The background is a solid teal color. A large circle is centered on the page, with a thick orange border and a dark brown outer ring. Inside the circle, the text is centered and reads:

ISD-1000iO

Sound & Voice
Analytics
Installation Guide
- For Milestone VMS

Content

1. Product Configuration and Description

Pre-installation Requirement: Milestone VMS

2. Device HW Installation

3. Device HW Settings

4. Sound & Voice Analytics Server Program Setting

5. Abnormal Sound Event & Event Log Testing in Milestone

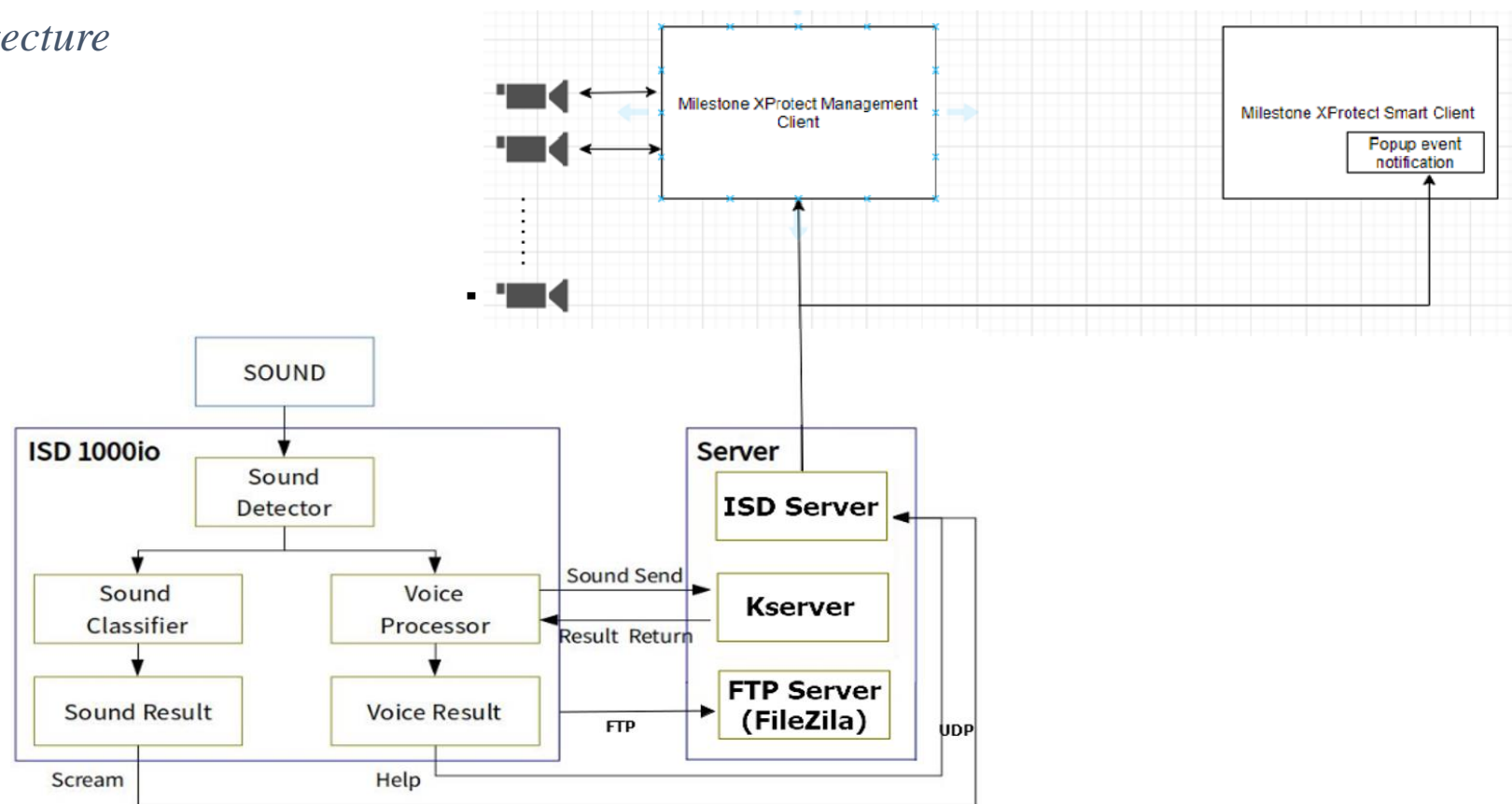
6. Summary



Product Configuration and Description

1 Integration Schematics: Sound and Voice Analytics – Milestone VMS

Figure 1 : Architecture



ISD-1000iO: External sound receiving hardware device with microphone that recognizes abnormal sound and voice.

ISD Server : Interworking program that transmits event data received through ISD-1000iO device to Milestone VMS.

Kserver : A voice recognition server program for classifying voice that received through the ISD-1000iO device.

FileZila : FTP server program to save the event sounds received through the ISD-1000iO device.

1 ISD-1000iO Voice recognition product configuration and description -1

◆ Product Components



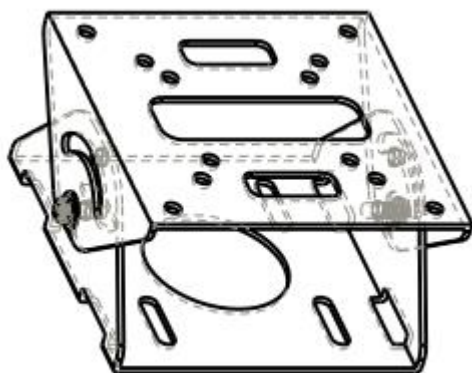
ISD-1000iO Device



Lower cover



Direct Current Power Unit (5V DC)




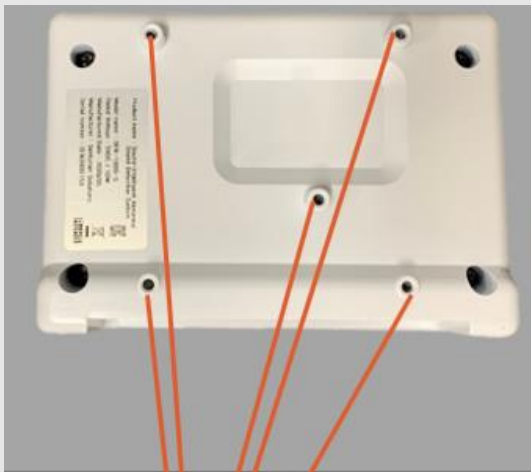
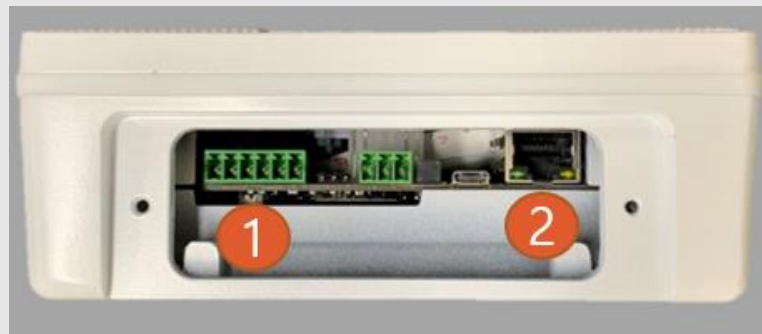
Angle adjusting/ Mount bracket



Etc





① ISD-1000iO Voice recognition product configuration and description -2

◆ Equipment Description

Front view	Back	Bottom
 <p>① Microphone for detecting abnormal sound ② LED for status indication (blue, green, red) ③ Waterproof flexible Connector</p>	 <p>VESA Mount hole</p>	 <p>① 5V IN Power Terminal ② RJ45 terminal</p>

1 ISD-1000iO Voice recognition product configuration and description -3

◆ Status LED Description

Explanation	Detailed image
<ul style="list-style-type: none"> "Turned on" until the device reboot (takes 3-5min) "Flashes" when sound source is detected (left) "Flashes" once per second during normal operation of device (center) Power "Always on" after system boot (right)	

※ Each LED direction is based on the front of the equipment.

Pre-installation Requirement






- Step 1. Milestone-related Program Installation**
- Step 2. Adding Camera to Milestone**
- Step 3. Neurolytics plugin Settings in MIP**
- Step 4. ISD Server Settings**
- Step 5. Adding MIP driver to Milestone**
- Step 6. Adding Metadata (Camera to MIP driver)**
- Step 7. SA Event and Alarm Settings**
- Step 8. CCTV Footage View grid Settings**

The detailed Milestone VMS user manual found in the following link

https://doc.milestonesys.com/latest/en-US/portal/htm/chapter-page-sc-user-manual.htm?TocPath=XProtect%20Smart%20Client%7CXProtect%20Smart%20Client%20user%20manual%7C___0

https://doc.milestonesys.com/sc/pdf/2020r3/en-US/MilestoneXProtectSmartClient_UserManual_en-US.pdf

Milestone – SA Plugin System; Installer & License files

	Name ▾
	1_Milestone installer
	2_Plugin file
	3_ISD1000iO installer files_Milestone VMS
	ISD-1000iO Speech Recognition+Milestone...

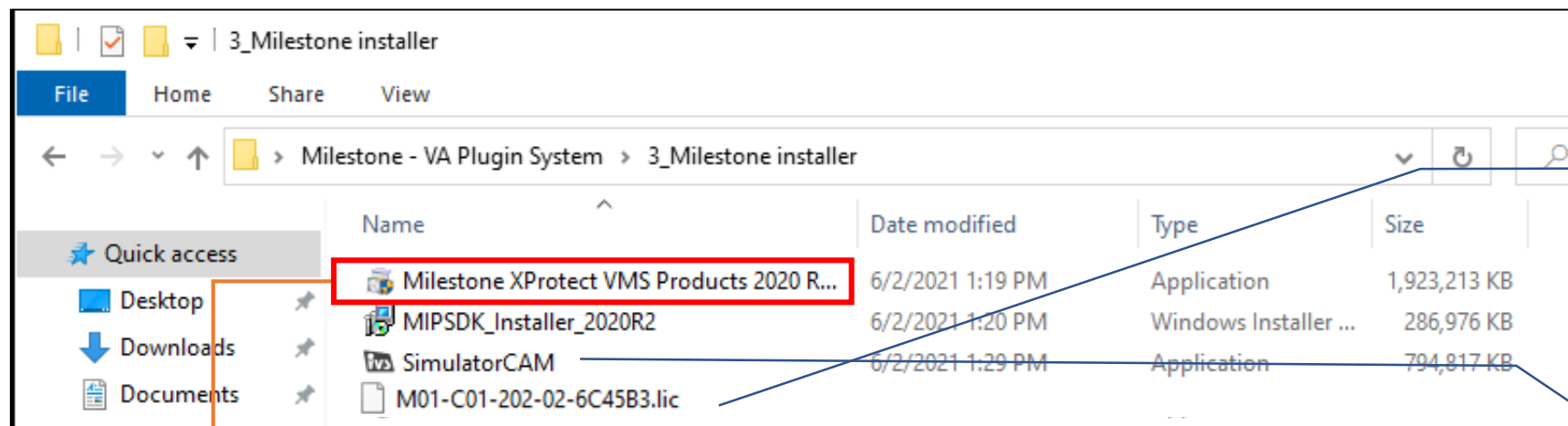
Make sure that all installer and relevant license files are received before starting the installation process

Download and install Visual C++ Redistributable Packages

<https://www.microsoft.com/en-us/download/confirmation.aspx?id=14632> (2010)

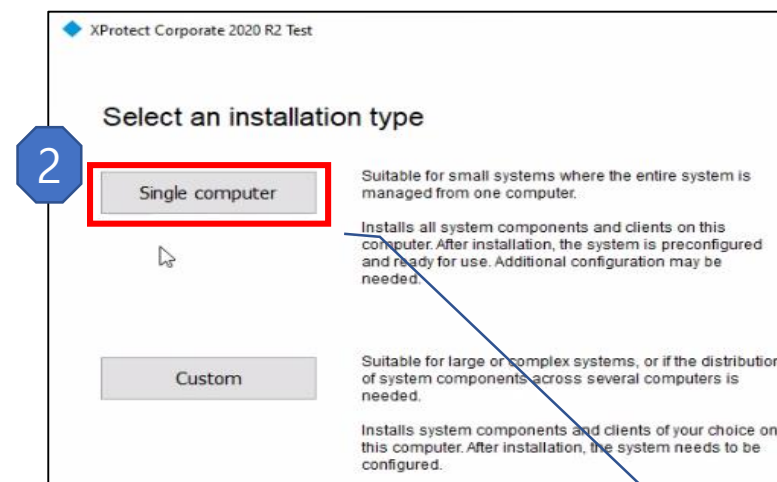
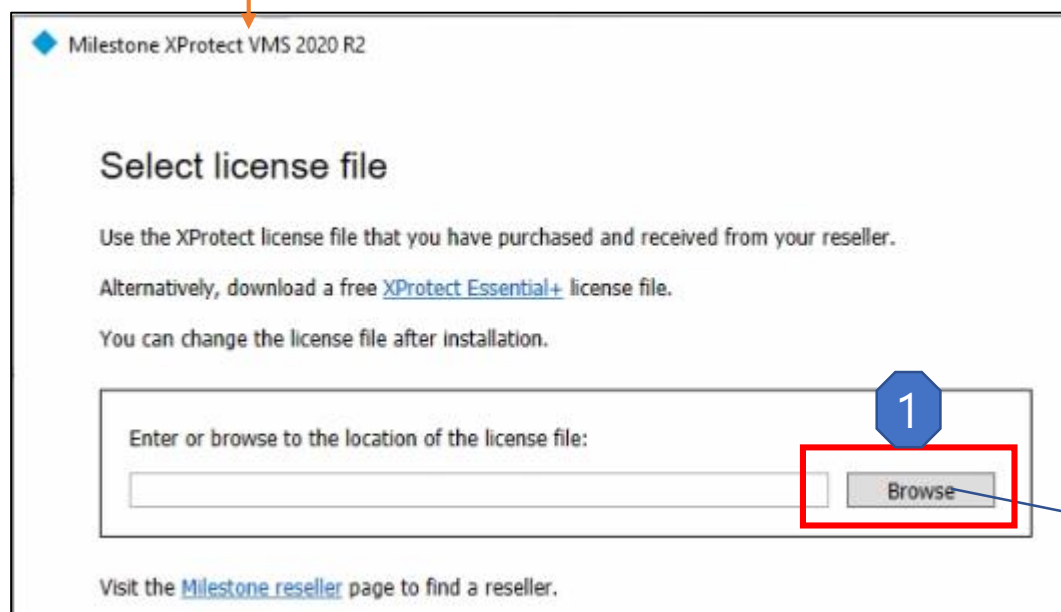
<https://www.microsoft.com/en-us/download/confirmation.aspx?id=48145> (2015)

Step 1. Milestone-related Program Installation



Milestone License

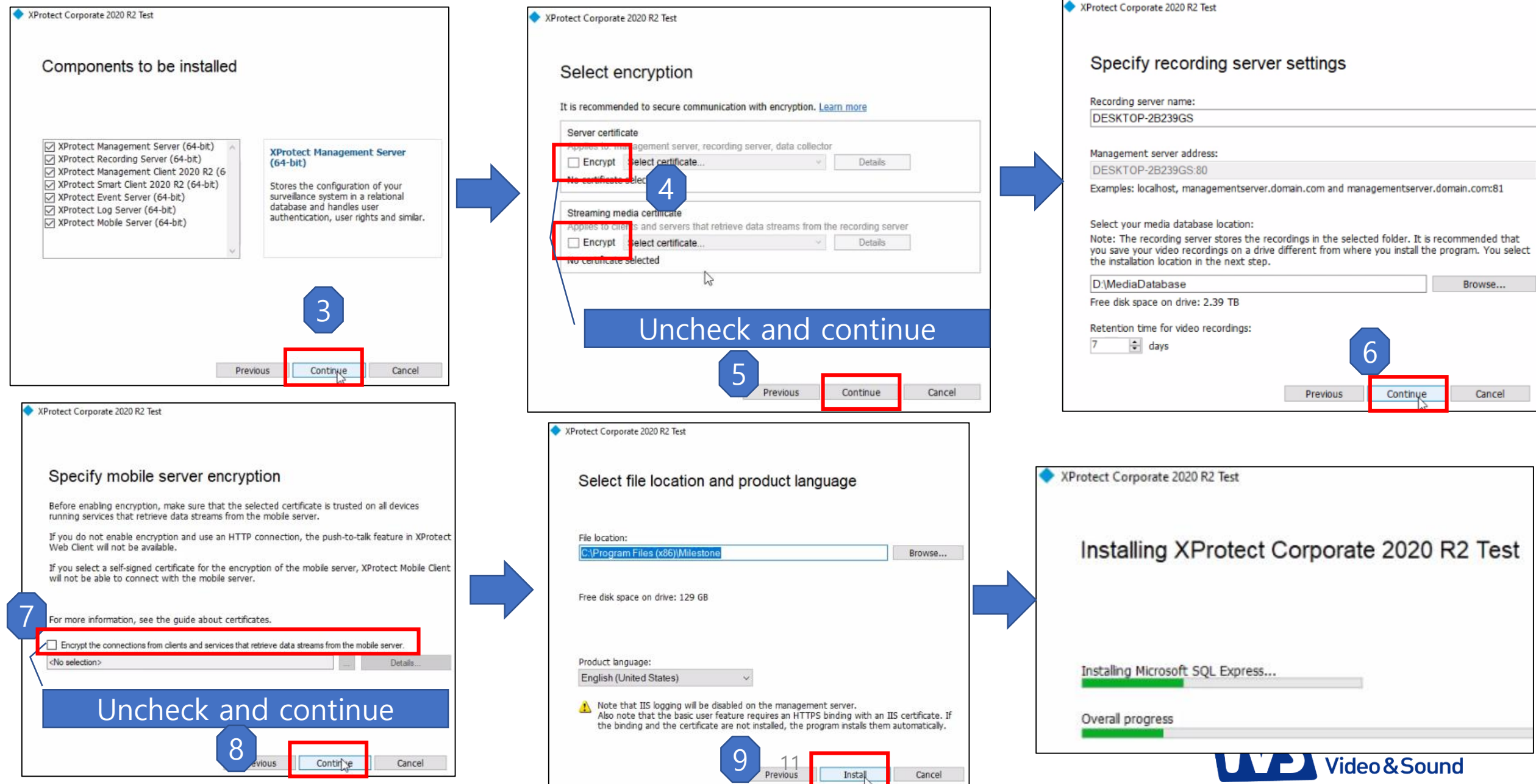
Optional for demo use
(if there are no real camera)



Locate Milestone License

Choose Single computer

Step 1. Milestone-related Program Installation



Step 1. Milestone-related Program Installation

XProtect Corporate 2020 R2 Test

The installation is complete

These components have been successfully installed. Click Continue to add hardware and users, or click Close to make the configurations in the Management Client.

XProtect Management Server (64-bit)

XProtect Recording Server (64-bit)

XProtect Event Server (64-bit)

XProtect Log Server (64-bit)

XProtect Management Client 2020 R2 (64-bit)

XProtect Smart Client 2020 R2 (64-bit)

XProtect Mobile Server (64-bit)

Share these addresses with your users for online access to the system.

Web Client address:
<http://DESKTOP-2B239GS:8081/>

Mobile Client address:
<http://DESKTOP-2B239GS/>

10

Continue Close

XProtect Corporate 2020 R2 Test

Enter user names and passwords for hardware

If you have changed hardware user names and passwords from the manufacturer defaults, add the values here. While scanning for hardware, the system will look for manufacturer default credentials as well as your customized credentials.

11

User name	Password
ivstech	*****

Enter user name/password and continue

12

Continue Close

XProtect Corporate 2020 R2 Test

Select the hardware to add to the system

☒ Discovered hardware:

No hardware found.

13

Previous Continue Close

Add users

You can add different types of users to access the system: Windows users or basic users. Basic users require a user name and a password. These users must be assigned to either the Operators role or the Administrators role.

14

15

User type: Basic user

User name: ivstech

Role: Administrators

Repeat password: *****

16

17

Add

User type: Basic user

User name: ivstech

Role: Administrators

Password: *****

Repeat password: *****

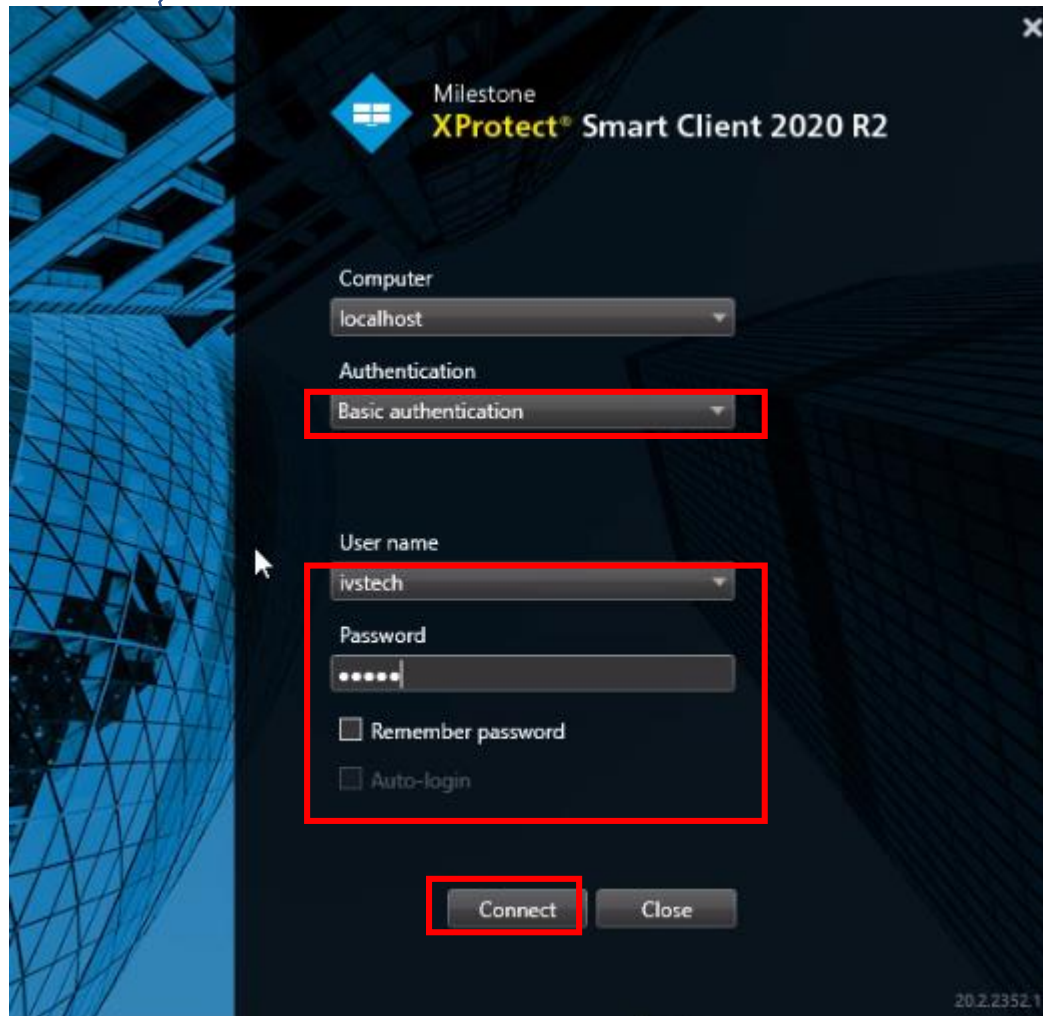
Add

18

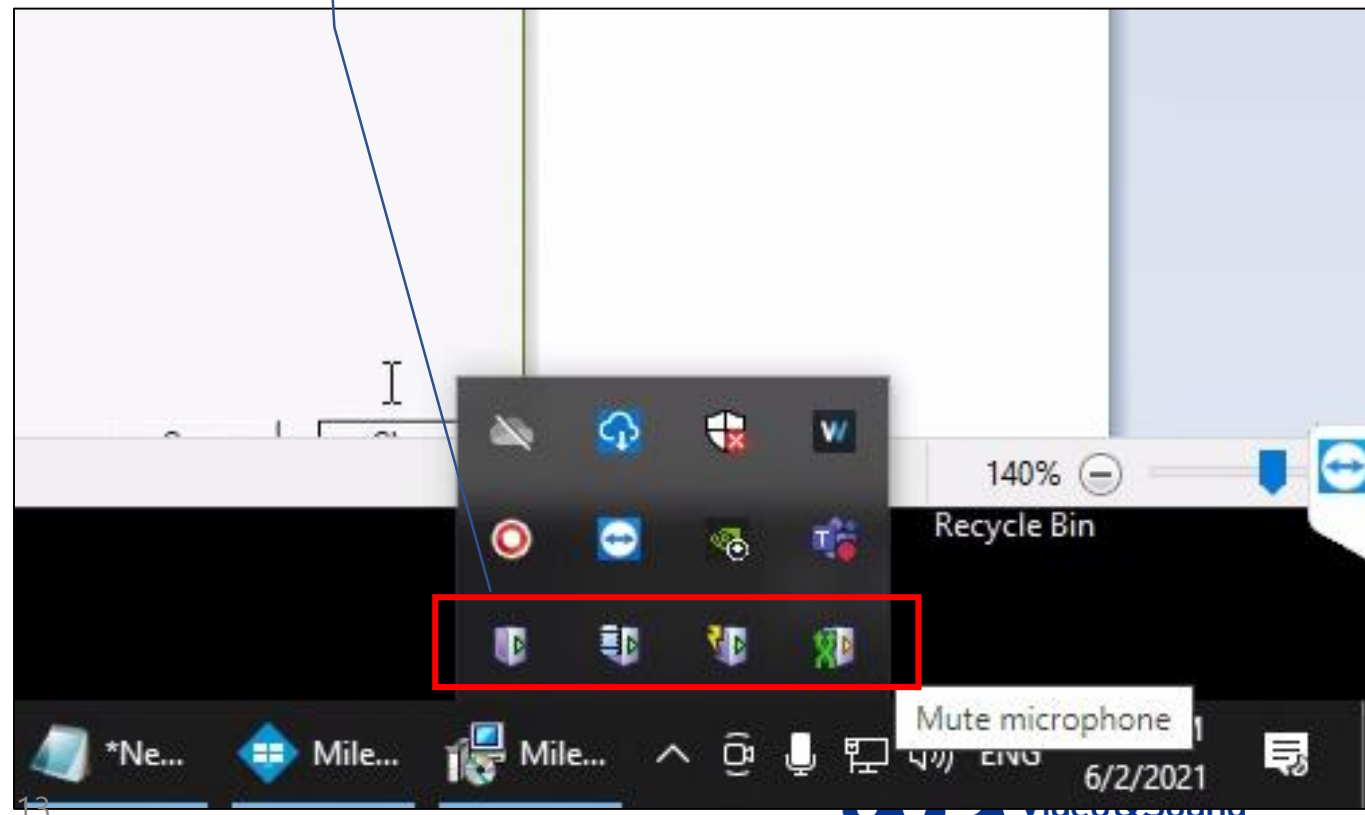
Continue Close

Step 1. Milestone-related Program Installation

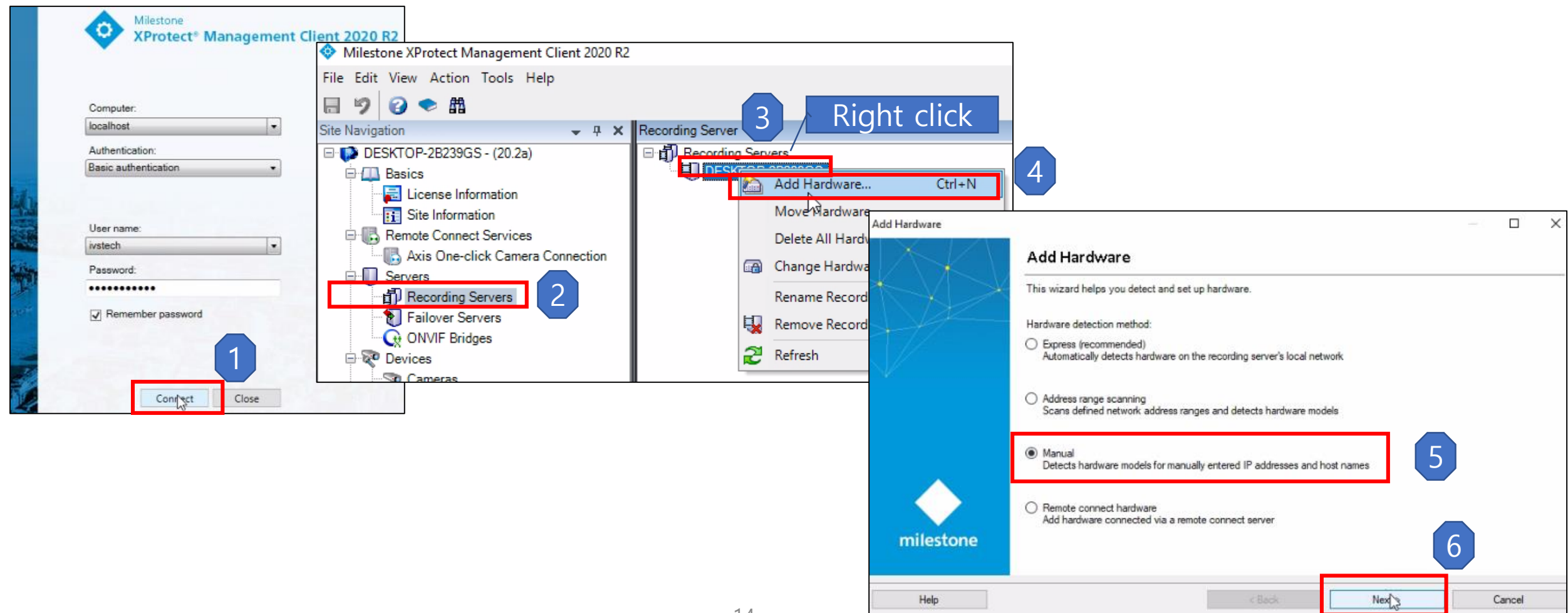
Run the "Smart client" & connect



Make sure all the Milestone sever programs are running in the background.
- It can be verified by "desktop tray" icon as shown below.



Step 2. Adding Camera to Milestone



Step 2. Adding Camera to Milestone

7

Optional. Specify additional user credentials to connect with if the hardware is not using the factory defaults.

Include	User name	Password	
<input type="checkbox"/>	(Factory default)	*****	
<input checked="" type="checkbox"/>	ivstech	*****	

8

Add Remove

9

Optional. Specify additional user credentials to connect with if the hardware is not using the factory defaults.

Include	User name	Password	
<input type="checkbox"/>	(Factory default)	*****	
<input checked="" type="checkbox"/>	ivstech	*****	

10

Help < Back Next > Cancel

11

Select which drivers to use when scanning for hardware.
The more drivers selected, the slower the scanning.

12

13

Universal

- ☒ Universal 1 channel driver
- ☐ Universal 16 channels driver
- ☐ Universal 64 channels driver

Next >

14

Enter the network address and port of the hardware you want to add.
Optionally, select the hardware model to speed up detection.

Address	Port	Use HTTPS	HTTPS port	Hardware model	
localhost	8554	<input type="checkbox"/>	443	Universal 1 channel driver	

15

Next >

Step 2. Adding Camera to Milestone

Add Hardware

Wait while your hardware is being detected.
Once detection has completed, select which hardware to add.

Detected hardware:

Add	Address	Port	Hardware model	Status
<input checked="" type="checkbox"/>	localhost	8554	Universal 1 channel driver	<input checked="" type="checkbox"/> Success

☒ Show hardware running on other recording servers

Help < Back **Next >** Cancel

Add Hardware

Hardware and cameras are enabled per default. Manually enable additional devices to be used.
The hardware and its devices will be assigned auto-generated names. Alternatively, enter names manually.

Hardware name template: Default Device name template: Default

☒ Hardware ☒ Camera ☐ Microphone ☐ Speaker ☐ Metadata ☐ Input ☐ Output

Hardware to Add	Enabled	Name
Universal 1 channel driver - localhost	<input type="checkbox"/>	
Hardware:	<input checked="" type="checkbox"/>	Universal 1 channel driver (localhost)
Camera port 1:	<input checked="" type="checkbox"/>	Universal 1 channel driver (localhost) - Camera 1
Microphone port 1:	<input type="checkbox"/>	Universal 1 channel driver (localhost) - Microphone 1

Help < Back **Next >** Cancel

Add Hardware

Select a default group for all devices type.
Alternatively, select device group individually for each device.

Default camera group: No group selected... **Cameras**

Default microphone group: No group selected...

Select Group

Cameras

Camera Group 1

OK

Devices

Devices	Add to Group
Cameras	
Universal 1 channel driver (localhost) - Cam...	Default Group

< Back **Finish** Cancel

Step 2. Adding Camera to Milestone

Recording Servers

DESKTOP-2R239GS

Universal 1 channel driver (localhost)

Universal 1 channel driver (localhost) - Camera 1

Universal 1 channel driver (localhost) - Microphone 1

1

Frames per second

RTSP Port

Streaming Mode

Video stream 2

Codec

Connection URI

Frames per second

RTSP Port

Streaming Mode

Video stream 3

Codec

Connection URI

Frames per second

RTSP Port

Streaming Mode

Video stream 4

Codec

Connection URI

Frames per second

RTSP Port

Streaming Mode

3

Milestone XProtect Management Client 2020

Do you want to save changes?

Yes

No

Cancel

4

Live: 1280x720 29KB

Universal 1 channel driver (localhost)

5

Device information

Name

Universal 1 channel driver (localhost) - Camera 1

Short name

Description

Hardware name

Universal 1 channel driver (localhost)

Port number

1

Positioning information

GPS coordinates

(Example: -33.856900, 151.215100)

Direction (a)

0

Degrees

Field of view (b)

0

Degrees

Depth (c)

0

Feet

Preview position in browser...

Illustration

North

a

b

c

2

Info

Settings

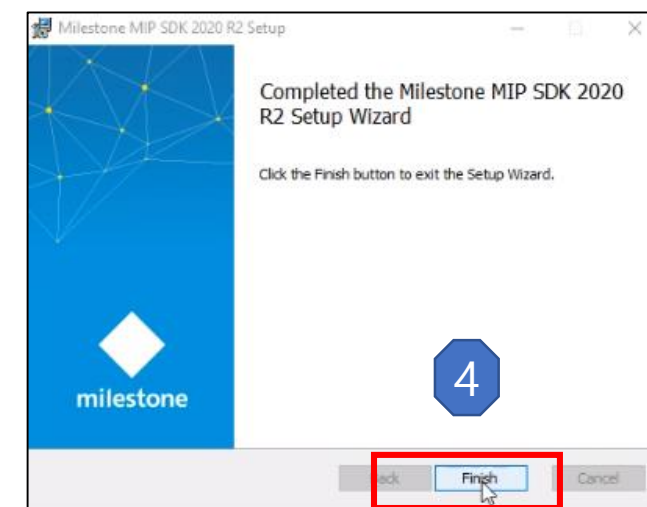
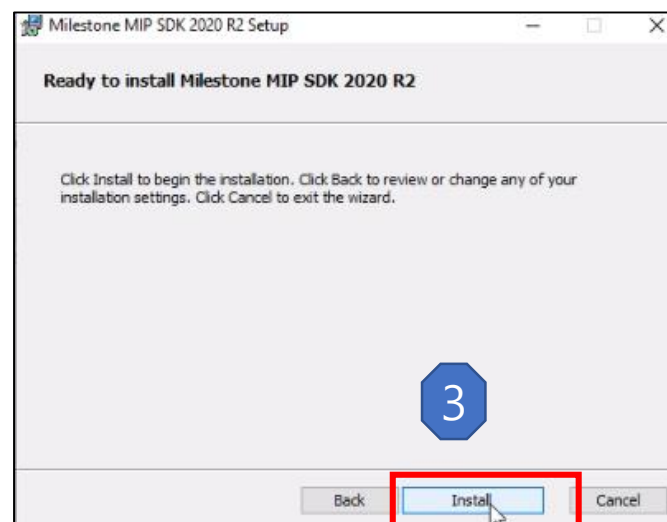
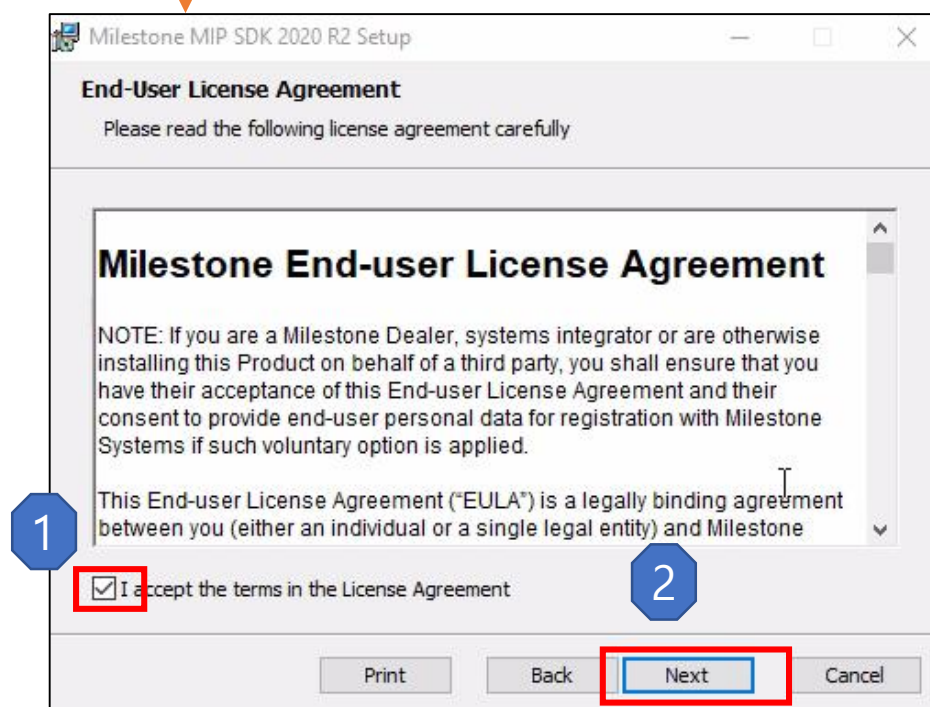
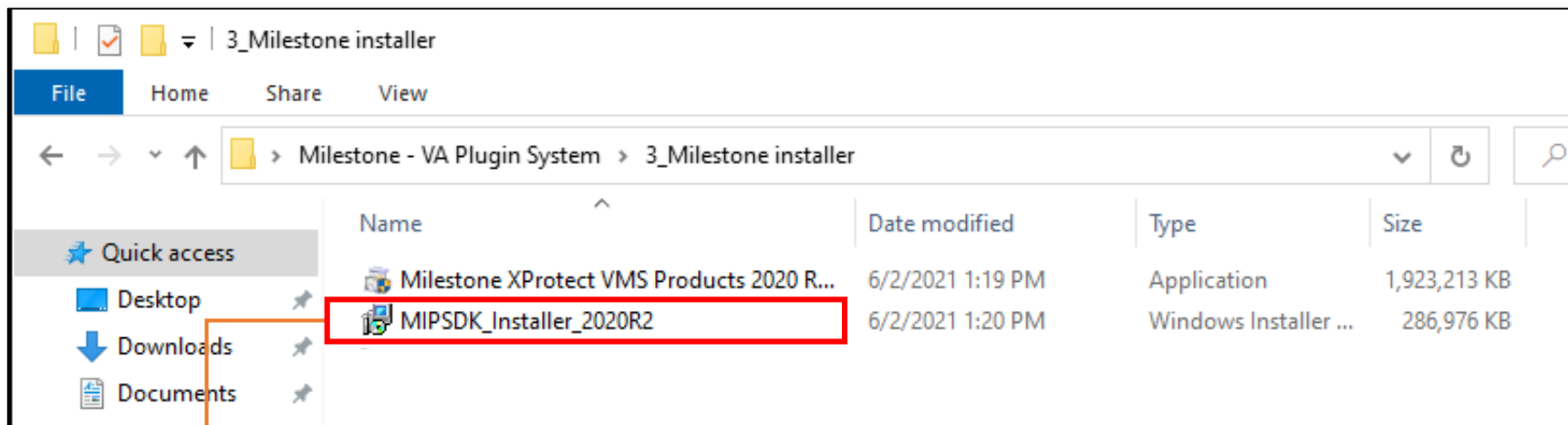
Streams

Record

Motion

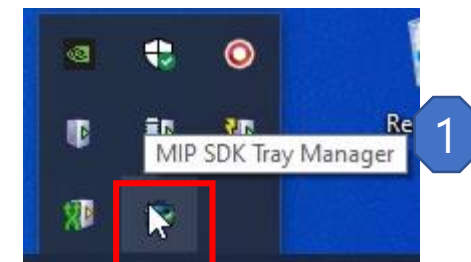
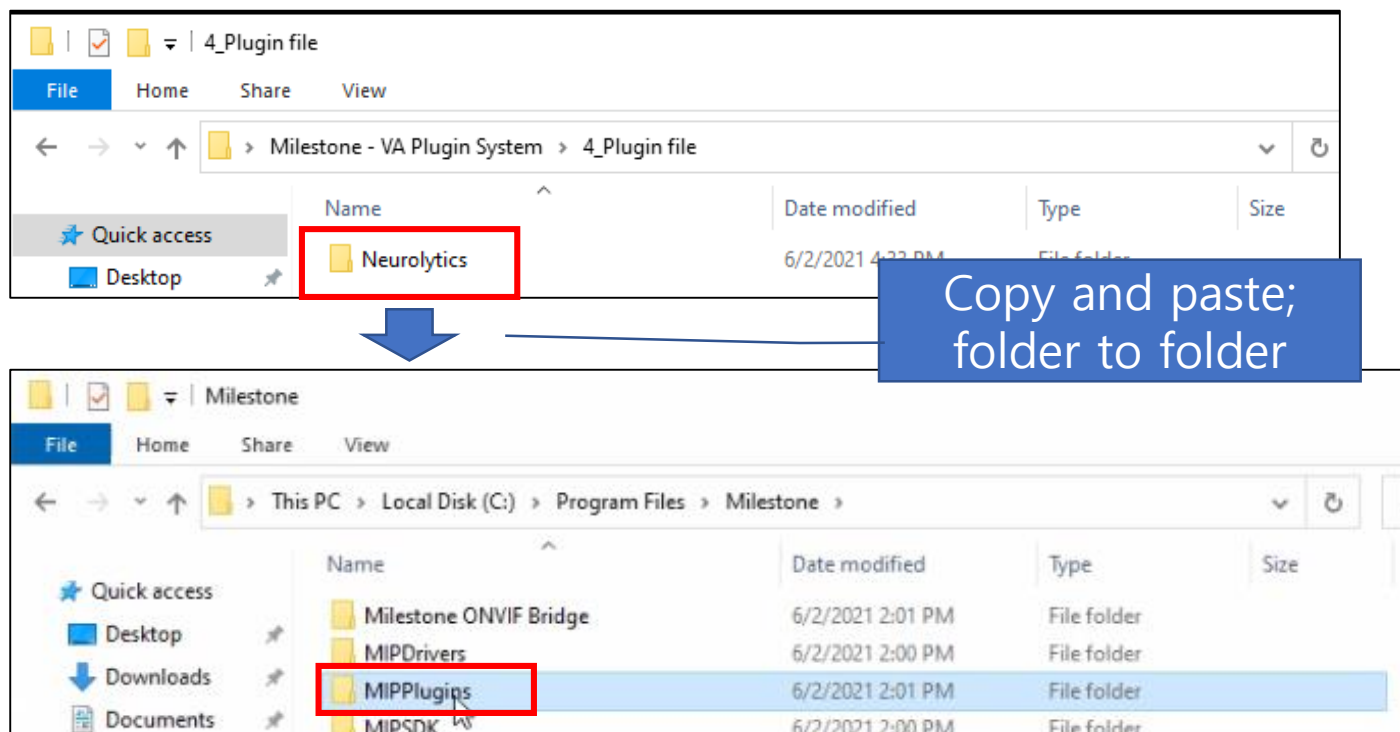
Fisheye Lens

Step 3. Neurolytics plugin Settings in MIP

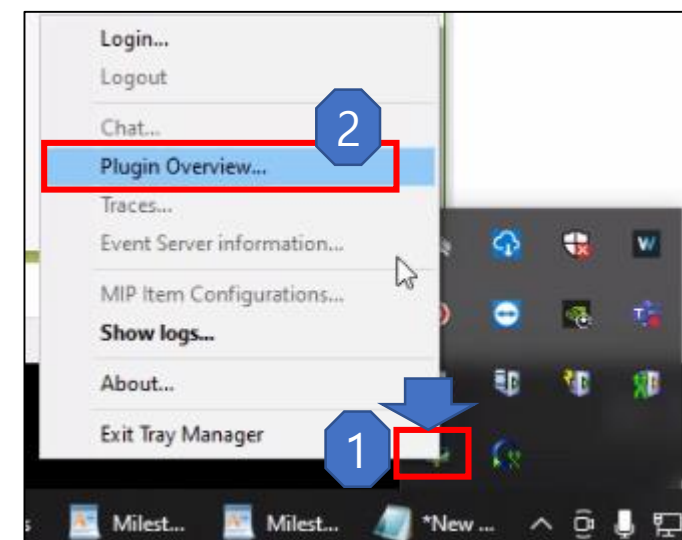


Step 3. Neurolytics plugin Settings in MIP

1. Run **MIPSDK_Installer** provided by Milestone.
2. Copy plugin folder named "**Neurolytics**" and paste the folder inside the path **C:\Program Files\Milestone\MIPPlugins**



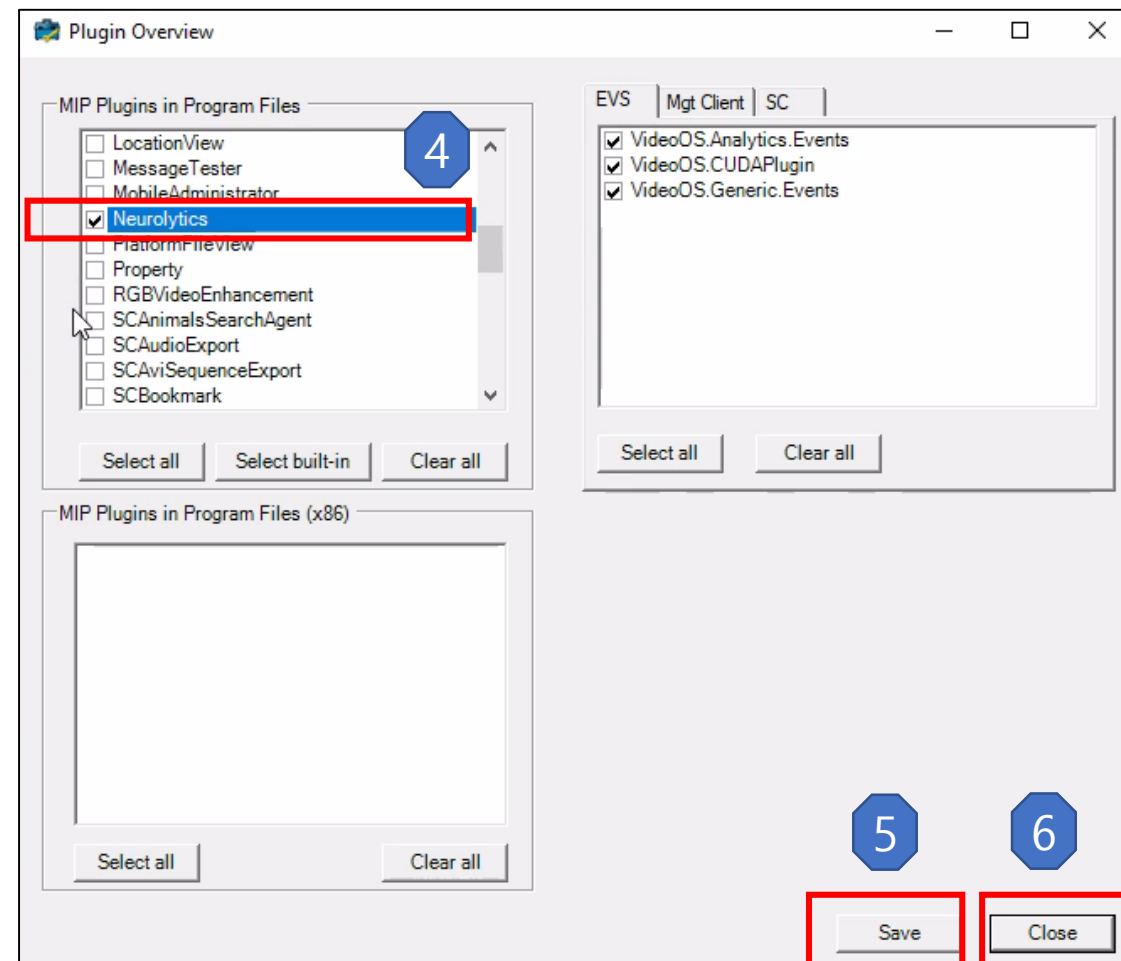
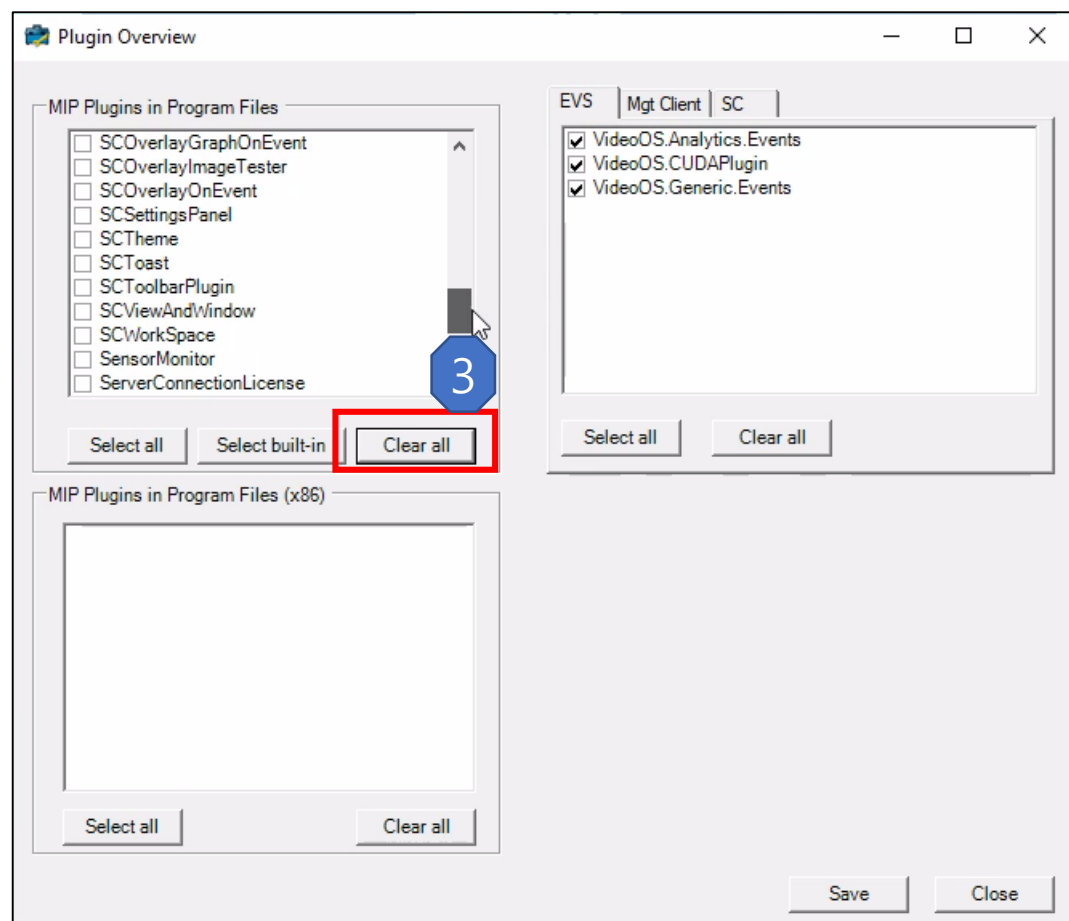
3. Enable **Neurolytics** plugin by opening "**Plugin Overview**" and choosing **Neurolytics** option in "**MIP SDK Tray Manager**" program as shown in the picture:



Step 3. Neurolytics plugin Settings in MIP

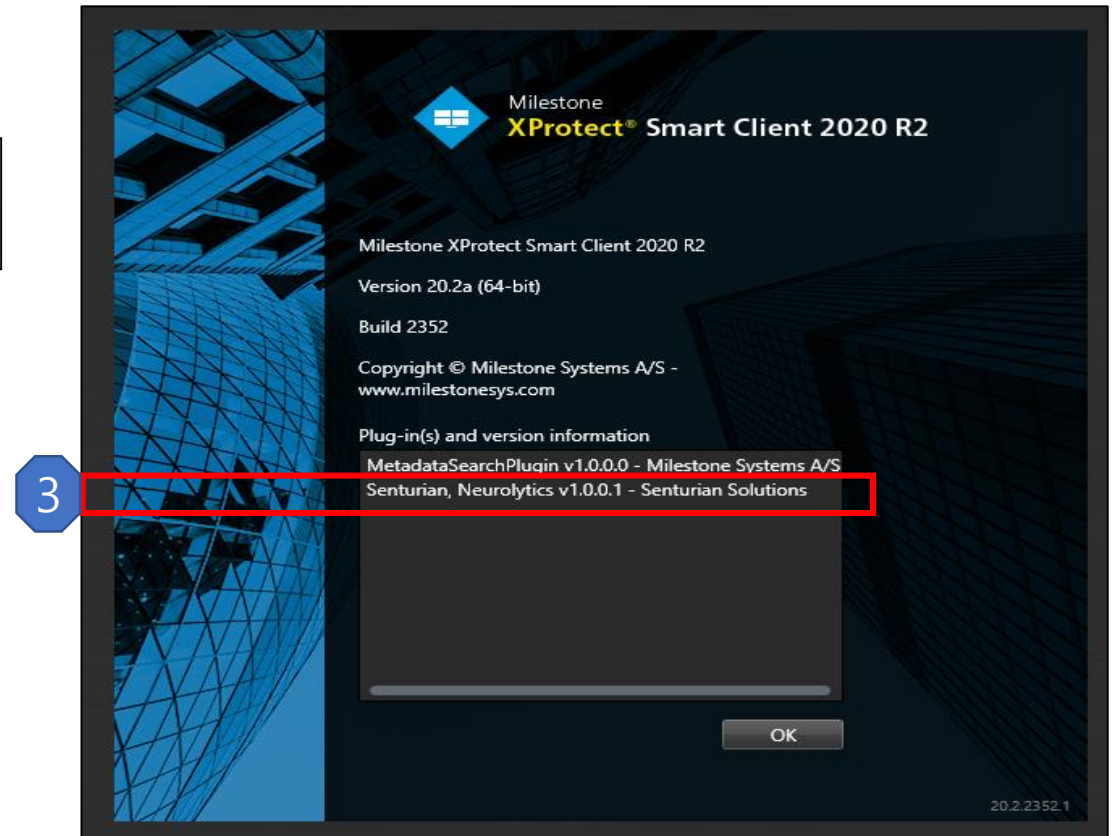
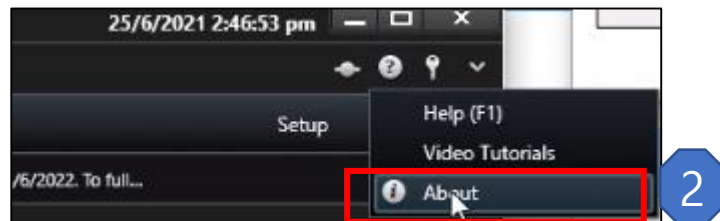
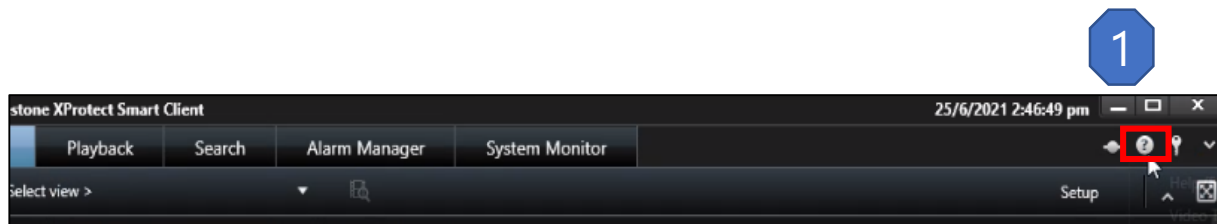
4. Unselect all plugin files by “**Clear all**”

5. Enable “**Neurolytics**” plugins by opening “**Plugin Overview**” and select in **Plugin Overview Manager** as shown in the picture. Press “**Save**”.



Step 3. Neurolytics plugin Settings in MIP

- ❖ To verify the **Neurolytics** plugin that installed was successful or not, open XProtect Smart Client program, and go to "**About**" option and click on.
- ❖ It was successful if a pop-up window show as below.



Step 4. ISD Server Settings -1

◆ ISDserver is an interworking program that transmits events to Milestone VMS.

Program image

A. ISDserver.exe Connection

1) Execute ISDserver.exe in the ISD folder.

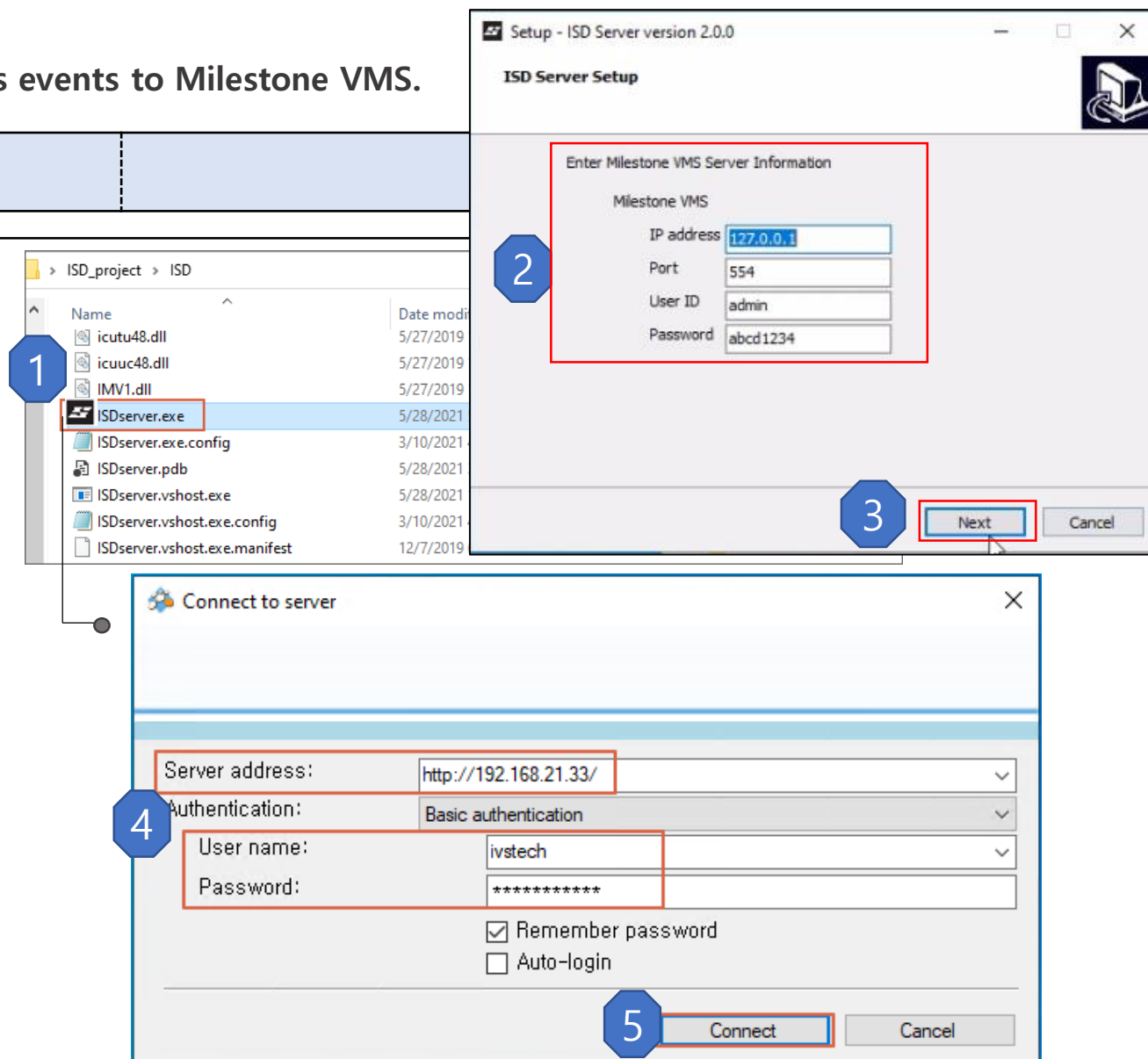
2) Milestone VMS is installed in the Server address of the "Connect to server" screen. Enter the IP address of the server.

※ When using Milestone and ISD together on a local server, Enter <http://localhost/>

4) Enter your Milestone account information in User Name and Password.

※ Milestone related information is changed according to the setting value when installing Milestone.

5) Click "Connect" button to connect to ISDserver.



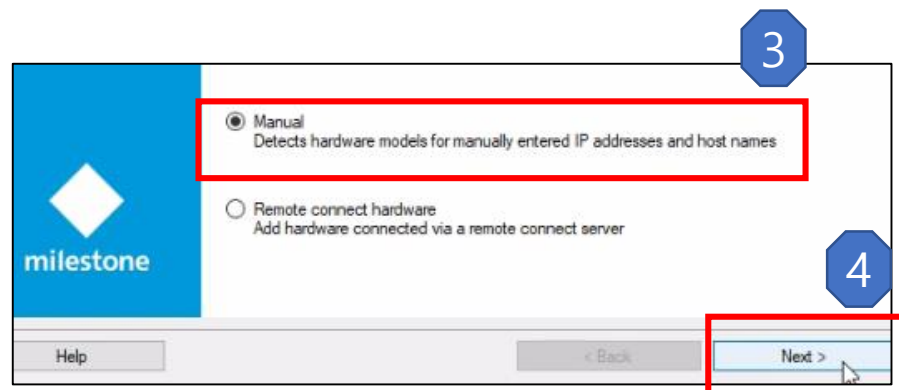
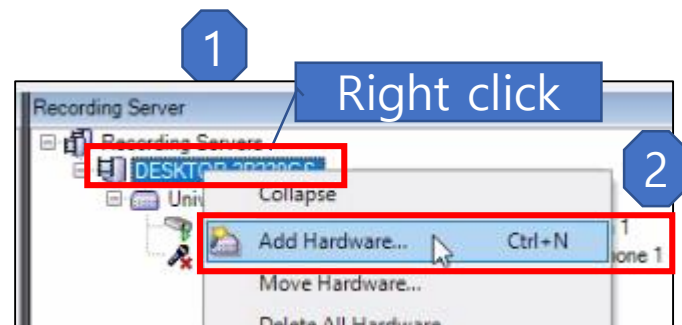
Step 4. ISD Server Settings -2

◆ ISDserver is an interworking program that transmits events to Milestone VMS.

Program image	Explanation
<div>B. ISDserver.exe settings</div> <div>1) Click "Choose Folder" to select a folder to extract camera information from.</div> <div>2) Click "Export" button to extract information of all cameras connected to Milestone VMS.</div> <div>※ After executing the ISDserver program, "Caminfo.txt" file is created in the selected folder.</div> <div>Information of all cameras connected to Milestone VMS is entered in the file.</div> <div>3) Click the "Start server" button to connect to the server.</div> <div>※ After clicking the button, "Waiting... " status and ready to link.)</div>	<div><div><div>ISD server</div><div><div>1</div><div>Choose Folder</div><div>C:\Users\WIV\STECH\De</div></div><div><div>2</div><div>Exported</div></div></div><div><div>3</div><div>Start server</div><div>Waiting ...</div><div>Close</div></div></div> <div><div>ISD</div><div><div>Caminfo.txt</div><div>Caminfo.txt - Notepad</div><div>CAM ID CAM NAME</div><div>de6439db-9a36-4c3e-9b37-9afc939ebfa7 MDC-L7290FTD-24 MDC-L7290FTD-24 (192.168.21.60) - Camera 1</div><div>67bcdbf2-35c1-42b3-a36c-76d6859882cf TRUEN Co., Ltd. IVS-P5236W12R (192.168.21.203) - Camera 1</div></div></div>

Step 5. Adding MIP driver to Milestone

Notes: MIP driver can only be added when the ISD server is running



Step 5. Adding MIP driver to Milestone

Collected hardware information:

Address	Port	Hardware model	Status
localhost	5000	MIP Driver	✓ Success

1

2

Next >

Hardware name template: Default

Device name: Default

check

3

4

Metadata

Hardware to Add	Enabled	Name
MIP Driver - localhost	<input checked="" type="checkbox"/>	
Hardware:	<input checked="" type="checkbox"/>	MIP Driver (localhost)
Metadata port 1:	<input checked="" type="checkbox"/>	MIP Driver (localhost) - Metadata 1
Metadata port 2:	<input checked="" type="checkbox"/>	MIP Driver (localhost) - Metadata 2
Metadata port 3:	<input checked="" type="checkbox"/>	MIP Driver (localhost) - Metadata 3
Metadata port 4:	<input checked="" type="checkbox"/>	MIP Driver (localhost) - Metadata 4
Metadata port 5:	<input checked="" type="checkbox"/>	MIP Driver (localhost) - Metadata 5
Metadata port 6:	<input checked="" type="checkbox"/>	MIP Driver (localhost) - Metadata 6

Next >

Select a default group for all device types.
Alternatively, select device group individually for each device type.

Default camera group: No group selected...

Default microphone group: No group selected...

Default speaker group: No group selected...

Default metadata group: No group selected...

Default input group: No group selected...

Default output group: No group selected...

5

Devices

- Metadata
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)
- MIP Driver (localhost)

Select Group

Metadata

Metadata Group 1

6

7

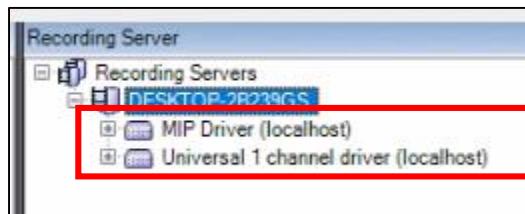
OK

Hardware	Default Group
MIP Driver (localhost) - Metadata 5	Default Group
MIP Driver (localhost) - Metadata 6	Default Group
MIP Driver (localhost) - Metadata 7	Default Group
MIP Driver (localhost) - Metadata 8	Default Group
MIP Driver (localhost) - Metadata 9	Default Group
MIP Driver (localhost) - Metadata 10	Default Group
MIP Driver (localhost) - Metadata 11	Default Group
MIP Driver (localhost) - Metadata 12	Default Group

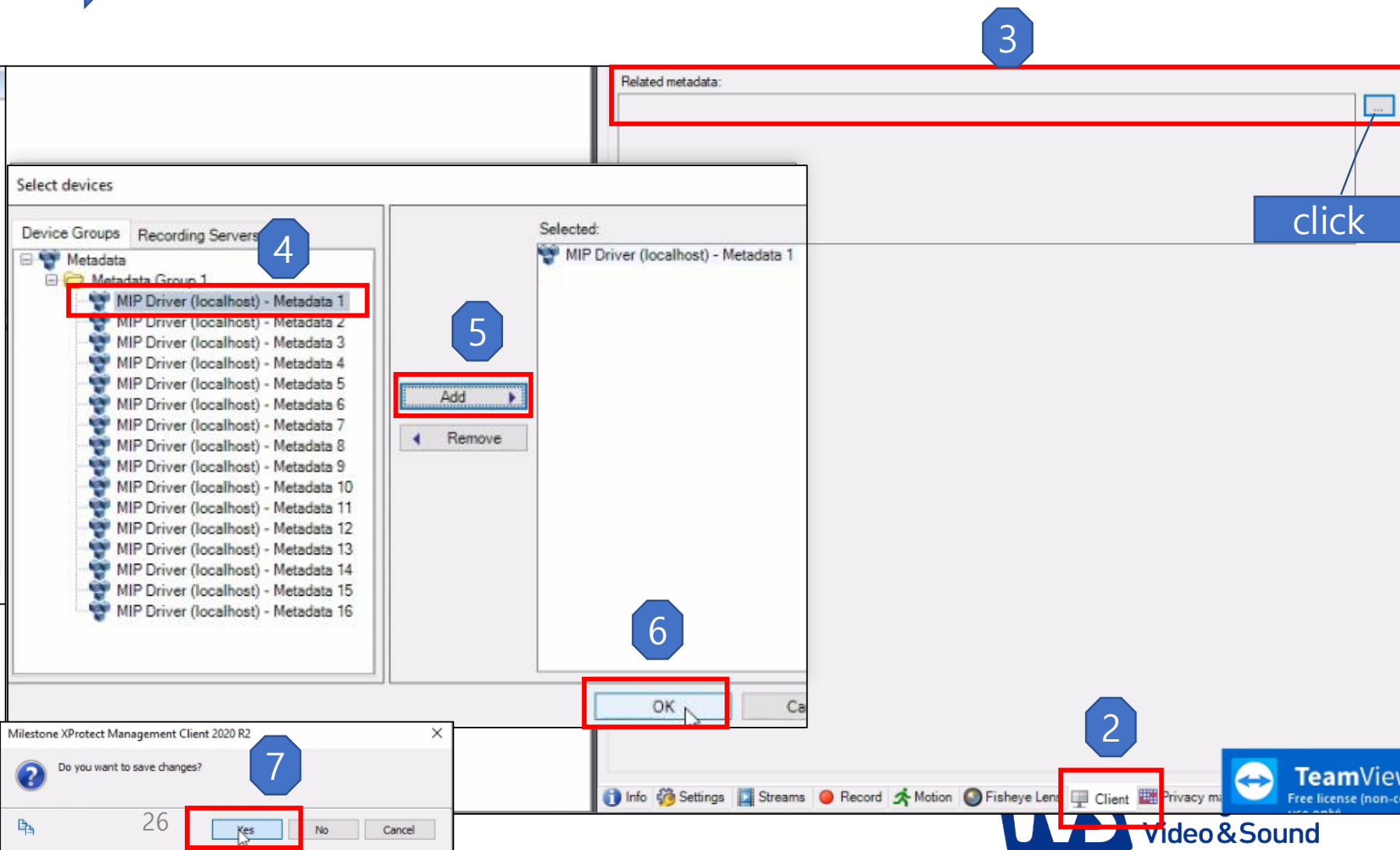
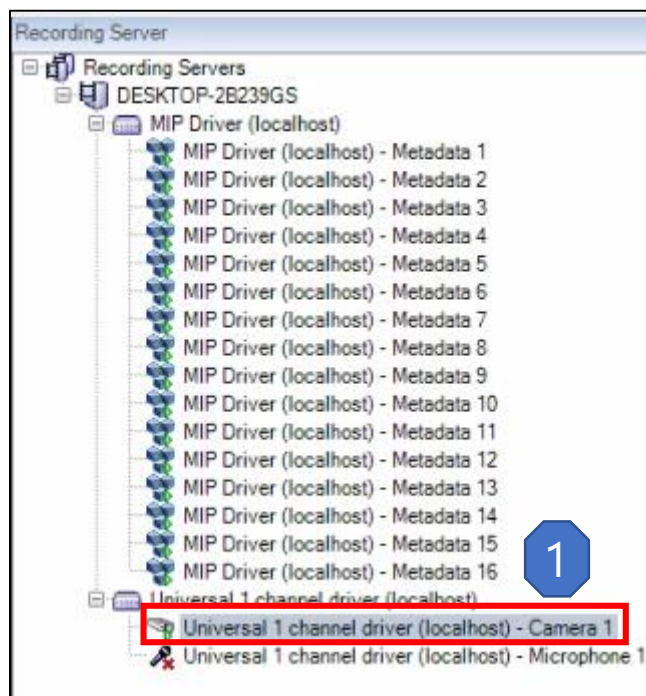
8

Finish

Step 6. Adding Metadata (Camera to MIP driver)



- Note that you have to associate metadata channels with cameras and MIP in a one-to-one mapping manner.



Step 7. SA Event and Alarm Settings

1

2

3

4

Right click

Analytics Events

Analytics Event

Name: ISDEvent

Description:

Do you want to save changes?

Yes No Cancel

1

2

3

Right click

Alarm Definitions

Alarm Definition

Alarm definition

Enable: ☒

Name: IVS

Instructions:

Trigger

Triggering event:

Sources:

Activation period

☒ Time profile: Always

☐ Event based: Start: Stop:

Map

An alarm only appears on the smart map if at least one source of the alarm is a camera.

Alarm manager view: ☐ Smart map ☒ Map

Related map:

Operator action required

Time limit: 1 minute

Events triggered:

Other

Related cameras:

Initial alarm owner:

Initial alarm priority: 1: High

Alarm category:

Events triggered by alarm:

Auto-close alarm: ☐

Alarm assignable to Administrators: ☒

Step 7. SA Event and Alarm Settings

Triggering event: Analytics Events

Sources: Select...

Activation period: ☒ Time profile: Always

Map: Alarm manager view: ☐ Smart map ☒ Map

Related map: Operator action required: Time limit: 1 minute

Events triggered: Other: Related cameras: Initial alarm owner: Initial alarm priority: 1: High

Alarm category: Select...

Select Sources dialog:

Type filter: All

Groups: Servers

DESKTOP-2B239GS

Camera Group 1

Universal 1 channel driver (l)

Add

Remove

Selected: Universal 1 channel driver (localh)

OK

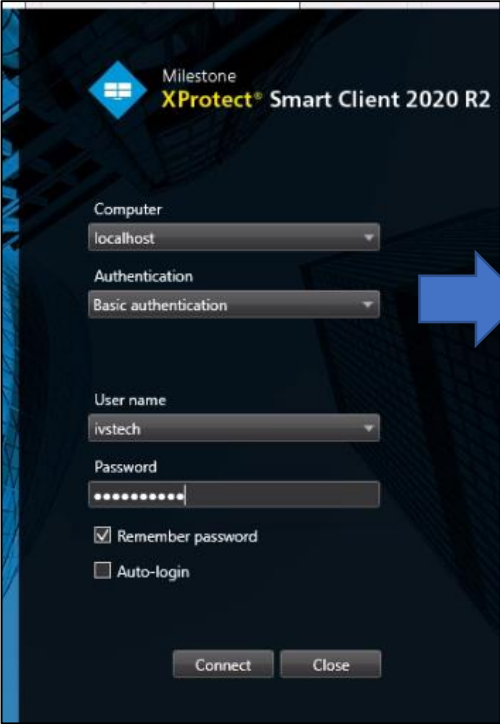
Cancel

Milestone XProtect Management Client 2020 R2

Do you want to save changes?

Yes No Cancel

Step 8. CCTV Footage View grid Settings



The login screen for Milestone XProtect Smart Client 2020 R2 is shown on the left. It includes fields for Computer (localhost), Authentication (Basic authentication), User name (ivstech), Password, and checkboxes for Remember password and Auto-login. A blue arrow points from the login screen to the main interface.

The main interface is shown in two states, illustrating the steps to configure the view grid:

1. Click the **Setup** button in the top right corner.
2. In the **Views** pane on the left, click the **Default group**.
3. Click the **Create New Group** button (represented by a grid icon).
4. In the **Views** pane, click the **New Group** button.
5. In the **System Overview** pane, click the **4:3** button.
6. In the **System Overview** pane, click the **4:3 Portrait** button.

The main interface displays the **XProtect** live view area, the **Views** pane, and the **System Overview** pane. The **System Overview** pane shows the **4:3** and **4:3 Portrait** buttons, which are highlighted with red boxes and numbered 5 and 6 respectively. The **Views** pane shows the **Default group** and **New Group** buttons, which are highlighted with red boxes and numbered 2 and 3 respectively. The **Setup** button is highlighted with a red box and numbered 1.

Step 8. CCTV Footage View grid Settings

The screenshot displays the Milestone XProtect Smart Client interface. The top navigation bar includes tabs for Live, Playback, Search, Alarm Manager, and System Monitor. The main window is titled 'XProtect' and shows a 'New View (2 x 1)' configuration. On the left, the 'Views' panel lists various view groups, including 'Default group', 'Default view group', 'New Group', 'New View (2 x 1)', and 'Private'. A red box highlights the 'Cameras' section, which contains a list of cameras: 'DESKTOP-2B239GS' and 'Camera Group 1'. A blue callout '8' points to the 'Cameras' section. Another red box highlights the 'Universal 1 channel driver (localhost)' camera under 'Camera Group 1'. A blue callout '9' points to this camera. A blue callout '9.1 Drag and drop' points to the 'Universal 1 channel driver (localhost)' camera. The main video feed area shows a black screen with the text 'Universal 1 channel driver (localhost) - Camera 1' and a message: 'Connected to server. The server has lost connection to the camera. Universal 1 channel driver (localhost) - Camera 1 http://desktop-2b239gs:7563/'. A blue callout '7' points to the 'Setup' button in the top right corner. A trial license notice is visible at the top of the video feed area.

Milestone XProtect Smart Client

6/2/2021 4:07:22 PM

Live Playback Search Alarm Manager System Monitor

XProtect

New View (2 x 1)

Views

Search views and cameras...

Default group

Default view group

New Group

New View (2 x 1)

Private

Cameras

DESKTOP-2B239GS

Camera Group 1

Universal 1 channel driver (localhost)

Universal 1 channel driver (localhost) - Camera 1

9.1 Drag and drop

Connected to server.
The server has lost connection to the camera.

Universal 1 channel driver (localhost) - Camera 1
http://desktop-2b239gs:7563/

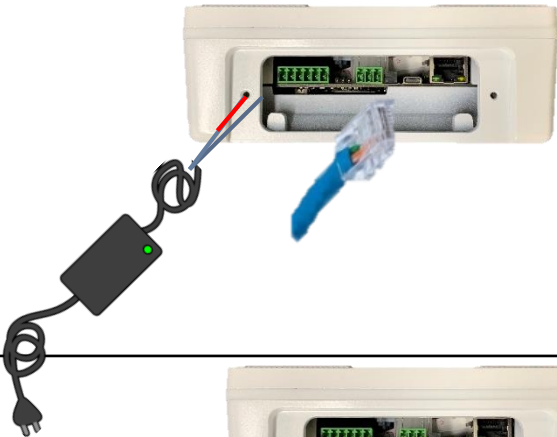
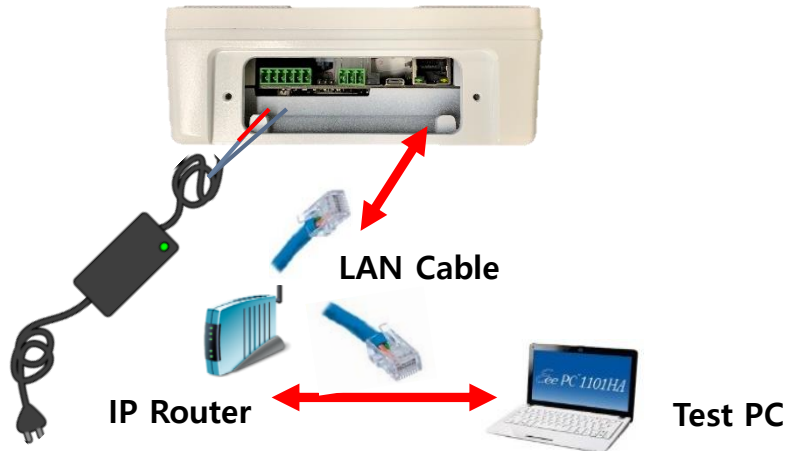
Setup

4:05:36 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 11/5/2021. To fully license the prod...

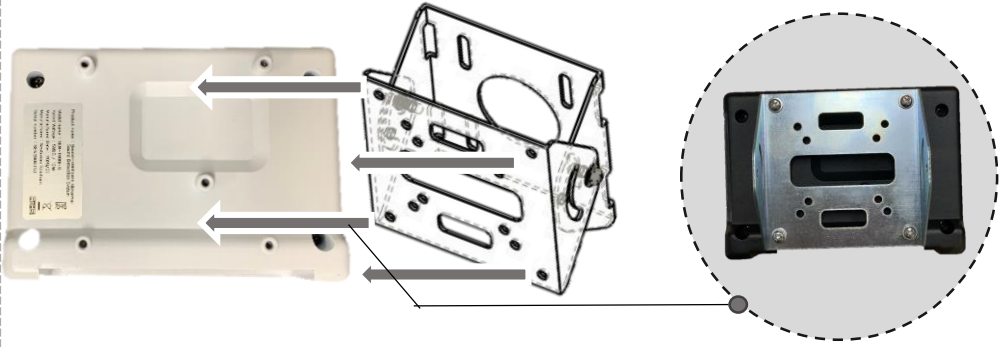
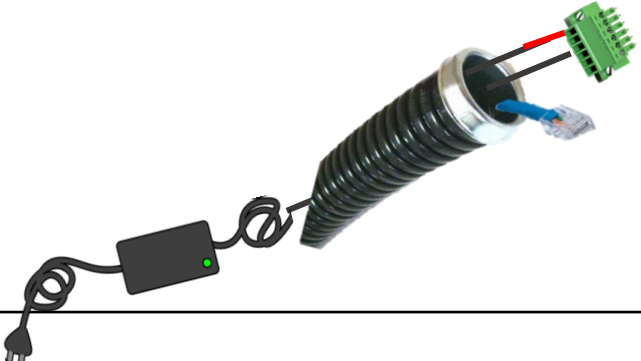


Device HW Installation

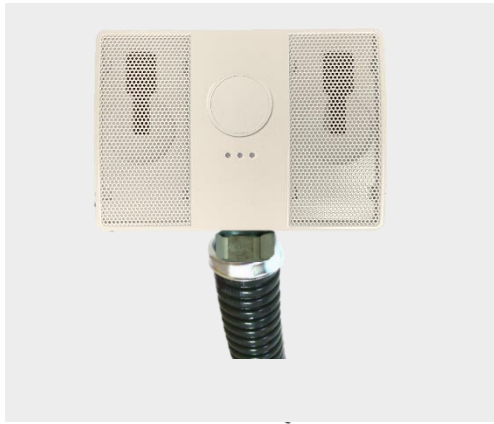

2 Device HW Installation -1

Explanation	Detailed image
<p>1. Power Supply</p> <p>This unit uses a 5V DC power adapter or For POE equipment, supply power through POE.</p>	 <p>The diagram shows a white rectangular device with its internal components exposed. A black power cable with a red and blue wire is plugged into the top of the device. A blue LAN cable is also plugged into the bottom of the device.</p>
<p>2. Equipment connection</p> <p>After powering on, connect the device to the router. Run the supplied SEN2000-ETHERNET.exe. SEN2000-ETHERNET: Tool to set network related setting, interworking information and threshold (volume bar) (See back page)</p>	 <p>The diagram shows the same white device as in the first image, but now it is connected to a network. A black power cable is plugged into the top. A blue LAN cable is plugged into the bottom. A red arrow points from the LAN cable to a blue IP Router. Another red arrow points from the IP Router to a laptop labeled 'Test PC'. The text 'LAN Cable' is written above the router, and 'IP Router' and 'Test PC' are written below the router and laptop respectively.</p>

② Device HW Installation -2

Explanation	Detailed image
<p>① Connect the angle source equipment and angle bracket.</p> <p>* Screws required for bracket mounting are included.</p>	 <p>After fastening the bracket</p>
<p>② Connecting blocks and RJ45 when installing waterproof flexible. pass all DC and UTP lines first.</p>	

② Device HW Installation -3

Explanation	Detailed image
<p>③ Waterproof flexible after connecting DC power and RJ45 (UTP cable) Replace the bottom cover with the connector attached.</p> <p>④ Attach abnormal sound equipment to the wall.</p>	<div><p>Field installation example)</p></div>

※ Notes on Installation

- ✓ There should be no obstacles near the equipment for smooth sound source detection.
- ✓ It is recommended to avoid installation where frequent noises occur.
- ✓ It is recommended to install at least at the height of 2M because there is a risk of damage.

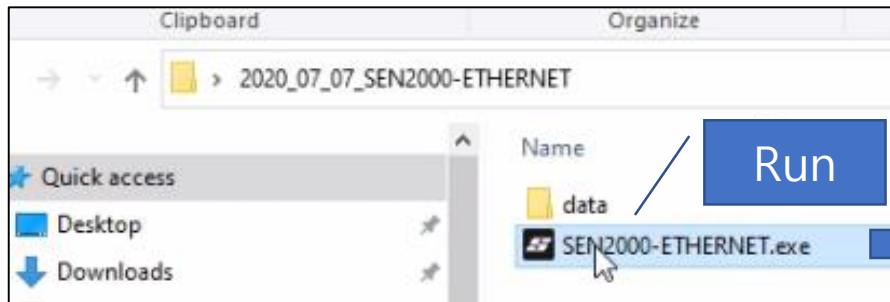


Device HW settings

3 Device HW settings

◆ ISD Ethernet is a tool program used to set up the equipment IP address.

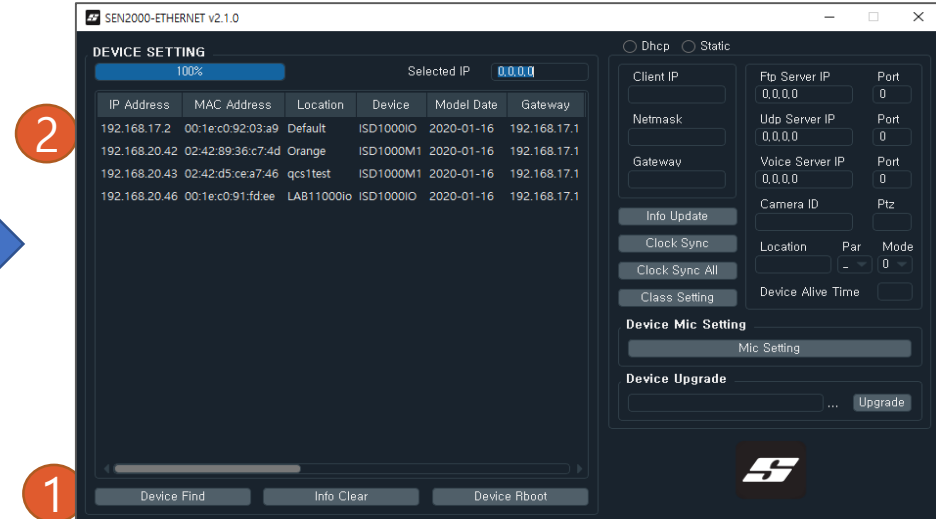
Explanation	Detailed image
-------------	----------------



1. Equipment IP Settings

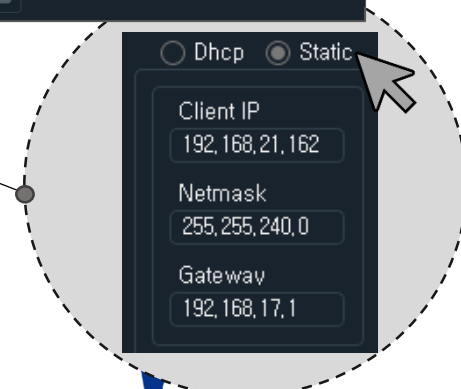
- 1) Click the 'Device Find' button to search for the connected device.
- 2) Find the IP of the device you want to set in the device list and **double click** it.
- 3) After checking 'Static' item, input the IP and network setting value of the device to be set in Client IP, Subnet mask, Gateway.

(You must check the Static radio button to activate each equipment.)



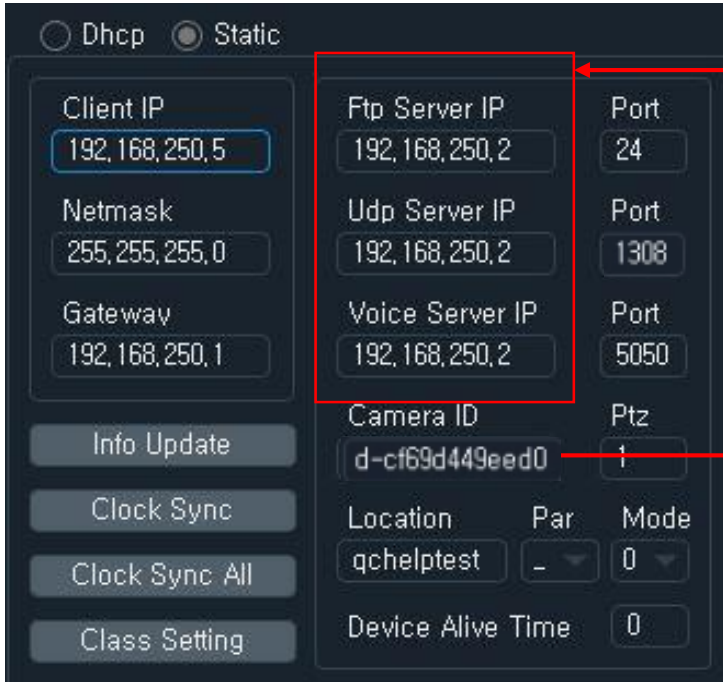
Example) If the equipment is set as follows


- ✓ Device IP: 192.168.21.162
- ✓ Subnet mask: 255.255.240.0
- ✓ Gateway : 192.168.17.1



3 Device HW settings

◆ Ethernet tool

Explanation	Detailed image
<h3>2. FTP Server setting</h3> <p>Enter FTP Server IP and PORT where detected sound will be uploaded. (By default, PORT uses 24.)</p> <p>※ The detected event source is uploaded to the FTP server.</p>	 <p>Server PC IP</p> <p>Camera ID that exported from ISDserver. - Refer page 23</p>
<h3>3. UDP Server Setting</h3> <p>Enter the Server IP and Port to receive UDP messages.</p> <p>(In case of linking with Milestone, PORT is 1308 and Serverip is the server IP where "ISD server" program is installed.)</p> <p>※ When interlocking with VMS, etc., interlock with UDP packet.</p>	
<h3>4. VOICE Server setting</h3> <p>Enter the Server IP and PORT where KServer (voice recognition server) will be installed.</p> <p>(Default port is 5050 and if changed, KSERVER program also You need to change the setting.)</p> <p>※ It analyzes / extracts the words included in the sound source stream input through the device.</p>	<ul style="list-style-type: none">✓ FTP Server PORT: 24✓ Udp Server PORT: 7085✓ Voice server PORT : 5050



3

Device HW settings

◆ Ethernet tool

Explanation	Detailed image
<p>5. Camera ID</p> <p>Enter the camera information to be linked. Refer to Slide #23 (You can check the camera information in "Caminfo.txt" that "Exported" from ISDServer.exe.)</p>	
<p>6. PTZ Initial number setting</p> <p>PTZ Set the initial number.</p>	
<p>7. Location setting</p> <p>Specify the equipment installation location.</p>	
<p>8. Par</p> <p>interlocking-formatted Separator Set (default: _)</p>	
<p>9. Mode</p> <p>Sets UDP packet interlocking format (default: 0)</p>	
<p>10. Device Alive Time</p> <p>Keep alive Set the interval for sending messages. (When it is set as 0, it is not transmitted. When it is linked with Milestone, it is set as 0.)</p>	

Explanation

Detailed image

11. Threshold Setting

Click "Device and Mic Settings" and "Connect" menu.

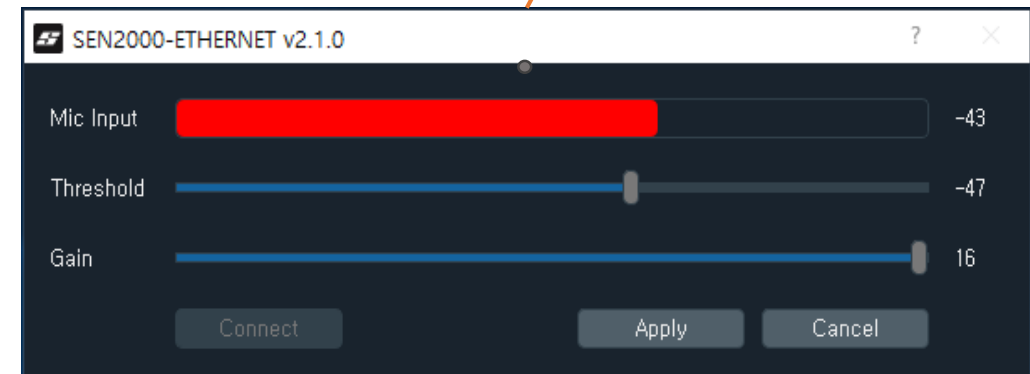
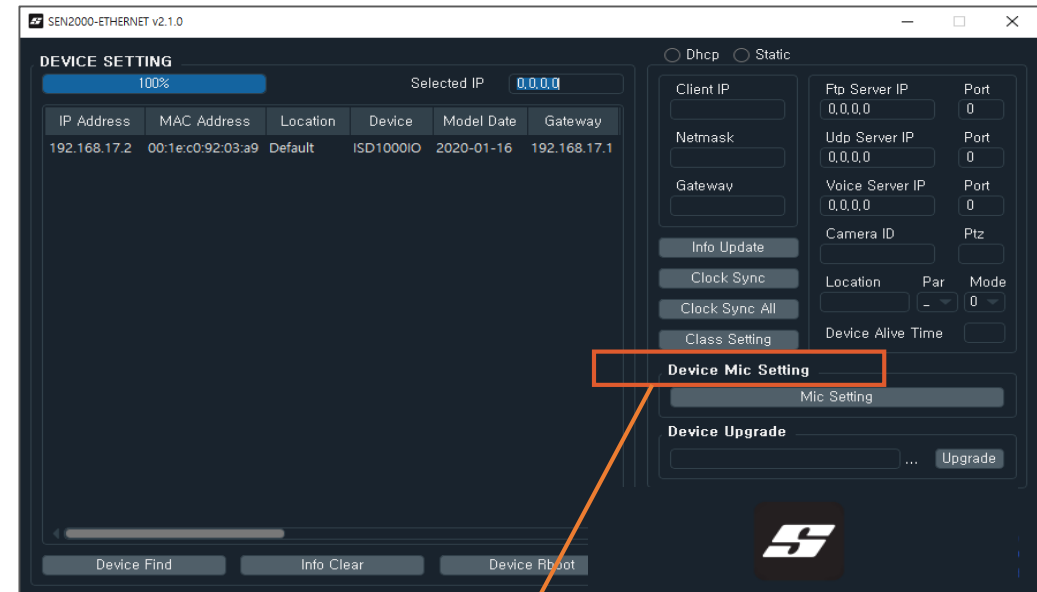
- Mic input: current environmental noise dB
- Threshold: set value, should be higher than Mic Input
- Gain: Microphone Gain Value

This function sets the dB value for detecting sound sources.

The more you set it to the right, the higher the volume of the sound source you want to detect.

Click the 'Info Update' button to apply the changes before setting the threshold.

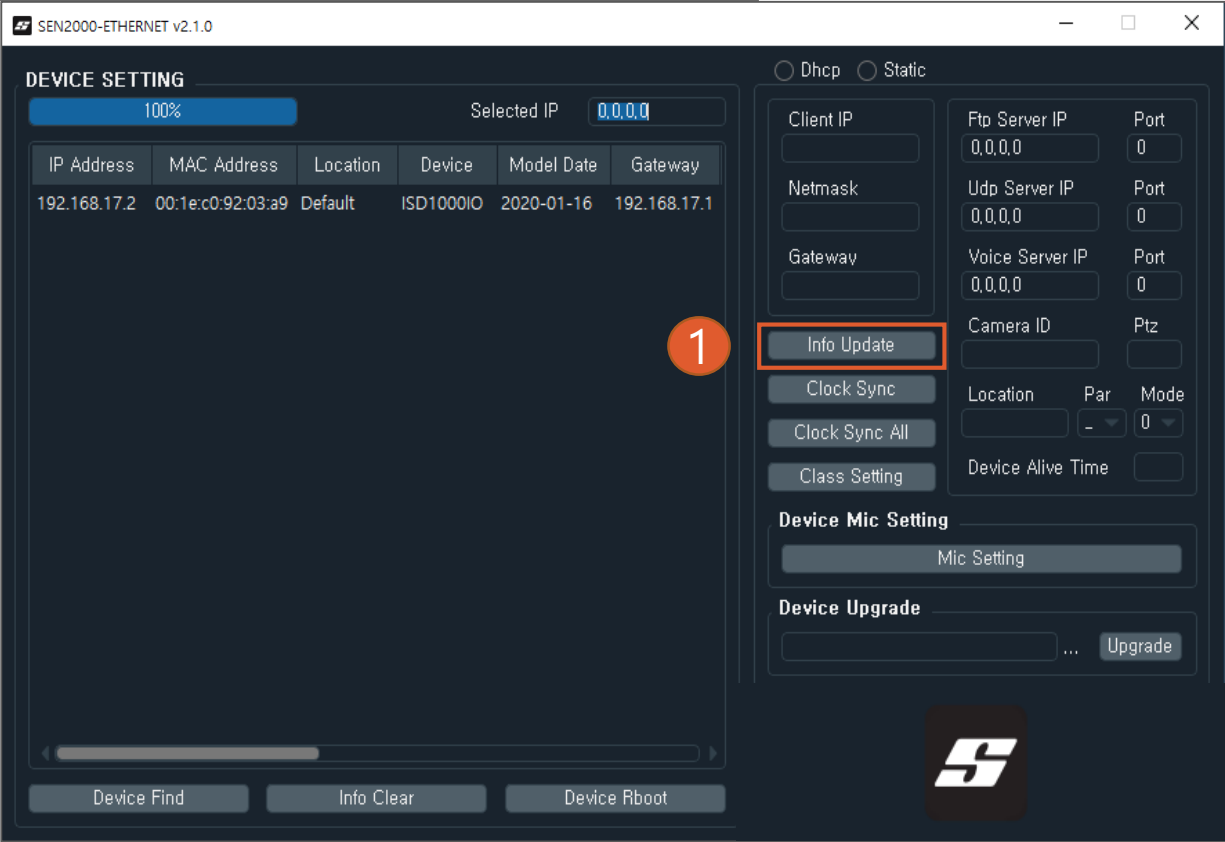
At this time, the device will reboot once.



3 Device HW settings

◆ Ethernet tool



Explanation	Detailed image
<p>12. class setting</p> <p>① Class Mode</p> <ul style="list-style-type: none">- Lite : ISD-1000M1 Ver- Full : ISD-1000iO Voice recognition Ver <p>② Target list</p> <p>Specify which event number to send the result to the VMS when classified as a class.</p> <p>(No event sent when set to 00)</p> <p>4. After clicking the 'Light' button, change the "Target List" as follows using "Edit" menu"</p> <p>0: Noise → 00 1: Scream → 05</p> <p>Remove other events or numbers by "Delete" menu</p>	<p>5. After editing with 'Edit' button be sure to click the "Update" button</p>

Explanation	Detailed image
<p>13. Info Update</p> <p>After class set, press "Info Update"</p> <p>⇒ The device start reboot</p> <p>⇒ Reboot takes roughly 5min</p>	 <p>The screenshot shows the 'SEN2000-ETHERNET v2.1.0' application window. On the left, under 'DEVICE SETTING', there is a table with columns: IP Address, MAC Address, Location, Device, Model Date, and Gateway. The table contains one row with values: 192.168.17.2, 00:1e:c0:92:03:a9, Default, ISD1000IO, 2020-01-16, and 192.168.17.1. Above the table, there is a 'Selected IP' field showing '0.0.0.0'. On the right side of the window, there are several configuration sections: 'Dhcp' and 'Static' radio buttons, 'Client IP', 'Netmask', 'Gateway', 'Fto Server IP', 'Udp Server IP', 'Voice Server IP', 'Camera ID', 'Ptz', 'Location', 'Par', 'Mode', 'Device Alive Time', 'Device Mic Setting', and 'Device Upgrade'. The 'Info Update' button is highlighted with a red circle and the number 1. At the bottom of the window, there are buttons for 'Device Find', 'Info Clear', and 'Device Reboot'.</p>



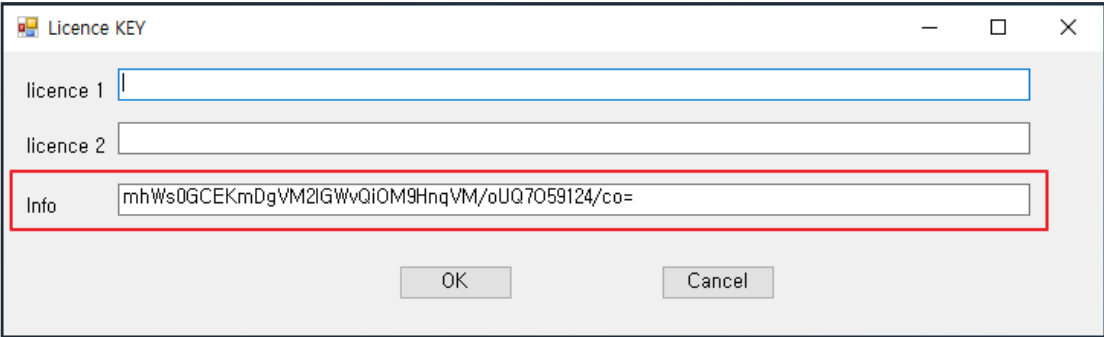
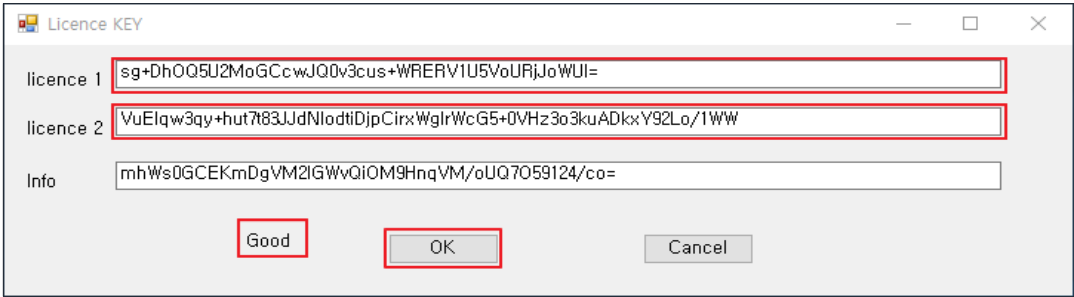
4

4. Sound & Voice Analytics Server Program Setting

-  KSERVER Settings
-  FTP Server Settings

4 KSERVER Settings-1

◆ KSERVER is a voice recognition server program that has the function of extracting the words contained in the sound source received through the ISD-1000iO voice recognition equipment.

Explanation	Program image
<p>A. KSERVER License</p> <p>1) When run "K server program", it will ask license</p> <p>2) Please send the "info" to IVS to deliver the license 1, 2,</p> <p>3) After plugin license it will show "Good" and click "ok"</p> <p>※ This license part, generate different "info" whenever you turn on. To keep in same, it is recommended to disable all Ethernet connections except just 1, in "device manager" menu.</p>	 <p>↓</p> 

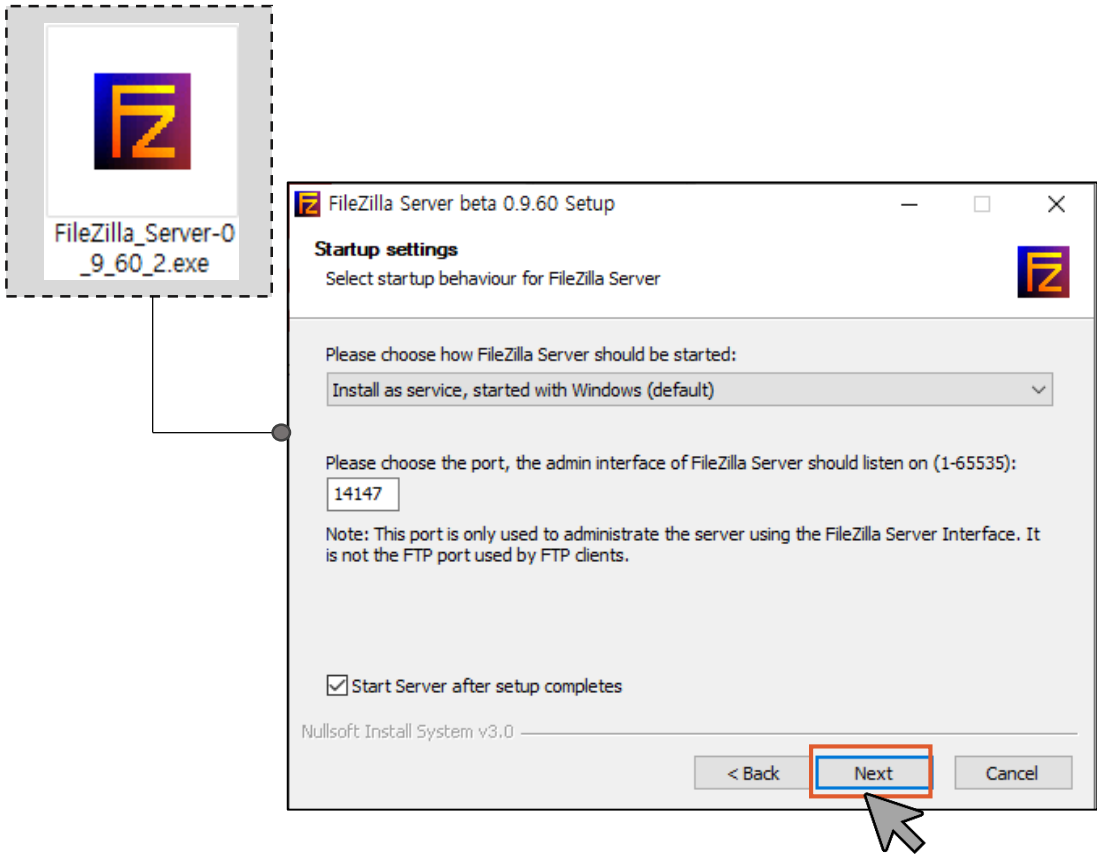
4 KSERVER Settings-2

◆ KSERVER is a voice recognition server program that has the function of extracting the words contained in the sound source received through the ISD-1000iO voice recognition equipment.

Explanation	Program image
<p>B. KSERVER setting</p> <p>1) ③ Specify the port to receive the sound stream from the item..</p> <p>(When changing from 5050 set as the default port, click Save Setting to apply.)</p> <p>2) Start button (item 1): Receives sound stream from abnormal sound source equipment and starts word extraction.</p> <p>3) Stop button (item 2): Receives sound stream from abnormal sound source equipment and stops word extraction.</p> <p>※ By default, it automatically start the program without clicking the Start button and receives a sound streams from the device.</p>	

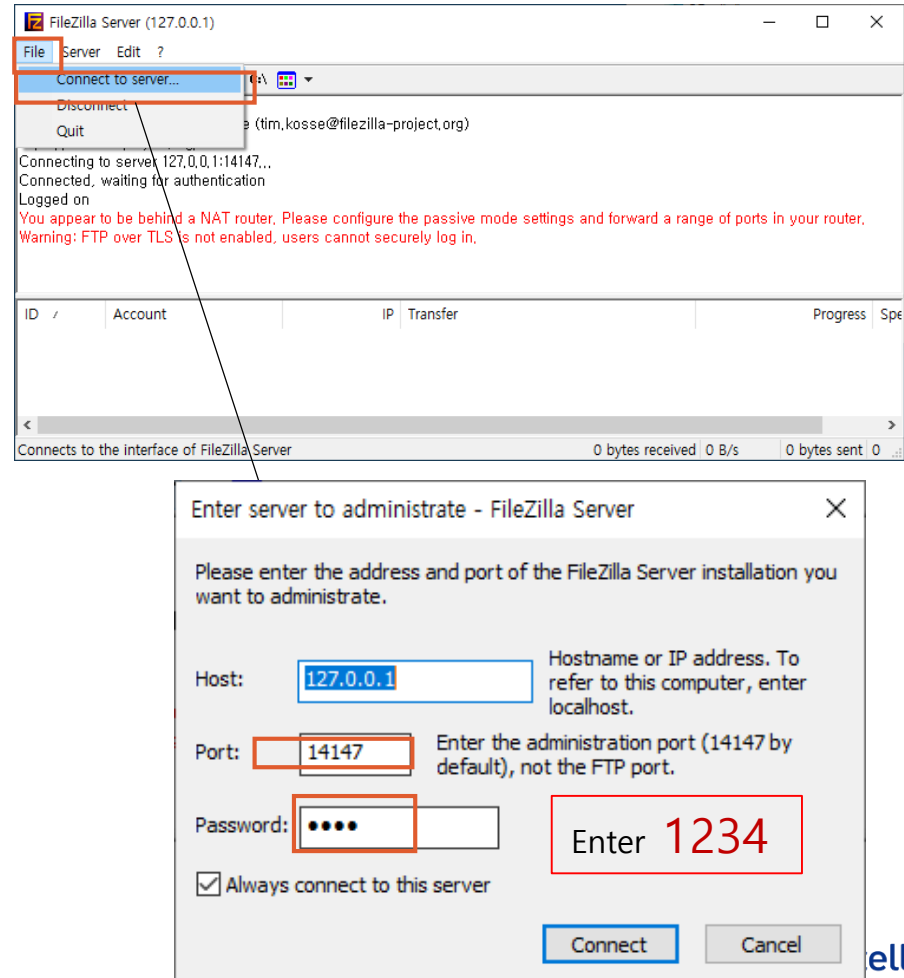
4 FTP Server Settings-1

◆ Save detected event sources on FTP server

Explanation	Program image
<p>1. FileZila FTP Server installation</p> <p>1) Double-click FileZila_Server.exe to run it.</p> <p>2) Click the Next button to proceed with the installation as shown.</p>	 <p>The screenshot shows the 'FileZilla Server beta 0.9.60 Setup' window. The 'Startup settings' section is active, asking to 'Select startup behaviour for FileZilla Server'. The dropdown menu is set to 'Install as service, started with Windows (default)'. Below this, there is a field for the port number, currently set to '14147'. A note states: 'Note: This port is only used to administrate the server using the FileZilla Server Interface. It is not the FTP port used by FTP clients.' At the bottom, there is a checkbox labeled 'Start Server after setup completes' which is checked. The 'Next' button is highlighted with a red rectangle and a mouse cursor is pointing at it. The 'Back' and 'Cancel' buttons are also visible.</p>

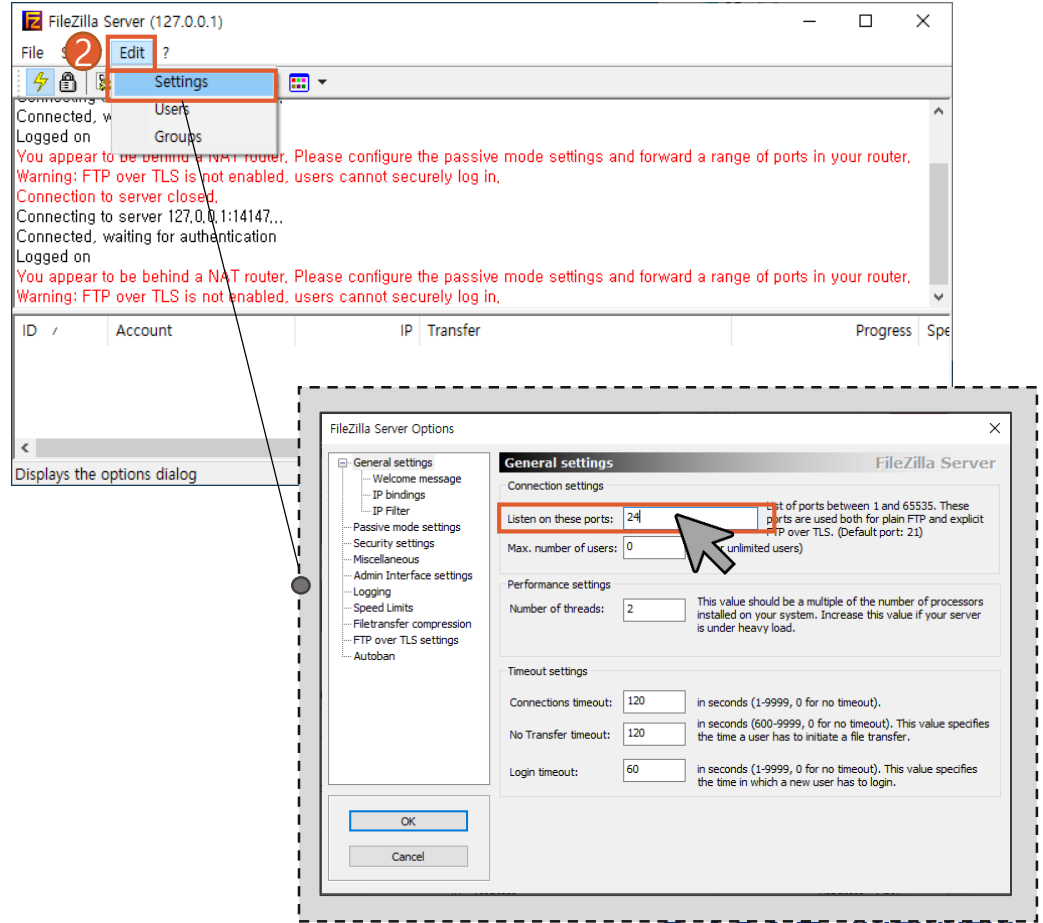
4 FTP Server Settings-2

◆ Save detected event sources on FTP server

Explanation	Program image
<p>1. FTP SERVER settings</p> <p>1) Run Connect to Server on the File tab, enter the following and click the Connect button.</p> <ul style="list-style-type: none">▪ HOST: 127.0.0.1▪ PORT: 14147▪ PASSWORD: 1234	

4 FTP Server Settings-3

◆ Save detected event sources on FTP server

Explanation	Program image
<h2>2. FTP port setting</h2> <p>1) Enter the Setting tab of the Edit tab and enter as follows.</p> <p>General settings – Listen on these ports: 24</p> <p>2) After completing the input, click the OK button on the bottom left.</p>	 <p>The screenshot shows the FileZilla Server (127.0.0.1) interface. The 'Edit' menu is open, and the 'Settings' option is highlighted. Below the menu, a warning message is displayed: 'You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router. Warning: FTP over TLS is not enabled, users cannot securely log in. Connection to server closed. Connecting to server 127.0.0.1:14147... Connected, waiting for authentication Logged on'. The 'FileZilla Server Options' dialog box is open, showing the 'General settings' tab. The 'Listen on these ports' field is set to 24. The 'Max. number of users' is set to 0 (unlimited users). The 'Performance settings' section shows 'Number of threads' set to 2. The 'Timeout settings' section shows 'Connections timeout' set to 120 seconds, 'No Transfer timeout' set to 120 seconds, and 'Login timeout' set to 60 seconds. The 'OK' button is highlighted at the bottom left of the dialog box.</p>

4 FTP Server Settings-4

◆ Save detected event sources on FTP server

Explanation

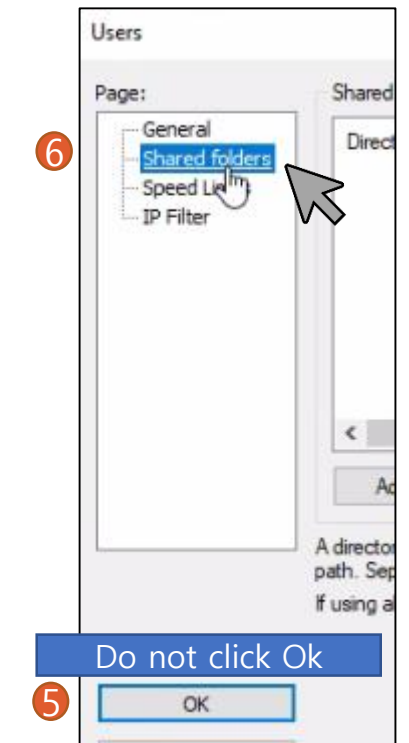
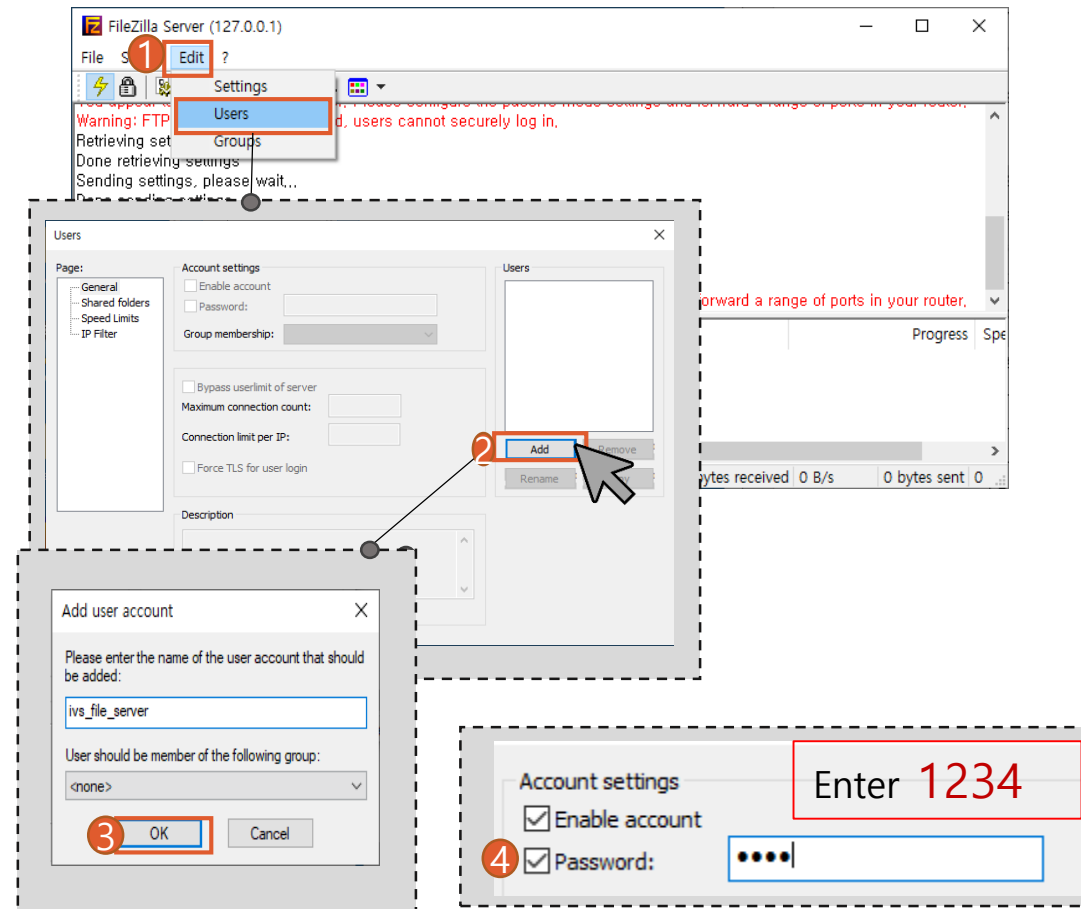
Program image

3. User settings

- 1) Click "User" in the "Edit" tab and proceed as follows:
- 2) Add an account using the "Add" button.
- 3) Create ID "**ivs_file_server**" (no space) and press "Ok"
- 4) In "Account settings", check password and enter "**1234**"

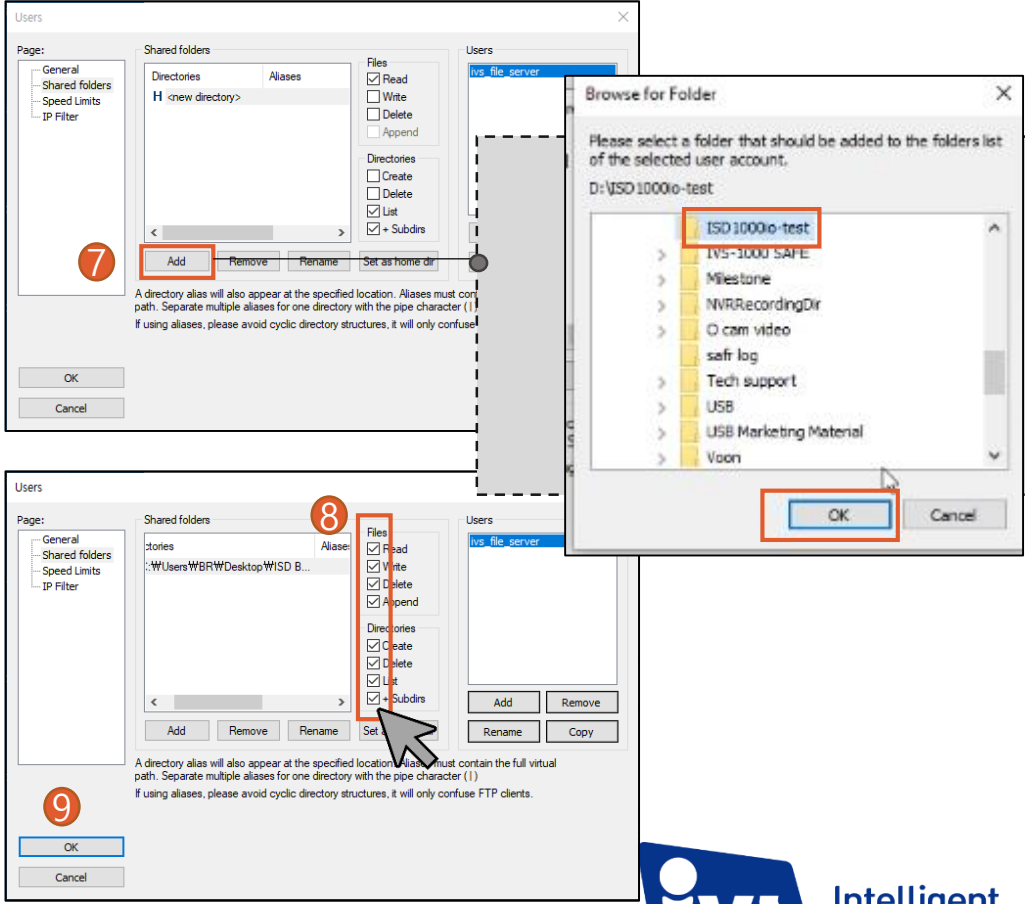
5) After completing ID and PW input in step 4 do not click the "OK" button on the bottom left (it is final step) but move to next step because step 6,7,8,9 yet to complete.

- 6) Click "Shared folder"



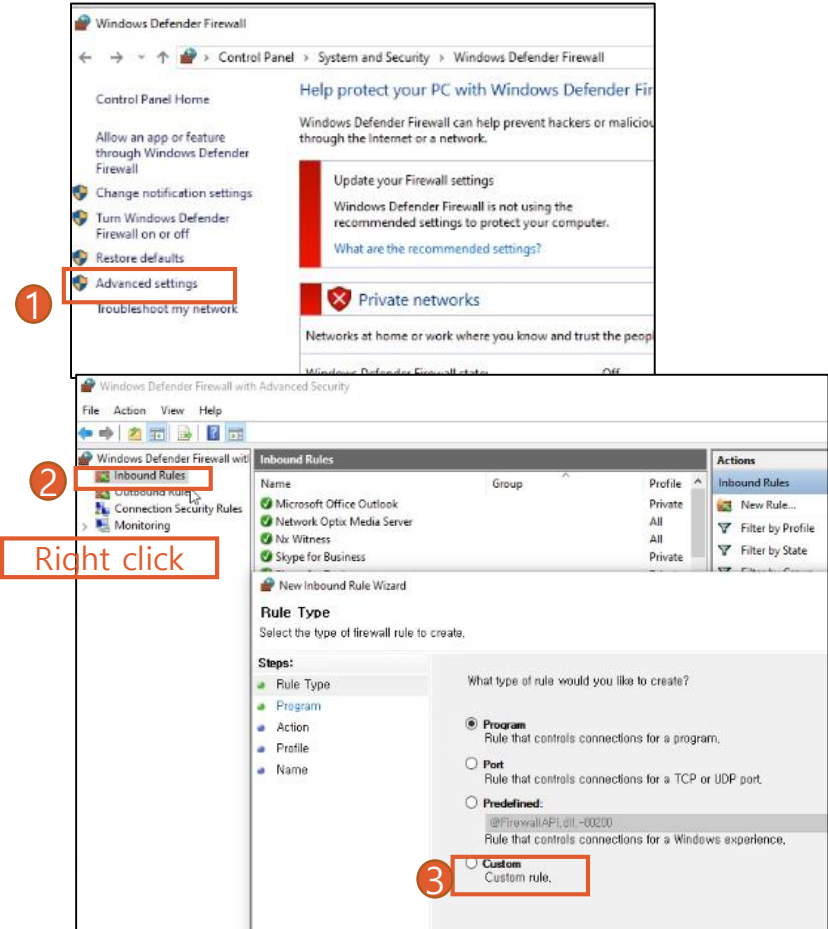
4 FTP Server Settings-5

◆ Save detected event sources on FTP server

Explanation	Program image
<p>7) Shared folder – Specify the file path to save using the "Add" button on the bottom left.</p> <p>8) Then click on the created path to specify the permissions.</p> <p>⇒ Check all</p> <p>⇒ " Read, Write, Delete, append, Create Delete, List, + Subdirs"</p> <p>9) After completing the input, click the OK button on the bottom left to complete the Filezilla setup.</p>	

4 FTP Server Settings-6

◆ Save detected event sources on FTP server

Explanation	Program image
<p>4. Firewall settings</p> <p>Run Windows Defender Firewall with Advanced Security.</p> <p>1) Run in 'Control Panel'-> Windows Defender Firewall-> "Advanced Settings" on the left</p> <p>2) Right-click "Inbound Rules" and click "New Rule". Not the one shown at far right</p> <p>3) Check the "Custom option" and click the "Next" button.</p> <p>4) Check "All programs" options and click the "Next" button.</p> <p>5) Click 'Next' until the 'Name' item appears and enter 'IVS_FTP' in the 'Name' field of the Name tab.</p>	

4 FTP Server Settings-7

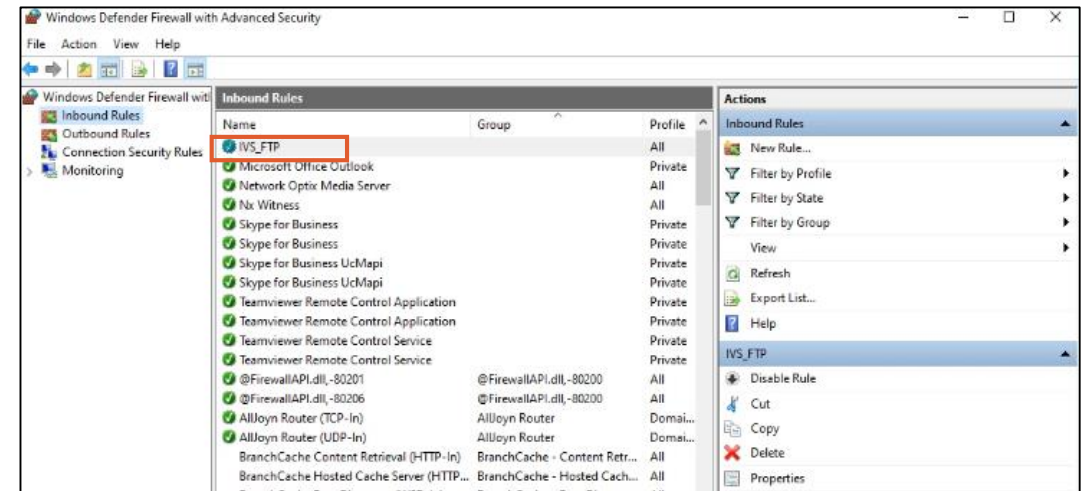
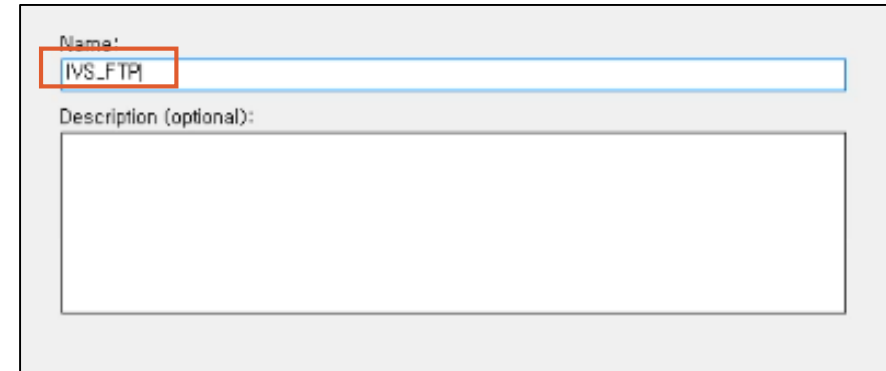
◆ Save detected event sources on FTP server

Explanation	Program image
-------------	---------------

6) Click 'Finish' to complete the rule creation.

When the setting is completed as above, the sound source is uploaded to the path.

5





Abnormal Sound Event & Event Log Testing in Milestone

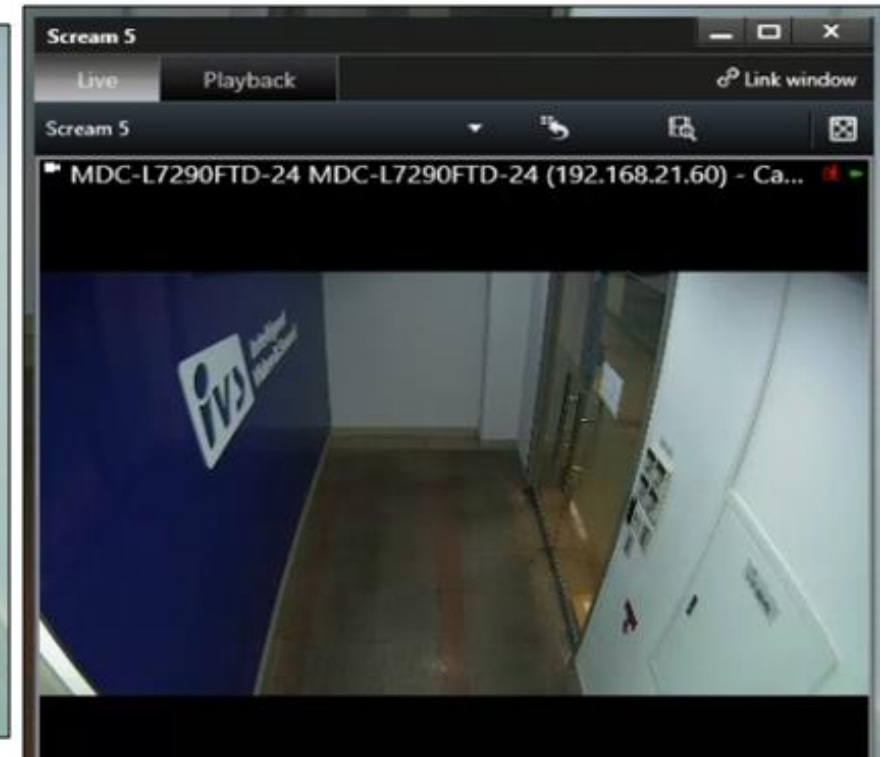
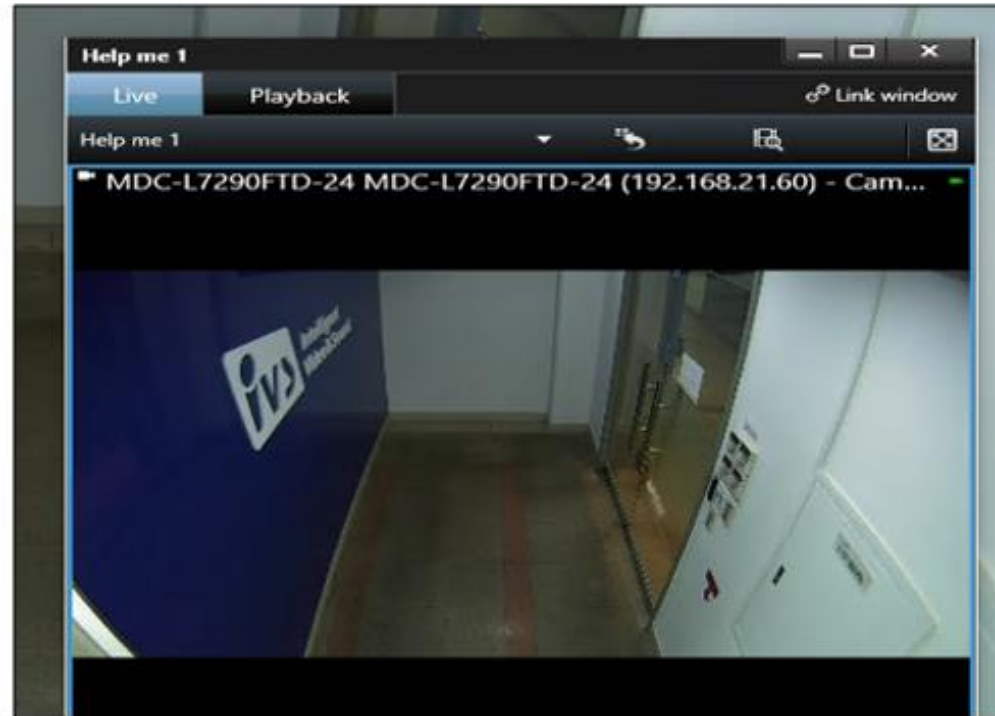
5

Checking the “Event” in Milestone

Program image

Event confirmation

When an event (“Help” or “Help me” or “Scream” is normally received, an event popup is displayed along with the event type as shown in the picture



5 Checking the "Event Log" in Milestone

Program image

The event log can be checked in the "Alarm Manager" tab as shown in the picture.

VAEvent = Video analytics Event

ISDEvent = Intelligent Sound Detector Event

Milestone XProtect Smart Client

6/17/2021 6:48:47 PM

Live Playback Search **Alarm Manager** System Monitor

6:48:36 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 5/27/2022. To fully license the product, please contact your reseller or find one on www.milestone.com.

No map has been selected

MDC-L7290FTD-24 MDC-L7290FTD-24 (192.168.21.60) - Camera 1 - 6/17/2021 4:32:26.113 PM

Zone#0

4:10 PM 4:20 PM 6/17/2021 4:32:26.598 PM 4:50 PM 5:00 PM

Quick Filters

- New (19)
- In progress (0)
- On hold (0)
- Closed (0)

Servers

- DESKTOP-AKKQPIL

Alarms No filter

Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
4:32:45 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2314
4:32:44 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2313
4:32:24 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2312
4:29:31 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2311
4:29:31 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2310
4:28:16 PM 6/17/2021	1	1	New	ISDEvent	MDC-L7290FTD-24 MDC-L		2309
4:27:23 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2308
4:27:23 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2307
4:26:52 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2306
4:26:52 PM 6/17/2021	1	1	New	VAEvent	MDC-L7290FTD-24 MDC-L		2305
4:26:00 PM 6/17/2021	1	1	New	VAEvent	Universal 1 channel driver (2304
4:26:00 PM 6/17/2021	1	1	New	VAEvent	Universal 1 channel driver (2303
4:26:00 PM 6/17/2021	1	1	New	VAEvent	Universal 1 channel driver (2302
4:26:00 PM 6/17/2021	1	1	New	VAEvent	Universal 1 channel driver (2301
4:25:58 PM 6/17/2021	1	1	New	VAEvent	Universal 1 channel driver (2300
4:25:58 PM 6/17/2021	1	1	New	VAEvent	Universal 1 channel driver (2299

Reports 1-19



Summary

6 Summary

Run all the program after closing all the program. All program should not be closed but can be minimized.

Program image

1. Run FileZilla program

- Login if need

2. Run ISD program

- Login server

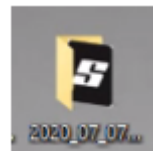
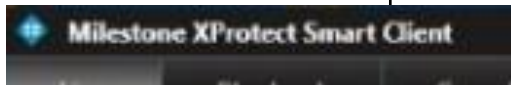
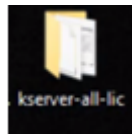
- Press "**Start server**" status should be "**Waiting**"

3. Run Kserver program

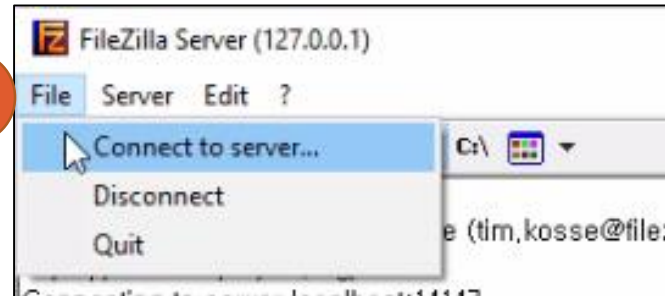
4. Run Milestone Client (No need to open Management server)

5. No need to run Ethernet program because HW reset is done by 1 time.

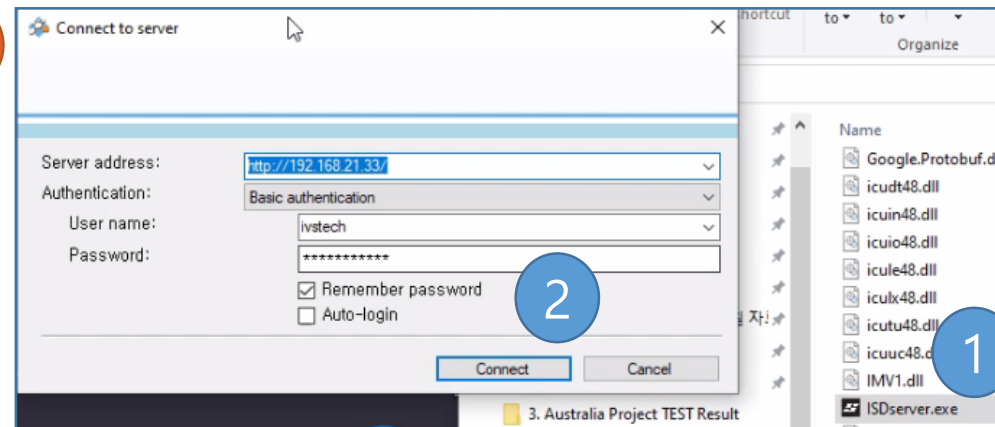
Run Ethernet when need to change HW settings such as IP address, etc.



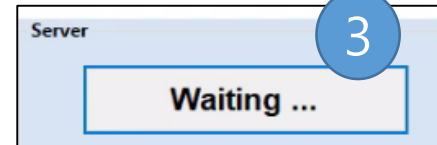
1



2



3





Thank you