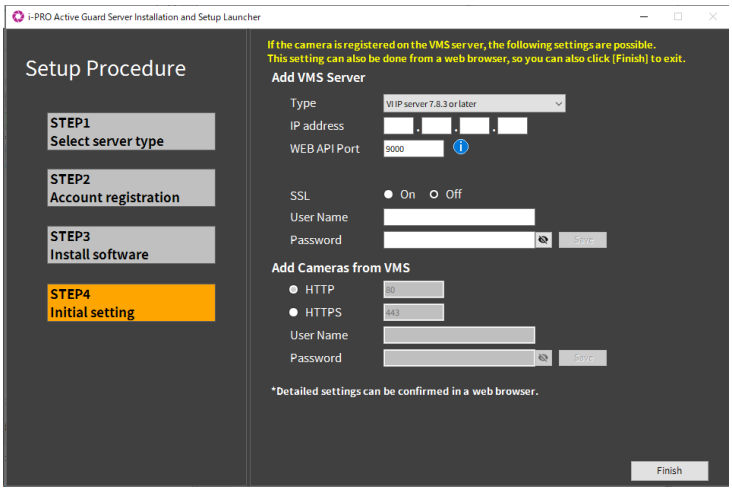


Configure port number, SSL and Data Encryption, Image data save path, Company name, Country and Purpose of use.

Click [Next].

Important:

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



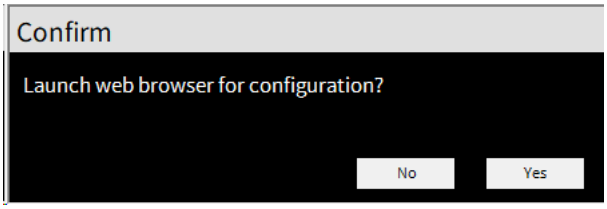
Register VMS Server and Cameras.
To finish the settings, click [Finish].
[Finish] can be clicked at any time without registering the VMS Server and Cameras.

・Add VMS Server

Set Type to “Genetec Security Center”, and set IP address, WEB API Port, SSL, User Name, Password.
Click [Save] to check the connection to VMS Server and save the settings if the connection is successful.

・Add Cameras from VMS

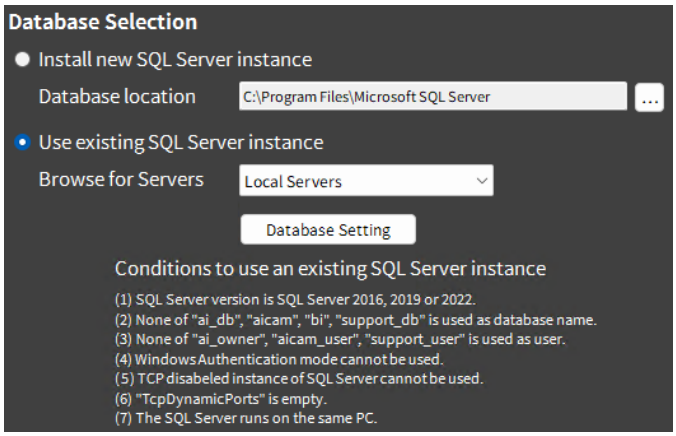
Set HTTP or HTTPS, HTTP port, HTTPS port, User Name, Password of the cameras registered on VMS Server.
Click [Save] to check the connection to the cameras and save settings if one or more connections are successful.
*Camera with AI Processing Relay will not be registered. register from web browser.



A dialog box will appear asking about launch web browser.
Please make your selection as necessary.
Refer to 4.3.2 for configuration.

4.3.1.1. Install SQL database to exist instance

The installer can create an SQL database to an existing instance on the local servers or network servers by selecting [Use existing SQL Server instance] in STEP 1.



Conditions to use an existing SQL Server instance

(1) SQL Server version is SQL Server 2016,2019 or 2022.

(2) None of “ai_db”, “aicam”, “bi”, “support_db” is used as database name.

(3) None of “ai_owner”, “aicam_user”, “support_user” is used as user.

(4) Windows Authentication mode cannot be used.

(5) TCP disabled instance of SQL Server cannot be used.

(6) “TCP Dynamic Ports” is empty.

(7) The SQL Server runs on the same PC.　* Local Servers only.

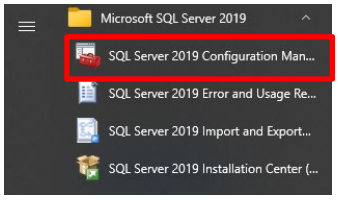
Note)

If you select [Use existing SQL Server instance] and install SQL, make sure TCP Port is configured.

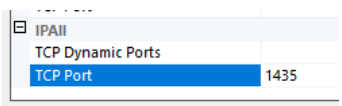
If the setting is blank, please set "1435".

1. Run “SQL Server Configuration Manager”

e.g.) SQL Server 2019

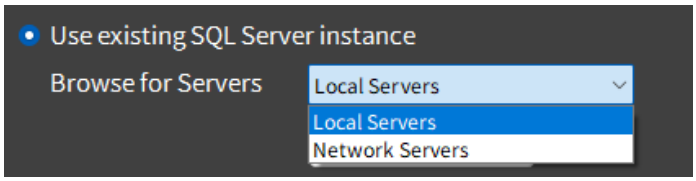


2. SQL Server Network Configuration　-　Protocols for (instance name) - TCP/IP - IP Addresses tab – IPAll - TCP Port=1435.



If 1435 is already in use, set another empty port. In case of i-PRO Active Guard server is already installed, uninstall and reinstall it after setting the port.

Select [Use existing SQL Server instance], then select [Local Server] or [Network Server] from the drop-down list and click [Database Setting] button.

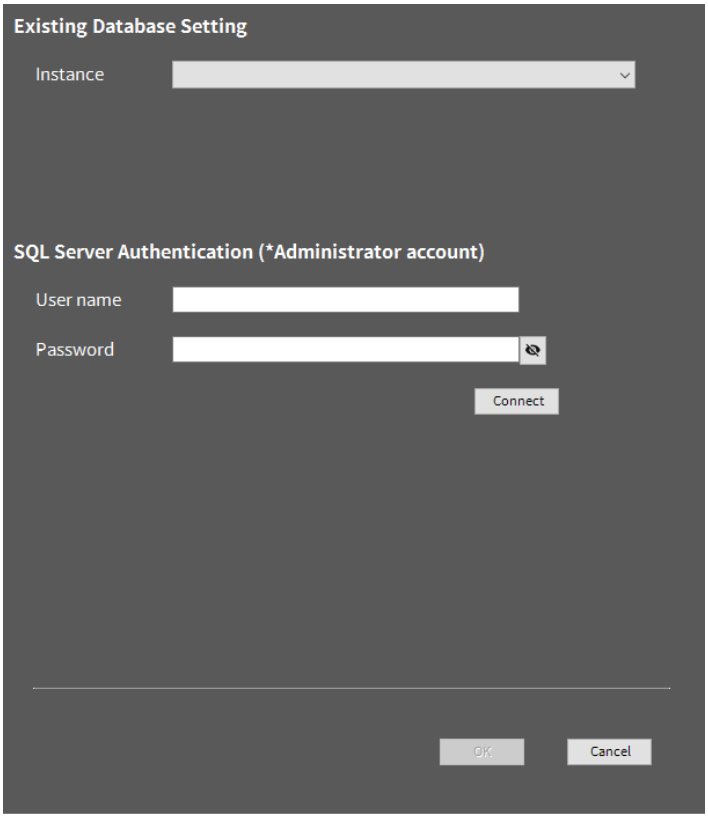


Note)

[Local Server]: Install the database on the PC where the installer is running.

[Network Server]: Install database on SQL server via TCP/IP.

For [Local Server]



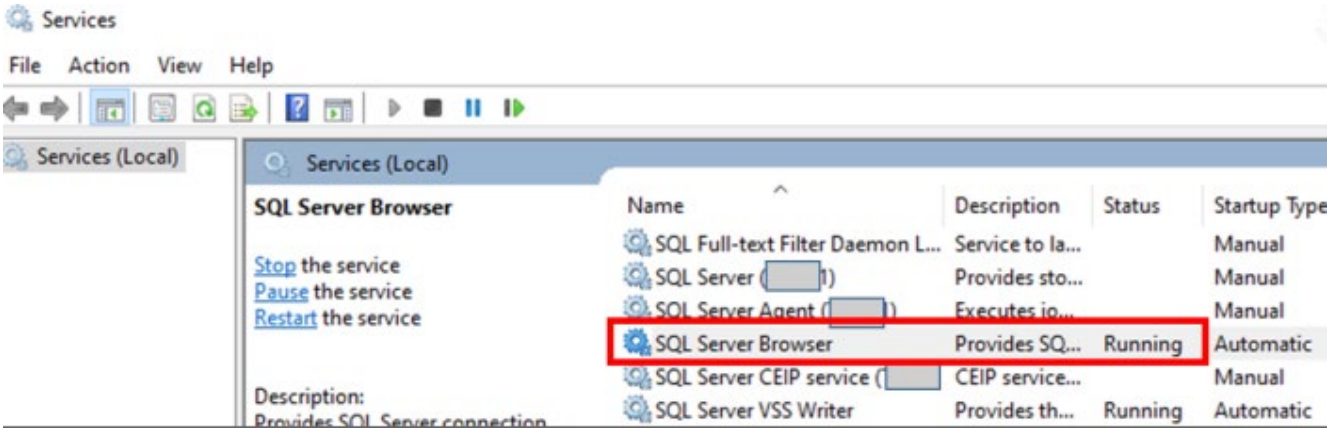
Select existing SQL Server instance, set administrator credentials and click [Connect].

If it shows success, click [OK].

For [Network Server]

There are two ways to use the SQL Server Browser or not.

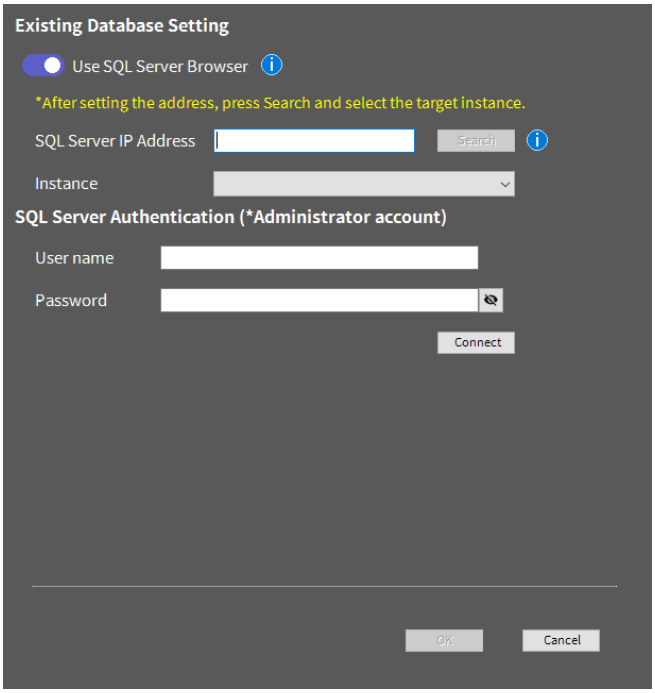
Confirm “SQL Server Browser” service status is Running or “Stopped”.



- When using SQL Server browser.

These ports need to be allowed from firewall configurations of the network server.

Port number	Protocol	Port usage
1434	UDP	Connection to SQL Server Browser
(instance port)	TCP	Connection to SQL server



[Use SQL Server Browser] is “On”.

Input [SQL Server IP Address] and click [Search].

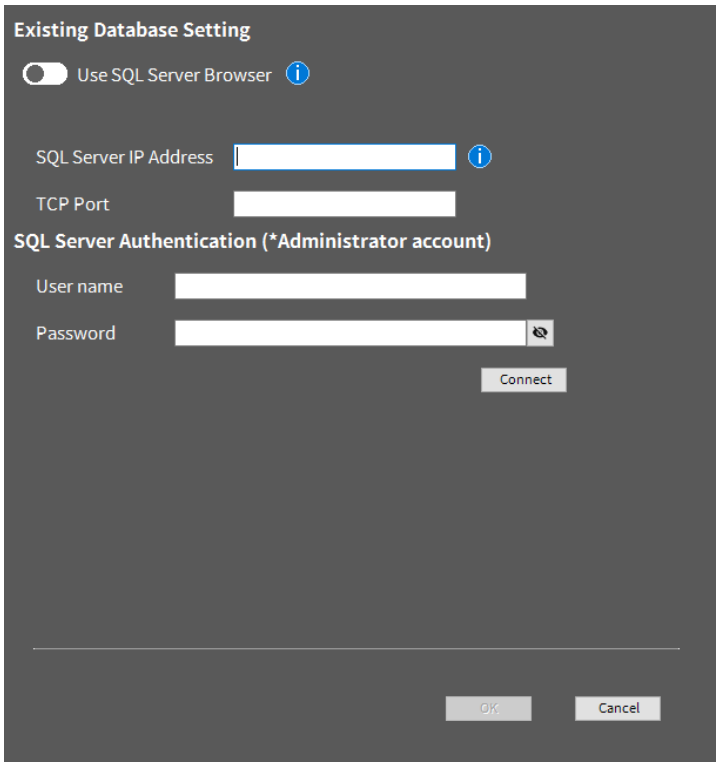
Select an instance from the Instance drop-down list, set administrator credentials and click [Connect].

If it shows success, click [OK].

- When not using SQL Server browser.

These ports need to be allowed from firewall configurations of the network server.

Port number	Protocol	Port usage
(instance port)	TCP	Connection to SQL server



[Use SQL Server Browser] is “Off”.
Input [SQL Server IP Address] and input [TCP Port].

Set administrator credentials and click [Connect].

If it shows success, click [OK].

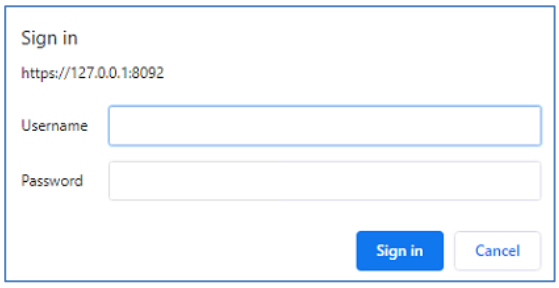
Note)
“Network Servers” can also specify FCI (failover cluster instances).
When using an FCI, input the IP address of the FCI in “SQL Server IP address”.

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.

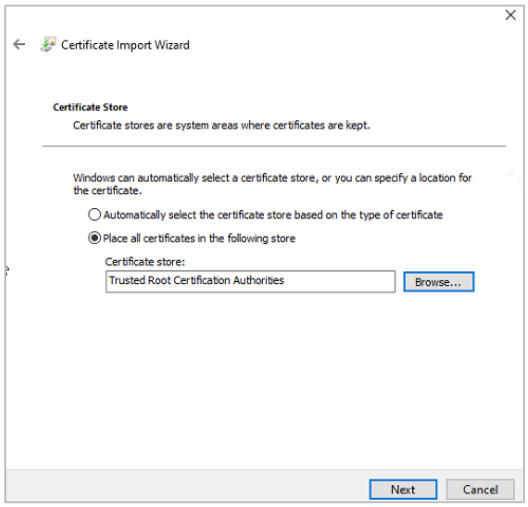
2) Double click the file and click “Install Certificate.”

3) Select “Local Machine” for Store Location

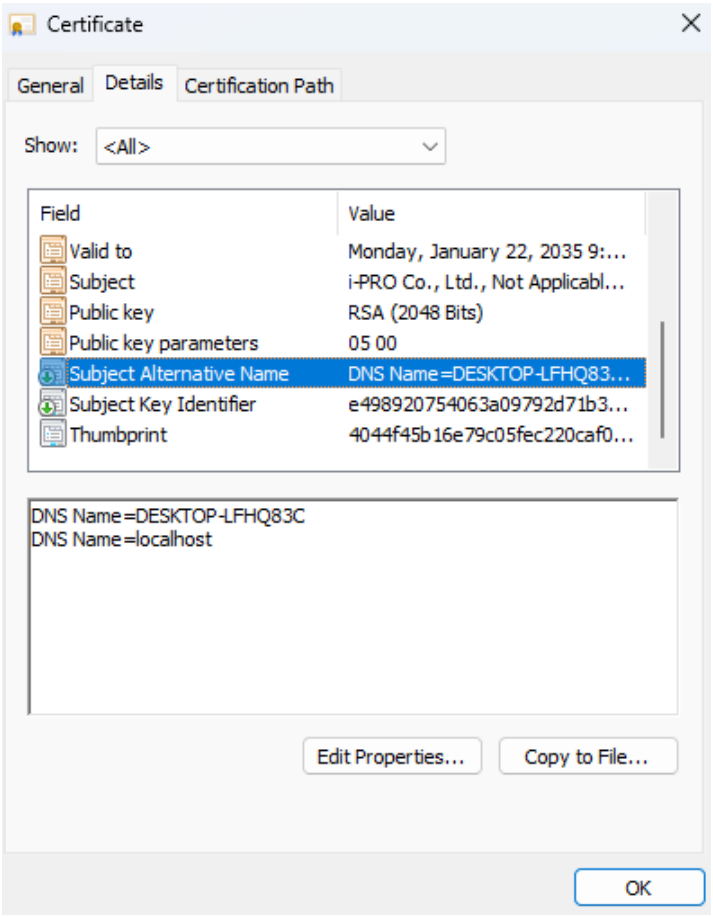
4) Select “Place all certificates in the following store and “Trusted Root Certification Authorities.”

Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.



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



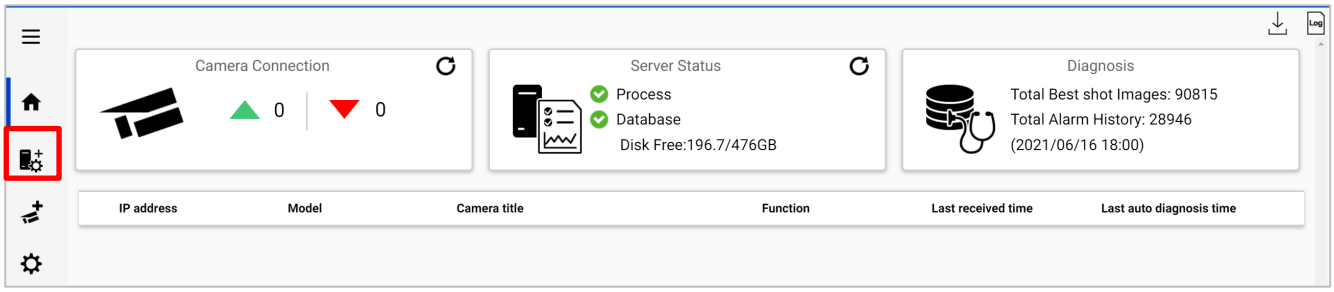
6) Open “C:¥Windows¥System32¥drivers¥etc¥hosts” and add IP address of i-PRO Active Guard server and xxxx (DNS Name that is not "localhost").

Ex) 192.168.0.125 DESKTOP-LFHQ83C

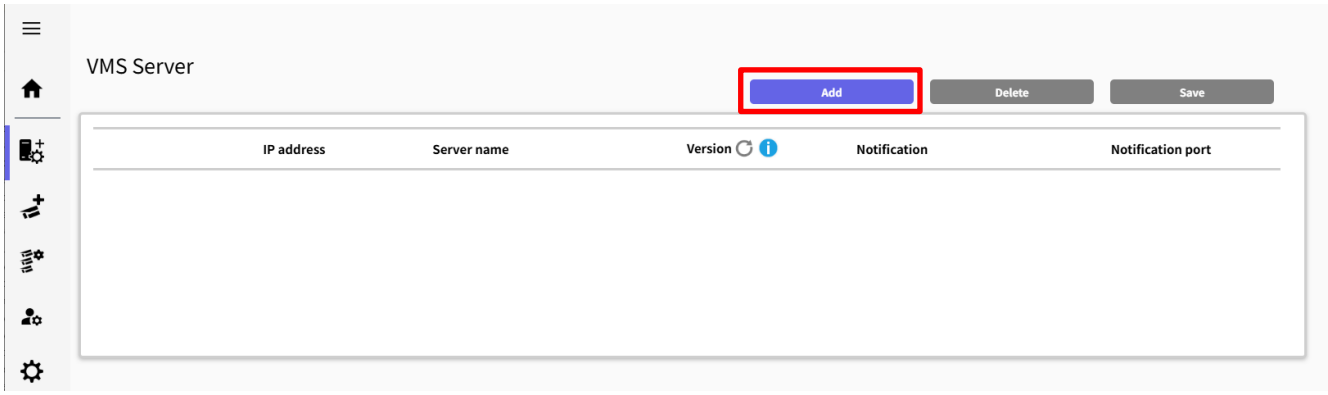
7) Access https://xxxx:8092 using web browser.

4.3.2.2. Register VMS

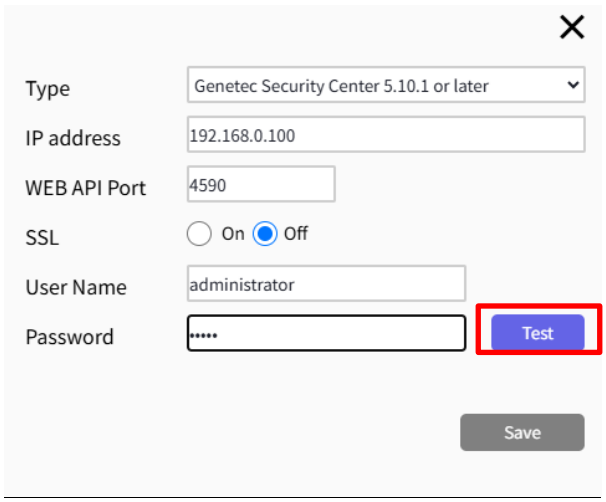
Click  (Register VMS)



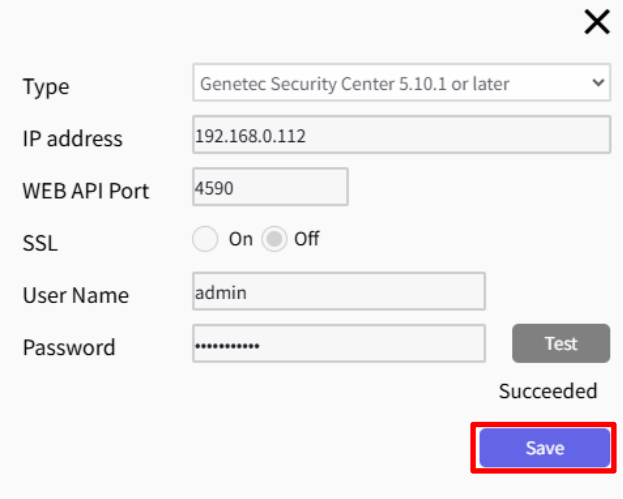
Click [Add]



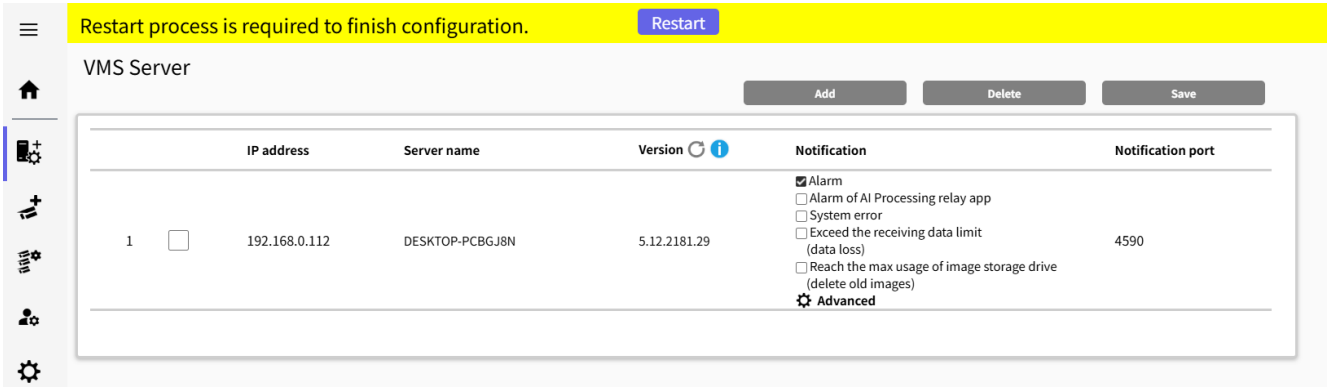
Input Security Center's information and click Test.



When Succeeded is shown, click Save.



Confirm VMS server is registered.



Note)

Restart button will appear on the top of screen, but you do not need click now.

You need to click Restart after completing all other configuration.

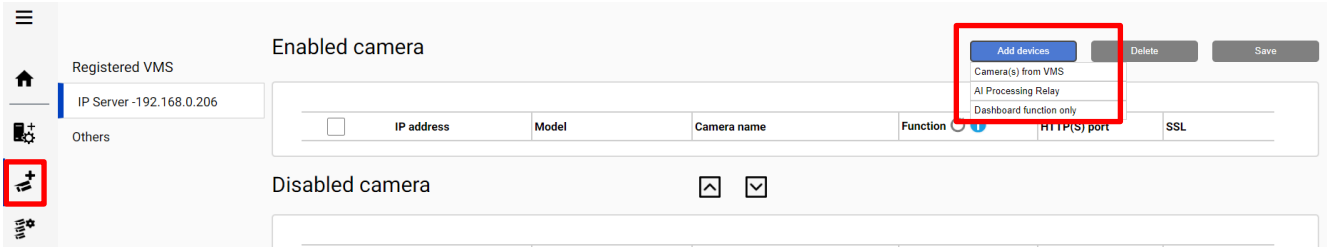
4.3.2.3. Register Cameras

Click  (Register Cameras)

Select [Add devices], and select camera registration method.

Click [Add devices] and select camera registration method.

- Camera(s) from VMS Please refer to [4.3.2.3.1].
- AI Processing Relay Please refer to [4.3.2.3.2].
- Dashboard function only Please refer to [4.3.2.3.3].

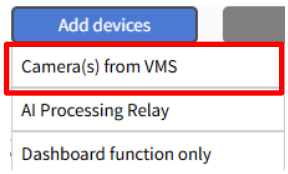


4.3.2.3.1. Camera(s) from VMS

Register the camera registered on the VMS to i-PRO Active Guard.

STEP1

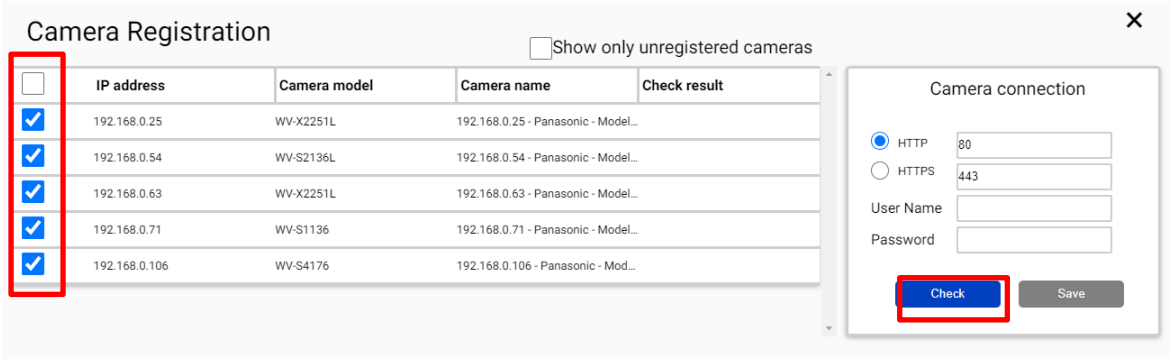
Click [Add devices] - [Camera(s) from VMS]



STEP2

All i-PRO cameras (including non-supported cameras) are shown.

Select cameras you want to register to i-PRO Active Guard, input camera's credentials and click [Check].



Note)

When a lot of cameras are registered on VMS Server, it may take time. (Maximum 900 seconds)

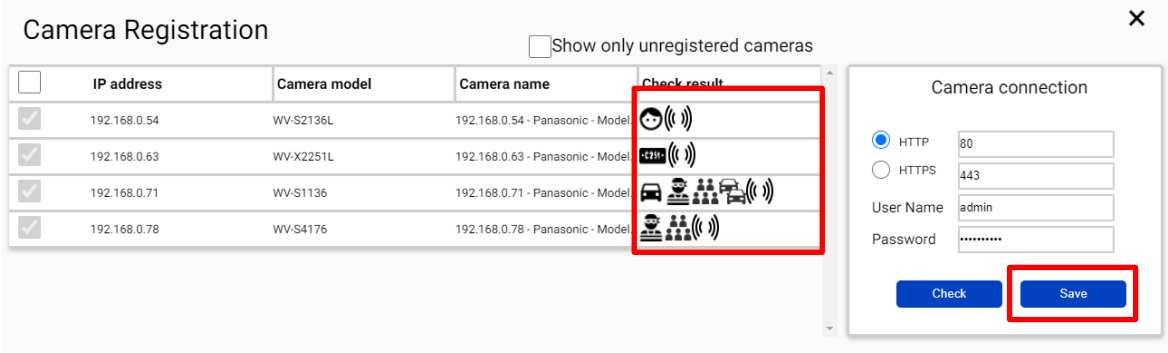
Camera can be sorted by [IP address], [Camera Type] or [Camera Name].

Unregistered cameras can be filtered by checking [Show only unregistered cameras].

STEP3

Icon related to AI function is shown for supported AI cameras.

Click [Save].

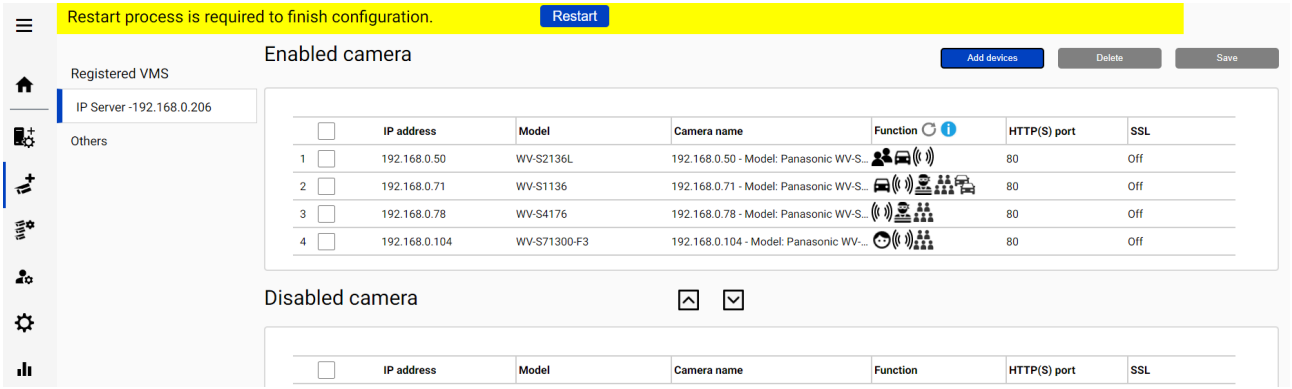


Note)

For information about icons, please refer to [4.3.2.3.4].

STEP4

Confirm cameras are registered.



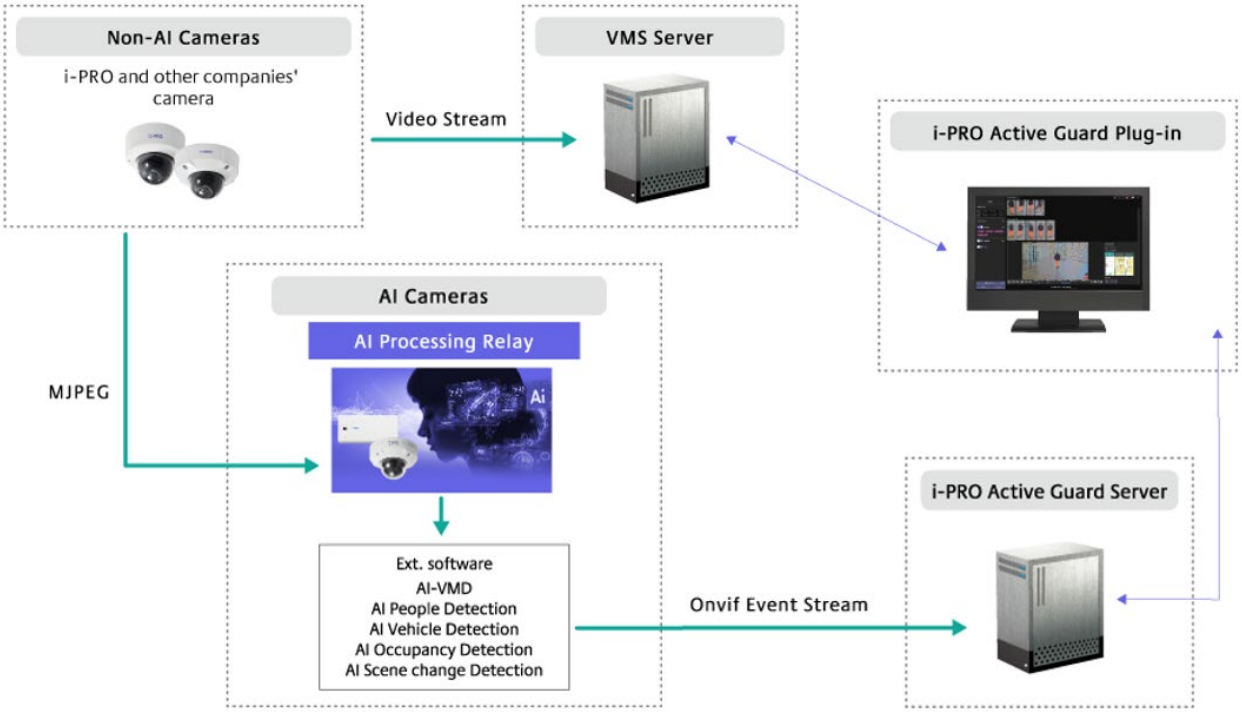
Note)

If multiple VMS are registered, it is necessary to register cameras by selecting each VMS from [Registered VMS] and [Add devices] - [Camera(s) from VMS].

4.3.2.3.2. AI Processing Relay

Register camera with AI Processing Relay application to i-PRO Active Guard.

[Overview of AI Processing Relay]



To use AI Processing Relay, you need to configure the AI camera, AI Processing Relay application, VMS Server, and i-PRO Active Guard. For details, please refer to each manual.

i-PRO Configuration Tool (iCT) version V4.20 or later is required for configuration.
Download iCT from the following link.
https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/knowledge-base/product-tips/active-guard-links

STEP1

(Setting target: AI camera and AI Processing relay application)

*For detailed, please refer to the manual.
https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/knowledge-base/product-tips/active-guard-links

(1) Confirm the operating conditions of the AI Processing Relay application.
(2) Install AI Processing Relay application and extension software.
(3) Configure settings for non-AI cameras.
(4) Configure AI Processing Relay application.
(5) Configure extension software that works with AI Processing Relay application

STEP2

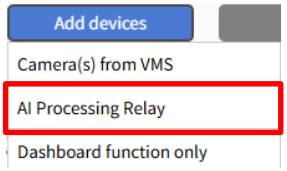
(Setting target: Security Center)

Register the non-AI camera set in step1-(3) to the Security Center.

STEP3

(Setting target: i-PRO Active Guard)

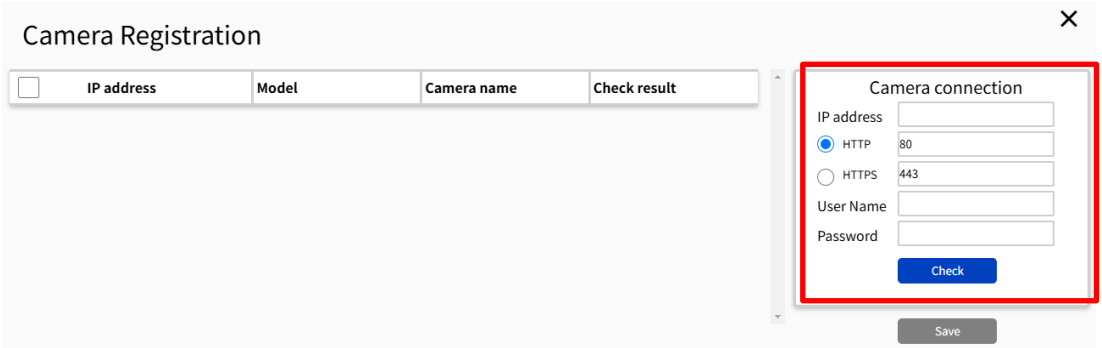
Click [Add devices] - [AI Processing Relay].



STEP4

(Setting target: i-PRO Active Guard)

Input the IP address and credentials of the AI camera to which have added AI Processing Relay App, click [Check].

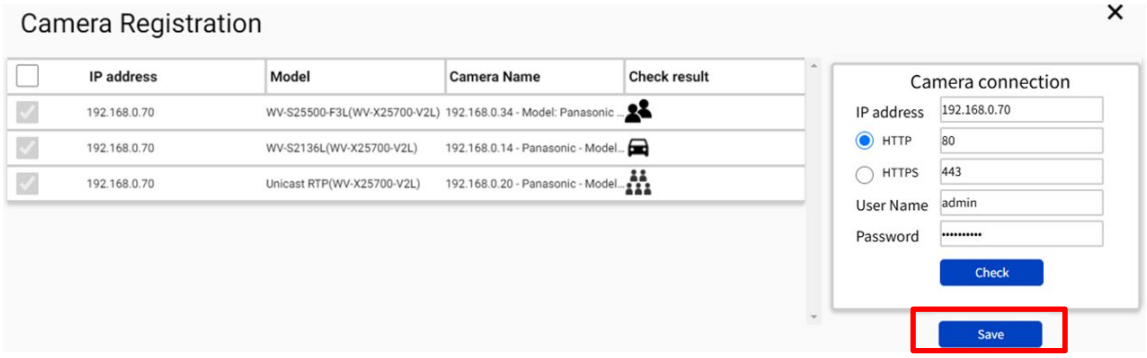


STEP5

(Setting target: i-PRO Active Guard)

Icon related to AI function is shown for supported AI cameras.

Click [Save].



Note)

- For information about icons, please refer to [4.3.2.3.4].
- Model in the camera list will be displayed as below.

"Non-AI camera model (AI camera model)"

ex) WV-S25500-F3L(WV-X25700-V2L)

↑ ↑

Non-AI camera AI camera with AI Processing Relay application

Important:

- If AI Processing Relay registration fails, please try the following steps.
  (1) Verify that the MAC address of the non-AI camera is displayed in the AI Processing Relay application settings using iCT.
  Non-AI camera whose MAC address is not displayed cannot be used in this system.
  (2) If MAC address is displayed, use iCT to reconfigure the AI processing relay application.

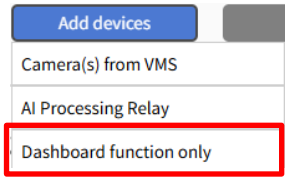
4.3.2.3.3. Dashboard function only

Register the camera to i-PRO Active Guard without registering camera to the VMS.

Cameras registered with this setting can only be used with the Dashboard function; they cannot be used with the i-PRO Active Guard plug-in.

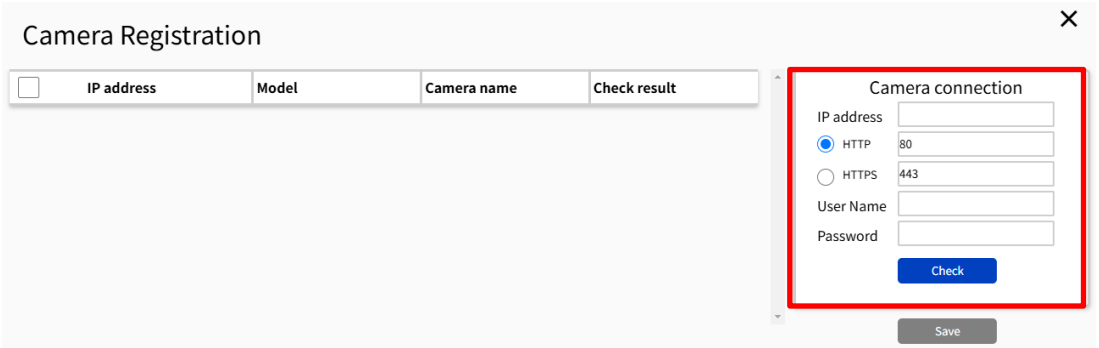
STEP1

Click [Add devices] - [Dashboard function only]



STEP2

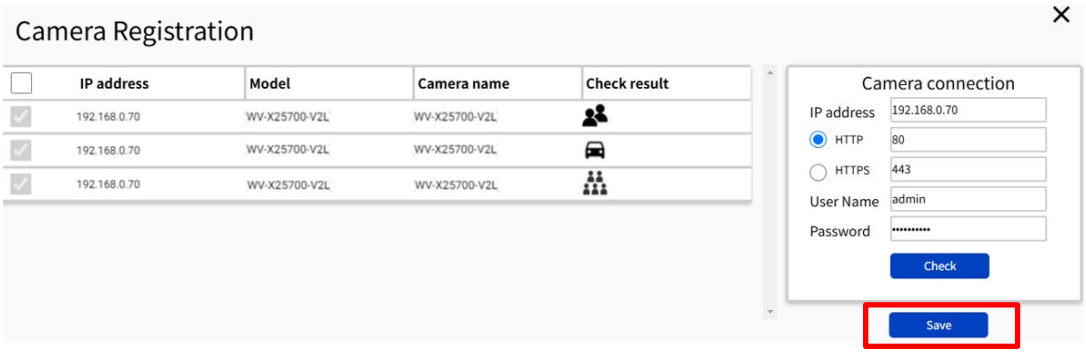
Enter IP address of the camera, credentials, click [Check].



STEP3

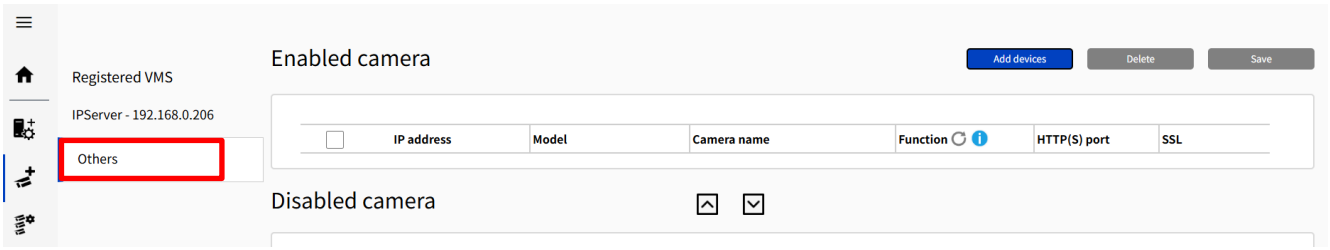
Icon related to AI function is shown for supported AI cameras.

Click [Save].



Note)

- For information about icons, please refer to [4.3.2.3.4].
- If you registered the camera from [Dashboard function only], select [Others] in [Registered VMS] and check the registration status.



4.3.2.3.4. AI function icon

 AI Face detection

 AI People detection

 AI Vehicle detection

 AI Video motion detection

 AI Sound detection

 AI Scene Change detection

 People Counting/Occupancy (*)

 Vehicle Counting

 On-site Learning Object Counting

 License plate detection

 Code detection

 Container detection

* The available functions differ depending on the installed application.

	Line Count	Area count	Heat map	Occupancy detection
WV-XAE200W	yes	-	yes	-
WV-XAE207W	-	yes	-	yes
WV-XAE300W	yes	yes	yes	yes

4.3.3. Restart process to apply changes

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

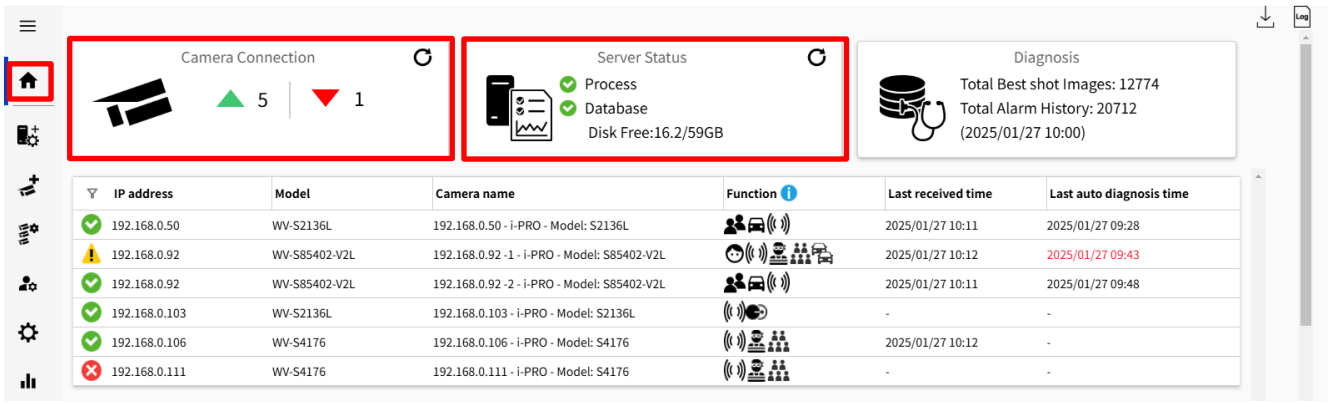
When you finish all configurations, click “Restart” from display bar above or Home screen.

4.3.4. Check

Click (Home)

- Check camera connection

Check all registered cameras are connected.



means the number of cameras connected.

(Meta data session between camera and i-PRO Active Guard server).

means the number of cameras disconnected.

When disconnection is detected, confirm network connection to camera.

- Check Server status

Check Process and Database shows status green.

Note)

When using existing SQL Server instance on network, Database shows status .

4.3.5. System configuration (optional)

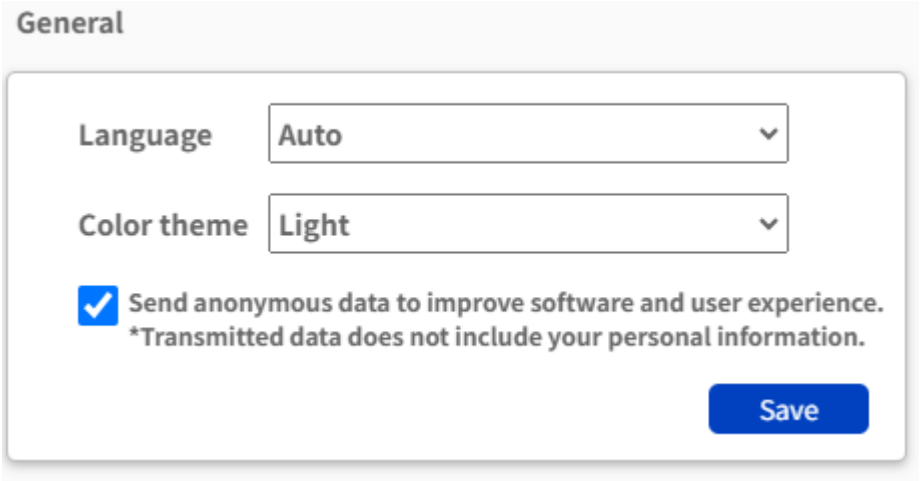
Click ⚙ (Configure system) and change settings if needed.

4.3.5.1. General

Language : Select [Auto], [English] or [Japanese]. (Default: Auto).
*When the language configuration for web browser is other than English or Japanese, English is shown.

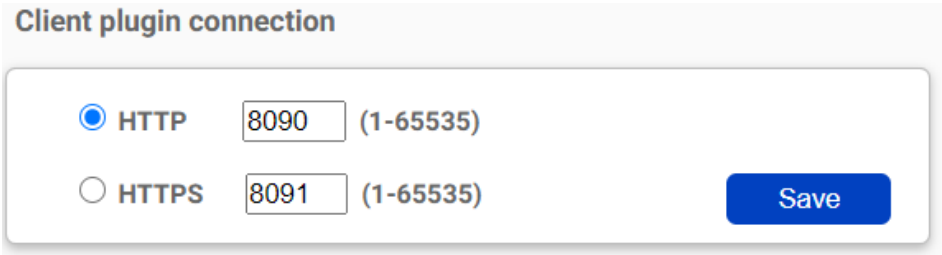
Color theme : Select [Light] or [Dark] for. (Default: Light).

Send anonymous data to improve software and user experience : Check or uncheck.
(Default: Set by install tool at 4.3.1)



4.3.5.2. Client Plug-in connection

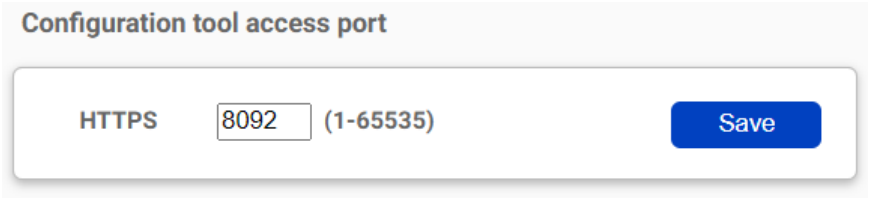
Select [HTTP] or [HTTPS] and port number (Default: Set by install tool at 4.3.1)



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 4.3.3, you need to access https://<ip>:<port> using new port number. Make a note not to forget.

4.3.5.4. Database

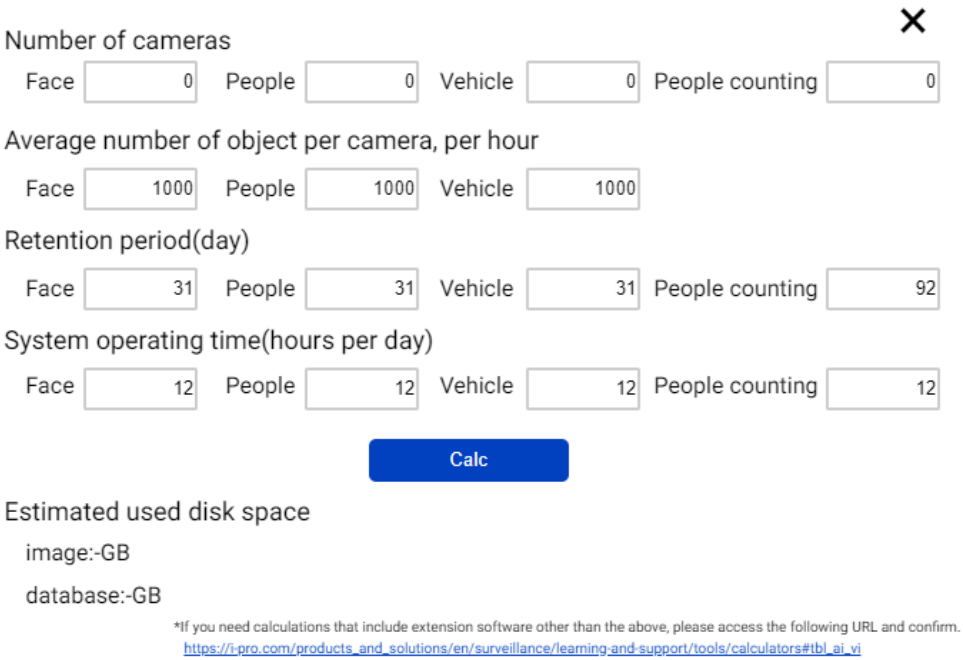
Configuration item	Comment
Storing images in database	All data(default): Store all data including images. Only alarm and statistics data: Store only alarm and statistics data Only statistics data: Store only statistics data
License plate number	Enable/Disable can be configured. (Default: Enable) Sets whether to store the license plate number in SQL Server.
Retention period	[For face images, people images, vehicle images, license plate images, code images, container images and alarm history] Using SQL Server Express Edition :1 – 31 days (Default: 31). Using SQL Server Standard Edition or higher:1 – 397 days (Default: 397). [For Count/ heat map/ statistics] Using SQL Server Express Edition :1 – 92 days (Default: 92). Using SQL Server Standard Edition or higher:1 – 732 days (Default: 732). 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 counting data expires, the data will be deleted from SQL server but automatically backed up as CSV file. Note) When enable, [Max usage of image storage drive] will be also enabled automatically. **Important:** ・ Statistics data in CSV backup files cannot be used on dashboard by itself. This data can be used only in comparison view and 1 day duration. * When [Comparison] is checked, and the [Display Duration] is selected for 1 day in Search Mode. ・ CSV is not available in the dashboard when using existing SQL Server instance on network server.

Configuration item	Comment
Max usage of image storage drive (*)	Enable/Disable and data size 10- 2000 (GB) can be configured. (Default: Disable) Note) When enabled, the used disk space of drive for storing best shot images exceed the setting value, the 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.
SQL Server data save path	SQL Server data save path is shown set by install tool at 4.3.1. You cannot change this after installation.
Estimated data points of detections (per sec)	50 -300 (Default: 100) *For people, 1 object is counted as 2 data points. For other objects, 1 object is counted as 1 data point. Note) If the number of object data from all cameras exceeds 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.

Estimated used disk space is shown.



Note)

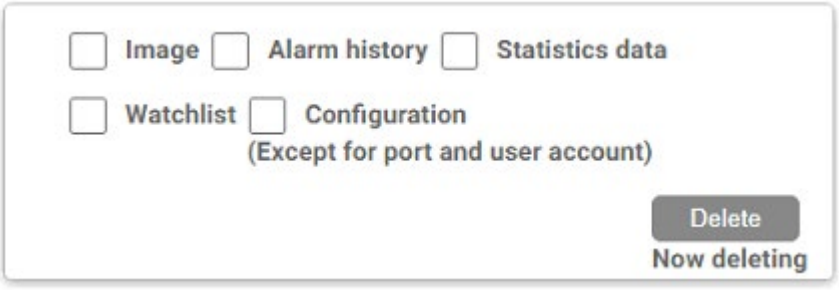
Estimated used disk space is just a reference. Actual data size highly depends on actual environment.

4.3.5.5. Initialization

Image: delete all best shot images.
Alarm history: delete all alarm history.
Statistics data: delete statistics data including heat map data.
Watchlist: delete all Faces watchlist, People watchlist, Vehicles watchlist, LPR watchlist (also registered license plate and group), OCR watchlist (also registered OCR Code and group) and Container watchlist (also registered container code and group). See the operation manual about watchlist.
Configuration: delete all registration data (VMS, Camera, and logs) except for port and user account.

Note)

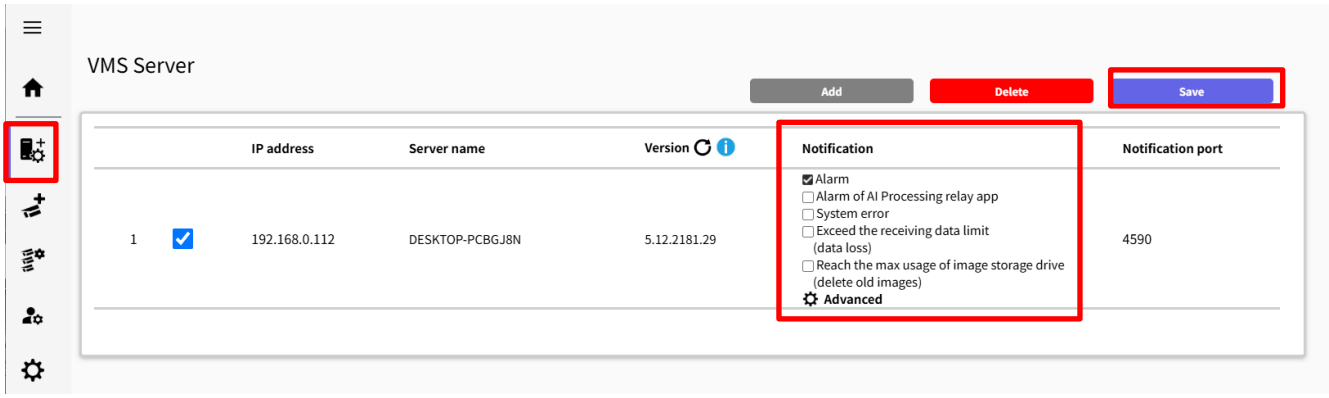
It may take time to delete images depending on the number of images. When deleting, the button will be as follows. Please update the page to confirm the latest status.



4.3.6. Notification to VMS Server (optional)

Some alarms and notification related to i-PRO Active Guard server failure can be enabled.
Actions on VMS side also can be configured (4.7 Custom alarm setup (optional))

Click  (Register VMS)



Check the following items that you want and [Save].

Alarm of AI Processing relay app

Notifies alarm of AI Processing relay app received by i-PRO Active Guard server.

System error

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

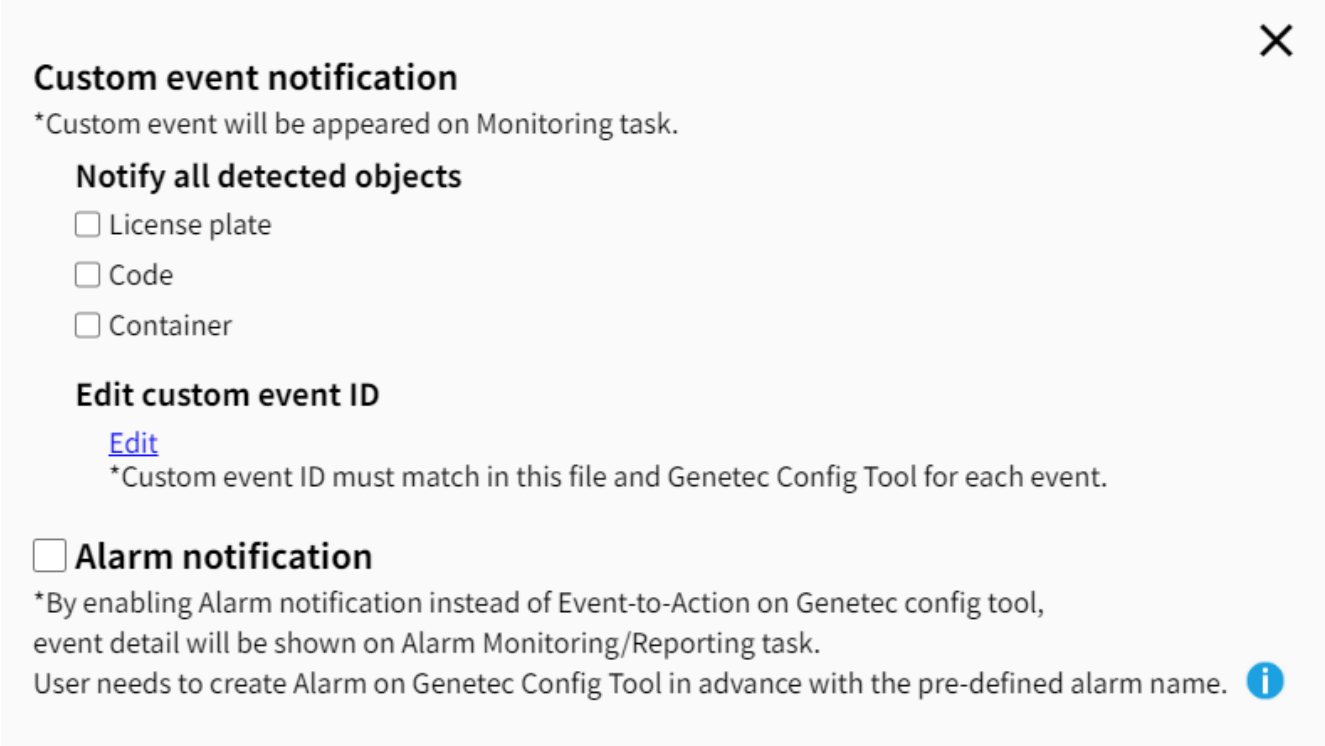
Exceed the receiving data limit (data loss)

Notification 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 disk space of image (delete old images)

Notification 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.

Advanced



Custom event notification

Configure settings related to custom events to be notified to Monitoring tasks.

Notify all detected objects

License plates

Notifies all detected license plates received by the i-PRO Active Guard server.

Code

Notifies all detected code received by the i-PRO Active Guard server.

Container

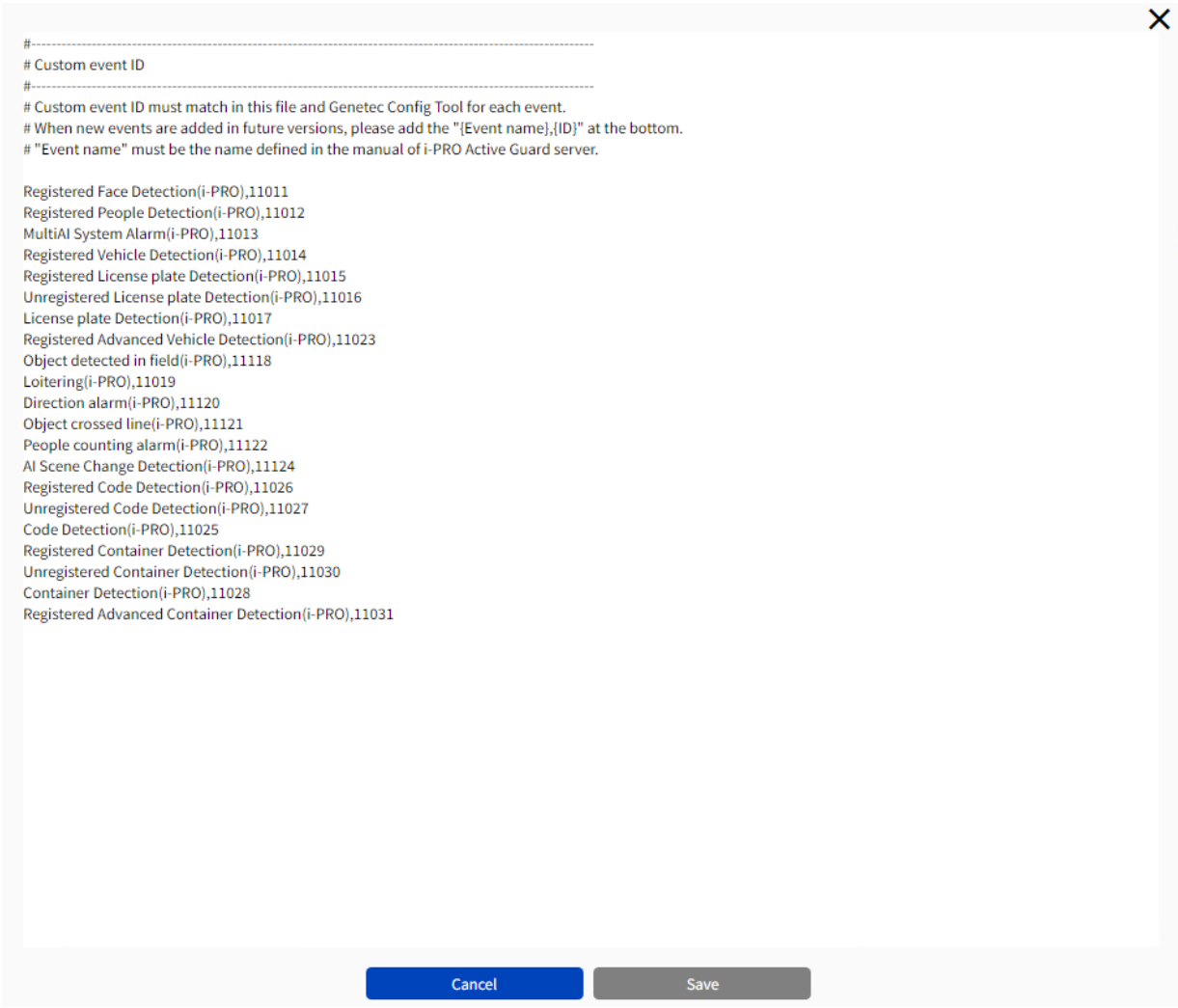
Notifies all detected container received by the i-PRO Active Guard server.

Edit custom event ID

Custom event ID can be edited.

Custom event ID must match in this setting and Genetec Config Tool. See 4.7.

“Event name” must match the list in Chapter 4.7.

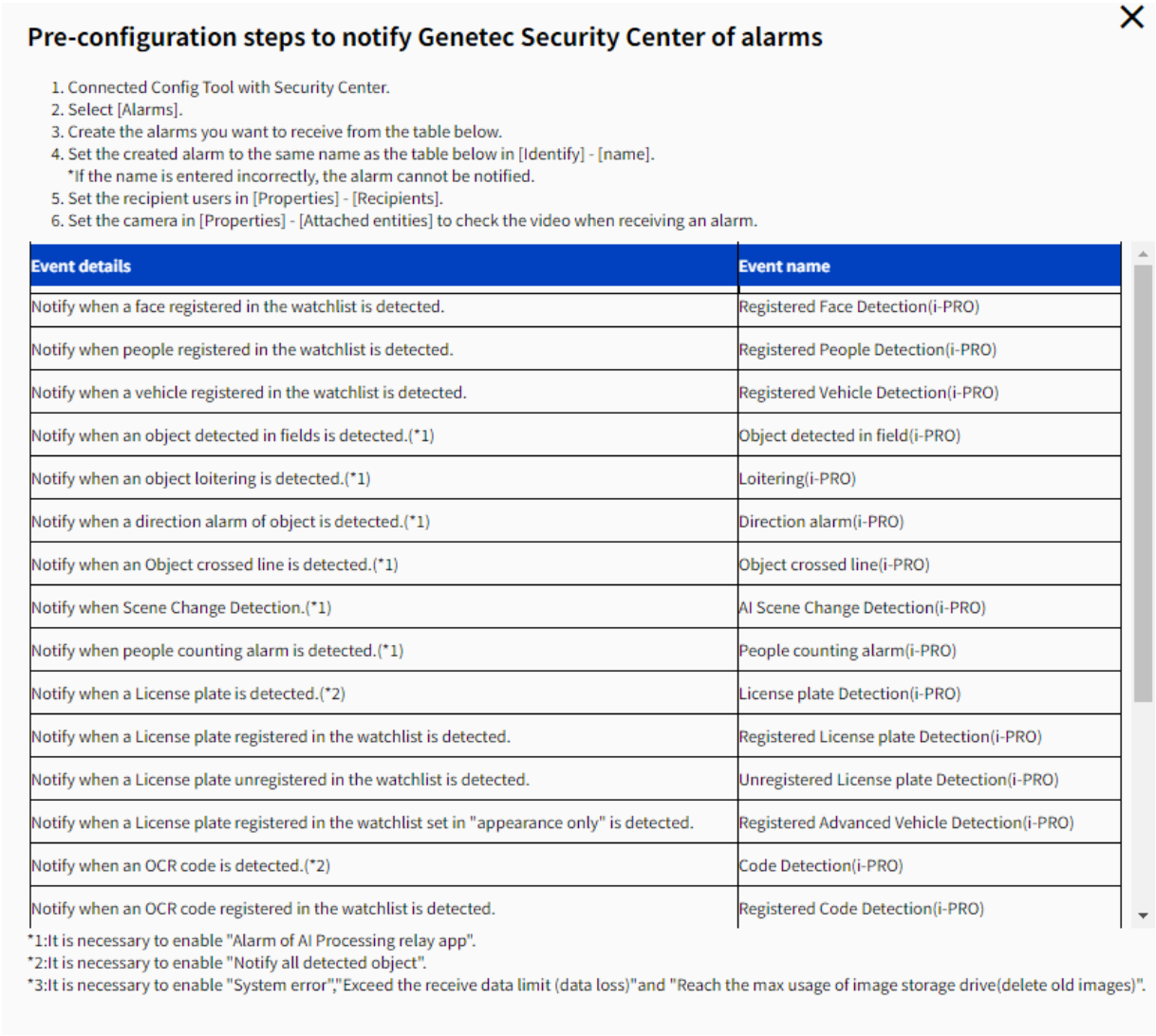


Note)

Customize can only be set when you log in from the PC on which the Active Guard server is installed.

Alarm notification

By enabling Alarm notification instead of Event-to-Action on Genetec config tool,
event detail will be shown on Alarm Monitoring/Reporting task.
Beforehand, users must configure create alarms and alarm reception settings with the Genetec Config Tool. See icon in web setting screen.



Pre-configuration steps to notify Genetec Security Center of alarms

1. Connected Config Tool with Security Center.
2. Select [Alarms].
3. Create the alarms you want to receive from the table below.
4. Set the created alarm to the same name as the table below in [Identify] - [name].
   *If the name is entered incorrectly, the alarm cannot be notified.
5. Set the recipient users in [Properties] - [Recipients].
6. Set the camera in [Properties] - [Attached entities] to check the video when receiving an alarm.

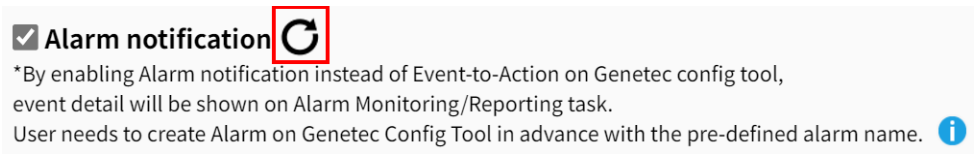
Event details	Event name
Notify when a face registered in the watchlist is detected.	Registered Face Detection(i-PRO)
Notify when people registered in the watchlist is detected.	Registered People Detection(i-PRO)
Notify when a vehicle registered in the watchlist is detected.	Registered Vehicle Detection(i-PRO)
Notify when an object detected in fields is detected.(*1)	Object detected in field(i-PRO)
Notify when an object loitering is detected.(*1)	Loitering(i-PRO)
Notify when a direction alarm of object is detected.(*1)	Direction alarm(i-PRO)
Notify when an Object crossed line is detected.(*1)	Object crossed line(i-PRO)
Notify when Scene Change Detection.(*1)	AI Scene Change Detection(i-PRO)
Notify when people counting alarm is detected.(*1)	People counting alarm(i-PRO)
Notify when a License plate is detected.(*2)	License plate Detection(i-PRO)
Notify when a License plate registered in the watchlist is detected.	Registered License plate Detection(i-PRO)
Notify when a License plate unregistered in the watchlist is detected.	Unregistered License plate Detection(i-PRO)
Notify when a License plate registered in the watchlist set in "appearance only" is detected.	Registered Advanced Vehicle Detection(i-PRO)
Notify when an OCR code is detected.(*2)	Code Detection(i-PRO)
Notify when an OCR code registered in the watchlist is detected.	Registered Code Detection(i-PRO)

*1:It is necessary to enable "Alarm of AI Processing relay app".
*2:It is necessary to enable "Notify all detected object".
*3:It is necessary to enable "System error","Exceed the receive data limit (data loss)"and "Reach the max usage of image storage drive(delete old images)".

Note)

If you have added/update alarms in Genetec Config Tool after enabling this setting, press the refresh (↻) button to update the alarms.

* Refresh button is only displayed when the setting is enabled.



Alarm notification ↻

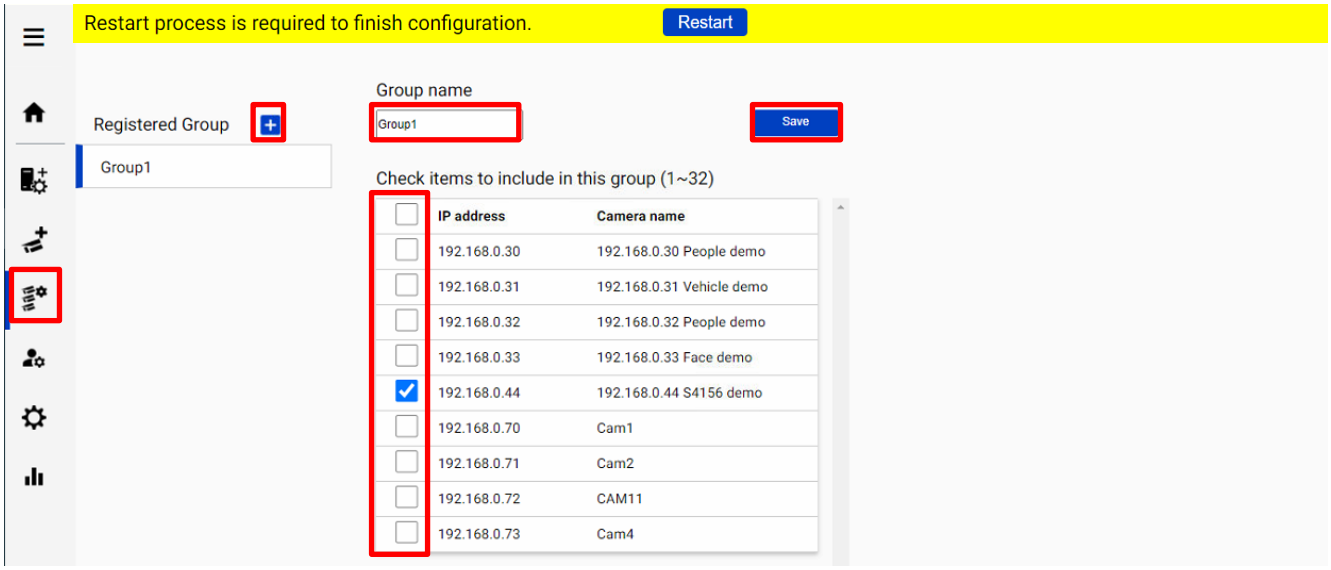
*By enabling Alarm notification instead of Event-to-Action on Genetec config tool,
event detail will be shown on Alarm Monitoring/Reporting task.
User needs to create Alarm on Genetec Config Tool in advance with the pre-defined alarm name.

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)

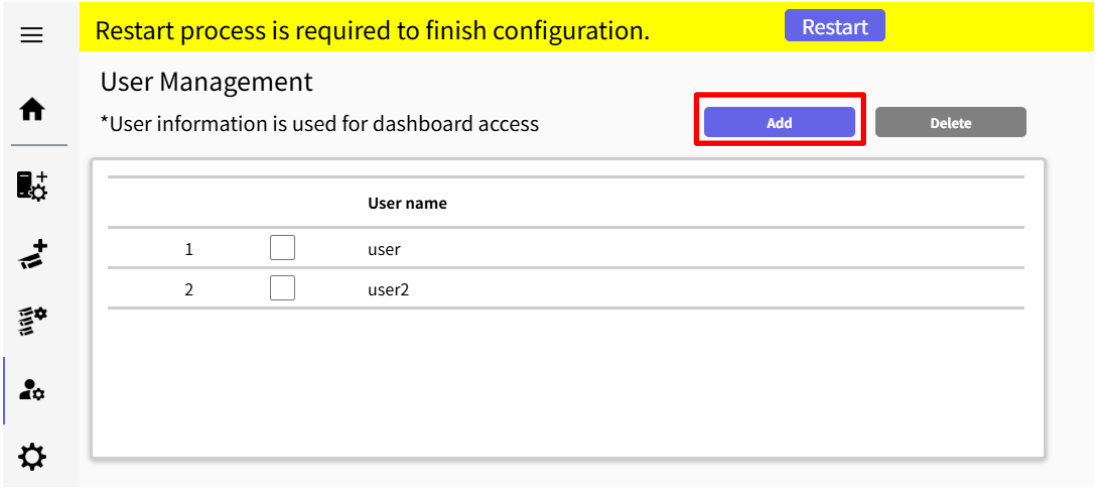
Up to 16 groups can be configured.

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

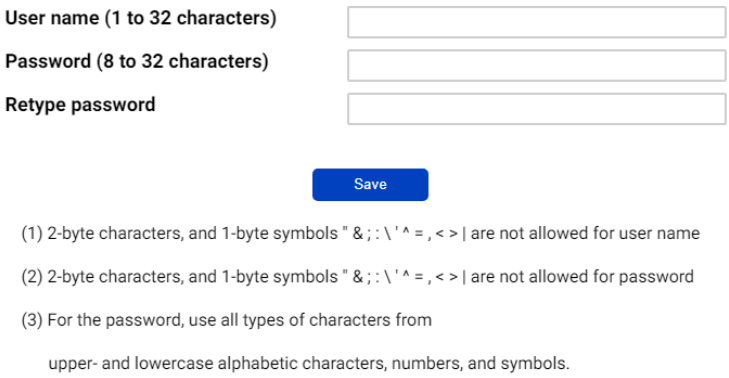
4.3.7.2. User Management

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)

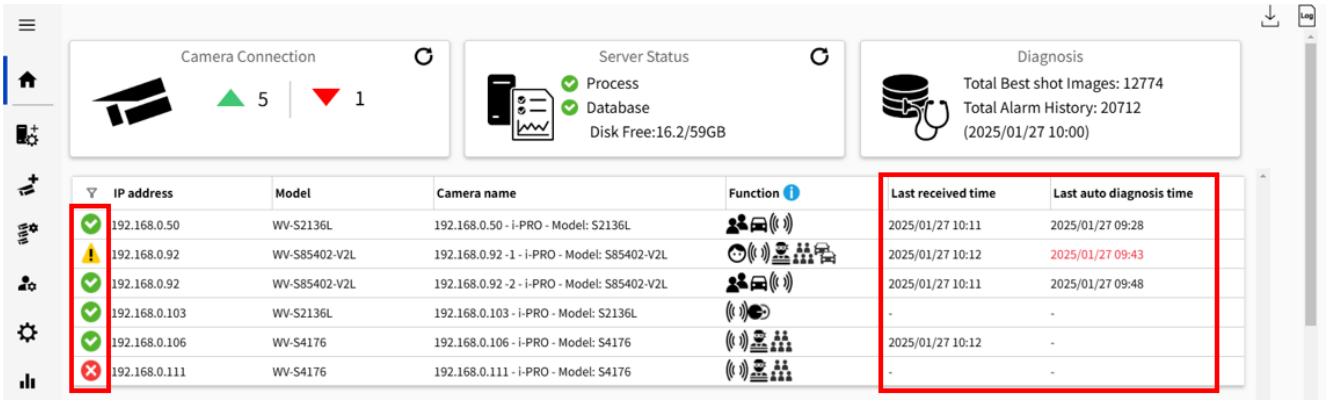
User information can also be used for Plug-in connection.

[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.

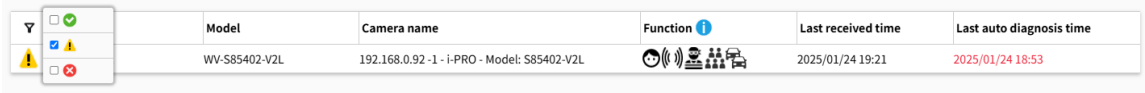
Metadata session is connected, but AI application on camera side may not work well. Check AI application on camera side is installed, schedule setting is on and also check whether “Last received time.”

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

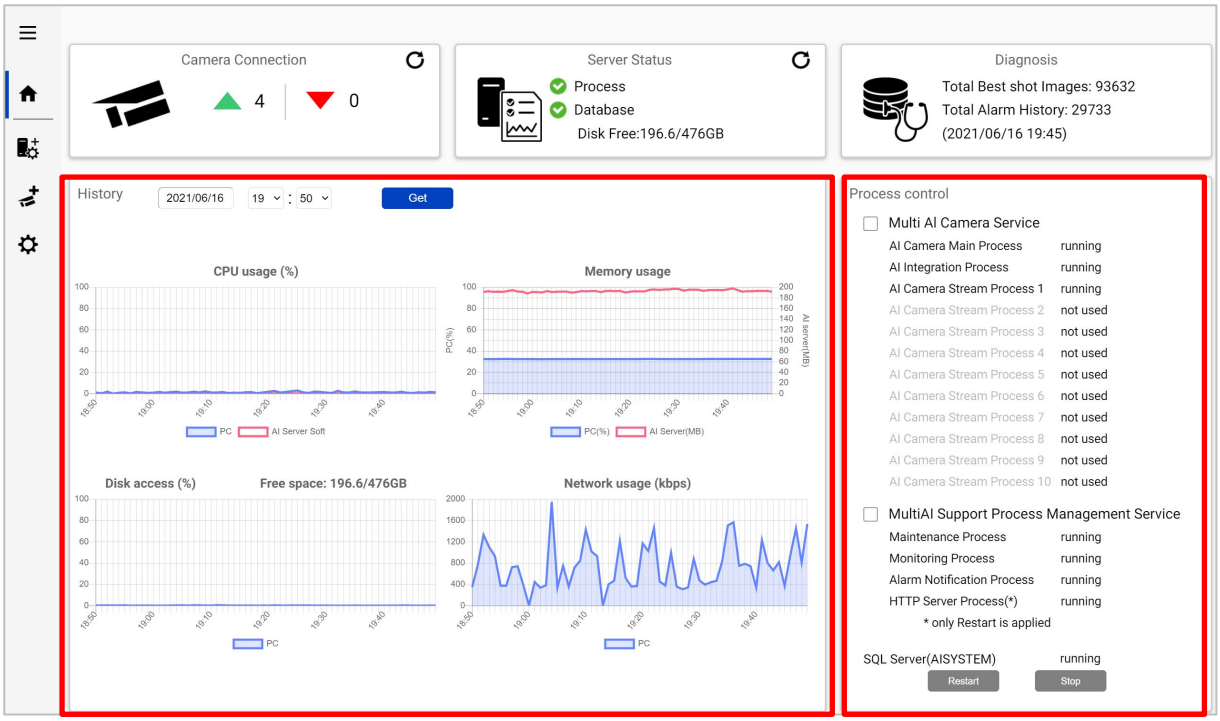
“**Last auto diagnosis time**” is the latest time when i-PRO Active Guard server tested connection to camera and database. The test executes every 5 minutes for a camera in order. When error occurs, the time is shown in red color. In that case, check Log and confirm the status of camera or database.

Note)

- When schedule setting for the AI application is off, last auto diagnosis will be failed. If it is intended, please ignore this indicator.
- icon allows filtering by camera connection.



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 the specified date is shown. Select the 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.

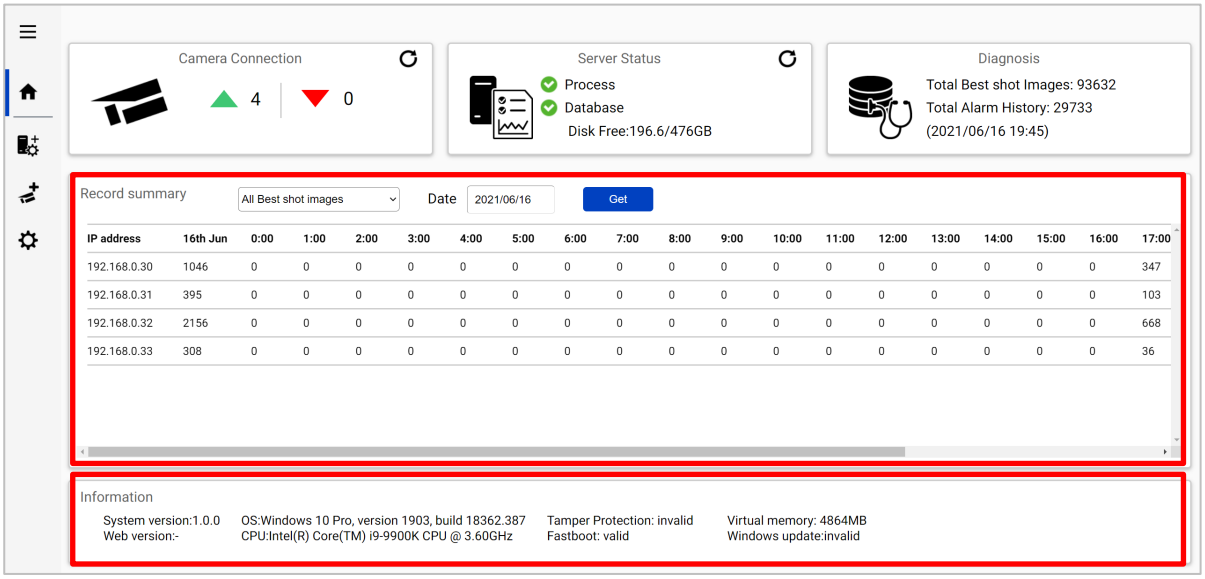
Process Control

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 “Support Process Management Service” are stopped (also see 5.6.1).
When investigation to system trouble is required, please check status, and try to restart.

Note)

When using existing SQL Server instance on network serve, SQL Server is not monitored.

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
- License plate images
- Code images
- Container images
- All alarm
- Registered face detection
- Registered people detection
- Registered vehicle detection
- Registered license plate detection (*1)
- Unregistered license plate detection (*1)
- Sound detection
- AI-VMD
- AI Occupancy detection
- AI Scene Change detection
- Registered code detection (*2)
- Unregistered code detection (*2)
- Registered container detection (*3)
- Unregistered container detection (*3)

(*1) About license plate detection.

- Registered license plate detection

  You will be notified when you set LPR watchlist to below settings on i-PRO Active Guard plug-in.

  - Set ”Detect by vehicle appearance only” to off,
    and set “Trigger” to “When license plates in the selected group was detected.”
  - Set ”Detect by vehicle appearance only” to on.

- Unregistered license plate detection

  You will be notified when you set LPR watchlist to below settings on i-PRO Active Guard plug-in.

  - Set ”Detect by vehicle appearance only” to off,
    and set “Trigger” to “When other license plate which is not in the selected group was detected.”

(*2) About code detection.

- Registered code detection

  You will be notified when you set OCR watchlist to below settings on i-PRO Active Guard plug-in.

  - Set “Trigger” to “When OCR Code in the selected group was detected.”

- Unregistered code detection

  You will be notified when you set OCR watchlist to below settings on i-PRO Active Guard plug-in.

  - Set “Trigger” to “When other OCR Code which is not in the selected group was detected.”

(*3) About container detection.

- Registered container detection

  You will be notified when you set Container watchlist to below settings on i-PRO Active Guard plug-in.

  - Set ”Detect by container details” to off, and set “Trigger” to “When Container code in the selected group was detected.”
  - Set ”Detect by container details” to on.

- Unregistered container detection

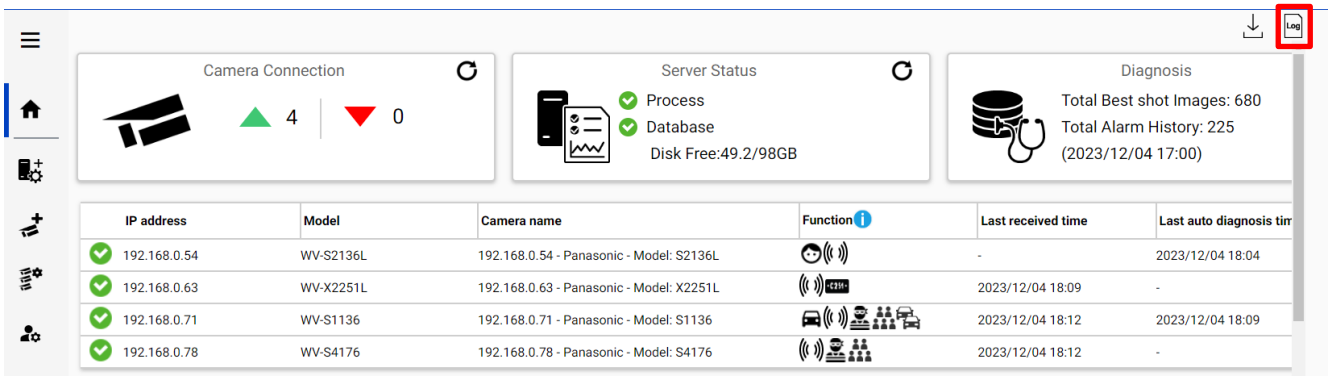
  You will be notified when you set Container watchlist to below settings on i-PRO Active Guard plug-in.

  - Set ”Detect by container details” to off,
    and set “Trigger” to “When other Container code which is not in the selected group was detected.”

Information

Software version, OS, windows configuration is shown.

4.3.8.4. Display log

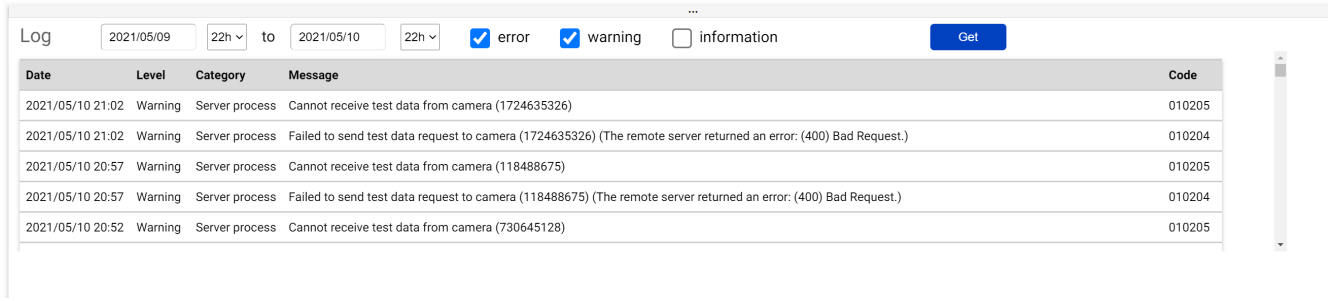


Click 

to show logs.

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

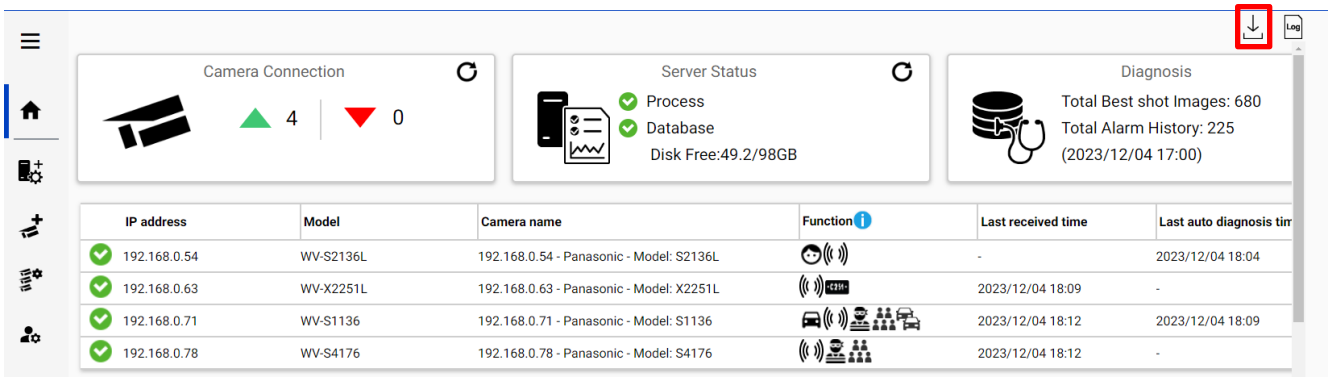
Detail for each message and troubleshoot for Code is shown on 6.Troubleshooting.



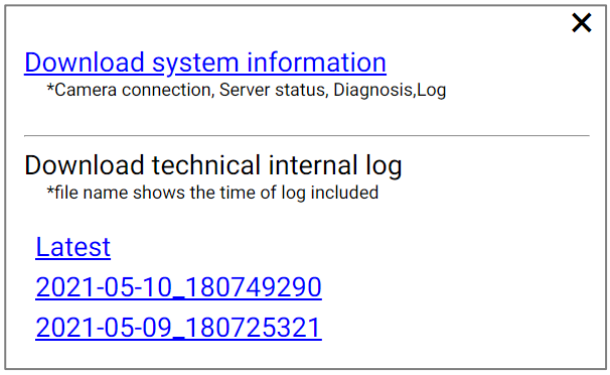
Note)

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 names “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 features.

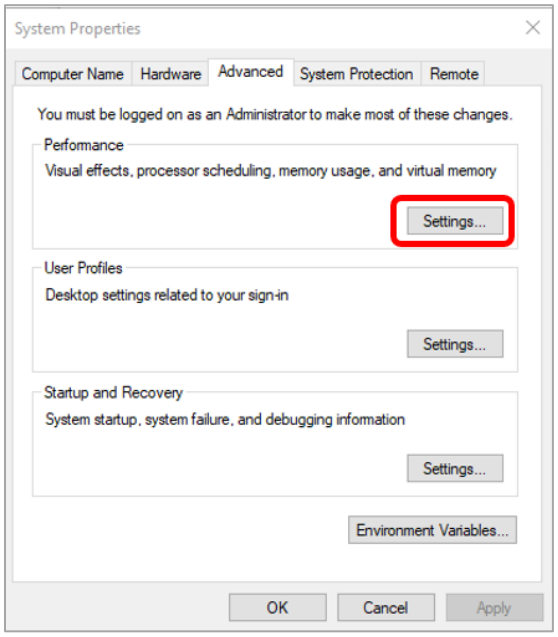
4.3.9.2. Disable Windows Update service

Windows updates are important to keep the system up to date, but auto update may require an unplanned restart, and a 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.

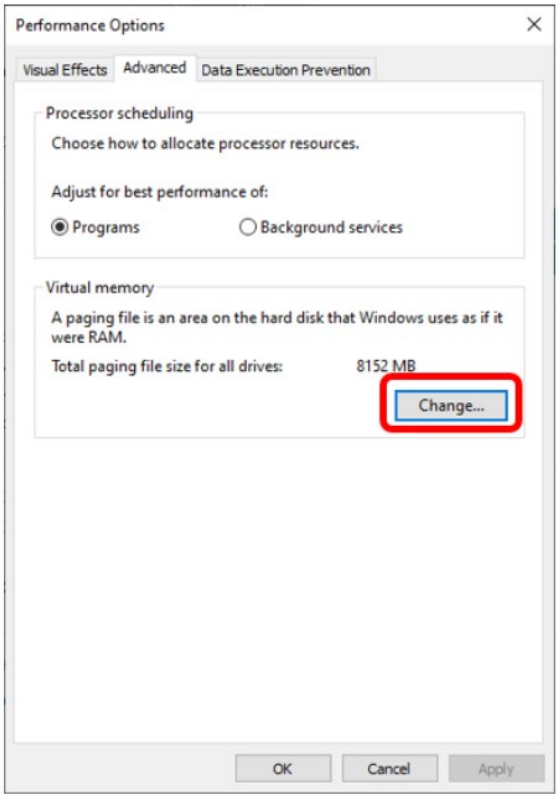
4.3.9.3. Virtual memory setting

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.

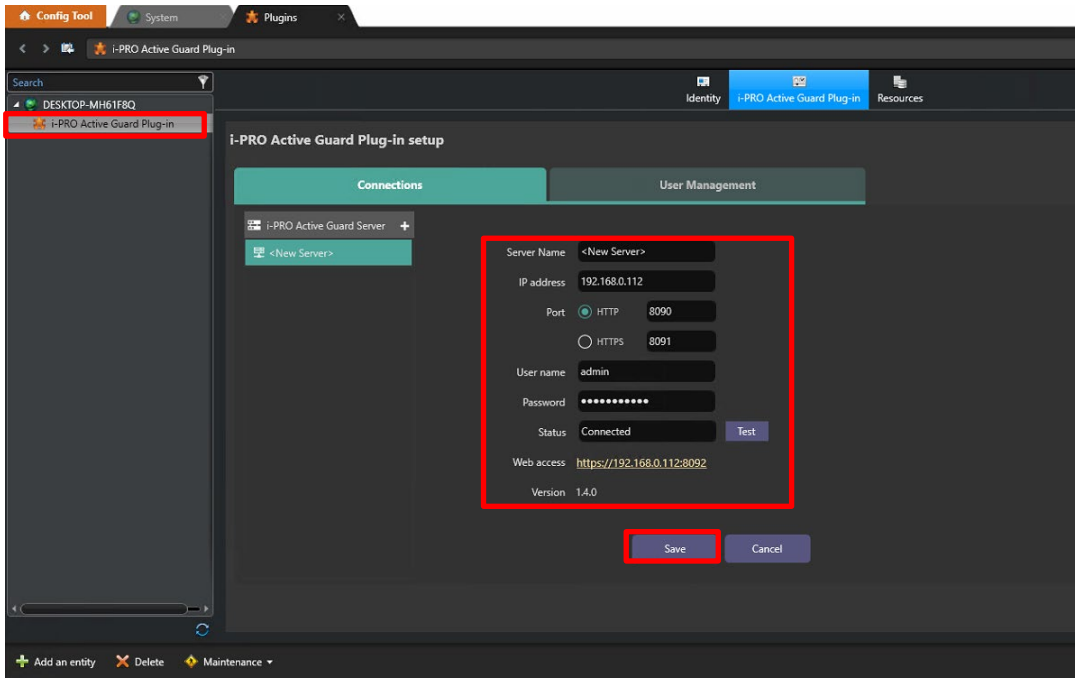
4.4. Install and setup Plug-in for Security Desk

4.4.1. Install Plug-in to Security Desk

Install Plug-in to PC that is Security Desk is installed referring to the section 4.2.2.1.

4.4.2. Connection to i-PRO Active Guard server

Connect Config Tool with Security Center. Select [Plugin], [i-PRO Active Guard Plugin].
Input Active Guard server information and Click [Test] and then click [Save].



Note)

If [i-PRO Active Guard Plugin] is not displayed, please restart Config Tool.

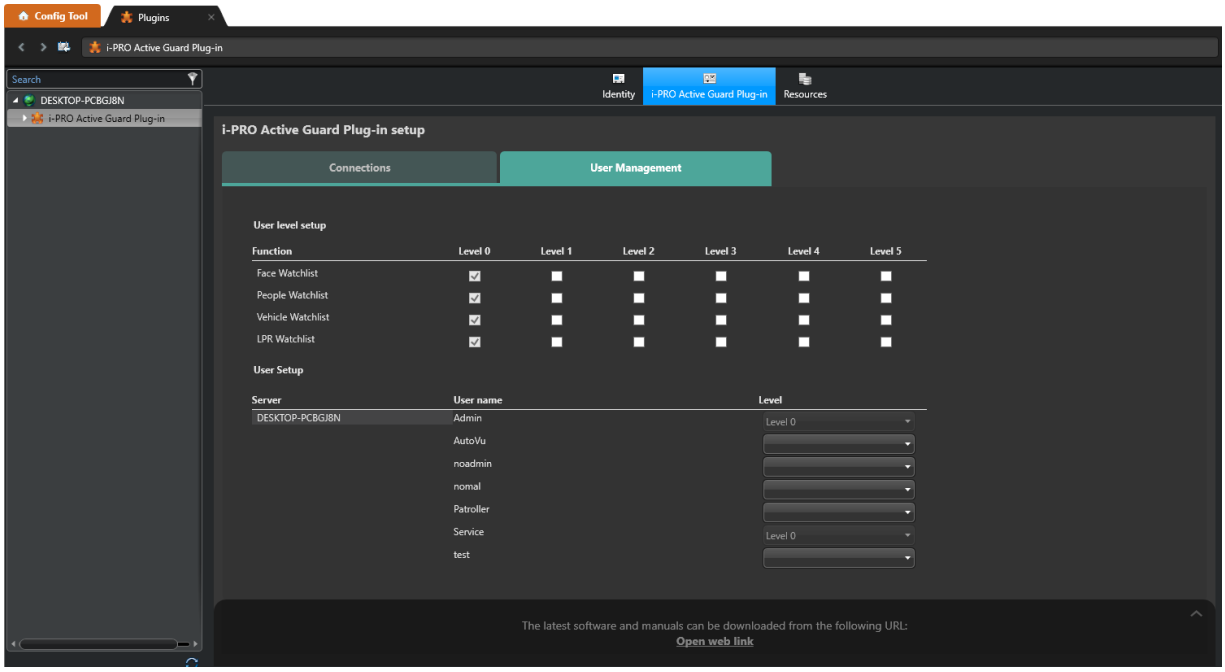
If Test failed, please check if credential is correct.

4.4.3. User Management (Optional)

4.4.3.1. Privileges for plug-in specific function

Configure User Management for access to watchlist such as [Face Watchlist], [People Watchlist], [Vehicle Watchlist], etc.

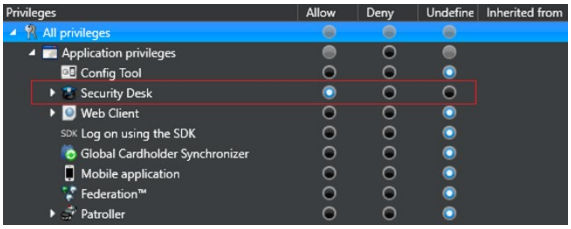
You need to also configure User settings ([Config Tool]- [User management] - [Privileges]) for not administrators to user watchlist.



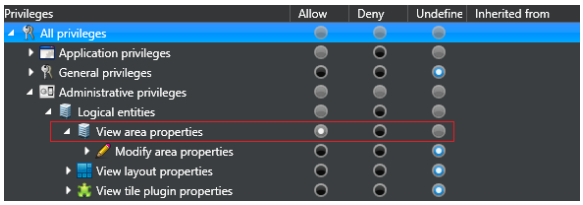
Required privileges to use plugin for non-administrator

If non-administrator uses this software, the following privileges be set to [Allow].

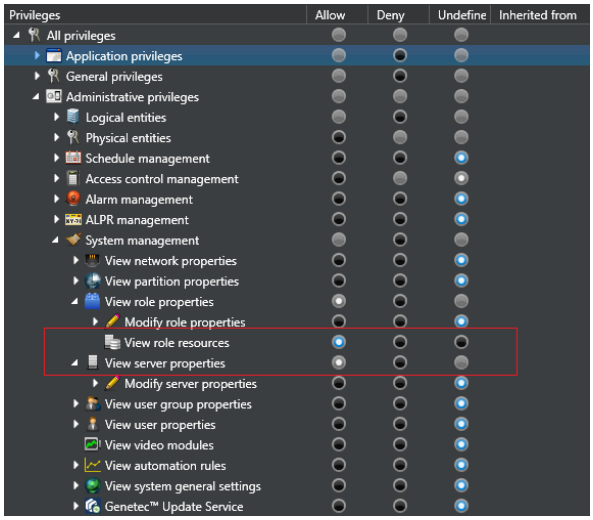
- [Application privileges] – [Security Desk]



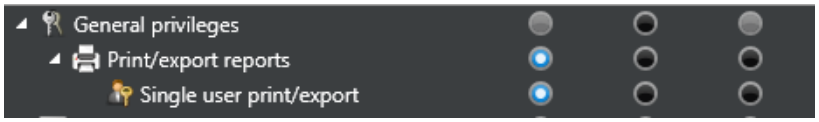
- [Administrative privileges] – [Logical entities] – [View area properties]



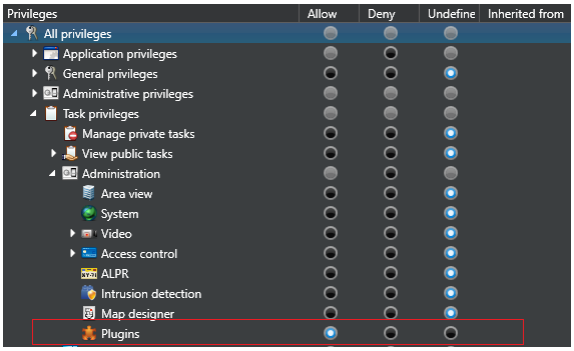
- [Administrative privileges] – [System management] – [View role properties] – [View server properties]



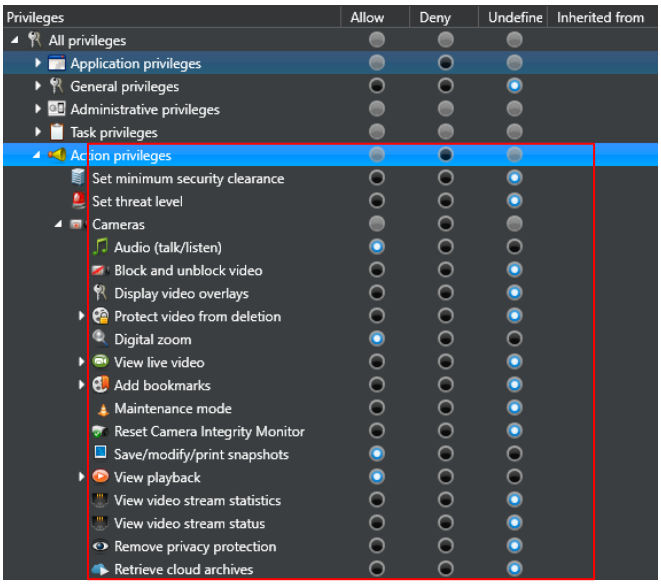
- [General privileges] – [Print/export reports] – [Single user print/export]



- [Task privileges] – [Administration] – [Plugins]

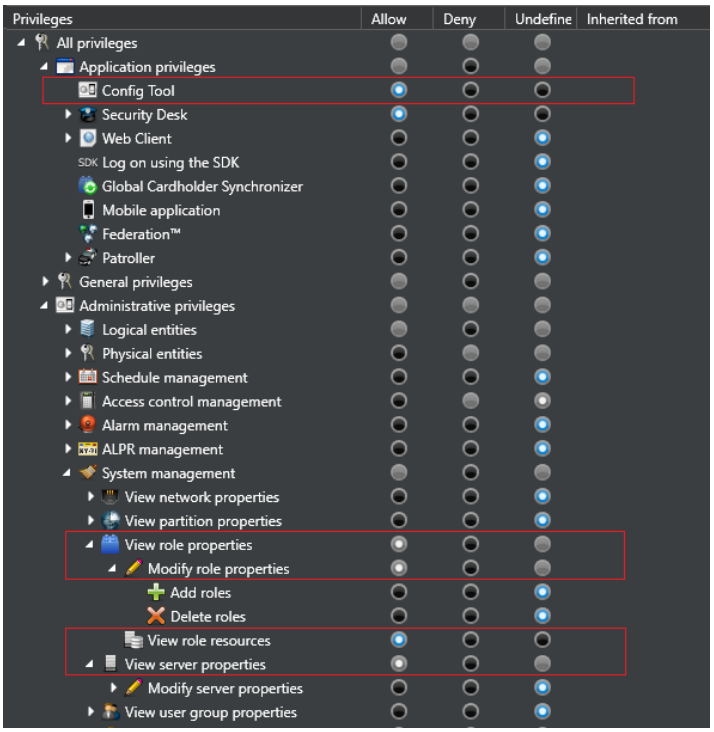


- [Action privileges] *Please allow the required features.



Note)

If you want the user to manage the i-PRO Active Guard Plug-in setup (connections setting and User management). The user needs to have privileges below

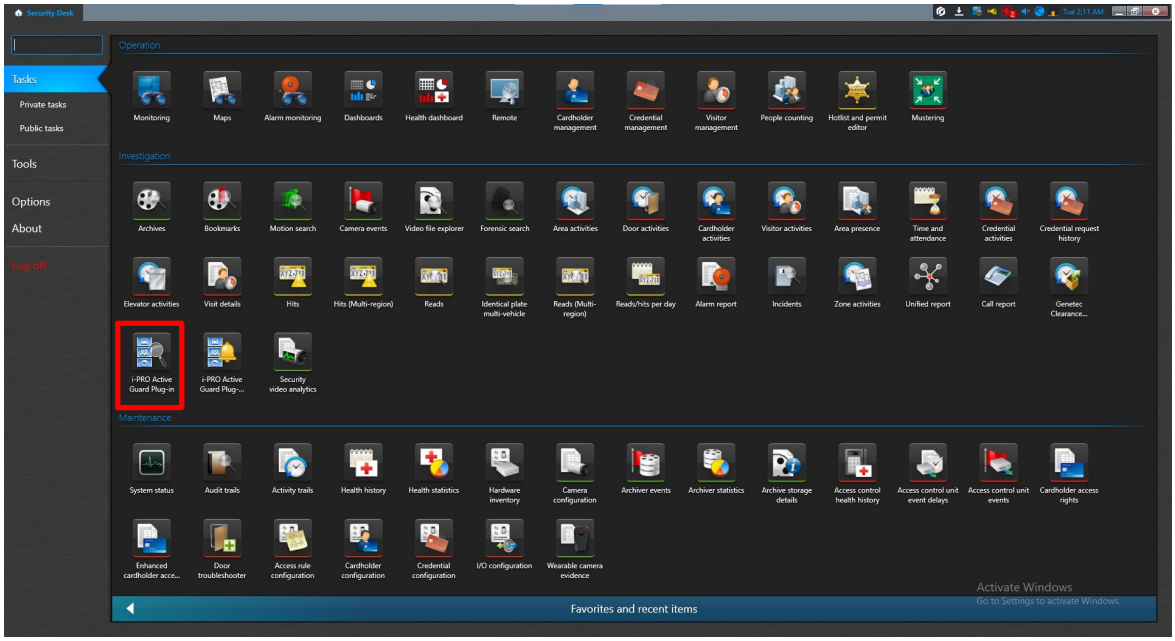


In addition to these, you may need to allow more privileges depending on the features of Security Center you use.

See manual of Security Center for details.

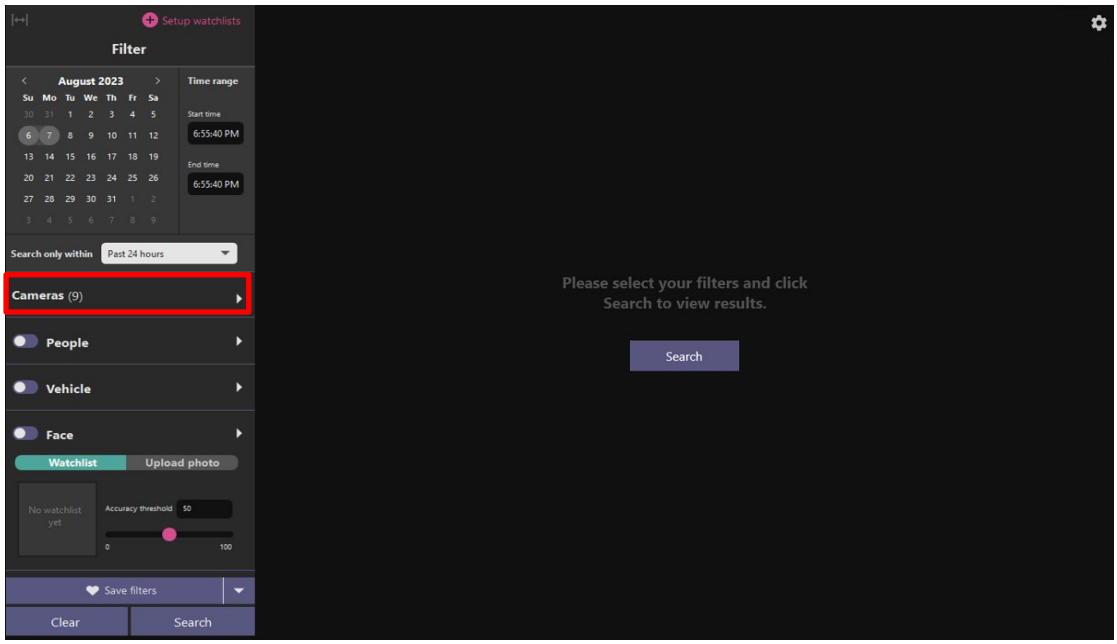
4.4.4. Check

Start Security Desk and select [i-PRO Active Guard Search].



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

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



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

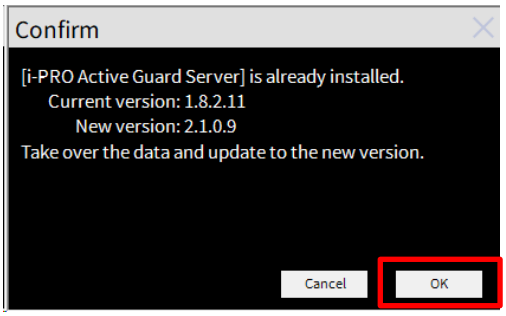
4.5. Upgrade i-PRO Active Guard server

Upgrade i-PRO Active Guard server by transferring settings and past data.

Important:

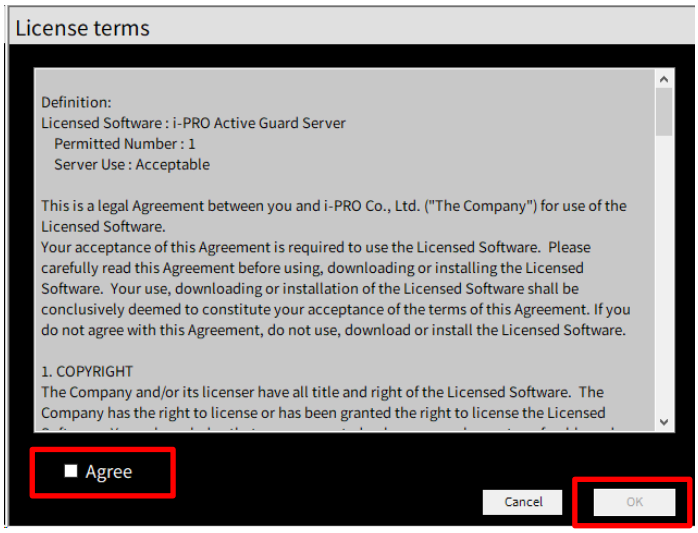
- When upgrading the version of i-PRO Active Guard server, do not uninstall the already installed version and SQL Server. If you uninstall it, you will not be able to use the past data.
- File path length of ***MultiAIStartup.exe*** must be less than 119.

Execute ***"MultiAIStartup.exe"*** as administrator.



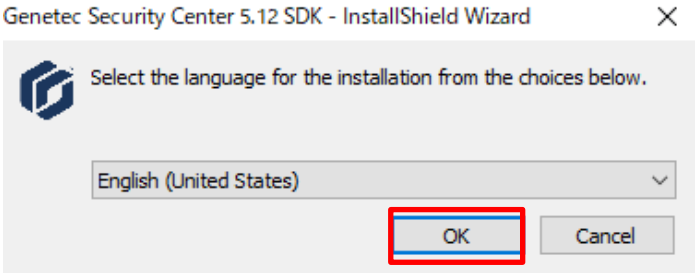
STEP1

Confirm the version and click [OK].



STEP2

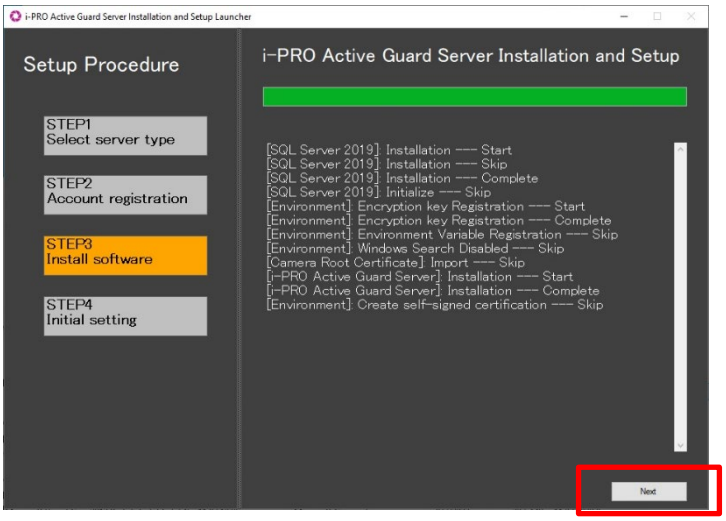
Check for [Agree] for License terms and [OK].



STEP3

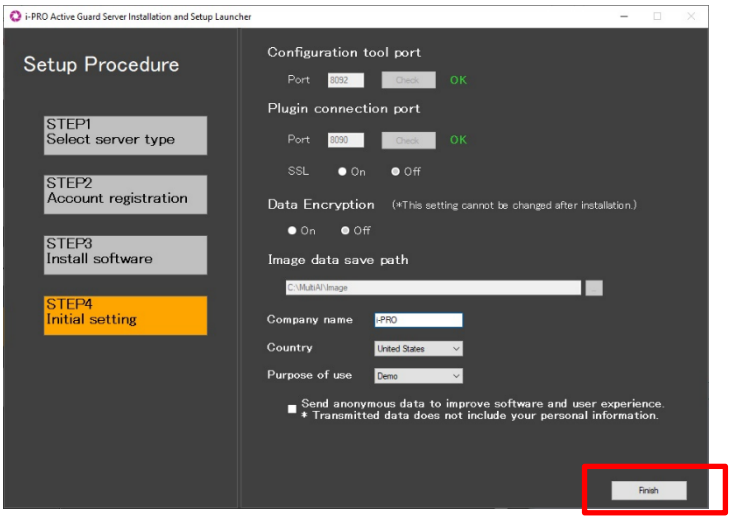
(Only if the image on the left is displayed)

Follow the instructions to install Genetec SDK.



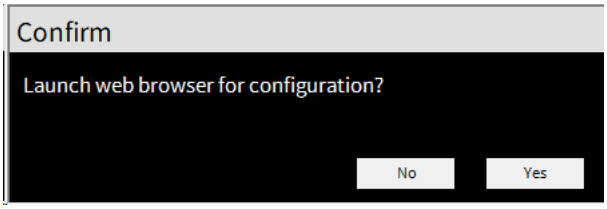
STEP4

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



STEP5

Click [Finish].



STEP6

A dialog box will appear asking about launch web browser.

Please make your selection as necessary.

4.6. Upgrade Plug-in

Upgrade i-PRO Active Guard Plug-in by transferring settings.

STEP1

Search for Services App in search box and run it.

Select “Genetec Server” and “Stop” in right-click menu.

STEP2

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.

STEP3

In Services App, select “Genetec Server” and “Start” in right-click menu.

4.7. Custom alarm setup (optional)

Registered face detection, Registered people detection and system alarm of i-PRO Active Guard server and etc. event can be used as custom event on Security Center.

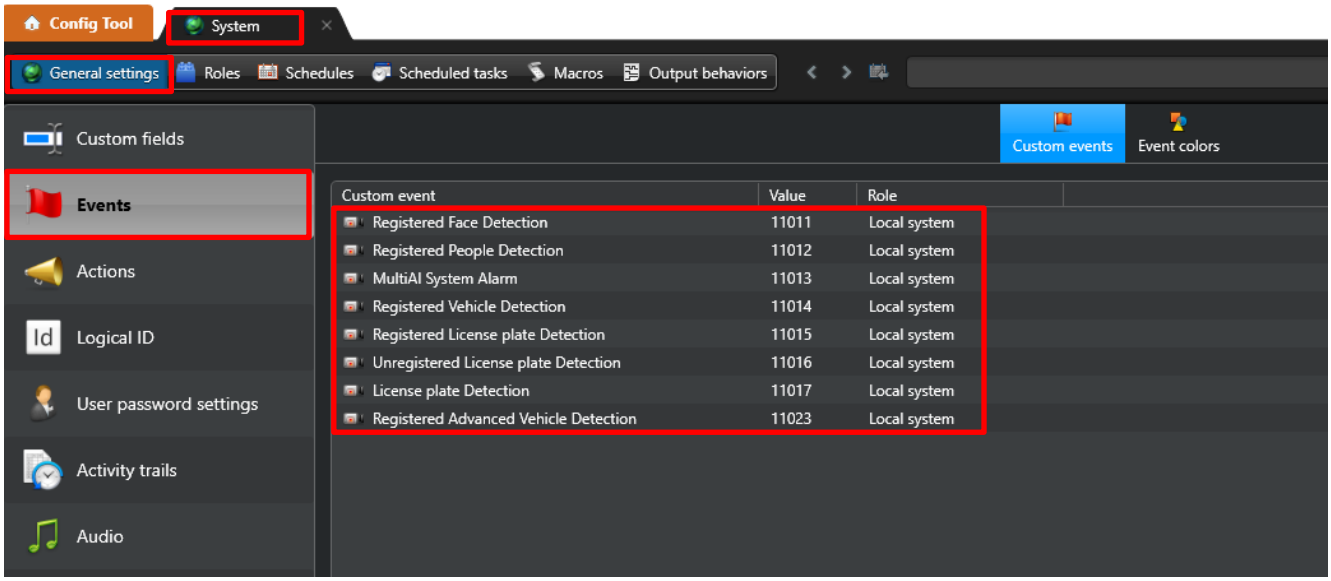
STEP1

Connect Config Tool with Security Center. Select [System] - [General settings] - [Events].

Confirm “Registered Face Detection”, “Registered People Detection”, “Registered Vehicle Detection” and “Multi-AI system Alarm” and etc. exist.

These are added automatically when Security Center is registered to i-PRO Active Guard server (4.3.2.2)

If there are any shortfalls, please add them manually by following the Note) instructions.



Note)

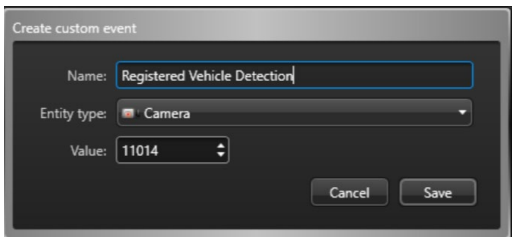
Custom events may not add automatically in upgrade i-PRO Active Guard server.

- Case of upgrading from V1.51 or earlier to V1.60 or later,
  "Registered Vehicle Detection" will not be added automatically.
- Case of upgrading from V1.60 or earlier to V1.70 or later,
  “Registered License plate Detection”, “Unregistered License plate Detection”, “License plate Detection”, “Registered Advanced Vehicle Detection” will not be added automatically.
- Case of upgrading from V1.82 or earlier to V2.00 or later,
  “Code Detection(i-PRO)”, “Registered Code Detection(i-PRO)”, “Unregistered Code Detection(i-PRO)”, “Container Detection(i-PRO)”, “Registered Container Detection(i-PRO)”, “Unregistered Container Detection(i-PRO)”, “Registered Advanced Container Detection(i-PRO)” will not be added automatically.

If you want to add Custom events or change custom event ID, please follow these steps to manually create a custom event.

(1) Create custom events in the Security Center.

Set the Name and Value according to the table below.



(2) Add i-PRO Active Guard's custom event ID settings by following the steps.

- Use the PC where the i-PRO Active Guard server is installed and log in to the web settings.
- Edit custom events ID in the i-PRO Active Guard web settings.

[Register VMS] – [“Advanced” of Notification column] – [Edit custom event ID]

Add the Name and Value as "{Event name},{ID}" at the bottom according to the table below.

Default Value	Event name	Description
11011	Registered Face Detection(i-PRO)	Notify when a face registered in the watchlist is detected.
11012	Registered People Detection(i-PRO)	Notify when people registered in the watchlist is detected.
11013	MultiAI System Alarm(i-PRO)	(Alarm, System error, Exceed the receiving data limit, Reach the max usage of image storage drive *1) Notify when system errors or events occur.
11014	Registered Vehicle Detection(i-PRO)	Notify when a vehicle registered in the watchlist is detected.
11015	Registered License plate Detection(i-PRO)	Notify when a License plate registered in the watchlist is detected. (*2)
11016	Unregistered License plate Detection(i-PRO)	Notify when a License plate unregistered in the watchlist is detected. (*2)
11017	License plate Detection(i-PRO)	(Notify all detected license plate *1) Notify when a License plate is detected.
11023	Registered Advanced Vehicle Detection(i-PRO)	Notify when a License plate registered in the watchlist set in "appearance only" is detected. (*2)
11025	Code Detection(i-PRO)	(Notify all detected code *1) Notify when a code is detected.
11026	Registered Code Detection(i-PRO)	Notify when a code registered in the watchlist is detected. (*3)

Default Value	Event name	Description
11027	Unregistered Code Detection(i-PRO)	Notify when a code unregistered in the watchlist is detected. (*3)
11028	Container Detection(i-PRO)	(Notify all detected container *1) Notify when a container is detected.
11029	Registered Container Detection(i-PRO)	Notify when a container registered in the watchlist is detected. (*4)
11030	Unregistered Container Detection(i-PRO)	Notify when a container unregistered in the watchlist is detected. (*4)
11031	Registered Advanced Container Detection(i-PRO)	Notify when a container registered in the watchlist set in “appearance only” is detected. (*4)
11018	Object detected in field(i-PRO) (AI Processing relay app)	(Alarm of AI Processing relay app *1) Notify when an object detected in field is detected.
11019	Loitering (i-PRO) (AI Processing relay app) Note) Please put a space after " Loitering "	(Alarm of AI Processing relay app *1) Notify when an object loitering is detected.
11020	Direction alarm(i-PRO) (AI Processing relay app)	(Alarm of AI Processing relay app *1) Notify when a direction alarm of object is detected.
11021	Object crossed line(i-PRO) (AI Processing relay app)	(Alarm of AI Processing relay app *1) Notify when an Object crossed line is detected.
11022	People counting alarm(i-PRO) (AI Processing relay app)	(Alarm of AI Processing relay app *1) Notify when people counting alarm is detected.
11024	AI Scene Change Detection(i-PRO) (AI Processing relay app)	(Alarm of AI Processing relay app *1) Notify when Scene Change Detection.

*1: i-PRO Active Guard Server configuration required. Please refer to 4.3.6.

*2: About notification of Registered License plate Detection.

- Registered License plate Detection

  You will be notified when you set LPR watchlist to below settings on i-PRO Active Guard plug-in.

  Set “Detect by vehicle appearance only” to off,

  and set “Trigger” to “When license plates in the selected group was detected”.

- Unregistered License plate Detection

  You will be notified when you set watchlist to below settings on i-PRO Active Guard plug-in.

  Set “Detect by vehicle appearance only” to off,

  and set “Trigger” to “When other license plate which is not in the selected group was detected”.

- Registered Advanced Vehicle Detection

  Set “Detect by vehicle appearance only” to on.

*3: About notification of Registered Code Detection.

- Registered Code Detection

You will be notified when you set OCR watchlist to below settings on i-PRO Active Guard plug-in.

Set “Trigger” to “When OCR Code in the selected group was detected.”

- Unregistered Code Detection

You will be notified when you set OCR watchlist to below settings on i-PRO Active Guard plug-in.

Set “Trigger” to “When other OCR Code which is not in the selected group was detected”.

*4: About notification of Registered Container Detection.

- Registered Container Detection

You will be notified when you set Container watchlist to below settings on i-PRO Active Guard plug-in.

Set “Detect by container details” to off,

and set “Trigger” to “When Container in the selected group was detected”.

- Unregistered Container Detection

You will be notified when you set Container watchlist to below settings on i-PRO Active Guard plug-in.

Set “Detect by container details” to off,

and set “Trigger” to “When other container which is not in the selected group was detected”.

- Registered Advanced Container Detection

Set “Detect by container details” to on.

Note）

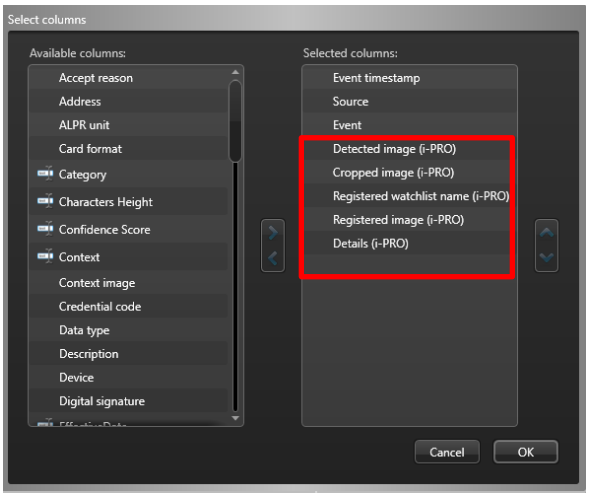
In case of duplicate “Value”, set “Value” to a valid (empty) number in Security Center.

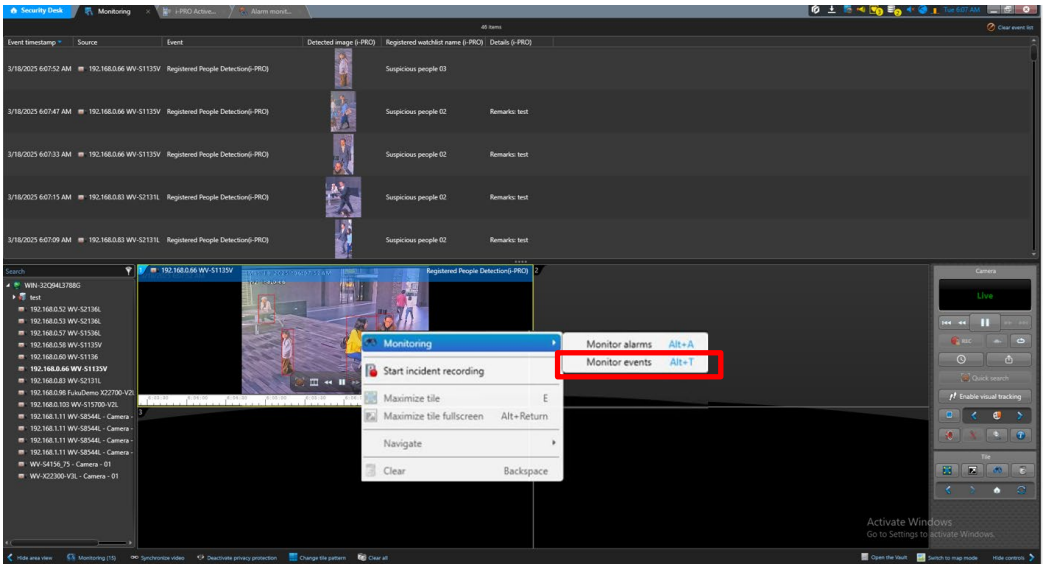
Next, also update i-PRO Active Guard's custom event ID settings.

“Event name” cannot be changed.

STEP2

By enabling [Monitoring] – [Event Monitoring], and add columns ending with (i-PRO) such as "Detected image(i-PRO)". This will display "Registered Face Detection", "Registered Person Detection", and "i-PRO Active Guard Server System Alarm", and etc.

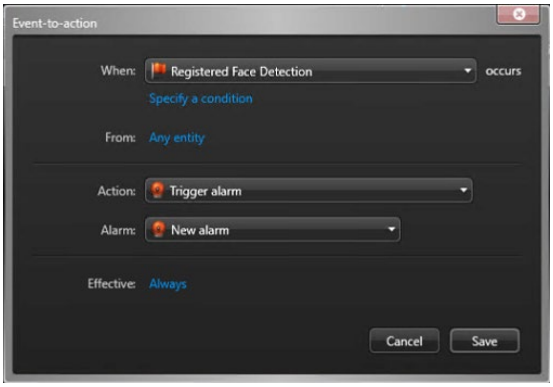


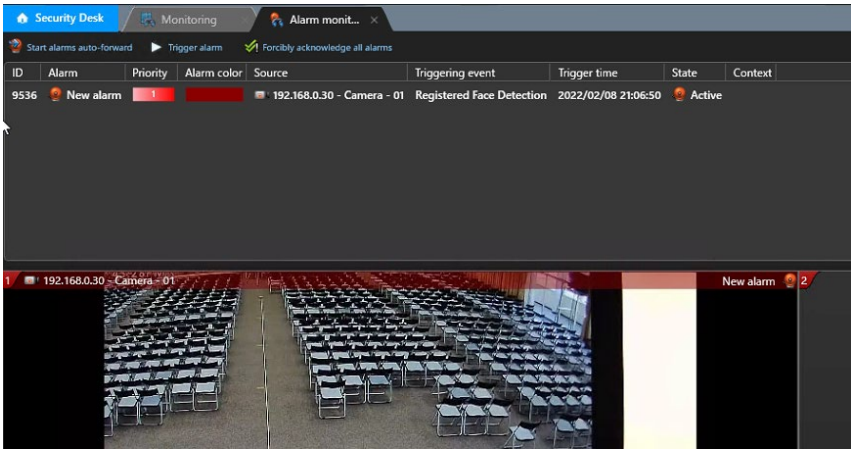


“Registered face detection”, “Registered people detection”, “system alarm of i-PRO Active Guard server”, and etc. event can also be shown as “Alarm” by configuring [Alarm] and [Actions].

STEP3

Select [Actions] setting. Set [When] to the custom event added in Step1 and select the camera for event source. And select [Action] in pull-down menu. (Other setting items depend on [Action].)





Note)

To use Multi-AI system Alarm, you also need to enable on i-PRO Active Guard configuration (Refer to 4.3.6).

5. When changing system component

5.1. Add system device

5.1.1. Add camera

STEP1

Register AI cameras to Security Center server using Security Desk (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)

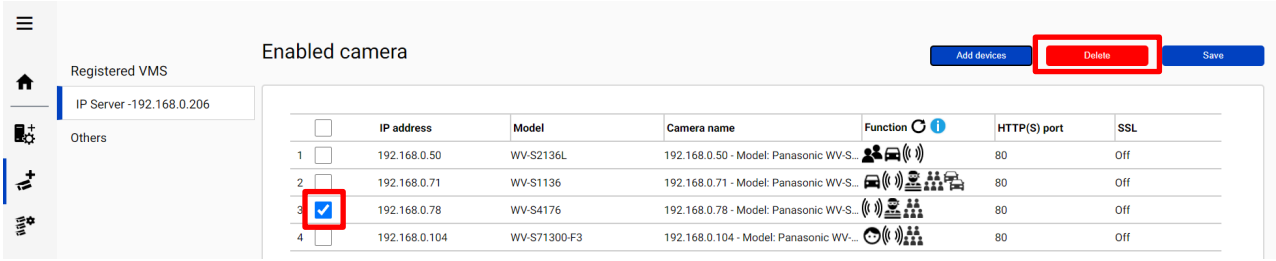
5.2. Delete system device

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)

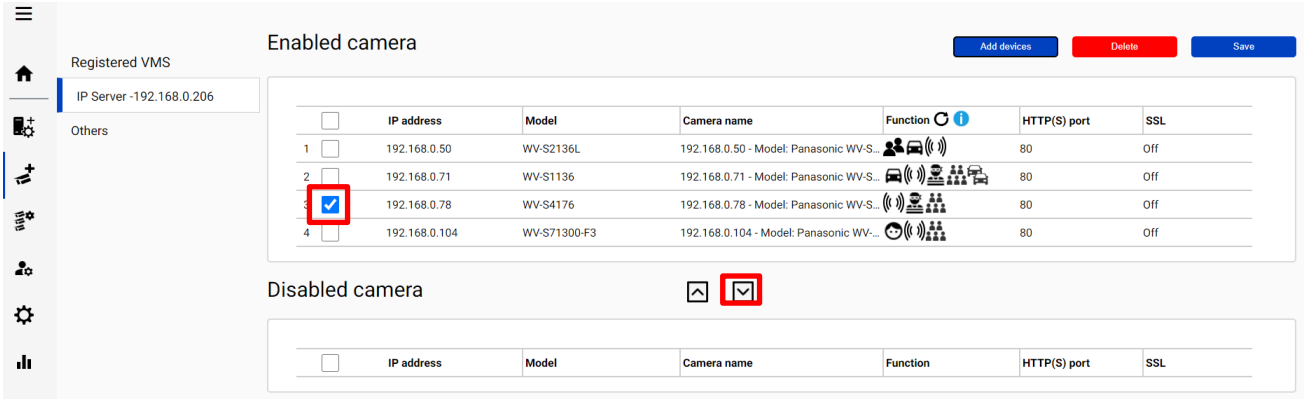
5.2.2. Disable camera

When you want to 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

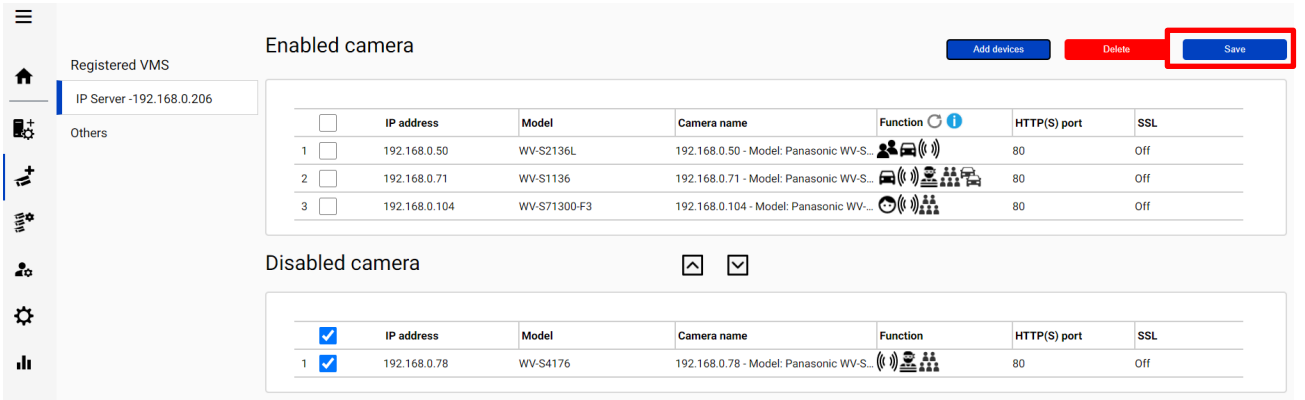
Check camera and move to Disabled camera from Register Cameras screen.

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].

The existing data of the camera will be available as long as retention period is not exceeded from Plug-in.

5.2.3. Delete Security Center

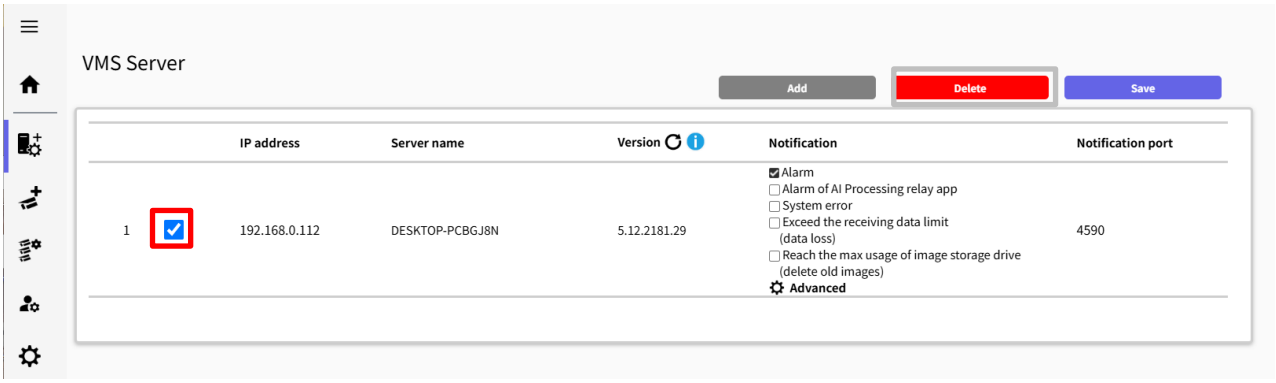
STEP1

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 Plug-in.

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

Best shot images and related database will be deleted when retention period exceeds.



STEP2

Restart process (Refer to 4.3.3)

5.3. Update registered device information

Important:

- When updating the devices registered to the i-PRO Active Guard server (ex. changing camera settings(*) or upgrading the Security Center version), be sure to update the camera and VMS information according to the procedures in this chapter.
  If you want to change the "IP address", please refer to 5.5.

  * The settings are below.
    - Camera's settings. (ex. IP address, Camera name)
    - Camera's extension software settings.
      (ex. Installing and uninstalling camera's extension software, Line name of AI-VMD)

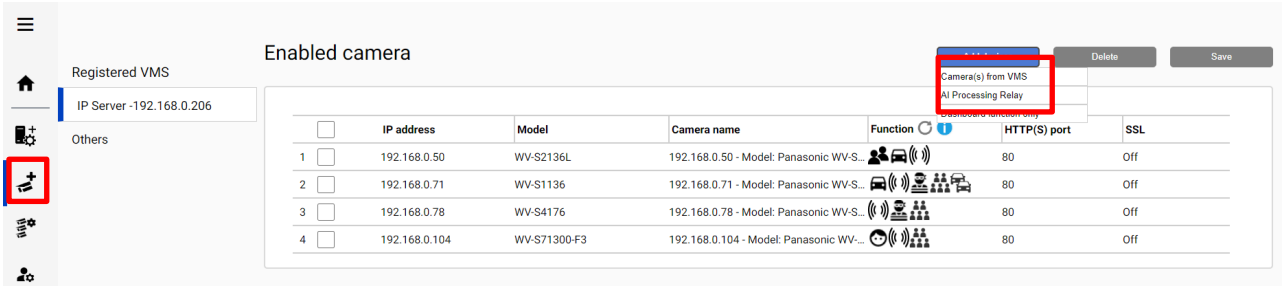
5.3.1. Update camera and extension software settings

STEP1

Change settings using iCT. (Refer to 4.1)

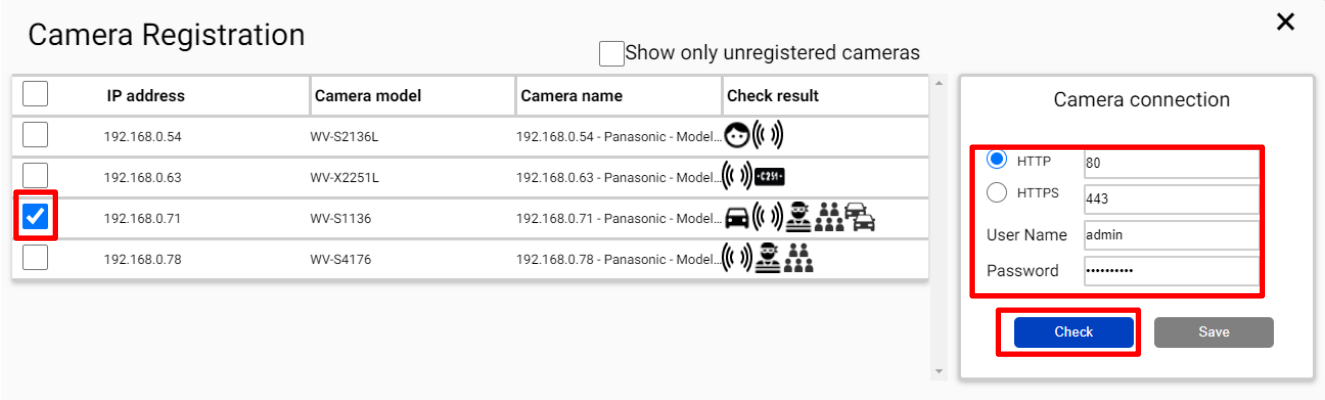
STEP2

Click [Add devices] - [Camera(s) from VMS] on Register Cameras screen.



STEP3

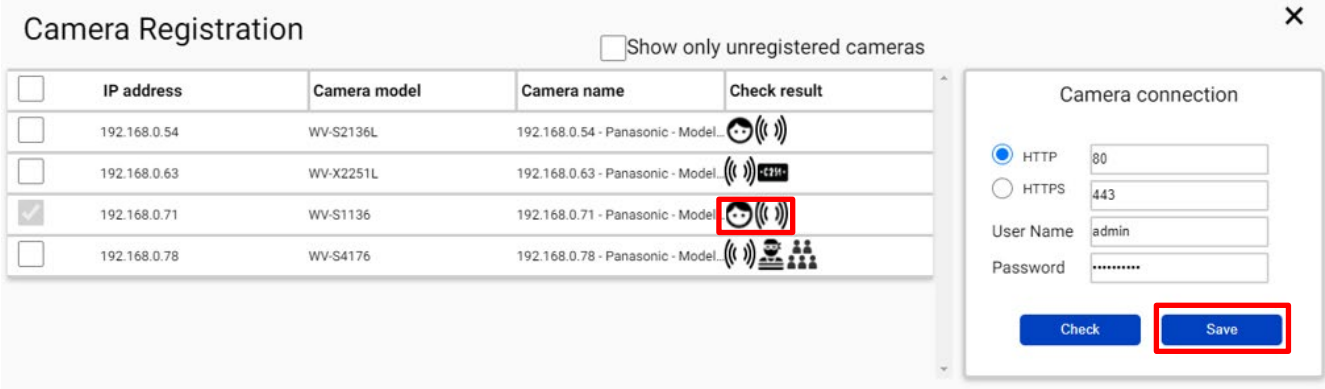
Select the camera and input credentials and [Check].



STEP4

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

(See 4.3.2.3 about the meaning of icons).



STEP5

Restart process (Refer to 4.3.3)

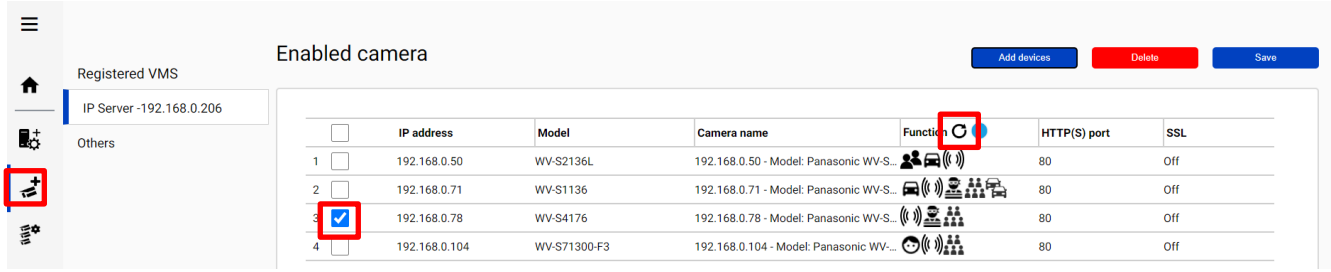
5.3.2. Update extension software settings

STEP1

Change extension software settings using iCT. (Refer to 4.1)

STEP2

Check the target camera and click  on Register Cameras screen.



Note)

This function cannot update the camera's settings. (ex. IP address, Camera Name)

If there is an abnormal value, please try to update using method 5.3.1.

STEP3

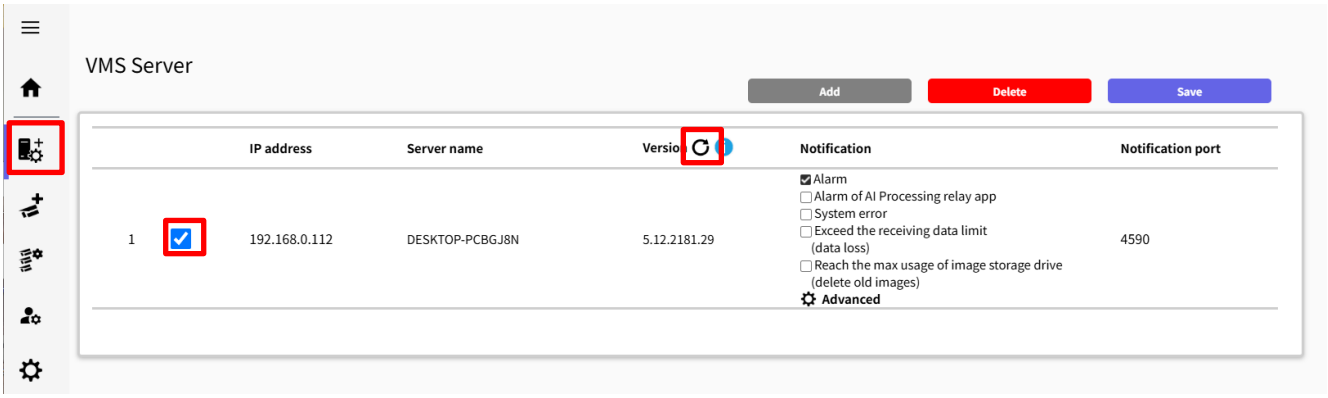
Confirm that the icon has been updated.

(See 4.3.2.3 about the meaning of icons).

5.3.3. Update VMS Server version information

STEP1

Check the VMS and click ↻ on Register VMS screen.



STEP2

Confirm that the version of VMS has been updated.

Note)

・When updating from version V5.12.1 or earlier to V5.12.2 or later, and if you want to attach detection images to Monitoring tasks, please execute the following “Setup.exe” included with the “i-PRO Active Guard Server” installer and install the Genetec SDK.

Path: 04¥Tools¥Security_Center_v5.12.2.0_b2181.29_SDK¥Setup.exe

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].

5.4.2. Uninstall i-PRO Active Guard server

STEP1

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

STEP2

Find [i-PRO Active Guard Server] and [Uninstall].

Delete “C:¥MultiAI” folder if exist.

Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.

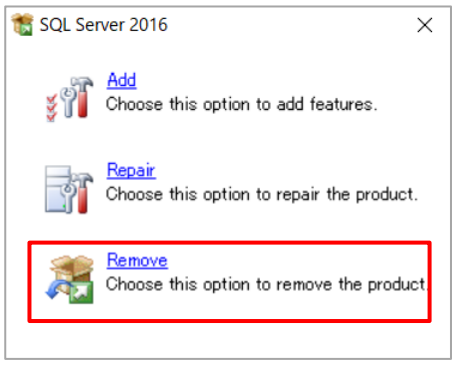
5.4.2.1. Uninstall SQL Server instance of i-PRO Active Guard server

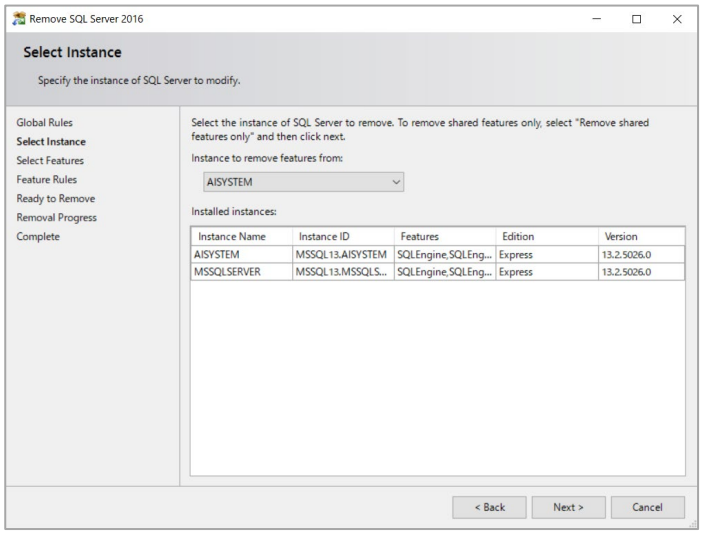
・If you select "Install a new SQL Server instance" in database selection for installation.

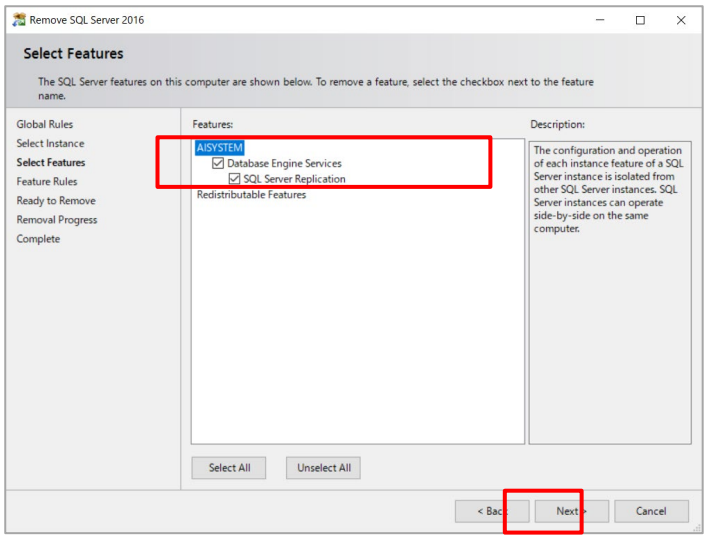
STEP1

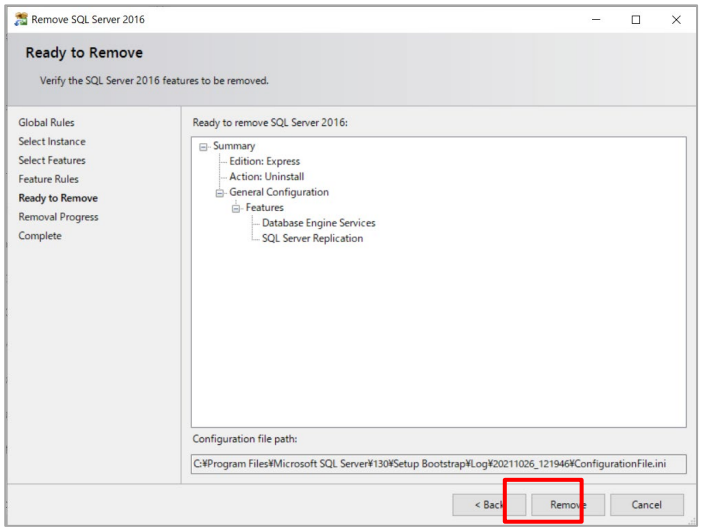
Find [Microsoft SQL Server 2016 (64 bit)] or [Microsoft SQL Server 2019 (64 bit)] and [Uninstall].

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.
- The instance name "AISYSTEM" is the default name. If you have specified an instance name as described in section 4.3.1, replace "AISYSTEM" with the specified instance name in the following sections.

STEP2

Delete “C:¥Program Files¥Microsoft SQL Server¥MSSQL13.AYSYSTEM” folder or “C:¥Program Files¥Microsoft SQL Server¥MSSQL15.AYSYSTEM” folder.

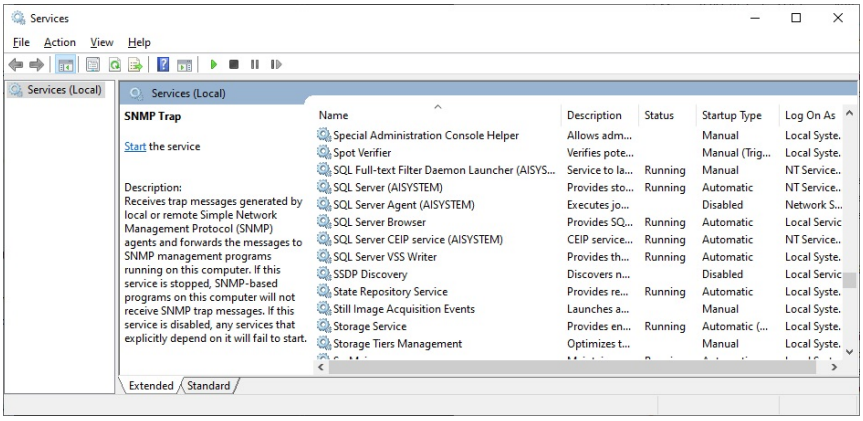
Note)

If any of the following services remain after uninstallation, please remove them manually.

- SQL Full-text Filter Daemon Launcher (AISYSTEM)
- SQL Server (AISYSTEM)
- SQL Server Agent (AISYSTEM)
- SQL Server CEIP service (AISYSTEM)

(1) How to display services

Search for Services App in search box and run it.

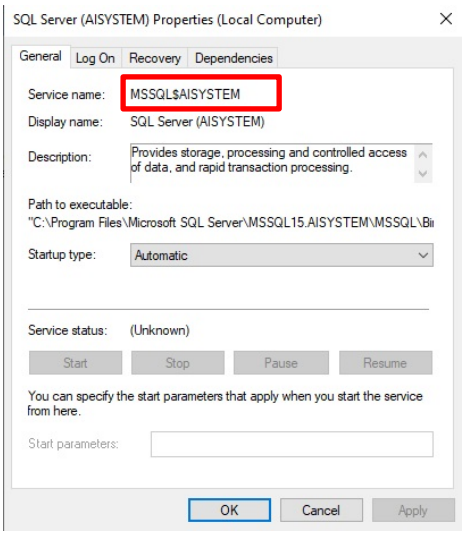


(2) How to delete a service

Start a command prompt as an administrator user and execute the following command.

sc delete “xxx”

“xxx" is the Service name that appears when the target is double-clicked.



e.g.) SQL Server (AISYSTEM)

sc delete MSSQL$AISYSTEM

5.4.2.2. Delete i-PRO Active Guard server databases and users in existing SQL Server instance

・If you select "Use existing SQL Server instance" in database selection for installation.

Important:

・ Other applications using SQL Server may be affected.
Please operate with caution and only when necessary.

STEP1

Please use “SQL Server Management Studio (SSMS)” to delete the following data from the instance where i-PRO Active Guard server is installed.

- Databases
  ・ai_db
  ・aicam
  ・bi
  ・support_db

- Security - Logins
  ・ai_owner
  ・aicam_user
  ・support_user

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 Security Center ([Config tool] – [Video] – [Property setting of Video unit]).

Once deleting cameras from Security Center 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 Security Center’s IP address

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

STEP1

Change Security Center’s IP address.

STEP2

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

STEP3

Register the Security Center 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 (Refer to 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.

Important:

- In the restore environment, the following settings must be the same as the backup environment.
  - SQL Server instance
    *Switching from local server to network server is not possible.
  - Administrator username and password.
  - Install path of i-PRO Active Guard server.

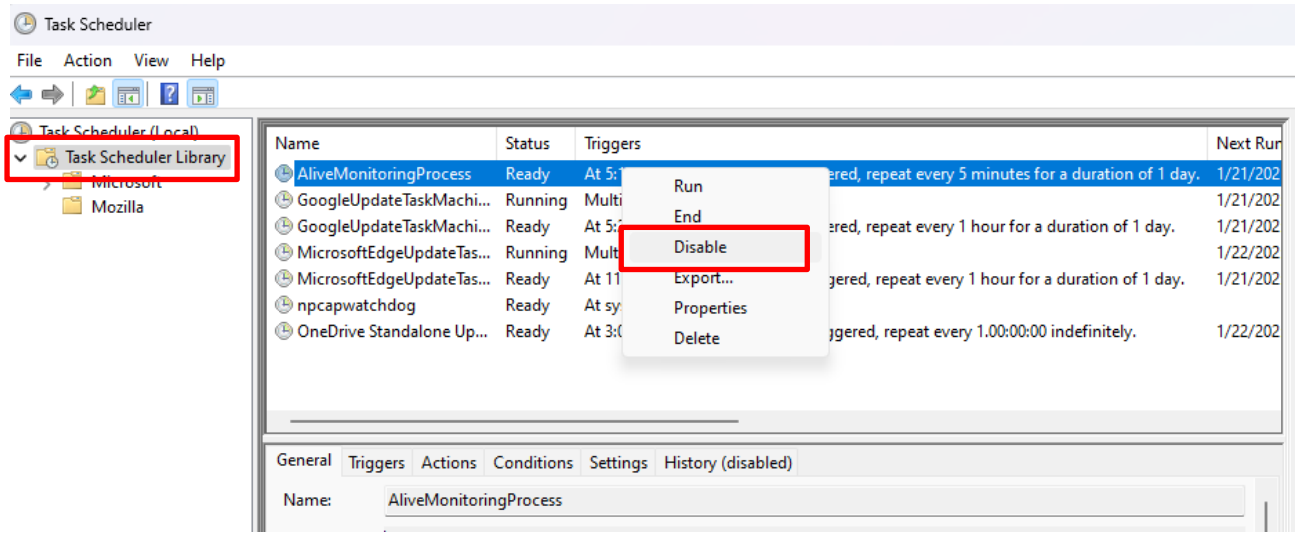
If the settings are different, you will need to reinstall the i-PRO Active Guard server in the restore environment.

5.6.1. Backup process

STEP1

Search for Task Scheduler App in search box and run it.

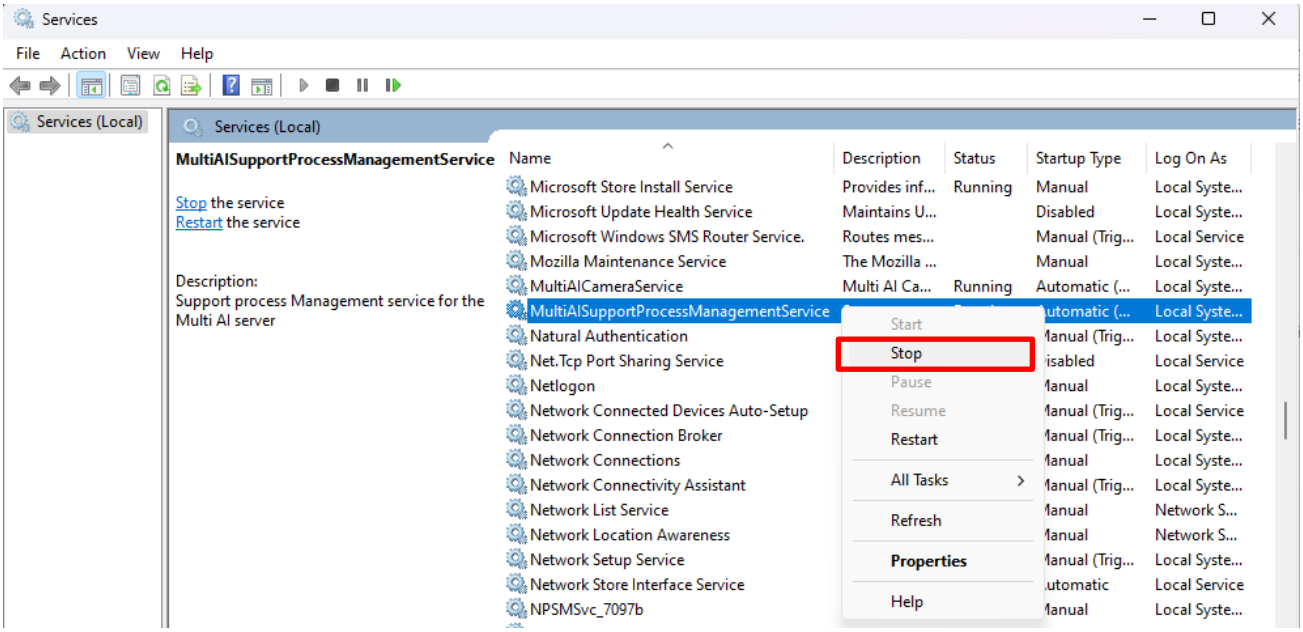
Right click and disable “AliveMonitoringProcess”



STEP2

Search for Services App in search box and run it.

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



STEP3

Browse to SQL Server data save path (set by install tool at 4.3.1.).

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.).

Default SQL Server data save path is below:

SQL server 2016

“C:¥Program Files¥Microsoft SQL Server¥MSSQL13.AISYSTEM¥MSSQL¥DATA”

SQL server 2019

“C:¥Program Files¥Microsoft SQL Server¥MSSQL15.AISYSTEM¥MSSQL¥DATA”

SQL server 2022

“C:¥Program Files¥Microsoft SQL Server¥MSSQL16.AISYSTEM¥MSSQL¥DATA”

STEP4

Copy “C:¥MultiAI¥Image” folder to safe location.

If you changed the image data save path, copy the folder.

Copy “C:¥MultiAI¥Backup” folder to safe location.

Note)

- The MultiAI and Image path above are the default, if you changed the path in section 4.3.1 or 4.3.5.4, please replace the path.

STEP5

Type “regedit” to Start menu and run. Right click two folders and export to safe location, respectively.

“¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Panasonic¥AiSystem” or

“¥HKEY_LOCAL_MACHINE¥SOFTWARE¥i-PRO¥AiSystem.”

“¥HKEY_LOCAL_MACHINE¥SOFTWARE¥WOW6432Node¥Panasonic¥AiSystem” or

“¥HKEY_LOCAL_MACHINE¥SOFTWARE¥WOW6432Node¥i-PRO¥AiSystem.”

STEP6

In Services App, right click and run for “MultiAICameraService”,

“MultiAISupportProcessManagementService” and “SQL Server (AISYSTEM),” respectively.

STEP7

In Task Scheduler App, right click and enable “AliveMonitoringProcess.”

5.6.2. Restore process

STEP1

Install i-PRO Active Guard Server in the restore environment with the same SQL instance, administrator username, and password and install path of i-PRO Active Guard server settings as in the backup environment.

Note)

- If you select "Use existing SQL Server instance" in database selection for installation, i-PRO Active Guard Server database and user must be deleted before installation.
  For delete database and user, see 5.4.2.2.
- If you select “Network Server” of "Use existing SQL Server instance" in database selection for installation, Set the SQL server IP, TCP port, etc. to the same settings as the backup environment.

STEP2

Search for Task Scheduler App in search box and run it.
Right click and disable “AliveMonitoringProcess”

STEP3

Search for Services App in search box and run it. right click and stop for “MultiAICameraService,” “MultiAISupportProcessManagementService” and “SQL Server (AISYSTEM),” respectively.

STEP4

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 SQL Server data save path and replace existing files.

Default SQL Server data save path is below:

SQL server 2016

“C:¥Program Files¥Microsoft SQL Server¥MSSQL13.AISYSTEM¥MSSQL¥DATA”

SQL server 2019

“C:¥Program Files¥Microsoft SQL Server¥MSSQL15.AISYSTEM¥MSSQL¥DATA”

SQL server 2022

“C:¥Program Files¥Microsoft SQL Server¥MSSQL16.AISYSTEM¥MSSQL¥DATA”

STEP5

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

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

Note)

- The MultiAI and Image path above are the default, if you changed the path in section 4.3.1 or 4.3.5.4, please replace the path.

STEP6

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

STEP7

In Services App, right click and run for “SQL Server (AISYSTEM).”

STEP8

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

Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.

(restore_user.bat)

```
@echo off
set SERVERNAME=localhost\AISYSTEM
sqlcmd -S %SERVERNAME% -i C:\MultiAI\tools\restore_user\restore_user.sql
IF %ERRORLEVEL% equ 0 GOTO OK
ECHO Failed
GOTO END
:OK
ECHO Succeeded
:END
PAUSE
```

Note)

If you selected “Use an existing SQL Server instance” in the database selection during installation, open the batch file in Notepad and modify the following.

- For “Local Server”

(1) Line 2.

Change the “AISYSTEM” to the specified instance name.

If instance name is “MSSQLSERVER”, set to blank.

Ex.) set SERVERNAME=localhost¥SAMPLEINSTANCE

- For “Network Server” and using SQL Server Browser

(1) Line 2.

Change the “localhost” to the specified SQL Server IP Address

Change the “AISYSTEM” to the specified instance name

If instance name is “MSSQLSERVER”, set to blank.

(2) Line 3.

Add “-U login id”, “-P password”, “-N” and “-C”.

Login id and password should be set to the administrator and password of the SQL instance.

Ex.)

```
set SERVERNAME=192.168.0.100¥SAMPLEINSTANCE
sqlcmd -S %SERVERNAME% -i C:¥MultiAI¥tools¥restore_user¥restore_user.sql -U admin
  -P password -N -C
```

- For “Network Server” and not using SQL Server Browser

(1) Line 2.

Change the “localhost” to the specified SQL Server IP Address

Change “¥AISYSTEM” to a comma + the specified TCP port number.

(2) Line 3.

Add “-U login id”, “-P password”, “-N” and “-C”.

Login id and password should be set to the administrator and password of the SQL instance.

Ex.)

```
set SERVERNAME=192.168.0.100,1435
sqlcmd -S %SERVERNAME% -i C:¥MultiAI¥tools¥restore_user¥restore_user.sql -U admin
  -P password -N -C
```

STEP9

In Service App, right click and run for “MultiAICameraService,”

“MultiAISupportProcessManagementService,” respectively.

STEP10

In Task Scheduler App, right click and enable “AliveMonitoringProcess.”

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

i-PRO Active Guard server location can be moved from Security Center’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 the 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.

Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.

STEP4

Search for Services App in search box and run it. 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 (Refer to 4.3.8.2).

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.

Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.

5.10. Change SQL Server administrator account

When you want to change the password of SQL Server administrator(sa) account, you need to change on PC that i-PRO Active Guard server is installed.

STEP1

Please use “SQL Server Management Studio (SSMS)” to change the passwords of the following account from the instance where the i-PRO Active Guard server is installed.

- Security – Logins
  - ・sa

STEP2

Execute “C:¥MultiAI¥tools¥ChangeSQLServerPassword¥ChangeSQLServerPassword.exe” as administrator and set password.

Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.

5.11. 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.

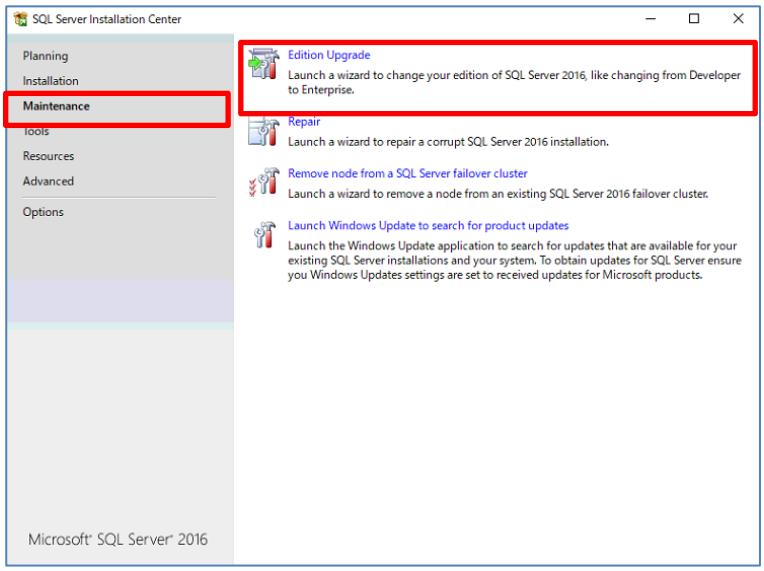
i-PRO Active Guard server software needs to be installed in advance.

STEP1

Start “setup.exe” from install media of SQL server Standard Edition.

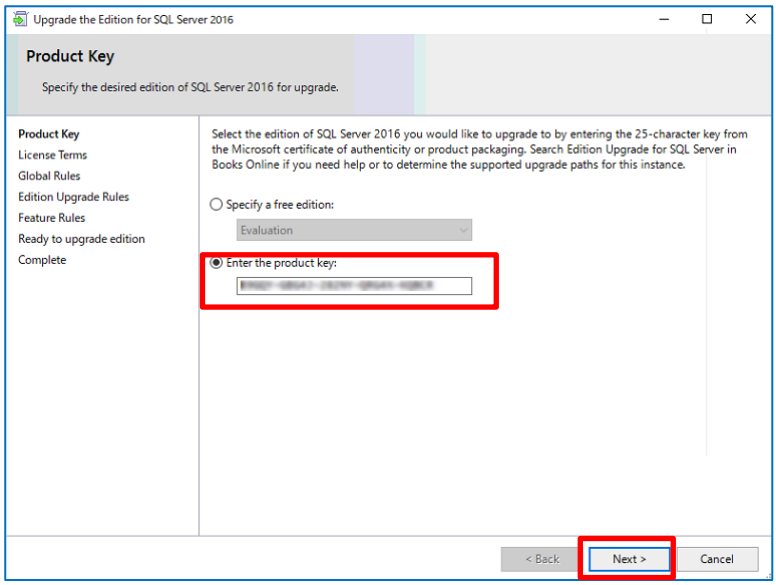
STEP2

Select [Edition Upgrade] from Maintenance.



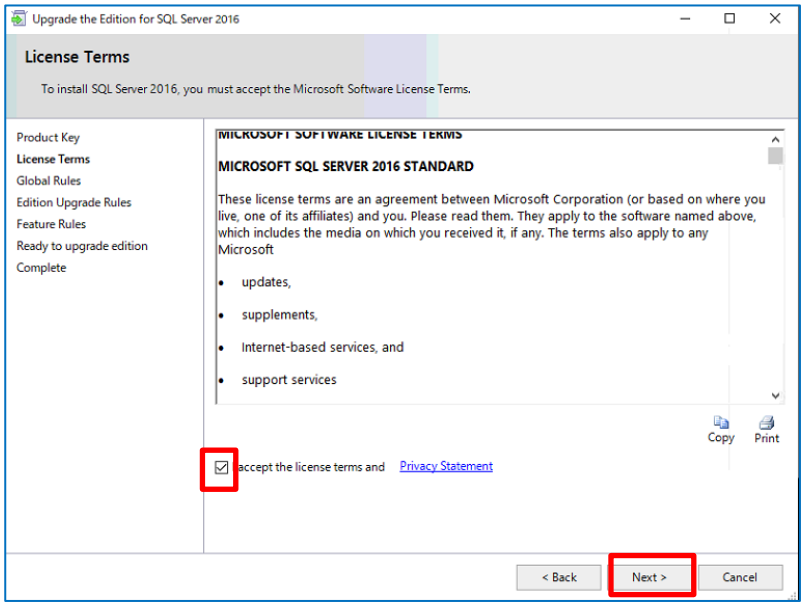
STEP3

Confirm product key is shown and click [Next].



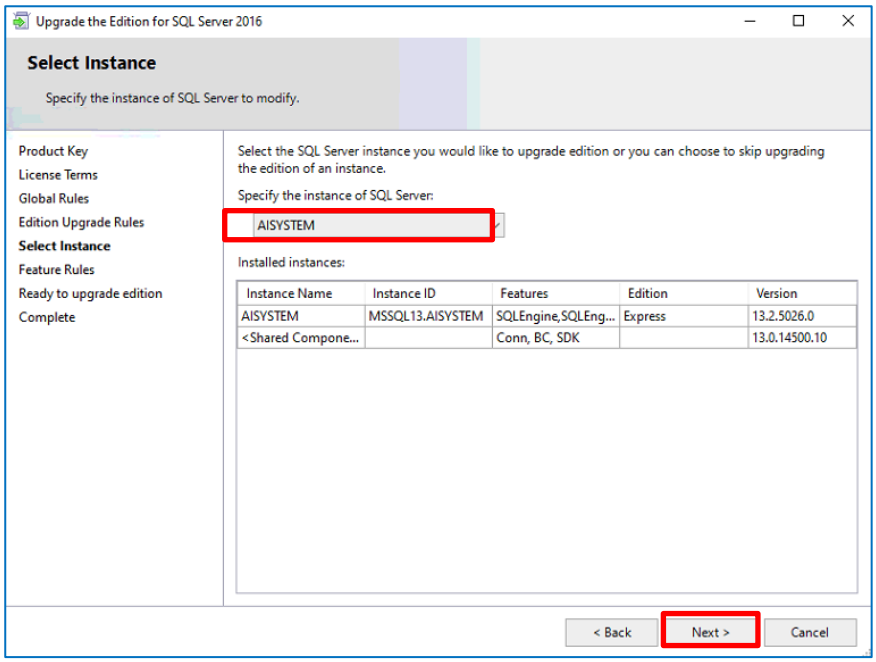
STEP4

Check for license term and click [Next].



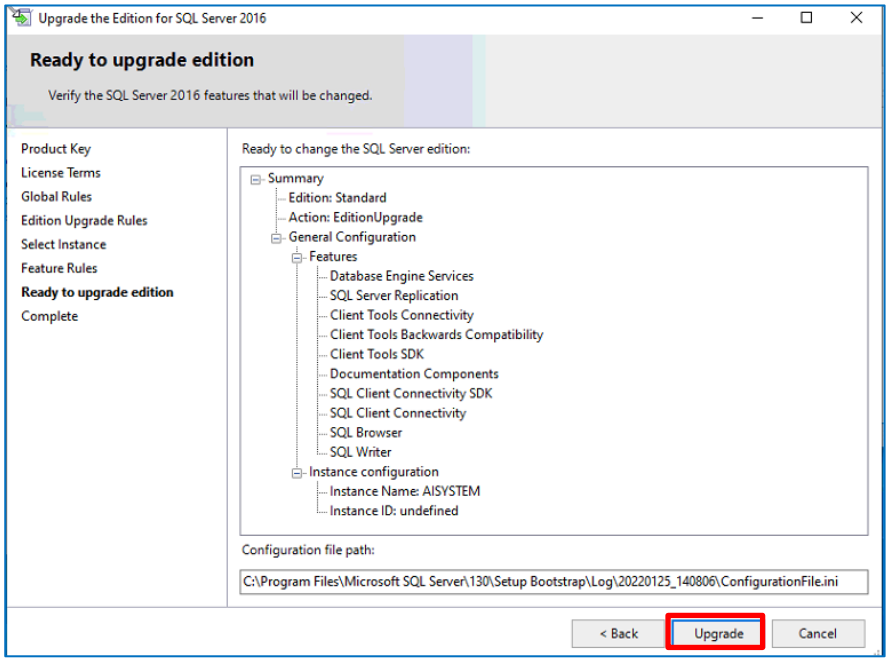
STEP5

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



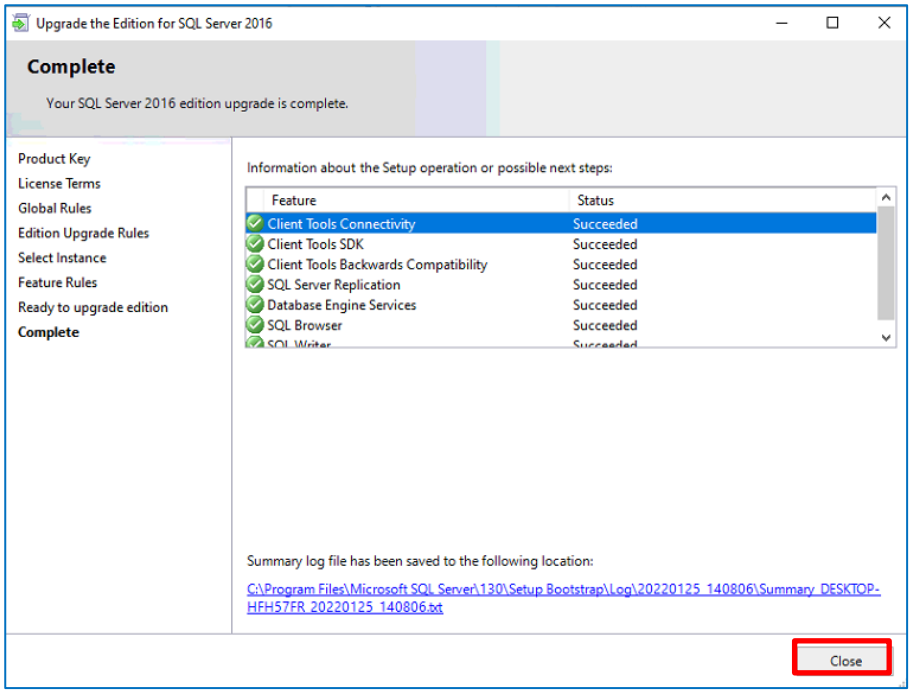
STEP6

Click [Upgrade]



STEP7

Click [Close]



5.12. Import/Export tool for Face Watchlist

This software is used when transferring Face Watchlist data to another i-PRO Active Guard server. You can obtain Face Watchlist data using the export function and register the obtained data to the server using the import function. Additionally, you can create a data file for importing.

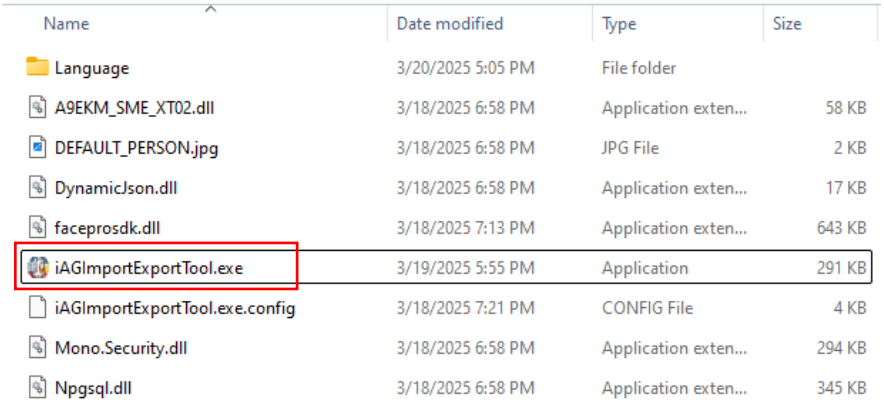
> Important:
> - To use this tool, you need to register a camera with AI Face Detection to i-PRO Active Guard server in advance.

STEP1

Execute “C:¥MultiAI¥tools¥ImportExport¥iAGImportExportTool.exe”.

Note)

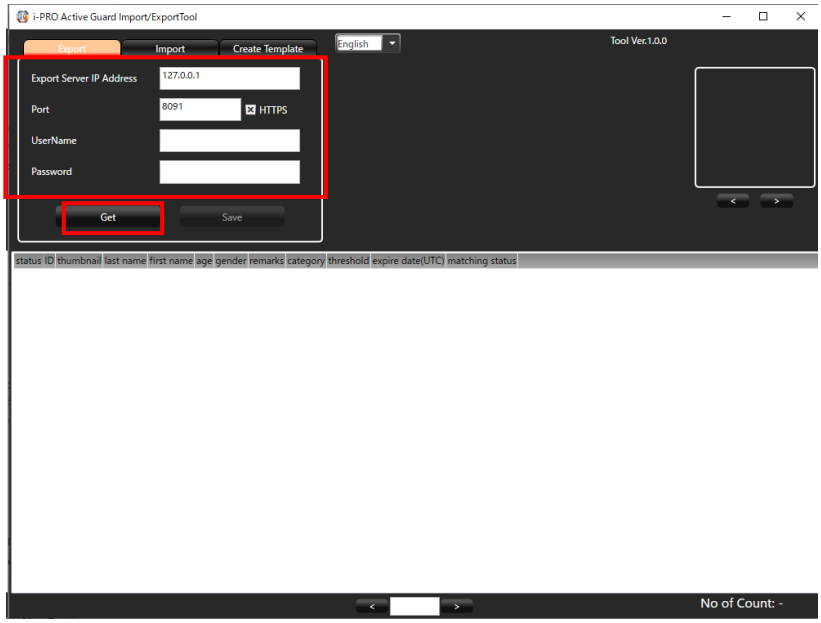
- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.



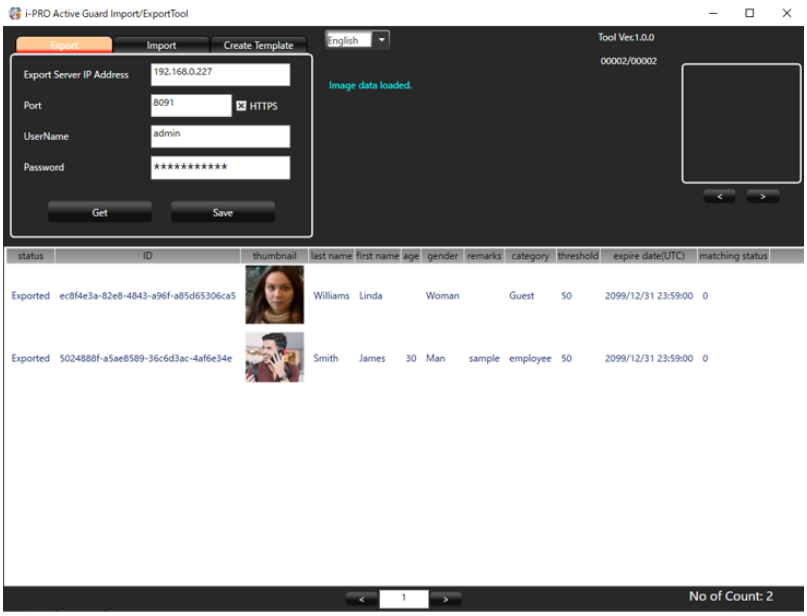
5.12.1. Export

STEP1

Input i-PRO Active Guard server's information and click [Get] in Export tab.



Once the export is complete, the list of facial images will be displayed.



STEP2

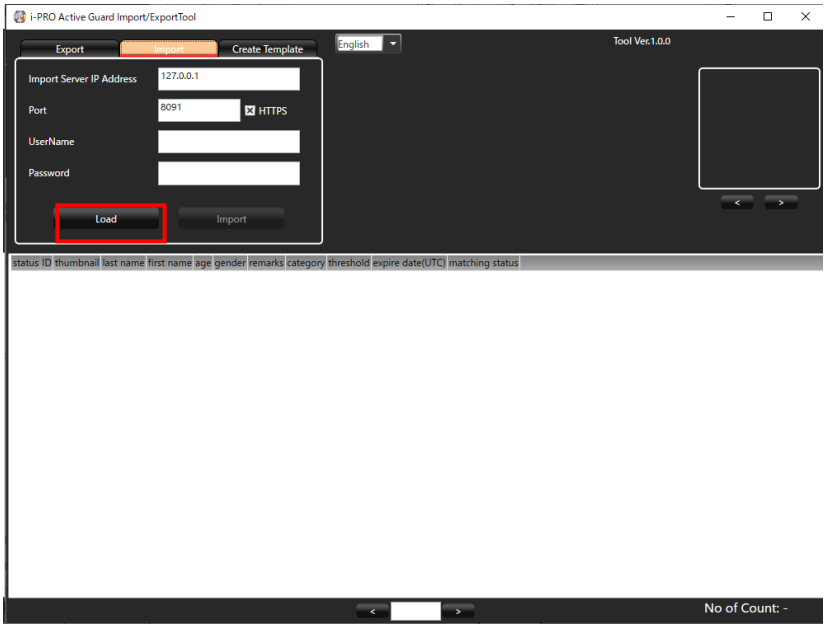
Click [Save].

Create an "**MatchingData**" folder in the specified folder and save the Image file and information file.

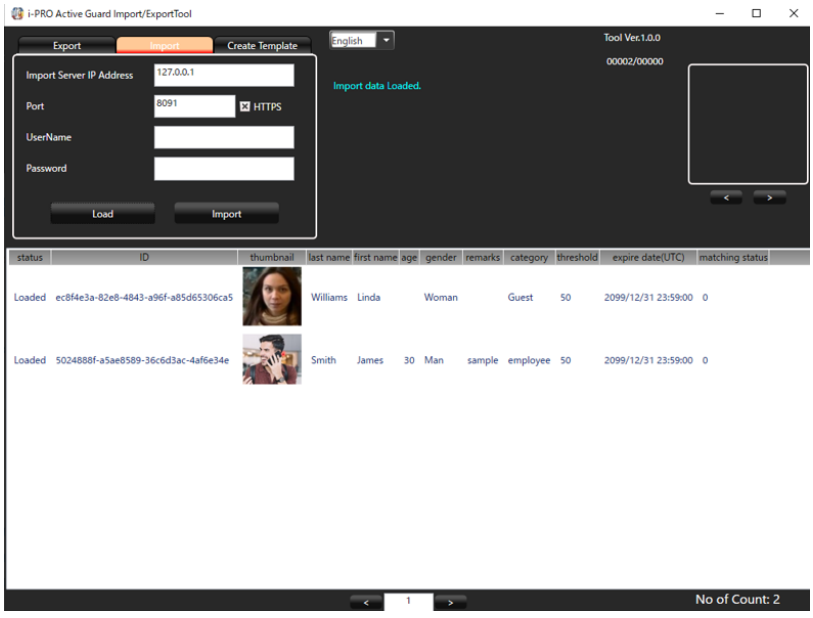
5.12.2. Import

STEP1

Click [Load] in the import tab and specify the folder “**MatchingData**” saved during export.

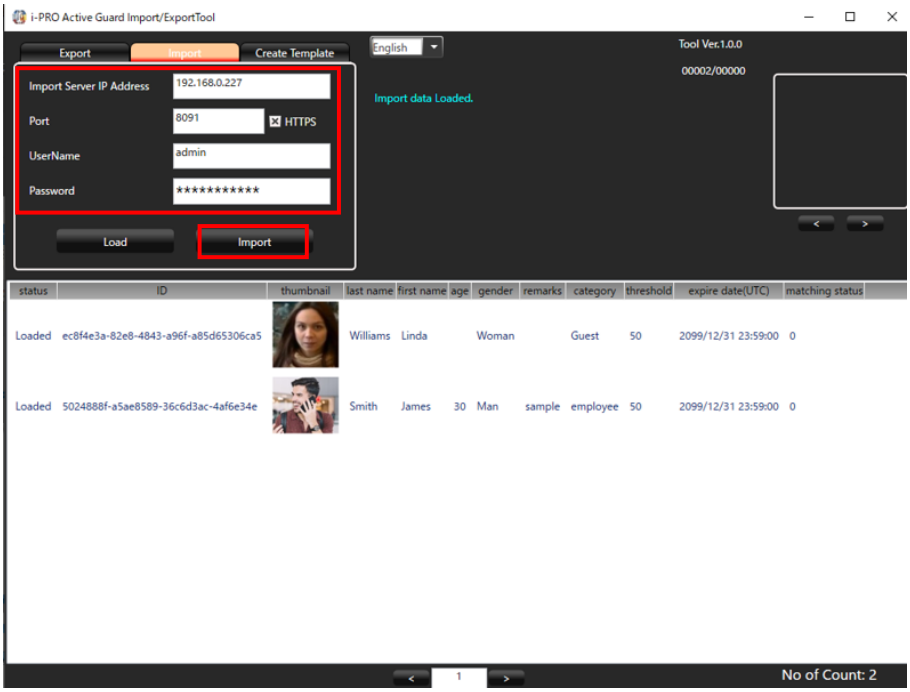


The saved data will be loaded.



STEP2

Input i-PRO Active Guard server’s information and click [Import].



During the import process, the "Importing" indicator will blink.

Once the import is complete, the blinking will stop.

Note)

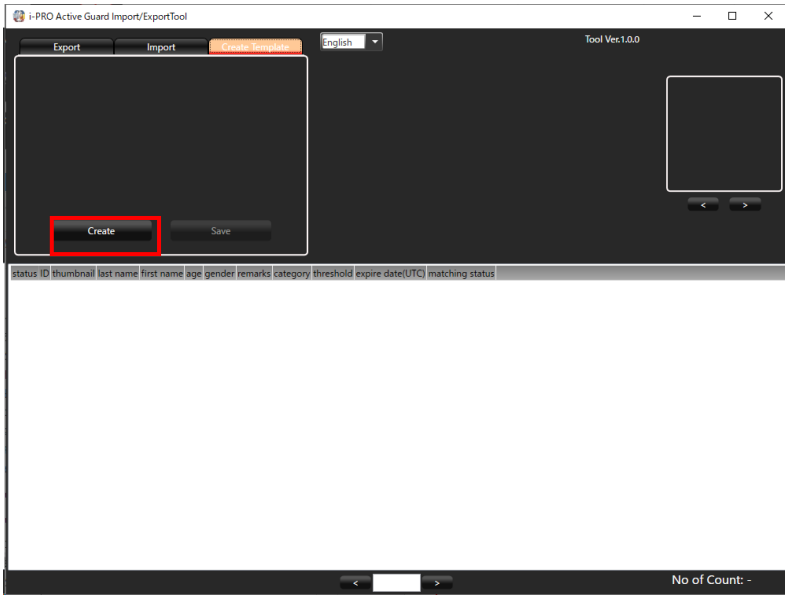
- It takes approximately 20 minutes to import 1,000 images.

5.12.3. Create Template

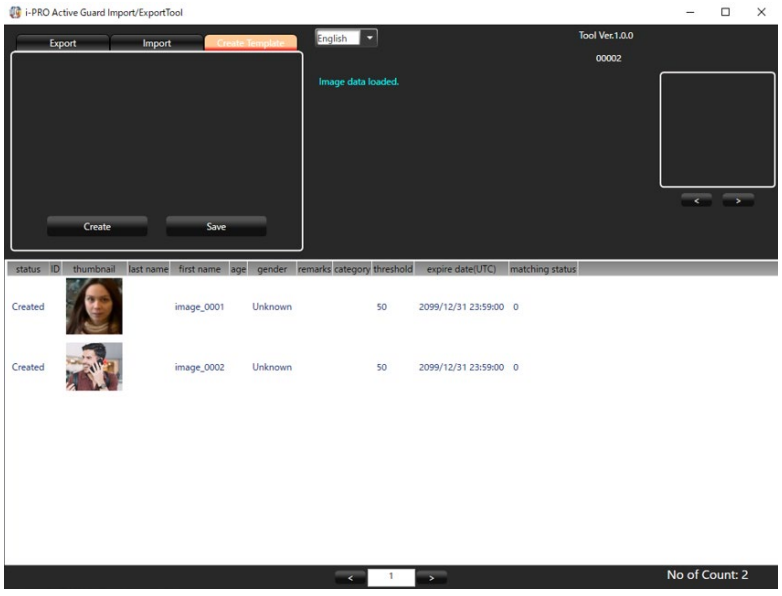
You can create a data file for importing.

STEP1

Click [Create] in the “Create Template” tab and specify the folder where the face images are saved.



Once all the facial image data (in .jpg format) under the specified folder is retrieved, a list of face images will be displayed.



STEP2

Click [Save].

Create an "MatchingData" folder in the specified folder and save the Image file and information file.

Created data can be registered to i-PRO Active Guard server using the import function.

5.12.4. CSV format

- File name: MatchingInfo.csv
- Encoding: UTF-8 with BOM
- The first line and second line don’t edit.

Column name	Value
rt_alarm_matching_info_id	It must be unique value You can use empty when registering a new watchlist.
thumbnail_file_path	Image file path (*local path)
matching_status	0: Matching On 1: Matching Off
first_name	(Text)
last_name	(Text)
age	0-999
gender	0: Male 1: Female 2: Arbitrary
remarks	(Text)
threshold	1-100
matching_list_id	Set same value of “rt_alarm_matching_info_id”
img_id	0-9 When multiple face images are registered for the same watchlist. It can be unique value
category	(Text)
expire_date	YYYY-MM-DD HH:MM:SS(UTC) *If you want to set “Validity period” to unchecked, set the following value. “2099-12-31 23:59:00”
delete_type_flg	1: Delete registration 3: Disable matching

(Sample)

```
L1: Matching Info Import Export Data,100100
L2: "rt_alarm_matching_info_id","thumbnail_file_path","matching_status","first_name","last_name","age","gender",
                    "remarks","threshold","matching_list_id","img_id","category","expire_date","delete_type_flg"
L3: T0001,"C:¥img¥1.jpg",0,"John","Due",21,0,"Remarks text1",50,"T0001",0,Category1,"2099-12-31 23:59:00","3"
L4: T0002,"C:¥img¥2.jpg",0,"John","Smith",32,0,"Remarks text2",50,"T0002",0,Category2,"2099-12-31 23:59:00","3"
L5: T0002,"C:¥img¥3.jpg",0,"John","Smith",32,0,"Remarks text2",50,"T0002",1,Category2,"2099-12-31 23:59:00","3"
```

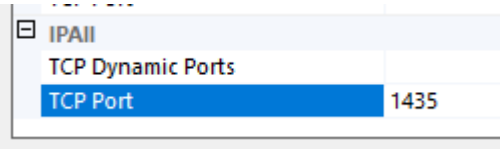
6. Troubleshooting

6.1. Trouble shooting for Installation and Setup

Problem	Cause and solution	Refer
“New version or same version is already installed”. message is displayed but [i-PRO Active Guard Server] does not exist.	Please check if [Multi AI Server] exists in the Programs and Features window. If it exists, please uninstall it.	5.4.2
It does not proceed from the “Now setting for middleware…” screen.	Please close the installer and try installing again.	4.3.1
Failed to install SQL server	There may be some data that was used in the past. If possible, uninstall programs related to SQL Server and i-PRO Active Guard Server and delete related folders.	5.4.2 5.4.2.1 5.4.2.2
	Check if the file path length of install package is less than 119 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	-
	If the installation fails even after restarting the PC, please execute “¥03_SQL¥SQLEXPRADV_x64_ENU¥1033_ENU_LP¥x64¥Setup¥SQLSUPPORT.MSI”. And then, execute “MultiAIStartup.exe” again.	

Problem	Cause and solution	Refer
	If the installation fails with the error “-2068052310”, If you are using [install to PC with VMS server], please contact your system administrator. If you are using [install to dedicated server PC], please try the following. Check if the following programs are present by going to “Control Panel¥All Control Panel Items¥Programs and Features”. - Microsoft ODBC Driver 17 for SQL Server - Microsoft OLE DB Driver for SQL Server - SQL Server Native Client If they exist, uninstall them, If present, uninstall and run “MultiAIStartup.exe” again.	
	If the installation fails with the error “-2061893606”, check the sector storage sizes. 1) Start a command prompt with administrator privileges, and for the C drive, please execute the following command. “fsutil fsinfo sectorinfo C:” 2) Check if the following items. - PhysicalBytesPerSectorForAtomicity - PhysicalBytesPerSectorForPerformance If greater than “4096”, consider installing on another SSD/HDD or another PC. If changing the PC is difficult, please consider the following Microsoft Troubleshooting Resolutions. We are unable to assist you with Microsoft troubleshooting. https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/database-file-operations/troubleshoot-os-4kb-disk-sector-size?tabs=registry-editor	
Screen transitions in the installer may take some time.	Any SQL Server service may not be running on the destination PC. If possible, please start SQL Server from Services or wait for a while until the screen transition.	

Problem	Cause and solution	Refer
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, another software uses 8092 or you changed after installation, enter the port number.	4.3.2.2
	Supported browser is Microsoft Edge 85(or later), Chrome 83(or later) and Firefox 95(or later.)	3.2
	Please confirm related service exists on PC that i-PRO Active Guard server is installed. Search for Services App in search box and run it. - MultiAICameraService - MultiAISupportProcessManagementService If these services do not exist, please perform the following steps. 1. Uninstall i-PRO Active Guard server. 2. Delete SQL instances or database related to i-PRO Active Guard server. 3. Confirm related services do not exist. If related services remain, start command prompt with administrator privileges and delete services with following command. sc delete MultiAICameraService sc delete SupportProcessManagementService 4. Reinstall i-PRO Active Guard server.	5.4.2 5.4.2.1 5.4.2.2 4.3.1

Problem	Cause and solution	Refer
	Please confirm related service is running on PC that i-PRO Active Guard server is installed. Search for Services App in search box and run it. - MultiAICameraService - MultiAISupportProcessManagementService - SQL Server (instance name) If stopped, right click and run.	5.6.1
Cannot log in to i-PRO Active Guard configuration	If you forget the administrator account, reset account from PC that i-PRO Active Guard server is installed.	5.9
	If you select [Use existing SQL Server instance] and install SQL, make sure TCP Port is configured. If the setting is blank, please set "1435". 1.Run “SQL Server Configuration Manager.exe” 2.SQL Server Network Configuration - Protocols for (instance name) - TCP/IP - IP Addresses tab – IPAll - TCP Port=1435. If 1435 is already used, set other empty port and uninstall i-PRO Active Guard server and install again. 	4.3.1 5.4.2
Cannot register VMS.	Check if IP address, port, protocol and credentials are correct.	4.3.2.2
	Check if web-SDK is enabled from Config tool on Security Center.	4.2.3
	Supported version of Security Center is SC 5.10.1.0 or later.	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 Security Center in advance.	4.2.1
	Check if “Digest” is used for authentication on camera side. ([Settings] - [User mng.] - [User auth.])	-
	Please try updating the camera’s firmware and AI application firmware	

Problem	Cause and solution	Refer
	Check if the number of cameras registered on Security Center exceeds 10,000. *The number of cameras includes cameras other than i-PRO cameras.	-
Plugin icons are not displayed in Security Desk	May not be displayed depending on the version of VMS and plug-ins. Please refer to version compatibility. https://i-pro.com/products_and_solutions/en/surveillance/learning-and-support/knowledge-base/product-tips/active-guard-links	
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
	Please confirm related service exists on PC that i-PRO Active Guard server is installed. Search for Services App in search box and run it. - MultiAICameraService - MultiAISupportProcessManagementService If these services do not exist, please perform the following steps. 1. Uninstall i-PRO Active Guard server. 2. Delete SQL instances or database related to i-PRO Active Guard server. 3. Confirm related services do not exist. If related services remain, start command prompt with administrator privileges and delete services with following command. sc delete MultiAICameraService sc delete SupportProcessManagementService 4. Reinstall i-PRO Active Guard server.	5.4.2 5.4.2.1 5.4.2.2 4.3.1

Problem	Cause and solution	Refer
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 Security Center. When you re-register the camera to Security Center 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 5.3
Face, People, Vehicle License plate, Code or Container images cannot be searched from Plug-in (the number of search results is 0).	Receiving status from each camera 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. note) License plate detection, Code detection and Container detection is not support “last diagnosis time”.	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.	-
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.	-
Notifications such as registered face detection or registered people detection cannot be shown	Check if custom event and actions (e.g., Trigger alarm) are configured. In case of duplicate custom event id, keep the id set on the i-PRO Active Guard server and change the id of the other event.	4.7
	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

Problem	Cause and solution	Refer
System alarm cannot be shown	Check if custom event and actions (e.g., Trigger alarm) are configured. In case of duplicate custom event id, keep the id set on the i-PRO Active Guard server and change the id of the other event.	4.7
Restore failed	Check the SQL Server instance. If the SQL Server instance is different from the backup, please install i-PRO Active Guard server again with the same SQL Server instance as the backup.	5.6
[i-PRO Active Guard Plugin] in Config Tool-Plugins is not displayed	Please restart Config Tool.	4.4.2

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 4.3.8.4)

Problem	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 do 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 disconnects	4355,4356,4358	Check network connection between camera and i-PRO Active Guard server. Check camera work (recording to VMS and live monitoring) If problem continues after restart 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, Vehicle, License plate, Code or Container Images cannot be searched from Plug-in (the number of search results is 0).	66052,66053	Receiving status from each camera 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.
False detection (Not face, people or vehicles are searched)	-	To avoid false detection, configure mask area using iCT (Refer to 4.1).

Problem	Error code	Cause and solution
Detection failure (Not face, people or vehicles are searched)		Please enable Stream1 in Security Center Administration settings. 1 Open the Video task and select the Roles and units. 2 Select the camera to configure, and then click the Video tab. 3 select a video stream1(H.264-1 or H.265/HEVC-1) tab at the bottom of the Video tab. 4 In the Stream usage section, turn on one or more items.
Detection images are not displayed in Monitoring tasks.	-	Please try the following: 1 Upgrade “Genetec Security Center” version to V5.12.2 or later. 2 Update VMS Server version information in i-PRO Active Guard Server. (refer to 5.3.3) 3 Execute the following “Setup.exe” included with the “i-PRO Active Guard Server” installer and install the Genetec SDK. Path: 04¥Tools¥ Security_Center_v5.12.2.0_b2181.29_SDK¥ Setup.exe 4 If Genetec SDK version earlier than 5.12.2181.29 is installed, please uninstall it.
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.

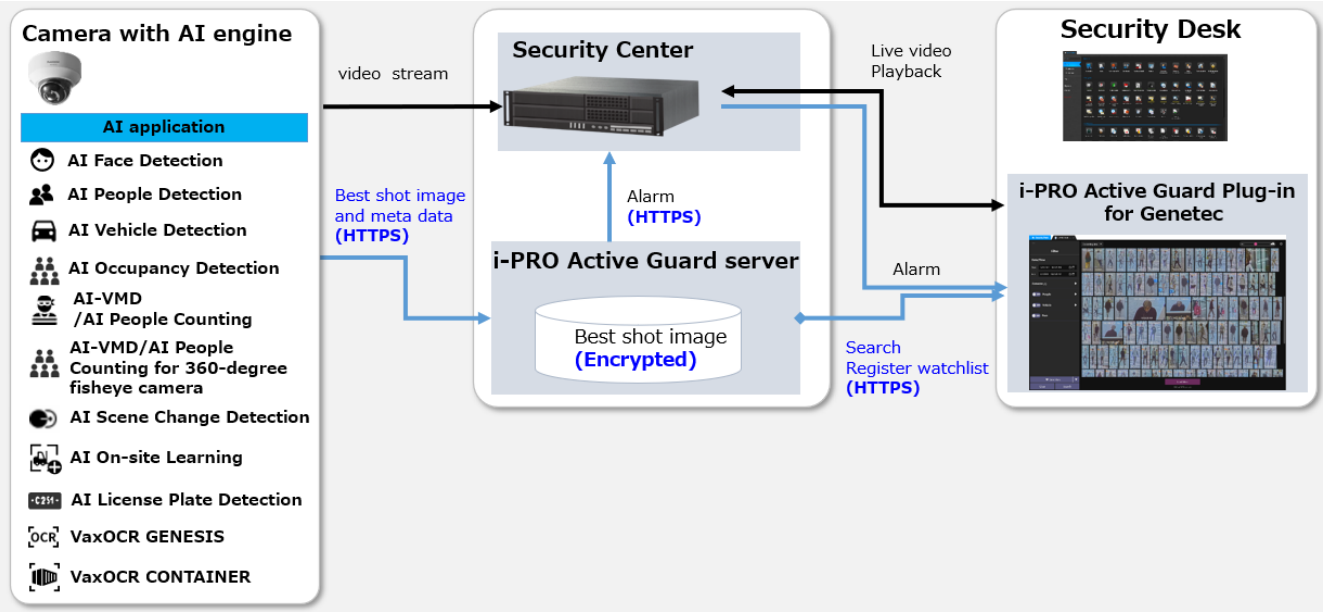
Problem	Error code	Cause and solution
Reach the max disk space of image (delete old images)	65795	Old images have been deleted by exceeding the settings for “Max usage of image storage drive”. If you need to store data for “Retention period”, configure mask area on camera side using iCT (Refer to 4.1) to reduce the number of detections.
The display of Web setting page is misaligned.	-	Please try clearing the cache in your web browser, and close the web browser, access it again.

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 Security Center 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 configuration (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

Select “use SSL connection” on Config tool (Refer to 4.2.3)

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, images 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.

7.3. How to use 3rd party extension software

3rd party camera extension software developed for i-PRO camera can be used in the i-PRO Active Guard system. Not all 3rd party extension software cannot be used, software that implements specific integration can be used. You can check the extension software that can be connected to i-PRO Active Guard from application list when released.

This document does not include install or configuration for 3rd party extension software itself and includes other procedure after them.

7.3.1. Required software version

i-PRO Active Guard server: v1.6.1 or later.

7.3.2. i-PRO Active Guard server configuration

This section describes the steps required to register camera with 3rd party extension software to i-PRO Active Guard server and receive event data.

STEP1

Edit configuration file to register the extension software.

Open the file “C:¥MultiAI¥Backup¥3rdpartyApp.config” in the PC that i-PRO Active Guard server software is installed.

Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.

Input the extension software name, event name and custom event id, and also enable the line by removing ";" at the beginning of the line.

Ex.)

```
application_name_1 = "SampleApplication"
event_name_1 = "SampleDetection"
genetec_custom_event_id_1 = 12000
```

Save and close the file after editing.

Note)

Up to 10 extension software and 10 events can be registered in a system.

The extension software name and event name of the extension software will be shown on application list when released. It will not work if any other name is configured.

For i-PRO Active Guard server v1.8.0 or later, you can register 3rd party LPR app.

If you would like to register as an LPR app, please add the below text to “3rdpartyApp.config”.

Ex.)

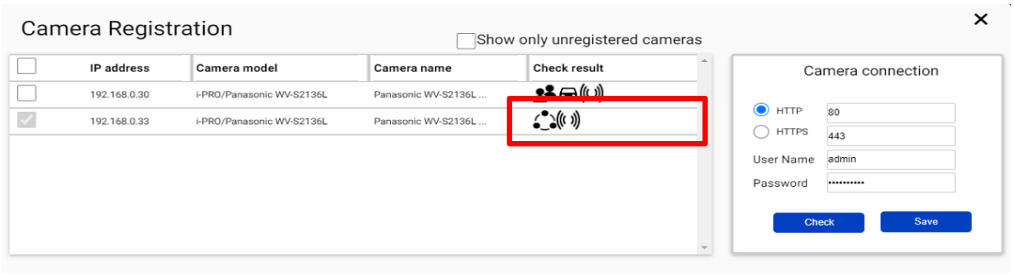
lpr_application_name = “ SampleApplication “

* For LPR app, "event_name" and “genetec_custom_event_id” not required.

For new installations of i-PRO Active Guard server v1.8.0 or later, the above LPR app sample text already included in “3rdpartyApp.config”.

STEP2

Register camera to i-PRO Active Guard server (Refer to 4.3.2.3).



When the 3rd party extension software is installed in the selected camera, icon will be shown in the [Check result]. If not shown, please check if configuration file is edited correctly.

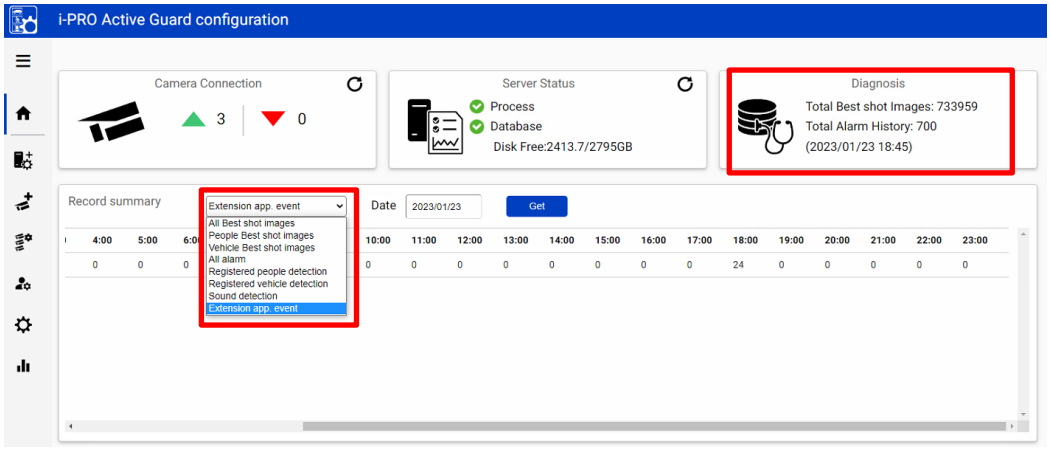
Note)

For LPR app is checked, icon will be shown.

STEP3

Check if an event has occurred (Optional).

[Extension app. event] can be selected to confirm the number of detections. (Refer to 4.3.8.3)



* It takes about 15 min for an event to appear on the screen after it has occurred.

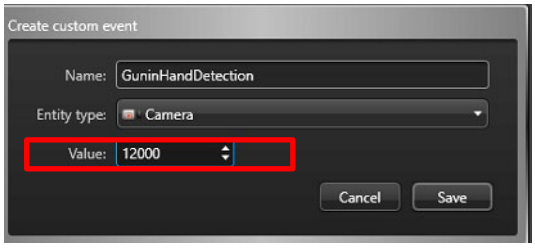
7.3.3. Configure custom event (mandatory)

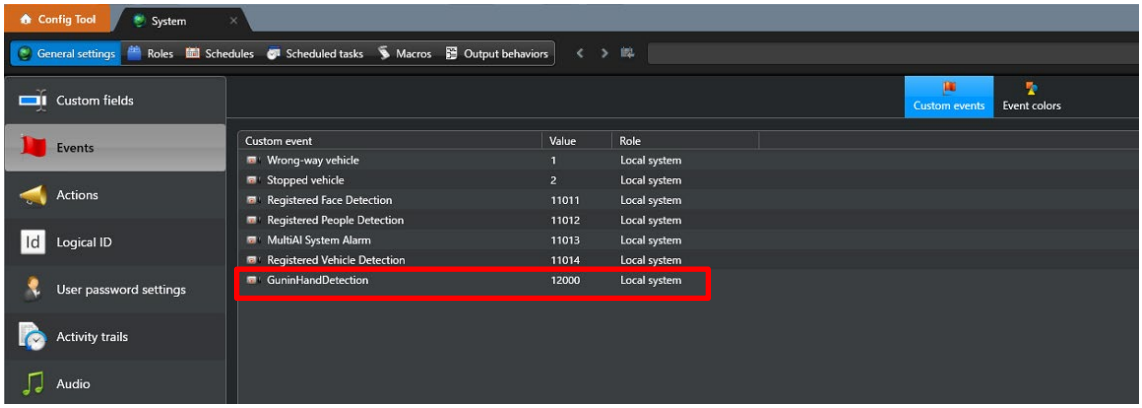
Similar to the procedure described in 4.7, 3rd party extension software event can be used as custom event.

Add extension software event with the value. The value should be matched with configured value in “C:¥MultiAI¥Backup¥3rdpartyApp.config” on i-PRO Active Guard server side.

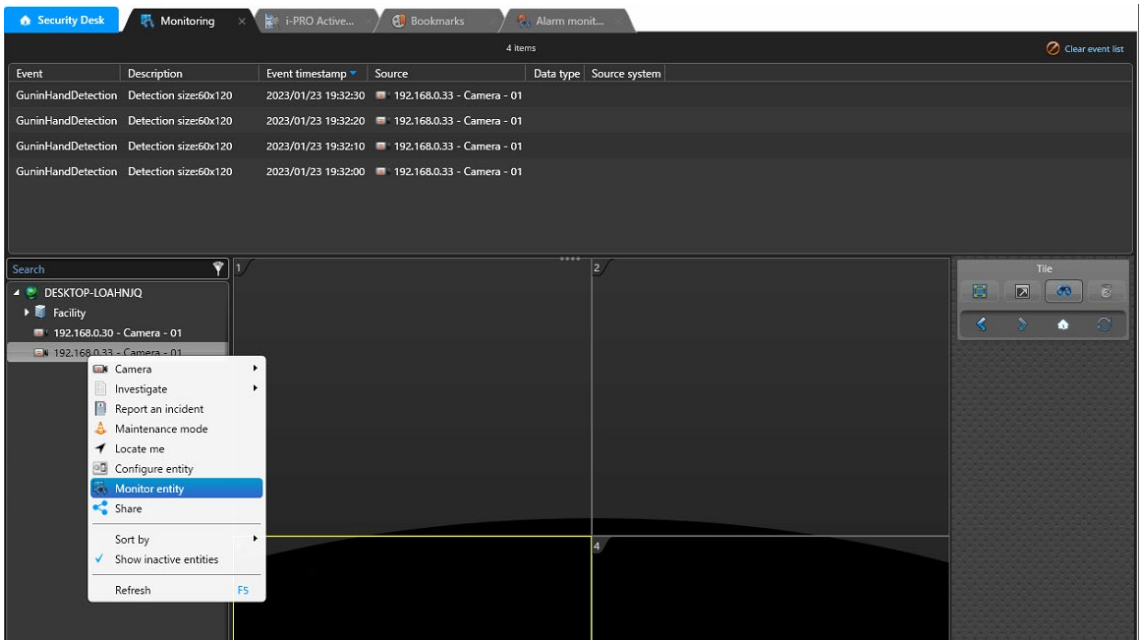
Note)

- The MultiAI path above is the default, if you changed the path in section 4.3.1, please replace the path.

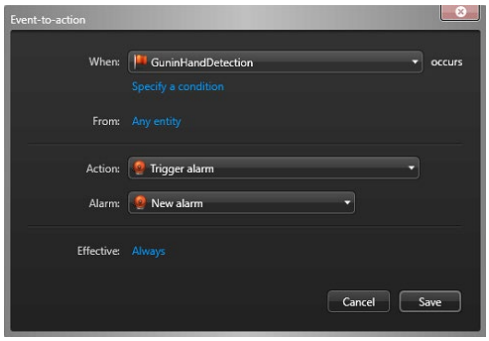


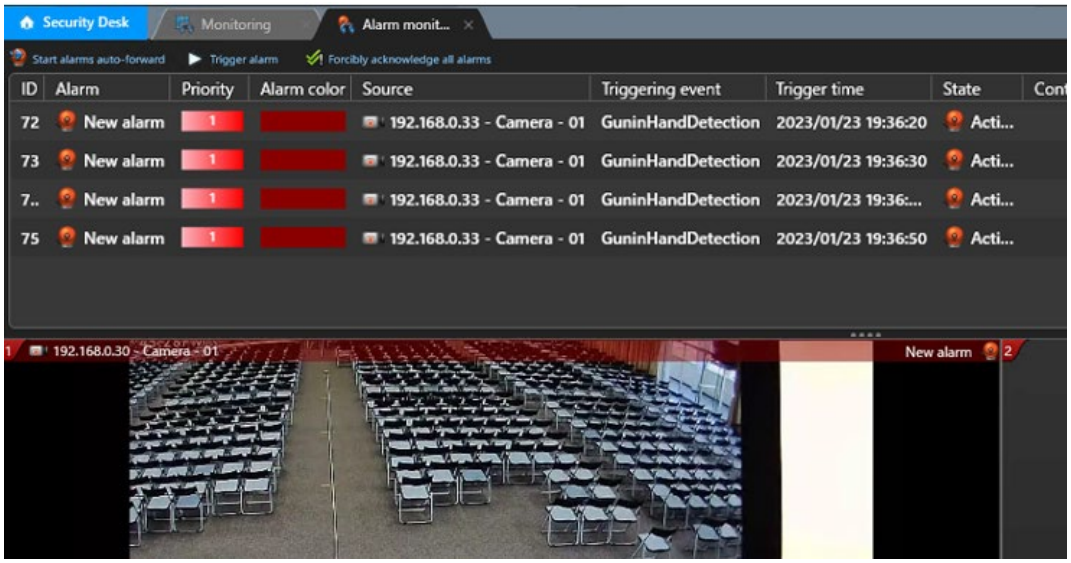


By enabling [Monitoring] – [Monitor entity], extension software event will be shown.


Security Desk
Monitoring
i-PRO Active...
Bookmarks
Alarm monit...
4 items
Clear event list
Event
Description
Event timestamp
Source
Data type
Source system
GuninHandDetection
Detection size:60x120
2023/01/23 19:32:30
192.168.0.33 - Camera - 01
GuninHandDetection
Detection size:60x120
2023/01/23 19:32:20
192.168.0.33 - Camera - 01
GuninHandDetection
Detection size:60x120
2023/01/23 19:32:10
192.168.0.33 - Camera - 01
GuninHandDetection
Detection size:60x120
2023/01/23 19:32:00
192.168.0.33 - Camera - 01
Search
DESKTOP-LOAHNJQ
Facility
192.168.0.30 - Camera - 01
Camera
Investigate
Report an incident
Maintenance mode
Locate me
Configure entity
Monitor entity
Share
Sort by
Show inactive entities
Refresh
F5
Tile

Configure Actions (Optional).





7.4. Specifications

The details of the specifications are as follows.

Scale	Supported camera	i-PRO network camera with AI engine
	Number of cameras	1 to 100 CH when installed with VMS server (AI Face Detection is up to 20) 1 to 300CH when installed in dedicated server (AI Face Detection is up to 100)
	Number of clients	No limitation (depending on limitation of VMS)
	Number of Recording server	- (only main server should be registered)
	Number of i-PRO Active Guard server per a client	No limitation (Depending on the capability of whole system)
Supported AI applications	For plugin	AI Face Detection / AI People Detection / AI Vehicle Detection / AI License Plate Detection / VaxOCR GENESIS / VaxOCR CONTAINER
	For dashboard	AI Face Detection, AI People Detection, AI Vehicle Detection, AI-VMD/AI People Counting for 360-degree fisheye camera, AI-VMD, On-site Learning, AI Occupancy detection, AI License Plate Detection.
Store	Retention period	Max. 31 days limitation for face, people, vehicle or license plate, code or container data / Max. 92 days limitation for count/heatmap/statistics data * Max. 397 days (/ 732 days for count/heatmap/statistics) by upgrading SQL Server Standard edition or higher
Post Search	Filter	People, Vehicle, LPR (attribute, date & time, camera, moving direction) OCR, Container (attribute, date & time, camera) Face (similar face, date & time and camera)
	Similar search	Yes (by same attribute information) *People and Vehicle (by same attribute information) and Face
	Sort	Descending date, Ascending date, Similarity (Face), Only high Relevance (People and Vehicle)
Alarm	Watch list alarm	Up to 30,000 faces, up to 12 people attributes, up to 12 vehicle attributes. Up to 12 LPR attributes or license plates group.

		Up to 12 OCR group. Up to 12 Container attributes or Container group. There is no limitation to the number of license plate, OCR code, container code and license plate group, OCR group, container group (*depending on the system design).
	Detection alarm	AI Sound Classification (Gunshot / Yell / Vehicle horn / Glass break) AI-VMD (Intruder / Loitering / Direction / Line cross) All License plate, all OCR code, all Container code / AI Scene change detection
	Related function	AI-VMD, AI Sound Classification, AI Occupancy Detection, AI Scene change detection are supported in Genetec Security Center and Security Desk (not plugin)
Playback/ Export	Playback	Playback video around the time of the bestshot on full and multi-view
	Export video	Save best shot image, Export video from Recording server
	Export Search result	HTML
Dashboard	Supported browser	Microsoft Edge, Google Chrome, and Firefox
	Chart	People counting, occupancy statistics and heatmap when using AI-VMD/AI People Counting for 360-degree fisheye camera. People counting and vehicle counting when using AI-VMD. People counting and occupancy statistics when using AI Occupancy Detection. On-site learning object counting when using AI-VMD with On-site Learning application. Data update interval is minimum 5 seconds for people/ vehicle/On-site learning object counting and 1 min for heat map/ LPR Counting. Age and gender statistics when using AI Face Detection. Data update interval is minimum 1 min. People attribute statistics when using AI People Detection. Data update interval is minimum 1 min. Vehicle attribute statistics when using AI Vehicle Detection. Data update interval is minimum 1 min.
	Customize	Contents, display size, location for each chart. 3 Layouts per user can be saved and 24 users can be

		registered. (Up to 4 users can be log-in at the same time) Basic display color theme (dark or light) Line chart type (Straight line / Smoothed line), line/area name for counting

7.5. Cautions when disposing of or transferring PCs

When disposing of or transferring a PC used with the i-PRO Active Guard system, be sure to follow the uninstallation procedure, see 5.4.