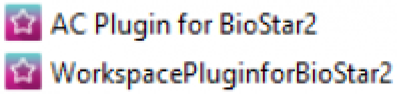
Table of Contents

System Configuration, BioStar 2, Milestone

How to utilize BioStar 2 integrating with Milestone

The summary of Procedure

1. Install BioStar 2.
2. Install one of Milestone XProtect VMS (with professional license or higher).
3. Install BioStar 2 Integration for Milestone XProject.

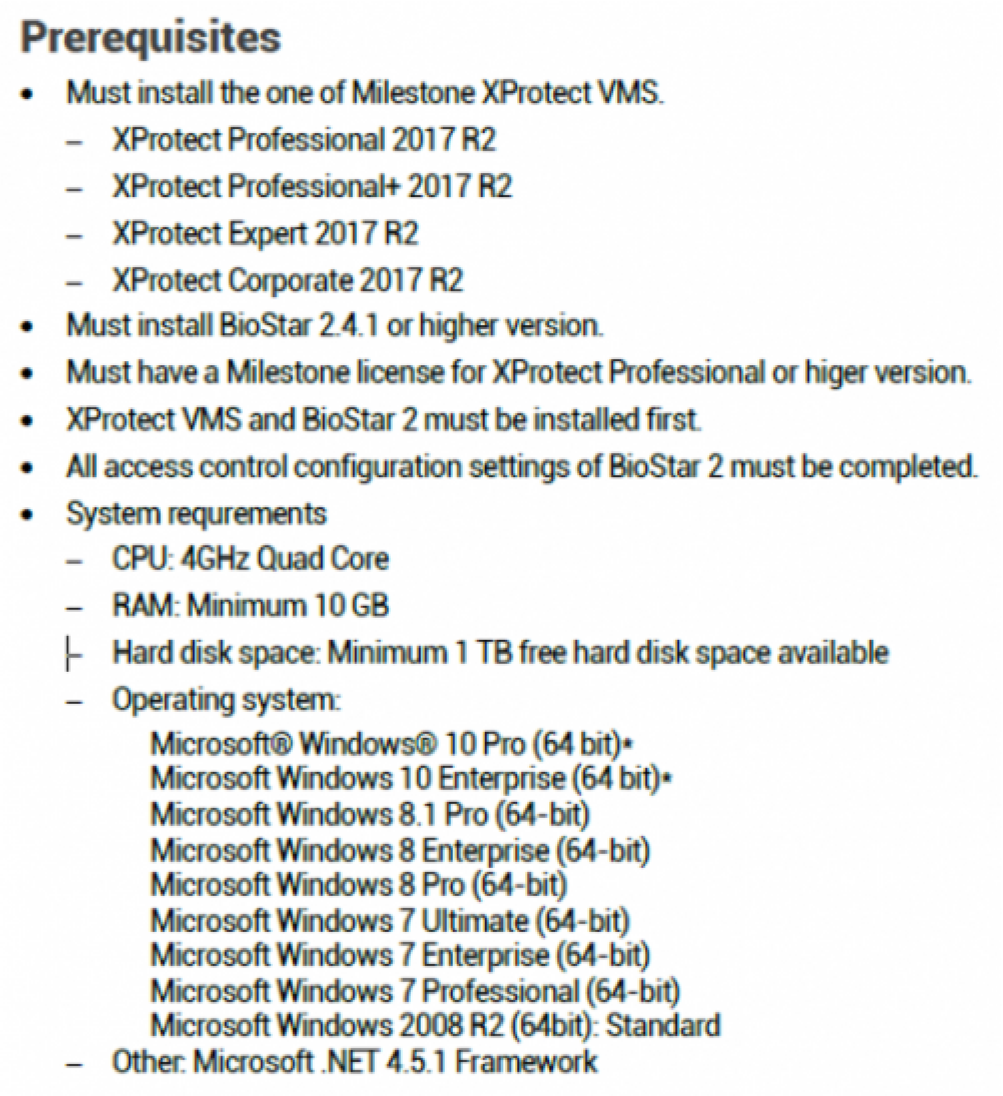


AC Plugin for BioStar2

WorkspacePluginforBioStar2

4. Add IP Camera in Milestone XProtect VMS.
5. Create new Access Control to connect Milestone to BioStar 2.
6. Utilize XProtect Smart Client.

Before you integrate Milestone with BioStar 2, check the Prerequisites below.



Prerequisites

- Must install the one of Milestone XProtect VMS.
  - XProtect Professional 2017 R2
  - XProtect Professional+ 2017 R2
  - XProtect Expert 2017 R2
  - XProtect Corporate 2017 R2
- Must install BioStar 2.4.1 or higher version.
- Must have a Milestone license for XProtect Professional or higer version.
- XProtect VMS and BioStar 2 must be installed first.
- All access control configuration settings of BioStar 2 must be completed.
- System requrements
  - CPU: 4GHz Quad Core
  - RAM: Minimum 10 GB
  - Hard disk space: Minimum 1 TB free hard disk space available
  - Operating system:

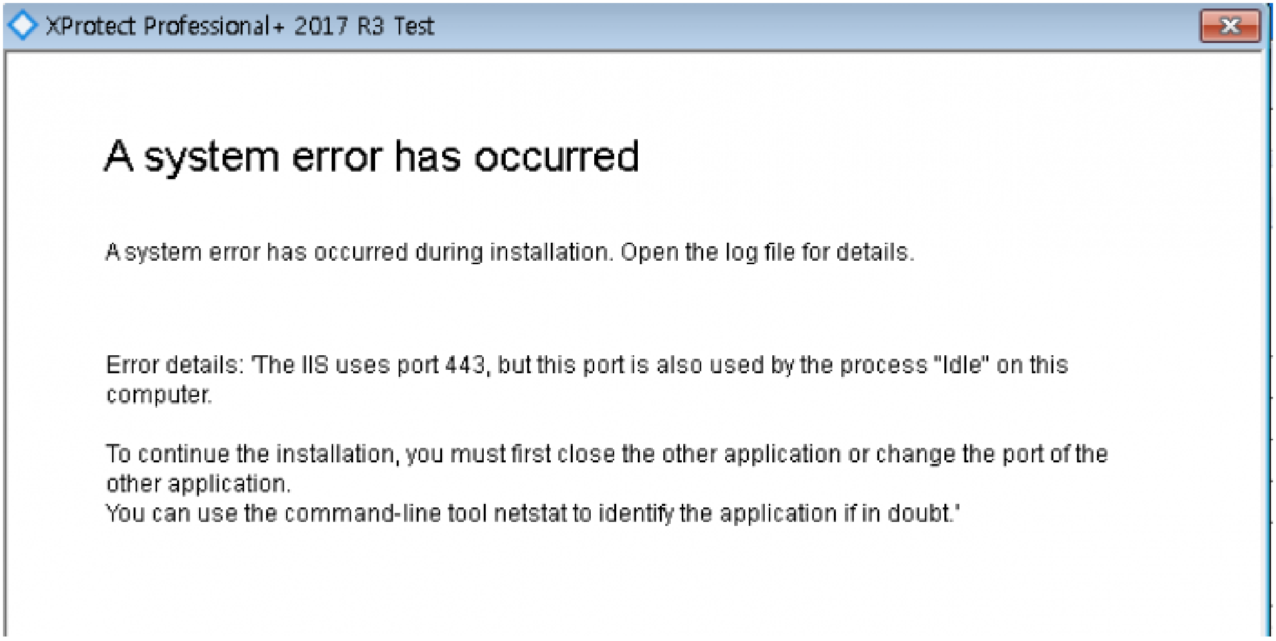
    Microsoft® Windows® 10 Pro (64 bit)*
    Microsoft Windows 10 Enterprise (64 bit)*
    Microsoft Windows 8.1 Pro (64-bit)
    Microsoft Windows 8 Enterprise (64-bit)
    Microsoft Windows 8 Pro (64-bit)
    Microsoft Windows 7 Ultimate (64-bit)
    Microsoft Windows 7 Enterprise (64-bit)
    Microsoft Windows 7 Professional (64-bit)
    Microsoft Windows 2008 R2 (64bit): Standard
  - Other: Microsoft .NET 4.5.1 Framework

Step 1: Install BioStar 2

Refer to the below link if you do not know how to install BioStar 2.
BioStar 2 Installation

If you use port number 443 and 9000 for BioStar 2, you should change it into other numbers. This is because the port number for BioStar 2 will have collided with the port number used when XProtect Management Client 2017 R3 is installed. When you set the port number 443 and 9000 for BioStar 2 and then try to install XProtect Management Client 2017 R3, you will get the below error.

When you set the port number 443 for BioStar 2 and then try to install XProtect Management Client 2017 R3, you will get the below error.



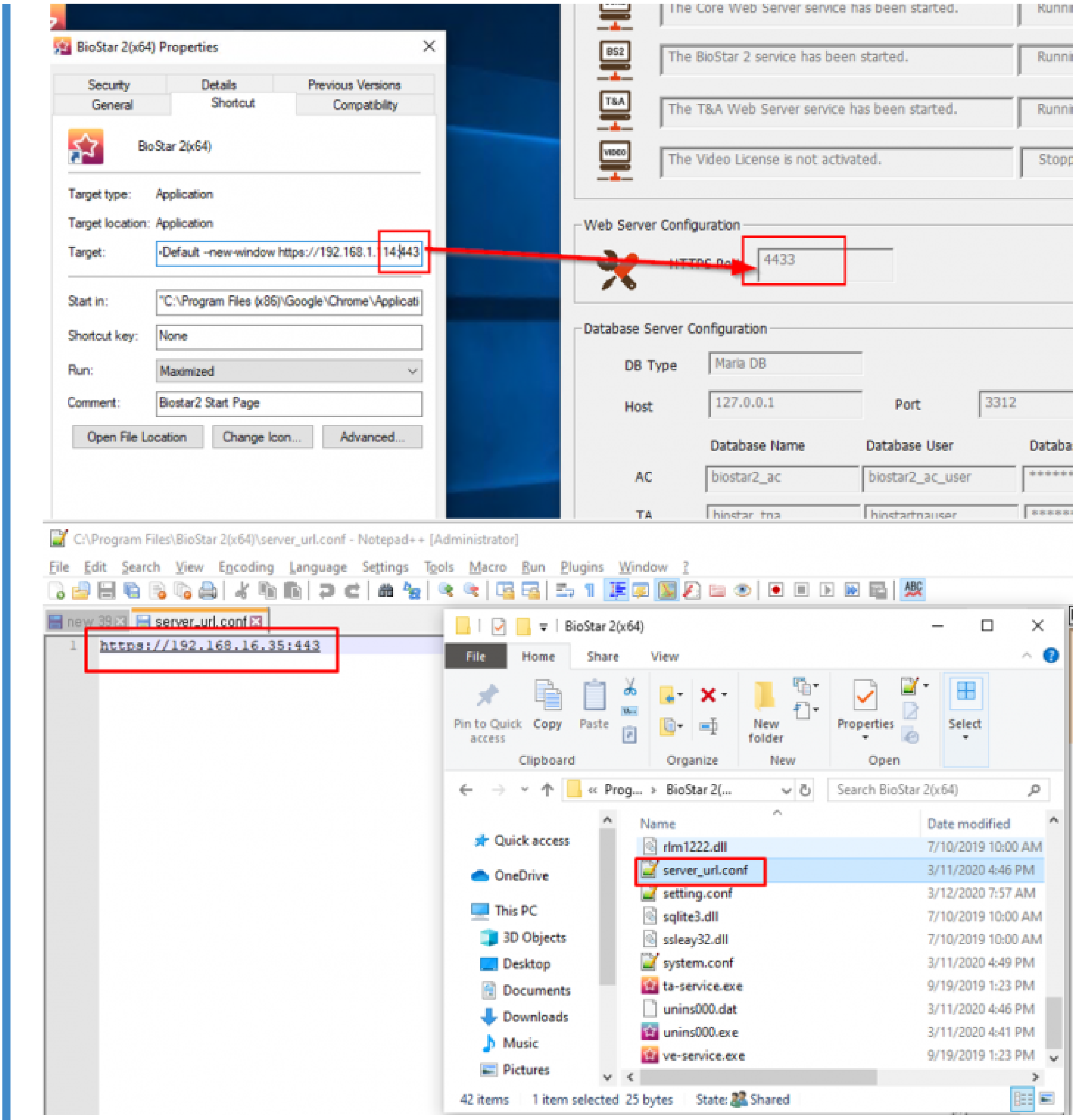
A system error has occurred

A system error has occurred during installation. Open the log file for details.

Error details: 'The IIS uses port 443, but this port is also used by the process "Idle" on this computer.

To continue the installation, you must first close the other application or change the port of the other application.
You can use the command-line tool netstat to identify the application if in doubt.'

Therefore we recommend that you change the port number for HTTPS on BioStar 2 and 9000 port to avoid port conflict issues. Also, even if you changed HTTPS port for BioStar 2, the icon and configuration file do not be changed automatically. So, please update manually the icon and 'server_url.conf' file to the port number for BioStar 2's HTTPS.



BioStar 2(x64) Properties

Target type: Application
Target location: Application
Target: -Default --new-window https://192.168.1.14:443
Start in: "C:\Program Files (x86)\Google\Chrome\Applicati
Shortcut key: None
Run: Maximized
Comment: Biostar2 Start Page

The Core Web Server service has been started.
The BioStar 2 service has been started.
The T&A Web Server service has been started.
The Video License is not activated.

Web Server Configuration
HTTPS Port 4433

Database Server Configuration
DB Type Maria DB
Host 127.0.0.1 Port 3312

	Database Name	Database User
AC	biostar2_ac	biostar2_ac_user
TA	biostar_tna	biostartnauser

C:\Program Files\BioStar 2(x64)\server_url.conf - Notepad++ [Administrator]

```
https://192.168.16.35:443
```

BioStar 2(x64)

Name	Date modified
rlm1222.dll	7/10/2019 10:00 AM
server_url.conf	3/11/2020 4:46 PM
setting.conf	3/12/2020 7:57 AM
sqlite3.dll	7/10/2019 10:00 AM
ssleay32.dll	7/10/2019 10:00 AM
system.conf	3/11/2020 4:49 PM
ta-service.exe	9/19/2019 1:23 PM
unins000.dat	3/11/2020 4:46 PM
unins000.exe	3/11/2020 4:41 PM
ve-service.exe	9/19/2019 1:23 PM

42 items 1 item selected 25 bytes State: Shared

Step 2: Install one of Milestone XProtect VMS (with professional license or higher)

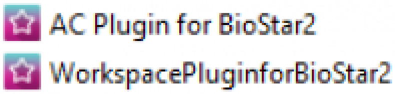
You can download the installation file of Milestone XProtect VMS in the below link.

https://www.milestonesys.com/support/resources/download-software/

While you install the application, it is required to activate Milestone’s license.

Step 3: Install BioStar 2 Integration for Milestone XProject

You should install two installation files below.
Please click the link to download the installation files.
(https://www.supremainc.com/en/solutions/suprema-integration-milestone.asp?sKIND_TYPE=GD01501
)

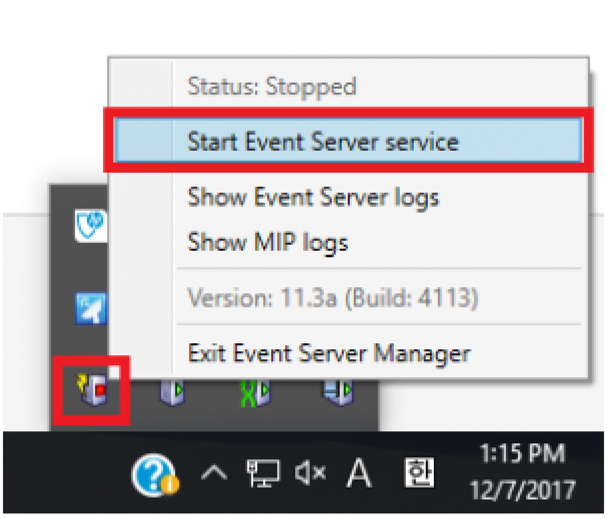


AC Plugin for BioStar2
WorkspacePluginforBioStar2

- AC Plugin for BioStar2.exe is used to connect the access control system and XProtect VMS.
- WorkspacePluginforBioStar2.exe provides the functionality for using BioStar 2 in the XProtect Smart Client.

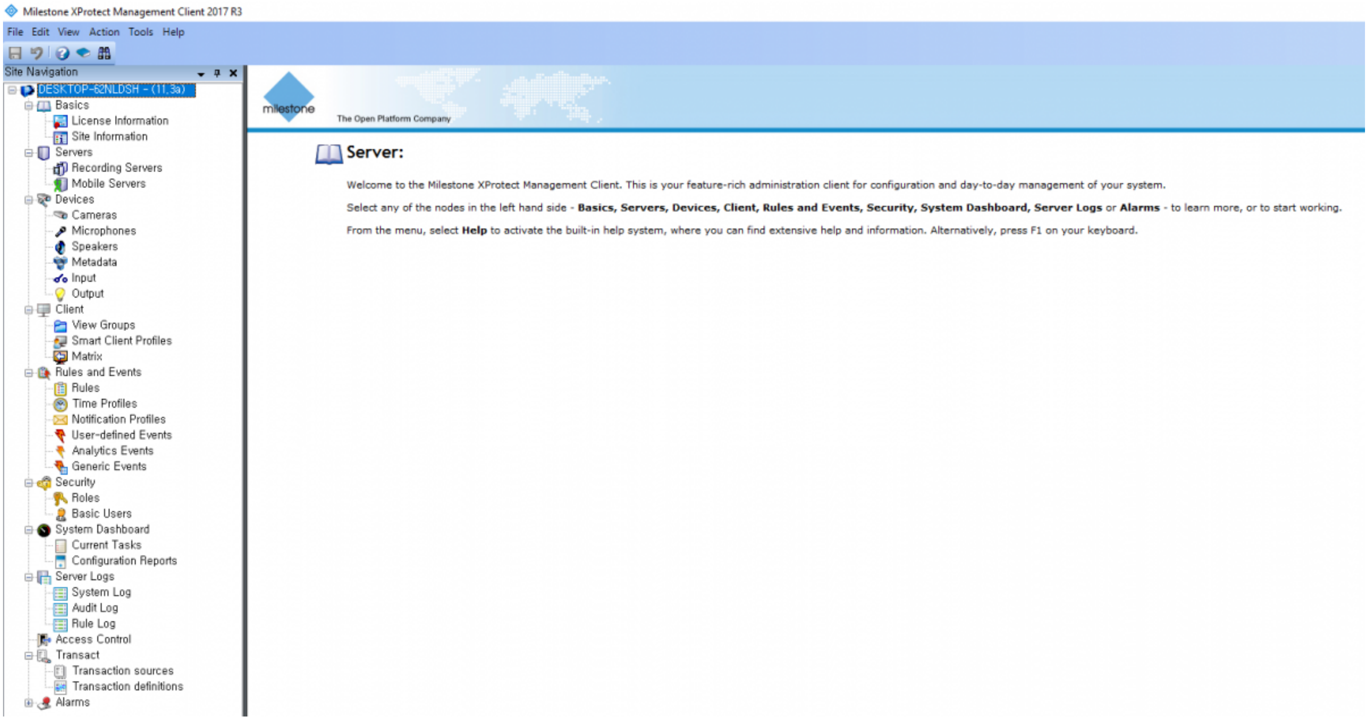
You can refer to BioStar2 Integration for Milestone XProtect Setup Guide to install them.

After succeeding in installation of two applications, start the Milestone XProtect Event Server manually. You can find it in the system tray and right-click on the below icon.


Status: Stopped
Start Event Server service
Show Event Server logs
Show MIP logs
Version: 11.3a (Build: 4113)
Exit Event Server Manager
1:15 PM
12/7/2017

Step 4: Add IP Camera in Milestone XProtect VMS

When you run XProtect Management Client 2017 R3 and connect to your PC, you can see the below screen.



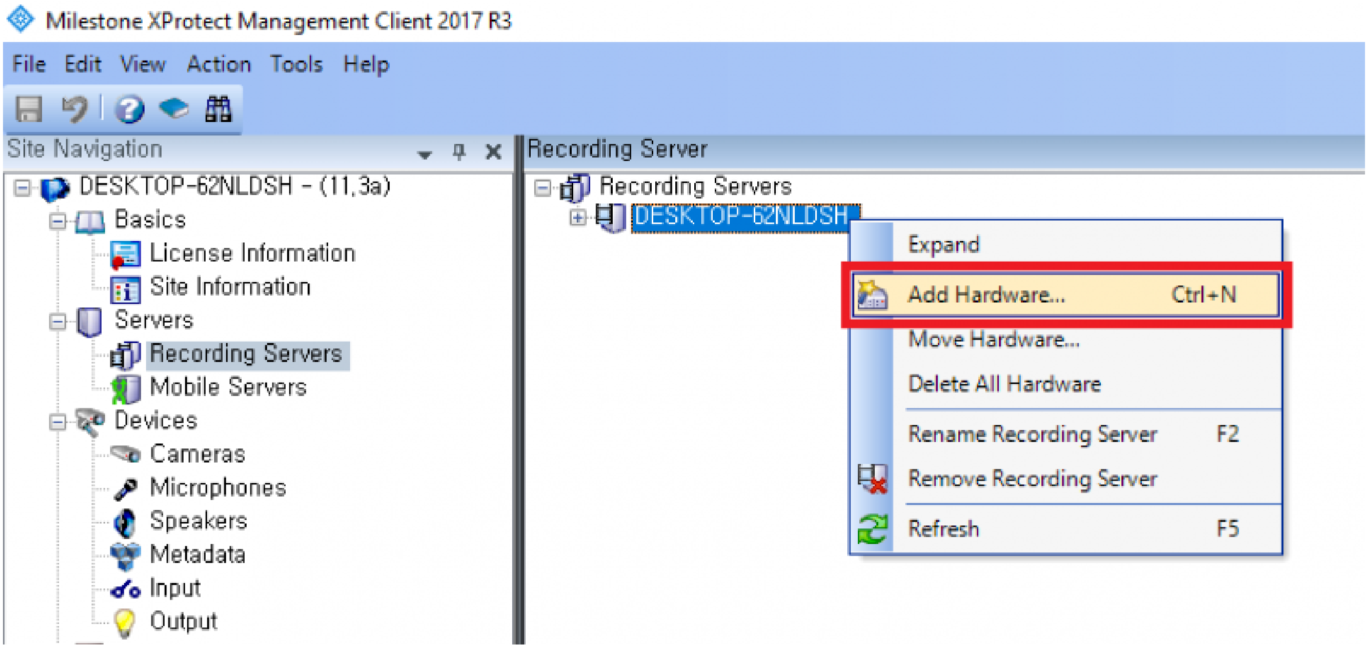
Server:

Welcome to the Milestone XProtect Management Client. This is your feature-rich administration client for configuration and day-to-day management of your system.

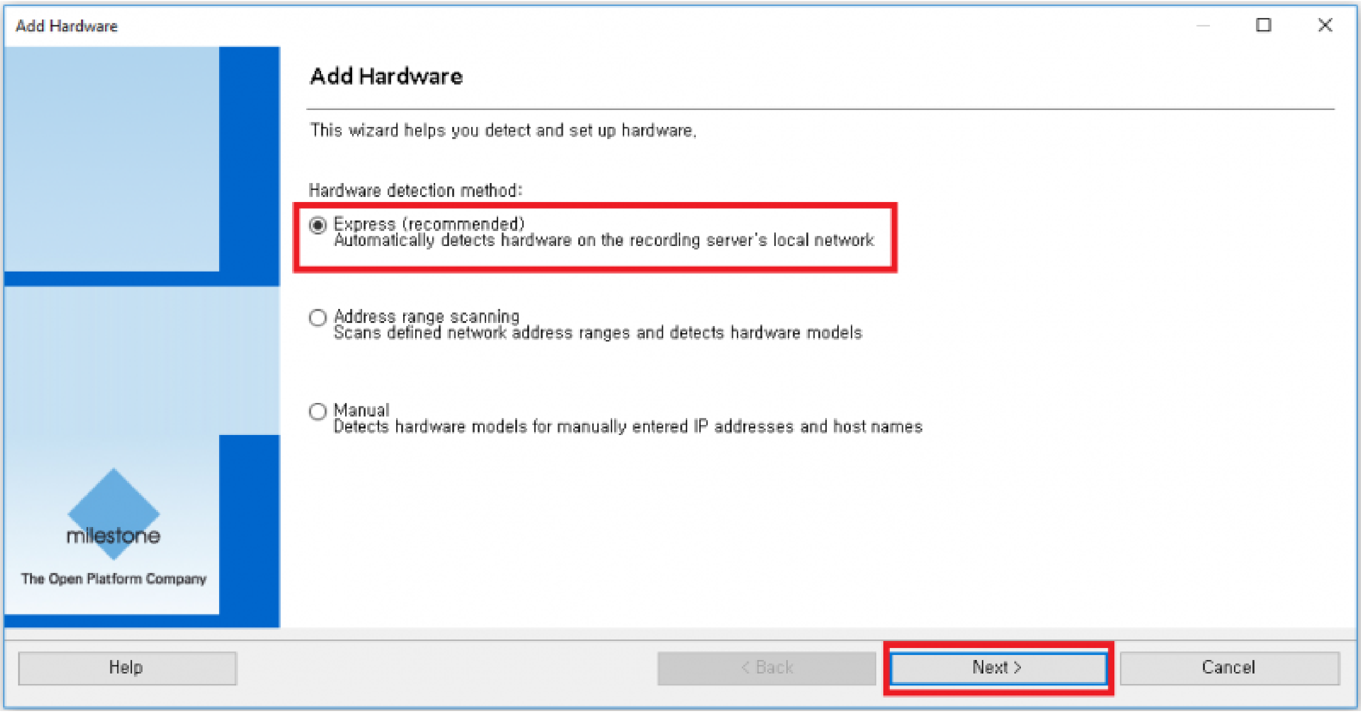
Select any of the nodes in the left hand side - **Basics, Servers, Devices, Client, Rules and Events, Security, System Dashboard, Server Logs** or **Alarms** - to learn more, or to start working.

From the menu, select **Help** to activate the built-in help system, where you can find extensive help and information. Alternatively, press F1 on your keyboard.

Prepare IP camera.
Go to **Servers** > **Recording Servers.**
Right click one of **Recording Servers** and select **Add Hardware.**



Select **Express (recommended)** and then click **Next** button.



Add Hardware

This wizard helps you detect and set up hardware.

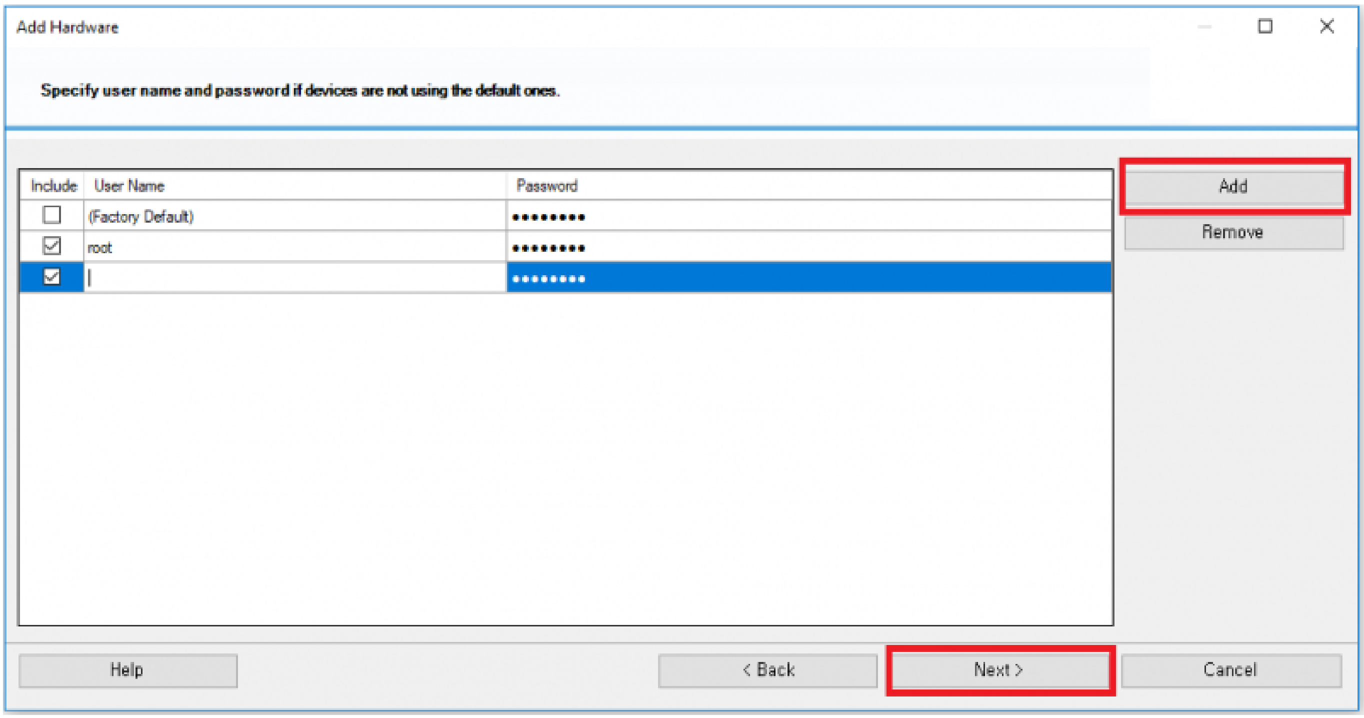
Hardware detection method:

● Express (recommended)
Automatically detects hardware on the recording server's local network

○ Address range scanning
Scans defined network address ranges and detects hardware models

○ Manual
Detects hardware models for manually entered IP addresses and host names

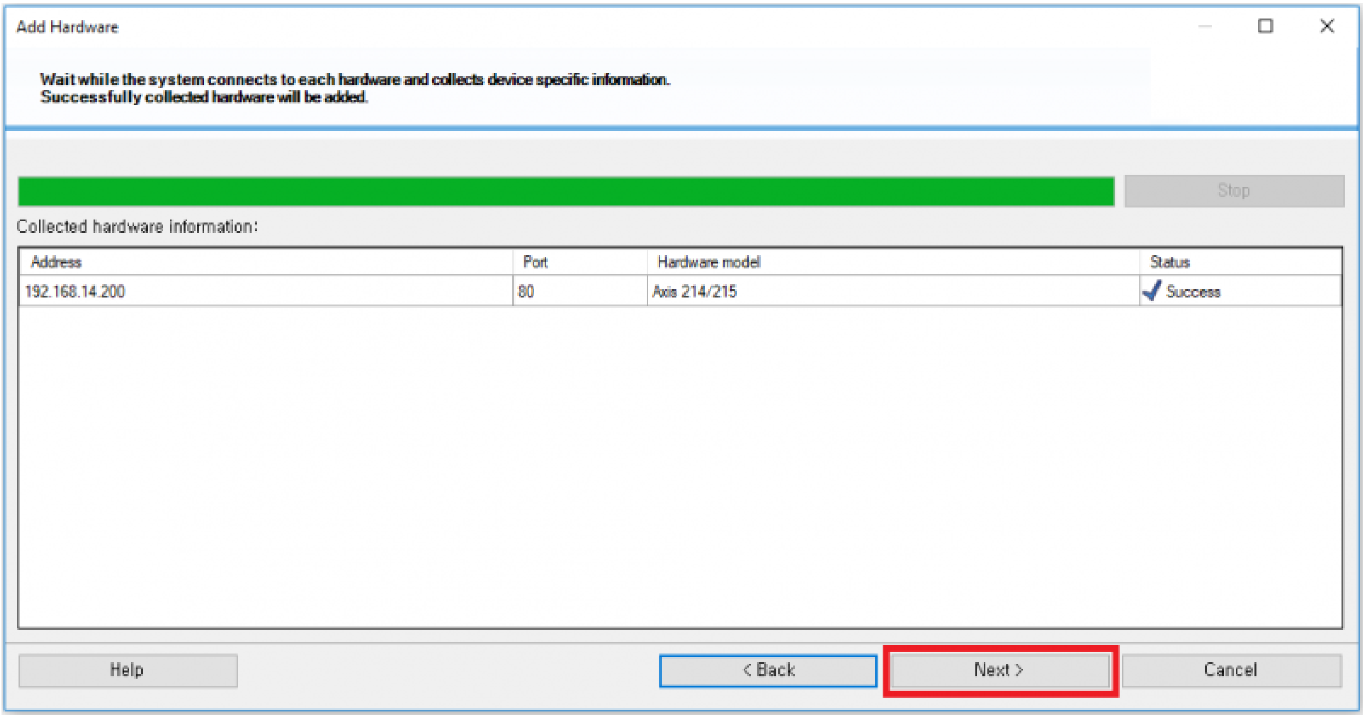
Add new user and enter User Name & Password for IP camera. Then, click Next button.



Specify user name and password if devices are not using the default ones.

Include	User Name	Password
□	(Factory Default)	••••••••
☑	root	••••••••
☑		••••••••

If you enter the information correctly, available camera will be found. To add IP camera, click **Next** button.



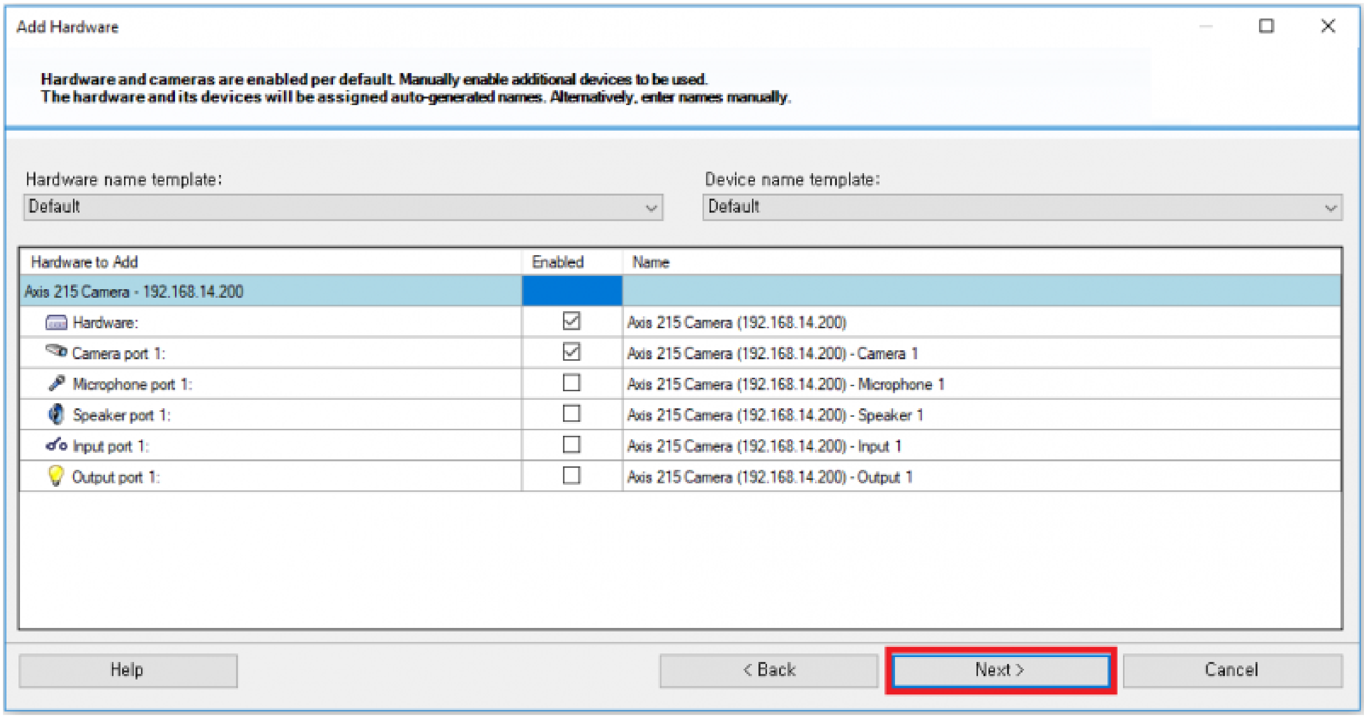
Add Hardware

Wait while the system connects to each hardware and collects device specific information.
Successfully collected hardware information will be added.

Collected hardware information:

Address	Port	Hardware model	Status
192.168.14.200	80	Axis 214/215	✓ Success

Click **Next** button.



Add Hardware

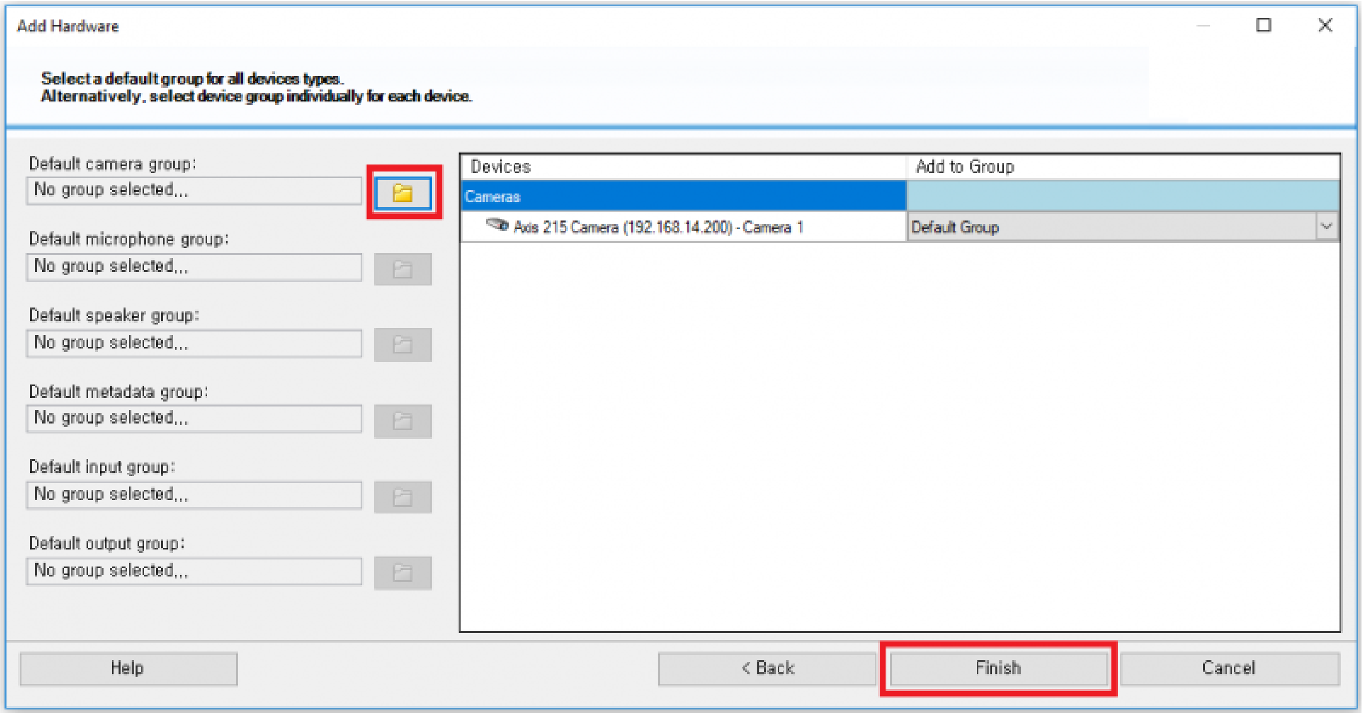
Hardware and cameras are enabled per default. Manually enable additional devices to be used.
The hardware and its devices will be assigned auto-generated names. Alternatively, enter names manually.

Hardware name template: Default

Device name template: Default

Hardware to Add	Enabled	Name
Axis 215 Camera - 192.168.14.200		
Hardware:	☑	Axis 215 Camera (192.168.14.200)
Camera port 1:	☑	Axis 215 Camera (192.168.14.200) - Camera 1
Microphone port 1:	☐	Axis 215 Camera (192.168.14.200) - Microphone 1
Speaker port 1:	☐	Axis 215 Camera (192.168.14.200) - Speaker 1
Input port 1:	☐	Axis 215 Camera (192.168.14.200) - Input 1
Output port 1:	☐	Axis 215 Camera (192.168.14.200) - Output 1

Click folder icon and select one default camera group. Then, click **Finish** button.



Add Hardware

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

Default camera group: No group selected...

Default microphone group: No group selected...

Default speaker group: No group selected...

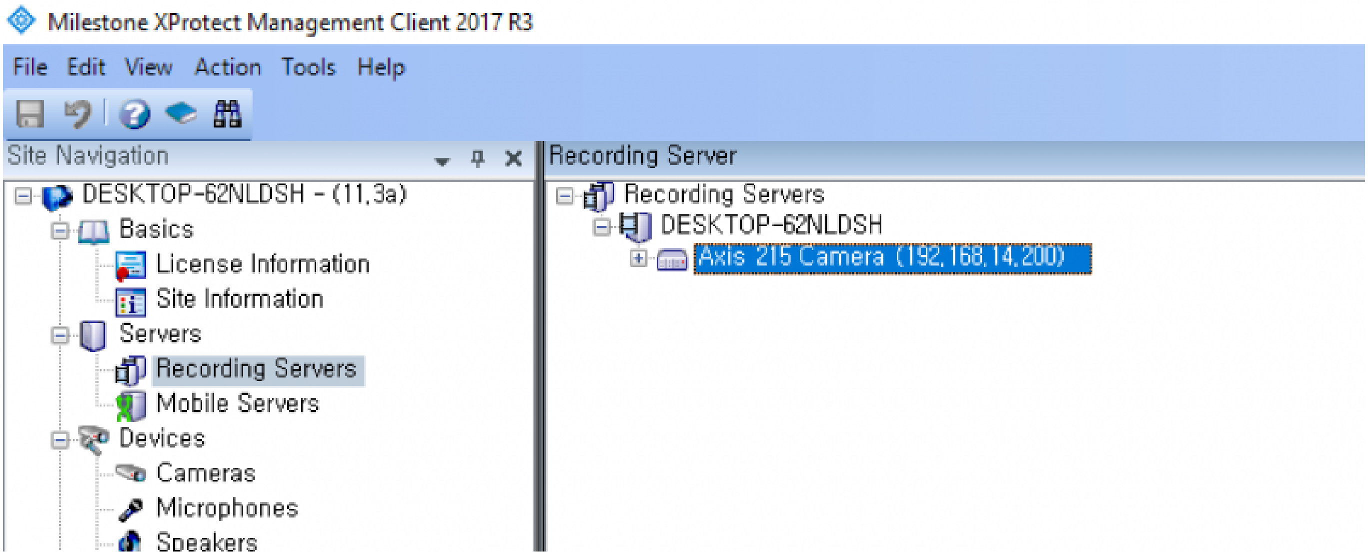
Default metadata group: No group selected...

Default input group: No group selected...

Default output group: No group selected...

Devices	Add to Group
Cameras	
Axis 215 Camera (192.168.14.200) - Camera 1	Default Group

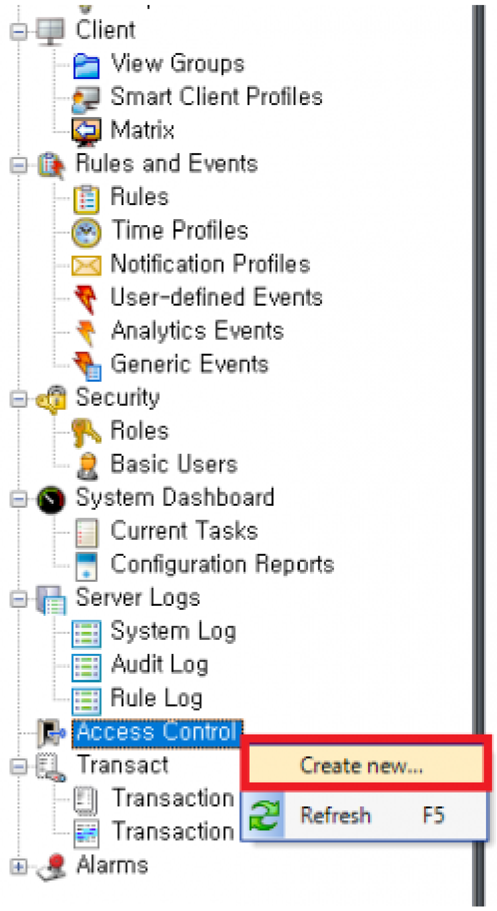
If you succeed in add IP camera, you can see your camera in the Recording Servers’s tree.



Milestone XProtect Management Client 2017 R3

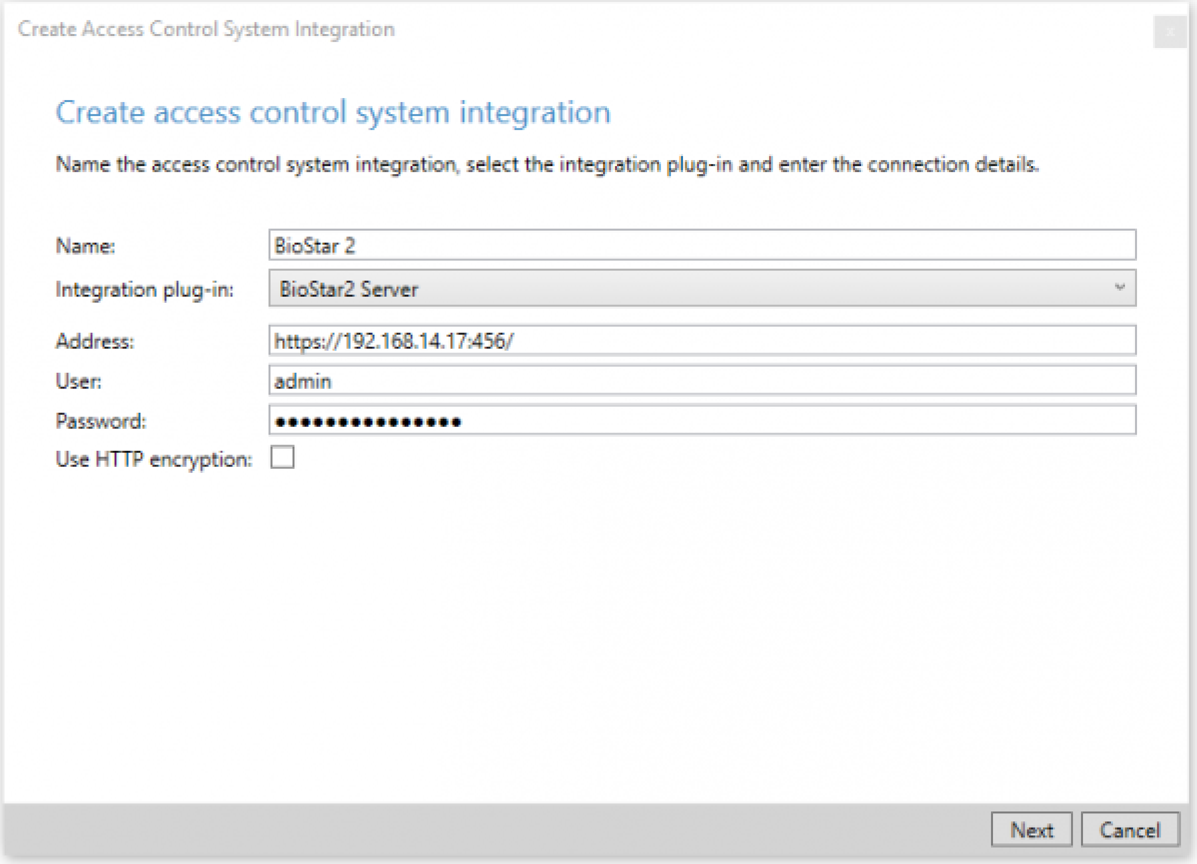
Step 5: Create new Access Control to connect Milestone to BioStar 2

Right click **Access Control** and select **Create new.**



Enter all items.

- Name: Enter name of Access Control you want to use
- Integration plug-in: Select **BioStar2 Server**
- Address: Enter URL for access to BioStar 2 (including port number)
- User: Login ID for BioStar 2
- Password: Password for BioStar 2



Create Access Control System Integration

Create access control system integration

Name the access control system integration, select the integration plug-in and enter the connection details.

Name: BioStar 2

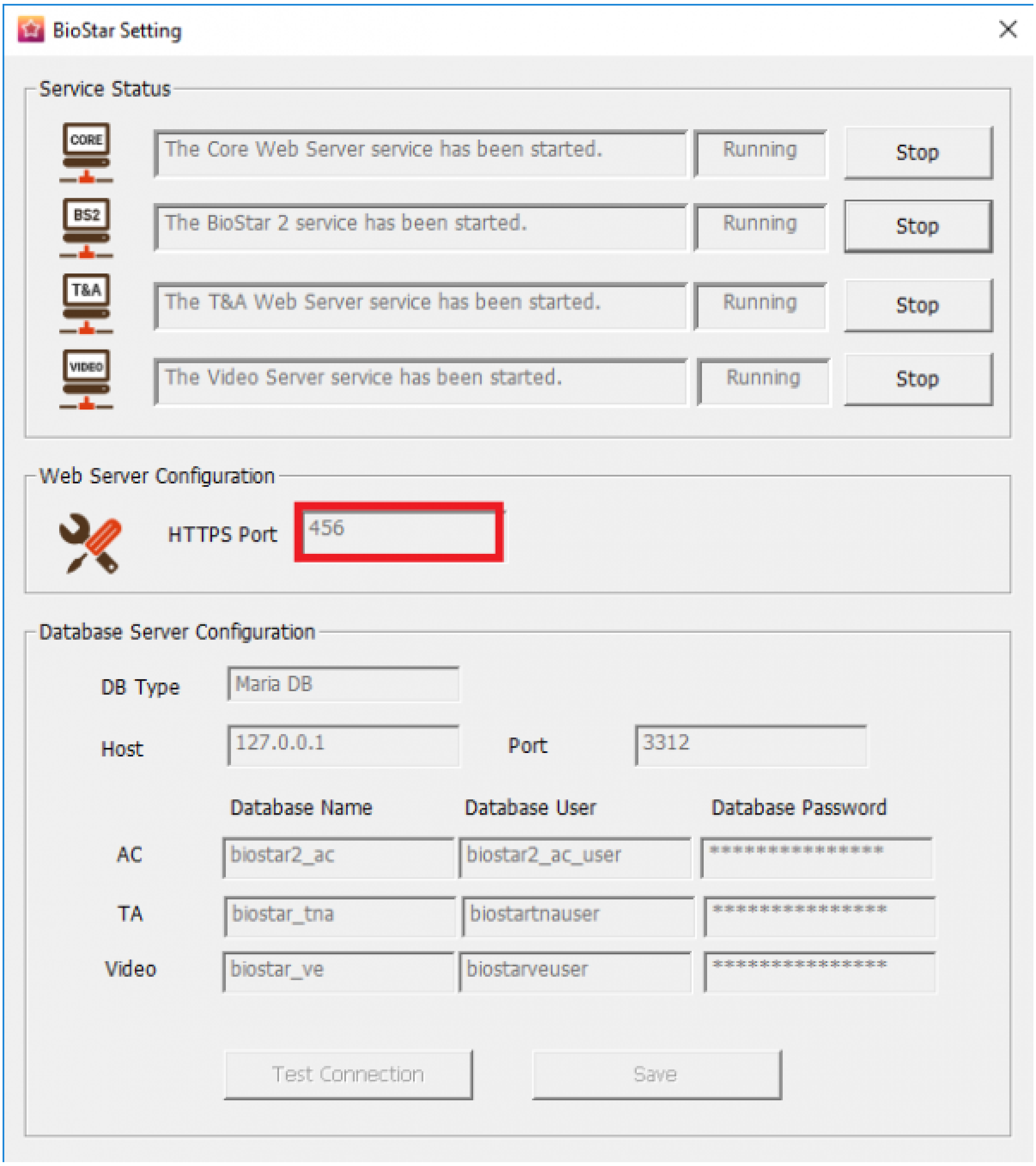
Integration plug-in: BioStar2 Server

Address: https://192.168.14.17:456/

User: admin

Password: ••••••••••••••••

Use HTTP encryption: □



The Core Web Server service has been started. Running

The BioStar 2 service has been started. Running

The T&A Web Server service has been started. Running

The Video Server service has been started. Running

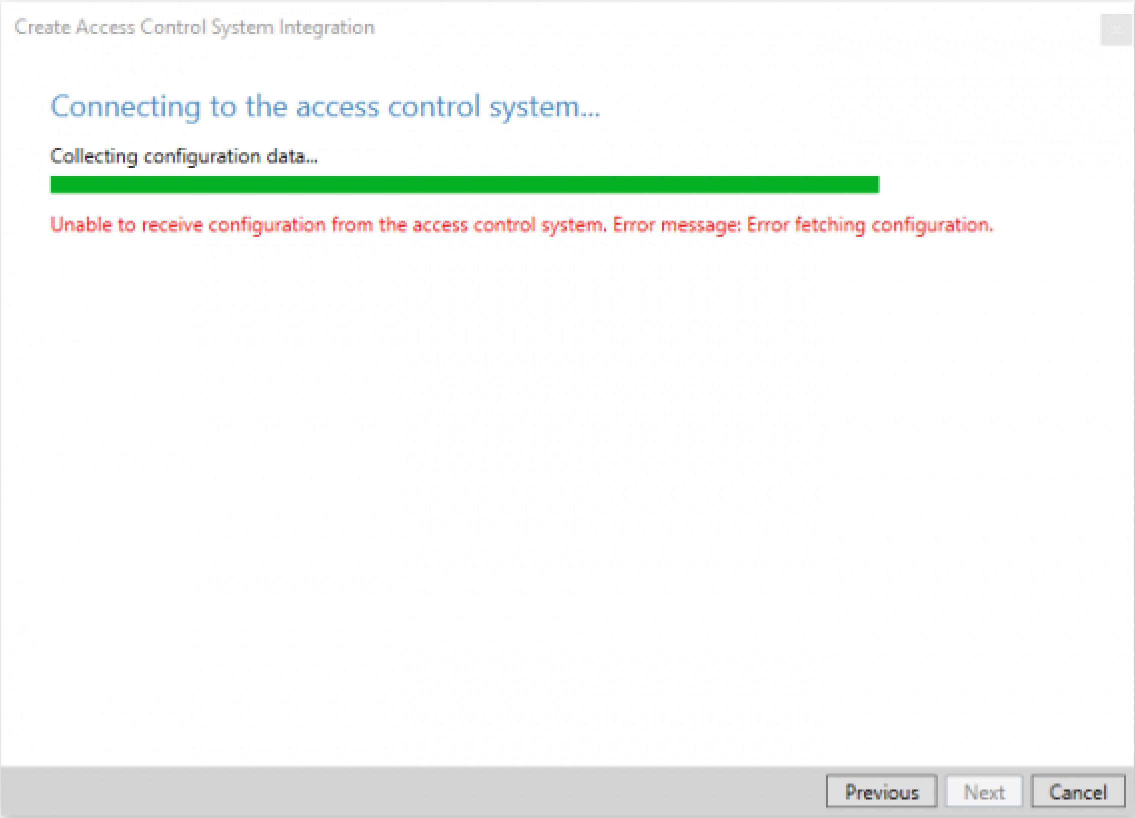
HTTPS Port 456

DB Type Maria DB

Host 127.0.0.1 Port 3312

	Database Name	Database User	Database Password
AC	biostar2_ac	biostar2_ac_user	***************
TA	biostar_tna	biostartnauser	***************
Video	biostar_ve	biostarveuser	***************

If you fail to connect to the access control system (BioStar 2 AC), you will get the below error. Please check if all settings are correct.



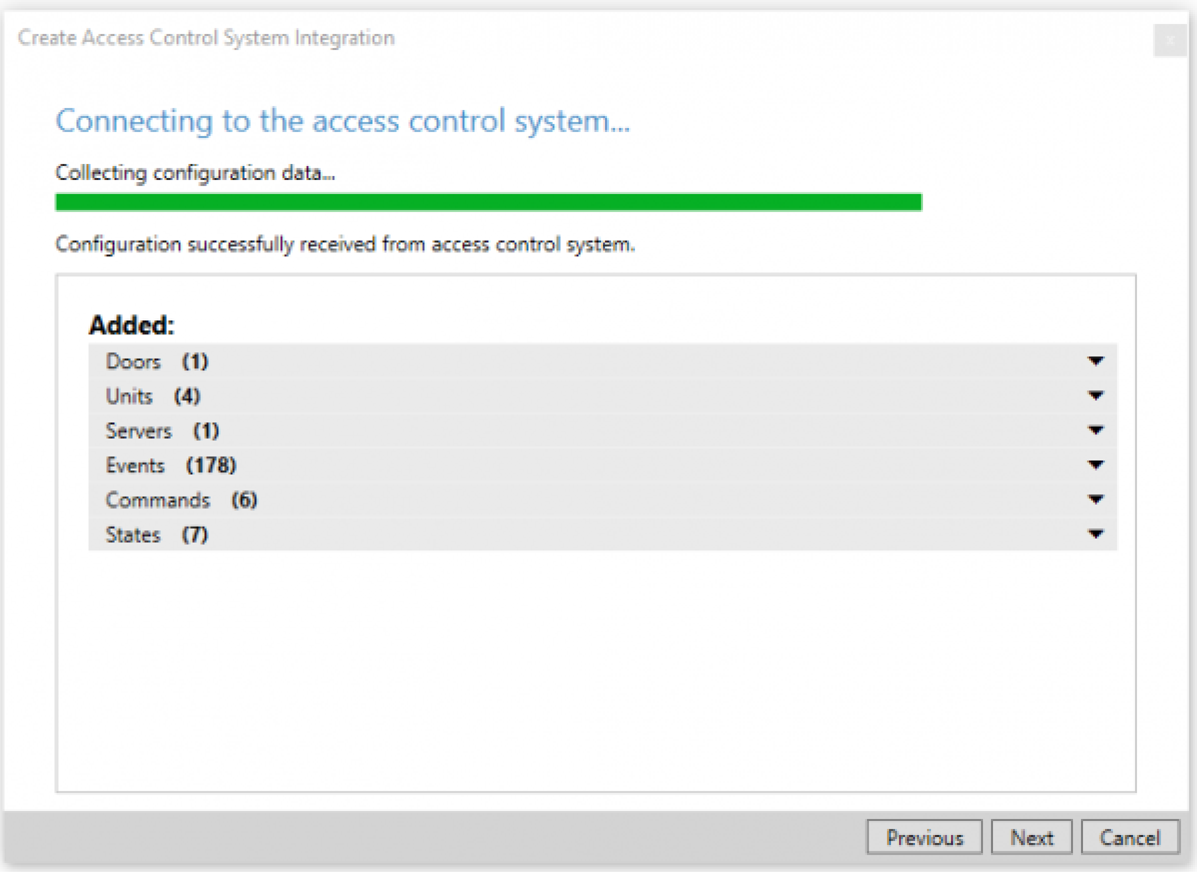
Create Access Control System Integration

Connecting to the access control system...

Collecting configuration data...

Unable to receive configuration from the access control system. Error message: Error fetching configuration.

If you succeed in connection to the access control system (BioStar 2 AC), you can see below picture.



Create Access Control System Integration

Connecting to the access control system...

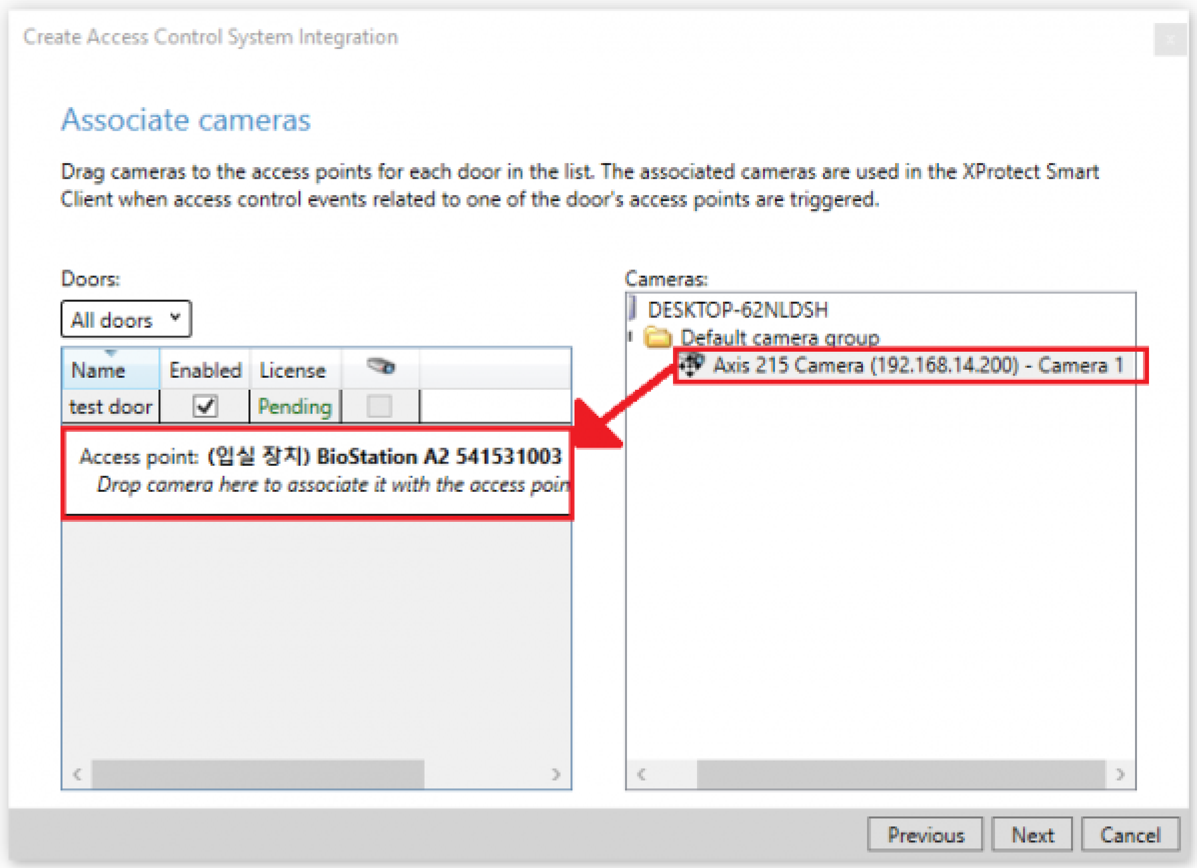
Collecting configuration data...

Configuration successfully received from access control system.

Added:

- Doors (1)
- Units (4)
- Servers (1)
- Events (178)
- Commands (6)
- States (7)

If BioStar 2 connected to Milestone successfully, the below screen will appear.
After selecting IP camera you will use in the right panel, **drag the cameras to the access points** for each door in the left list.



Create Access Control System Integration

Associate cameras

Drag cameras to the access points for each door in the list. The associated cameras are used in the XProtect Smart Client when access control events related to one of the door's access points are triggered.

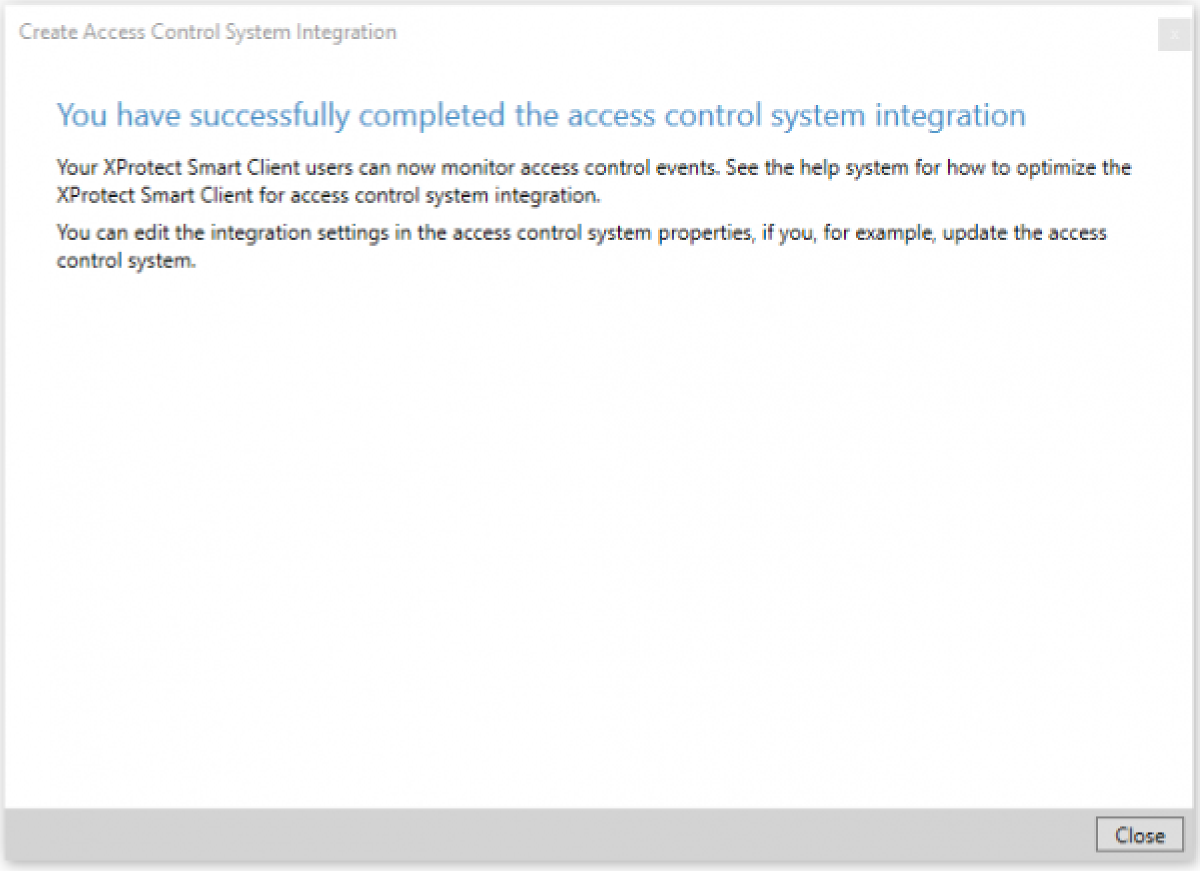
Doors: All doors

Name	Enabled	License	
test door	☑	Pending	□

Access point: **(입실 장치) BioStation A2 541531003**
Drop camera here to associate it with the access poin

Cameras:
- DESKTOP-62NLDSH
  - Default camera group
    - Axis 215 Camera (192.168.14.200) - Camera 1

If you succeeded in integrate Milestone with BioStar2 with IP camera, you can see below picture.



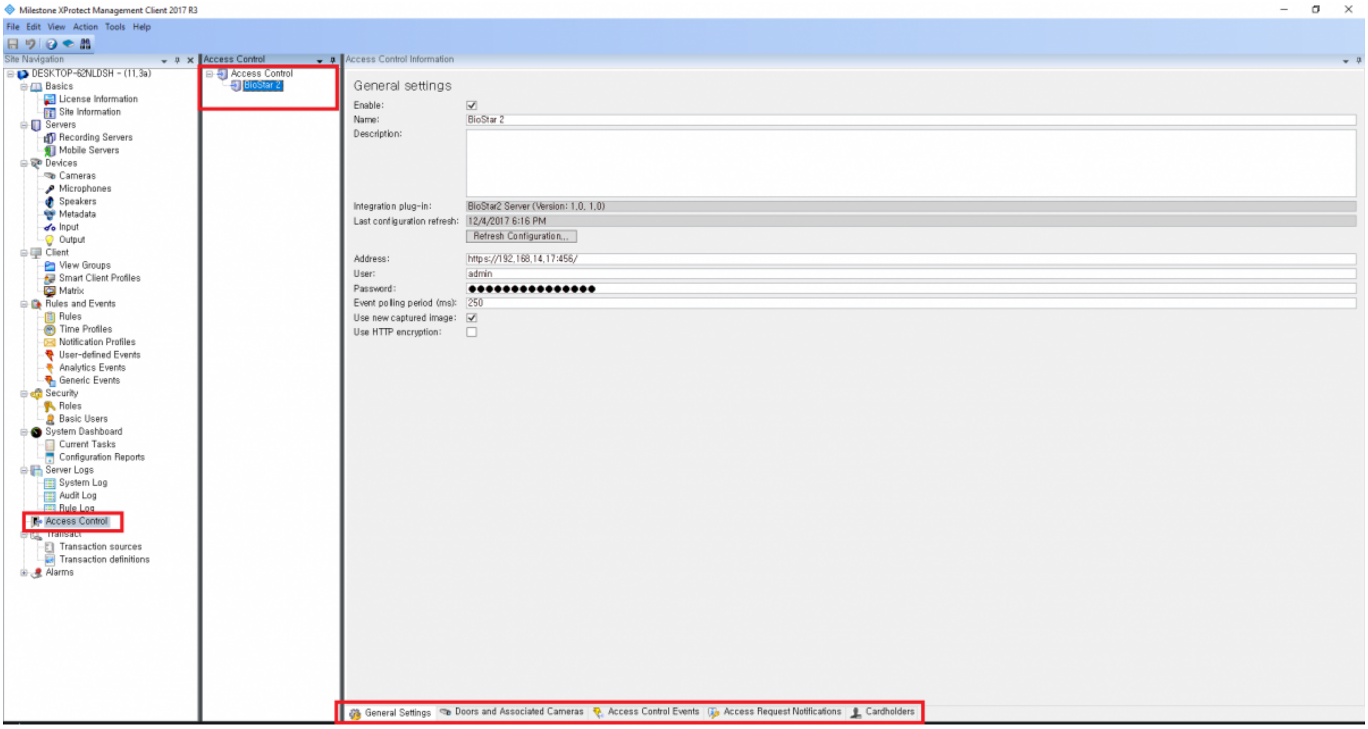
You have successfully completed the access control system integration

Your XProtect Smart Client users can now monitor access control events. See the help system for how to optimize the XProtect Smart Client for access control system integration.

You can edit the integration settings in the access control system properties, if you, for example, update the access control system.

Once you succeed in integration between BioStar 2 and Milestone, you can add/edit the access control properties at any time.
To manage them, you need to select one of Access Control.

At the bottom, there are 5 tabs you can configure.



General settings

Enable: ☑

Name: BioStar 2

Description:

Integration plug-in: BioStar2 Server (Version: 1.0. 1.0)

Last configuration refresh: 12/4/2017 6:16 PM

Refresh Configuration...

Address: https://192.168.14.17:456/

User: admin

Password: ●●●●●●●●●●●●●●●

Event polling period (ms): 250

Use new captured image: ☑

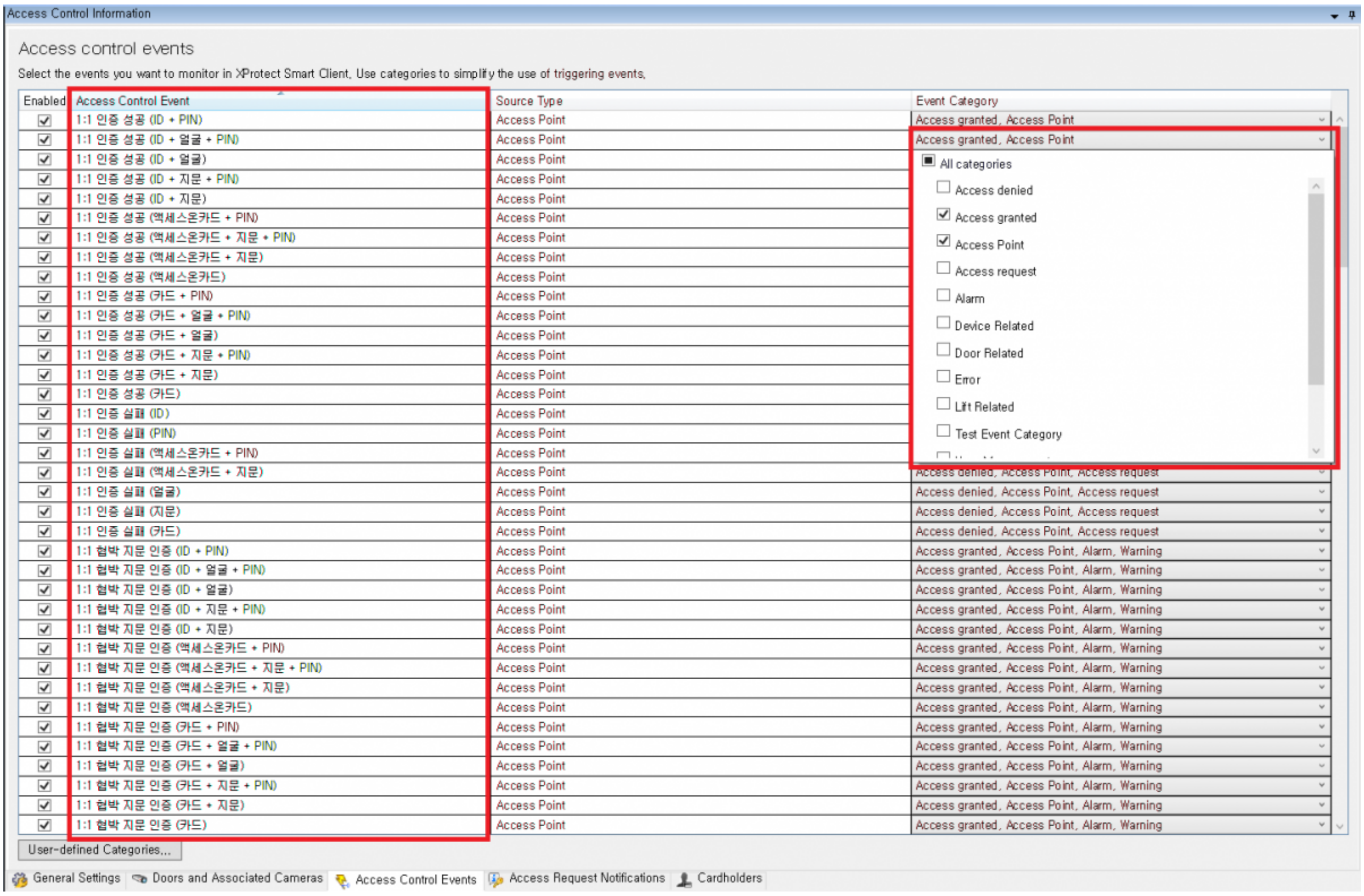
Use HTTP encryption: □

- General Settings: You can update the access control system name, network settings and login information.
- Doors and Associated Cameras: You can associate the cameras with access points.
- Access Control Events: You can activate or deactivate the access control event from BioStar 2, also create and assign the user-defined categories.
- Access Request Notifications: You can create an access control action or command which is performed by the operator on the associated access points. For example, when a card holder requests the door open, XProtect display a notification and then operator sending a door open command.
- Cardholders: You can view or search the cardholder information. The cardholder information is synchronized with user information of BioStar 2. In BioStar 2, user information includes user name, access group, RFID card number, fingerprint template, face template and PIN.

Major Features

Feature 1: Access Control Events

This function is used for classifying Access Control Events into certain Event Category. In general, there are a variety of different events in each access control system. To manage them efficiently in Milestone, you should map all access control events to certain Event Category.



Access Control Information

Access control events

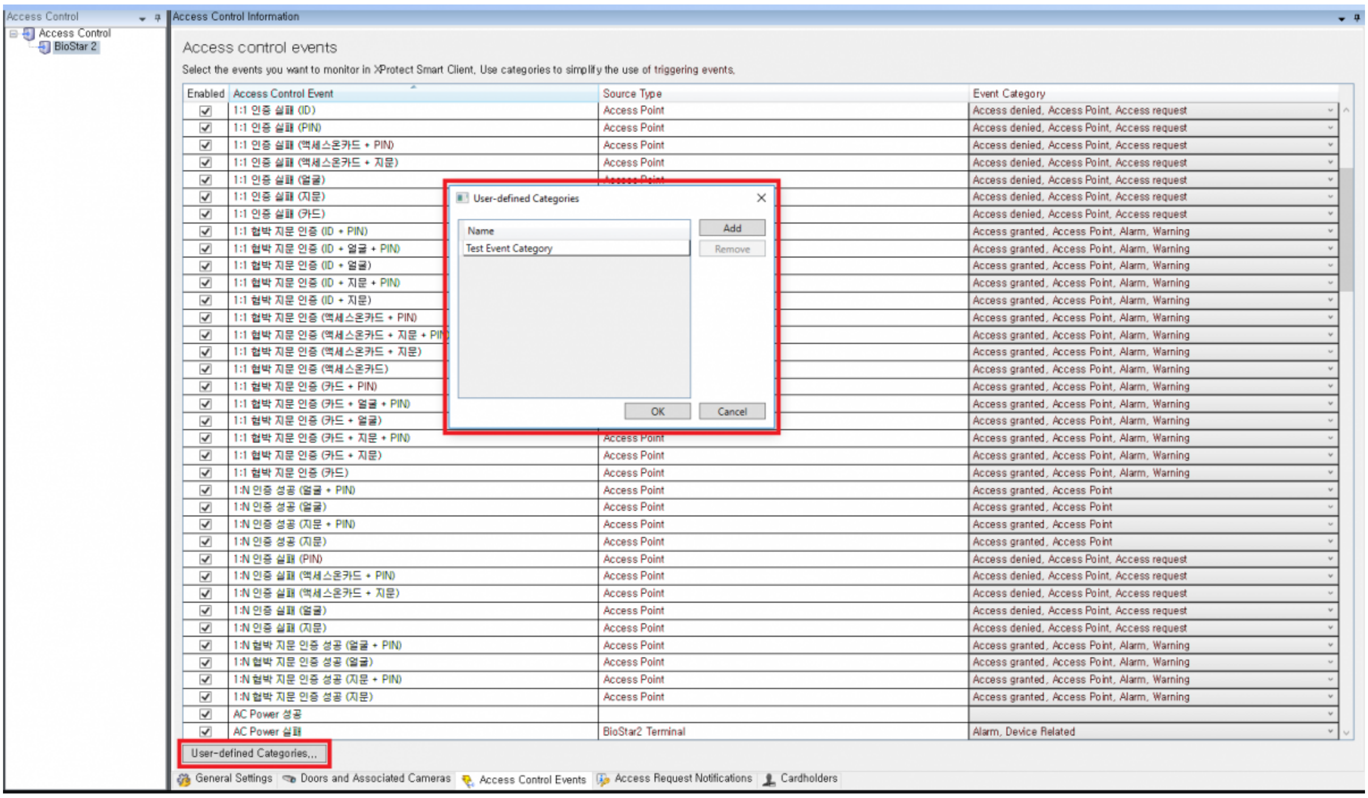
Select the events you want to monitor in XProtect Smart Client, Use categories to simplify the use of triggering events,

Enabled	Access Control Event	Source Type	Event Category
☑	1:1 인증 성공 (ID + PIN)	Access Point	Access granted, Access Point
☑	1:1 인증 성공 (ID + 얼굴 + PIN)	Access Point	Access granted, Access Point
☑	1:1 인증 성공 (ID + 얼굴)	Access Point	
☑	1:1 인증 성공 (ID + 지문 + PIN)	Access Point	
☑	1:1 인증 성공 (ID + 지문)	Access Point	
☑	1:1 인증 성공 (액세스온카드 + PIN)	Access Point	
☑	1:1 인증 성공 (액세스온카드 + 지문 + PIN)	Access Point	
☑	1:1 인증 성공 (액세스온카드 + 지문)	Access Point	
☑	1:1 인증 성공 (액세스온카드)	Access Point	
☑	1:1 인증 성공 (카드 + PIN)	Access Point	
☑	1:1 인증 성공 (카드 + 얼굴 + PIN)	Access Point	
☑	1:1 인증 성공 (카드 + 얼굴)	Access Point	
☑	1:1 인증 성공 (카드 + 지문 + PIN)	Access Point	
☑	1:1 인증 성공 (카드 + 지문)	Access Point	
☑	1:1 인증 성공 (카드)	Access Point	
☑	1:1 인증 실패 (ID)	Access Point	
☑	1:1 인증 실패 (PIN)	Access Point	
☑	1:1 인증 실패 (액세스온카드 + PIN)	Access Point	
☑	1:1 인증 실패 (액세스온카드 + 지문)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (얼굴)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (지문)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (카드)	Access Point	Access denied, Access Point, Access request
☑	1:1 협박 지문 인증 (ID + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드 + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드 + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드)	Access Point	Access granted, Access Point, Alarm, Warning

- ■ All categories
- ☐ Access denied
- ☑ Access granted
- ☑ Access Point
- ☐ Access request
- ☐ Alarm
- ☐ Device Related
- ☐ Door Related
- ☐ Error
- ☐ Lift Related
- ☐ Test Event Category

User-defined Categories...
General Settings
Doors and Associated Cameras
Access Control Events
Access Request Notifications
Cardholders

If you want to create customized Event Category, you can make it by clicking **User-defined Categories** button.



Access Control Information

Access control events

Select the events you want to monitor in XProtect Smart Client, Use categories to simplify the use of triggering events,

Enabled	Access Control Event	Source Type	Event Category
☑	1:1 인증 실패 (ID)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (PIN)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (액세스온카드 + PIN)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (액세스온카드 + 지문)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (얼굴)	Access Point	Access denied, Access Point, Access request
☑	1:1 인증 실패 (지문)		Access denied, Access Point, Access request
☑	1:1 인증 실패 (카드)		Access denied, Access Point, Access request
☑	1:1 협박 지문 인증 (ID + PIN)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 얼굴 + PIN)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 얼굴)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 지문 + PIN)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (ID + 지문)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드 + PIN)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드 + 지문 + PI		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드 + 지문)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (액세스온카드)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + PIN)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 얼굴 + PIN)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 얼굴)		Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드 + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:1 협박 지문 인증 (카드)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:N 인증 성공 (얼굴 + PIN)	Access Point	Access granted, Access Point
☑	1:N 인증 성공 (얼굴)	Access Point	Access granted, Access Point
☑	1:N 인증 성공 (지문 + PIN)	Access Point	Access granted, Access Point
☑	1:N 인증 성공 (지문)	Access Point	Access granted, Access Point
☑	1:N 인증 실패 (PIN)	Access Point	Access denied, Access Point, Access request
☑	1:N 인증 실패 (액세스온카드 + PIN)	Access Point	Access denied, Access Point, Access request
☑	1:N 인증 실패 (액세스온카드 + 지문)	Access Point	Access denied, Access Point, Access request
☑	1:N 인증 실패 (얼굴)	Access Point	Access denied, Access Point, Access request
☑	1:N 인증 실패 (지문)	Access Point	Access denied, Access Point, Access request
☑	1:N 협박 지문 인증 성공 (얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:N 협박 지문 인증 성공 (얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:N 협박 지문 인증 성공 (지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
☑	1:N 협박 지문 인증 성공 (지문)	Access Point	Access granted, Access Point, Alarm, Warning
☑	AC Power 성공		
☑	AC Power 실패	BioStar2 Terminal	Alarm, Device Related

User-defined Categories

Name
Test Event Category

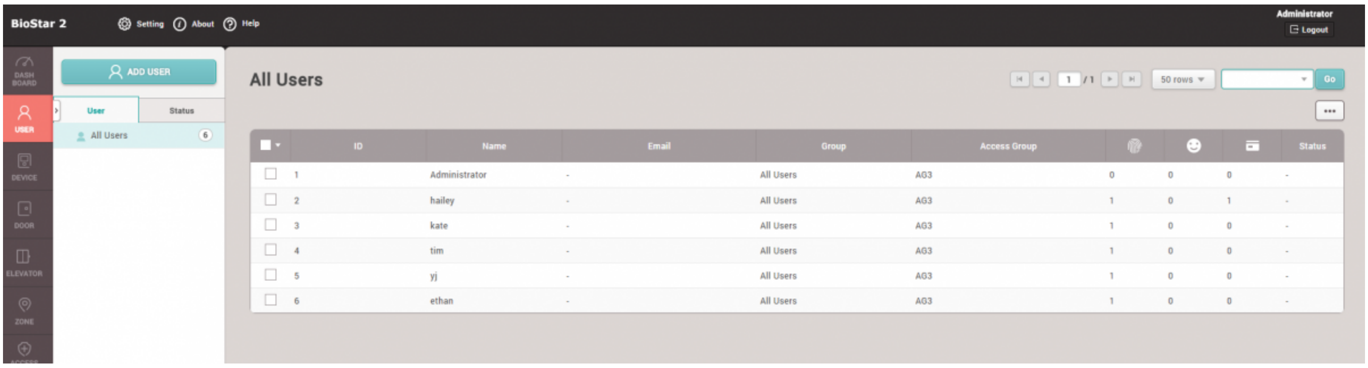
Add
Remove
OK
Cancel
User-defined Categories...
General Settings
Doors and Associated Cameras
Access Control Events
Access Request Notifications
Cardholders

Feature 2: Cardholders

The user who is enrolled in BioStar 2 is synchronized with the cardholder in Milestone.

List of all Users

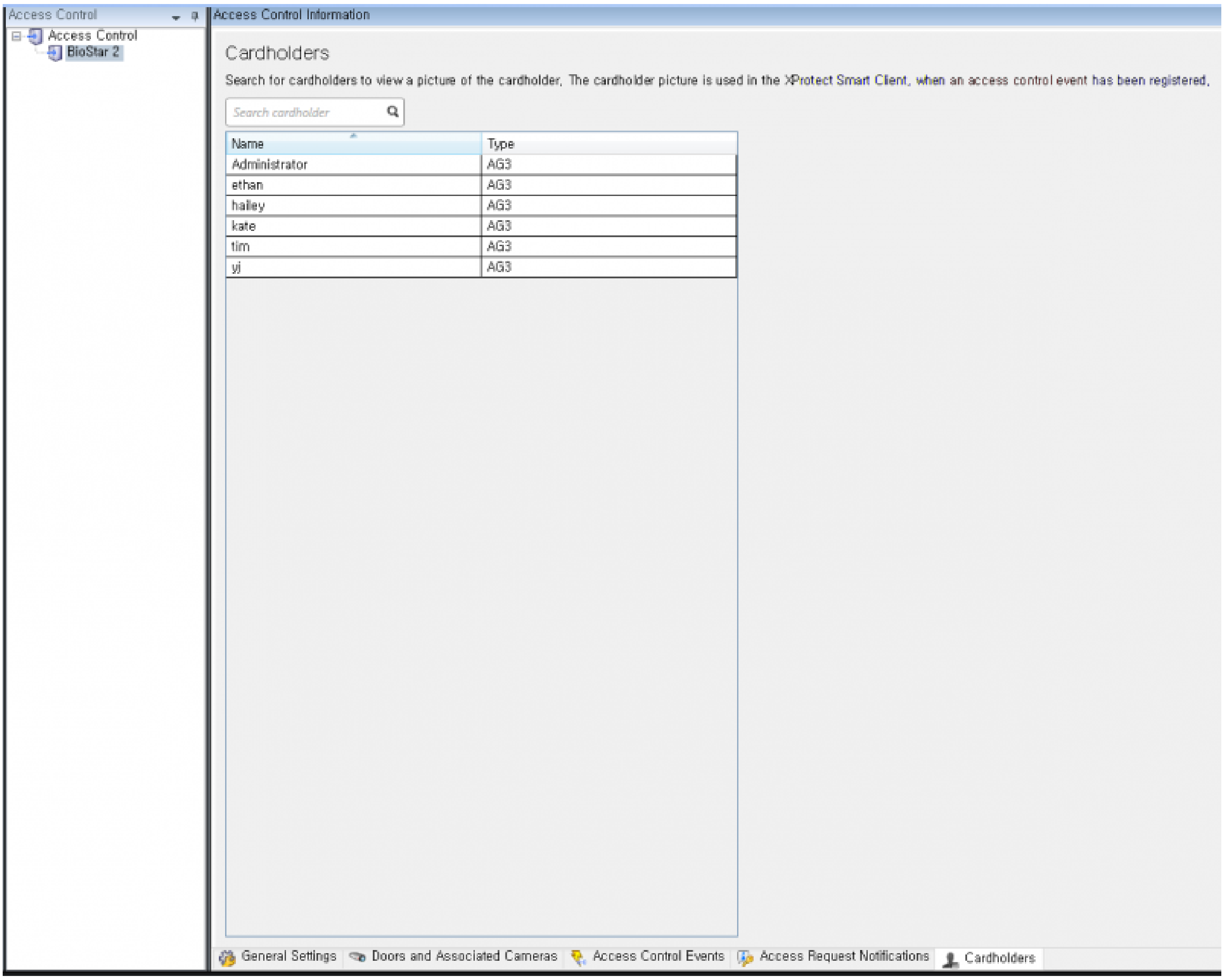
BioStar 2:



All Users

ID	Name	Email	Group	Access Group		☺		Status
1	Administrator	-	All Users	AG3	0	0	0	-
2	hailey	-	All Users	AG3	1	0	1	-
3	kate	-	All Users	AG3	1	0	0	-
4	tim	-	All Users	AG3	1	0	0	-
5	yj	-	All Users	AG3	1	0	0	-
6	ethan	-	All Users	AG3	1	0	0	-

Milestone:



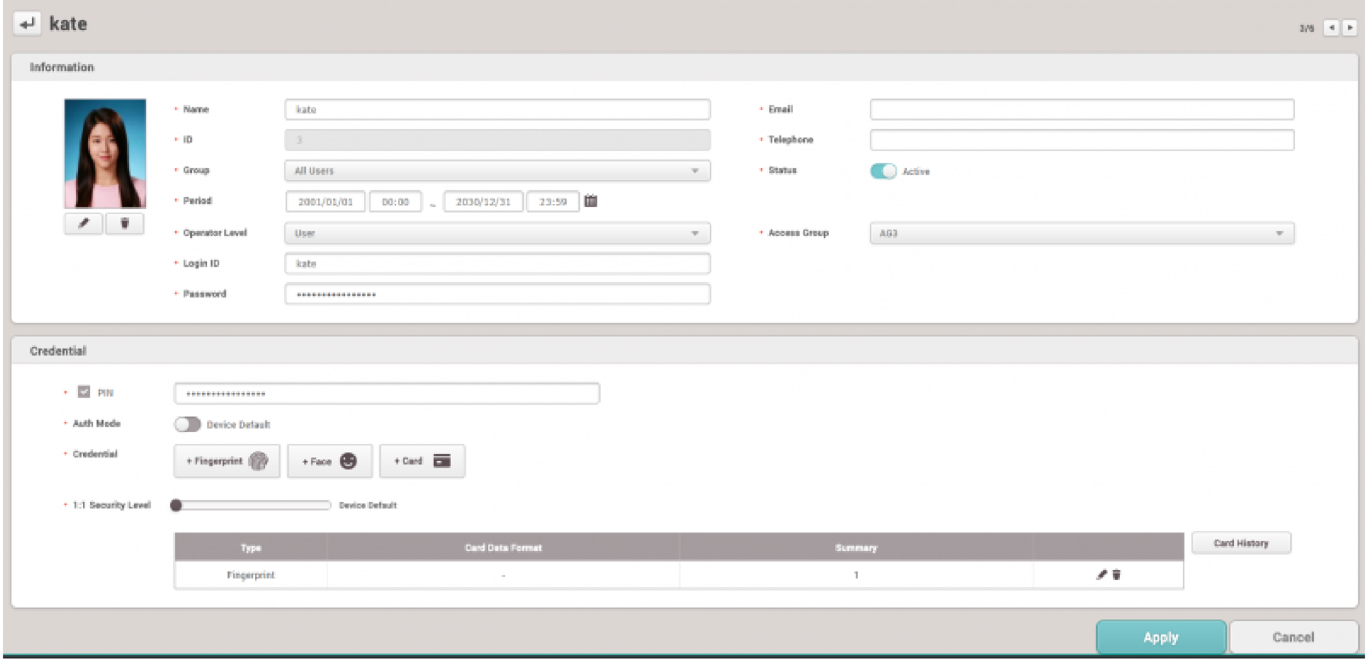
Cardholders

Search for cardholders to view a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an access control event has been registered.

Name	Type
Administrator	AG3
ethan	AG3
hailey	AG3
kate	AG3
tim	AG3
yj	AG3

User Details

BioStar 2:



kate

3/6

Information

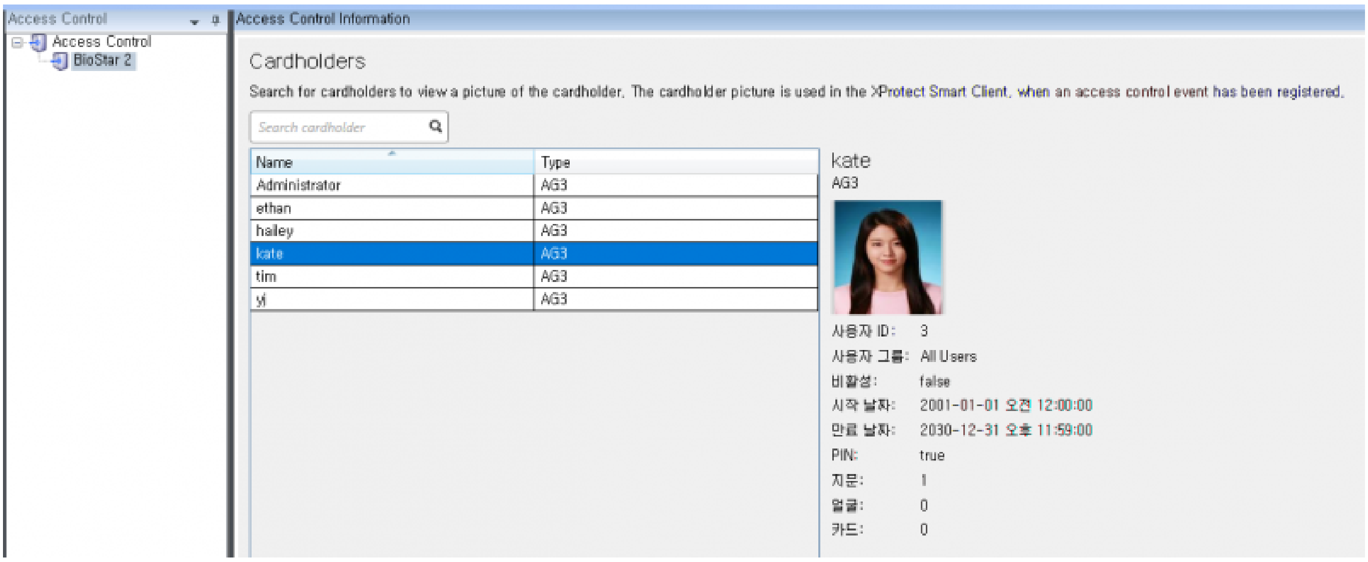
Name	kate	Email	
ID	3	Telephone	
Group	All Users	Status	Active
Period	2001/01/01 00:00 ~ 2030/12/31 23:59		
Operator Level	User	Access Group	AG3
Login ID	kate		
Password	****************		

Credential

☑ PIN	****************
Auth Mode	Device Default
Credential	+ Fingerprint + Face + Card
1:1 Security Level	Device Default

Type	Card Data Format	Summary	
Fingerprint	-	1	

Milestone:



Cardholders

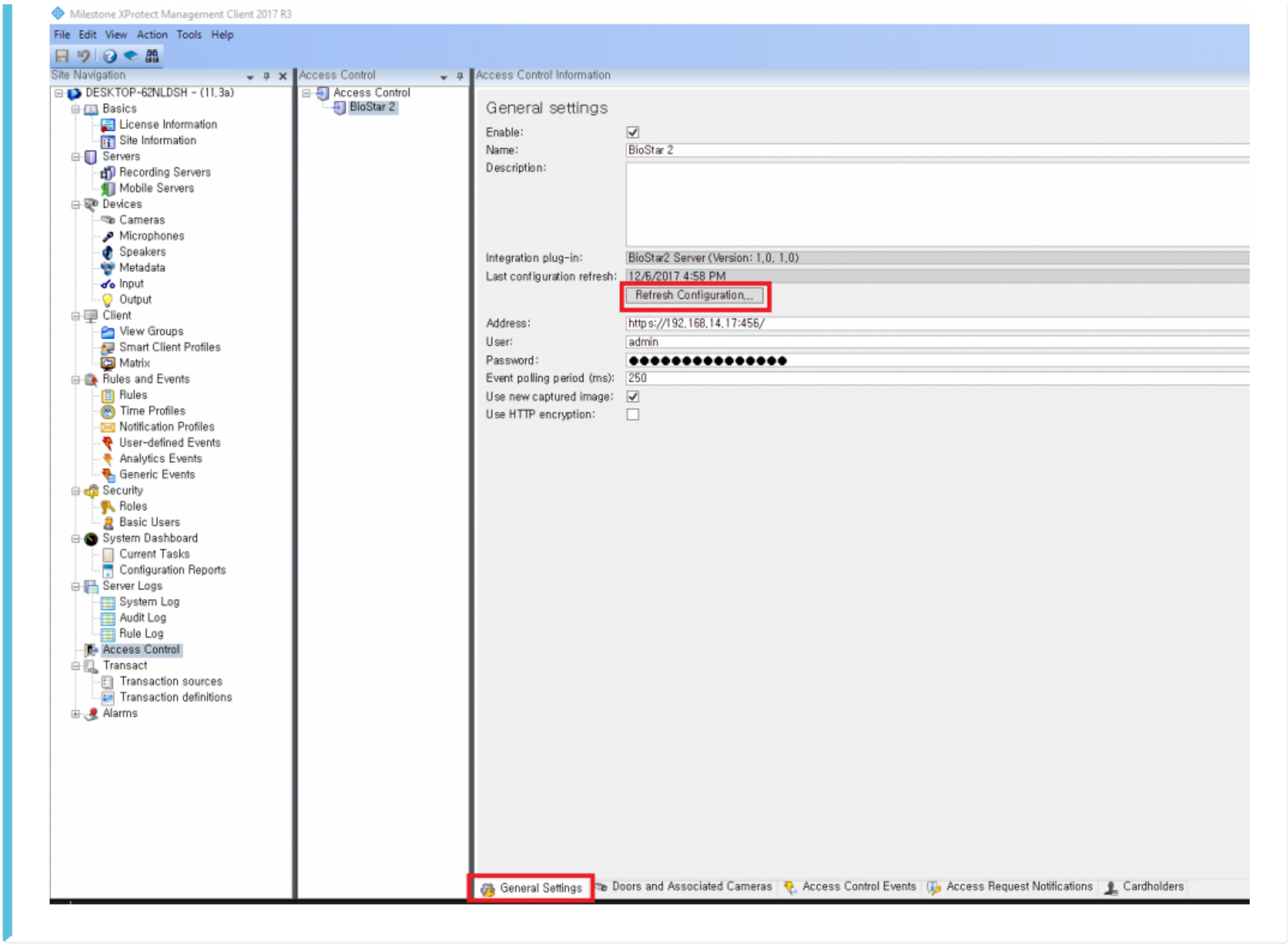
Search for cardholders to view a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an access control event has been registered.

Name	Type
Administrator	AG3
ethan	AG3
hailey	AG3
kate	AG3
tim	AG3
yj	AG3

kate
AG3

사용자 ID:	3
사용자 그룹:	All Users
비활성:	false
시작 날짜:	2001-01-01 오전 12:00:00
만료 날짜:	2030-12-31 오후 11:59:00
PIN:	true
지문:	1
얼굴:	0
카드:	0

Although the information on user/door/device is changed except for real-time events in BioStar 2, it will not be updated in Milestone automatically. In these cases, you should click **Refresh Configuration** button in Milestone (**Access Control** > **General Settings**). Otherwise, the user information between BioStar 2 and Milestone are different.



General settings

Enable: ☑

Name: BioStar 2

Description:

Integration plug-in: BioStar2 Server (Version: 1.0, 1.0)

Last configuration refresh: 12/6/2017 4:58 PM

Address: https://192.168.14.17:456/

User: admin

Password: ●●●●●●●●●●●●●●●●

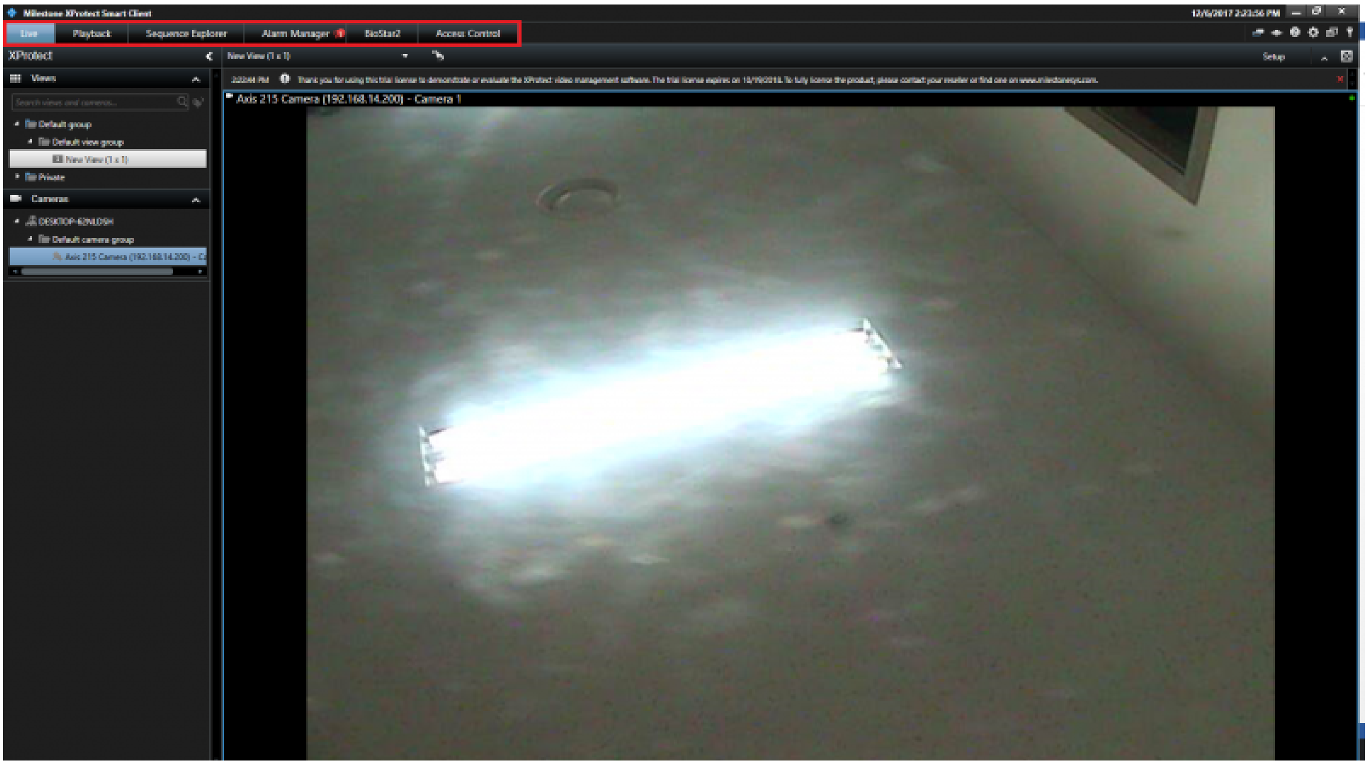
Event polling period (ms): 250

Use new captured image: ☑

Use HTTP encryption: ☐

Step 6: Utilize XProtect Smart Client

If you succeed in integration with Milestone with BioStar2, you can monitor real-time video, identify the detected alarm from the door, access to BioStar 2 and check the event logs displayed in BioStar 2 by utilizing XProtect Smart Client.



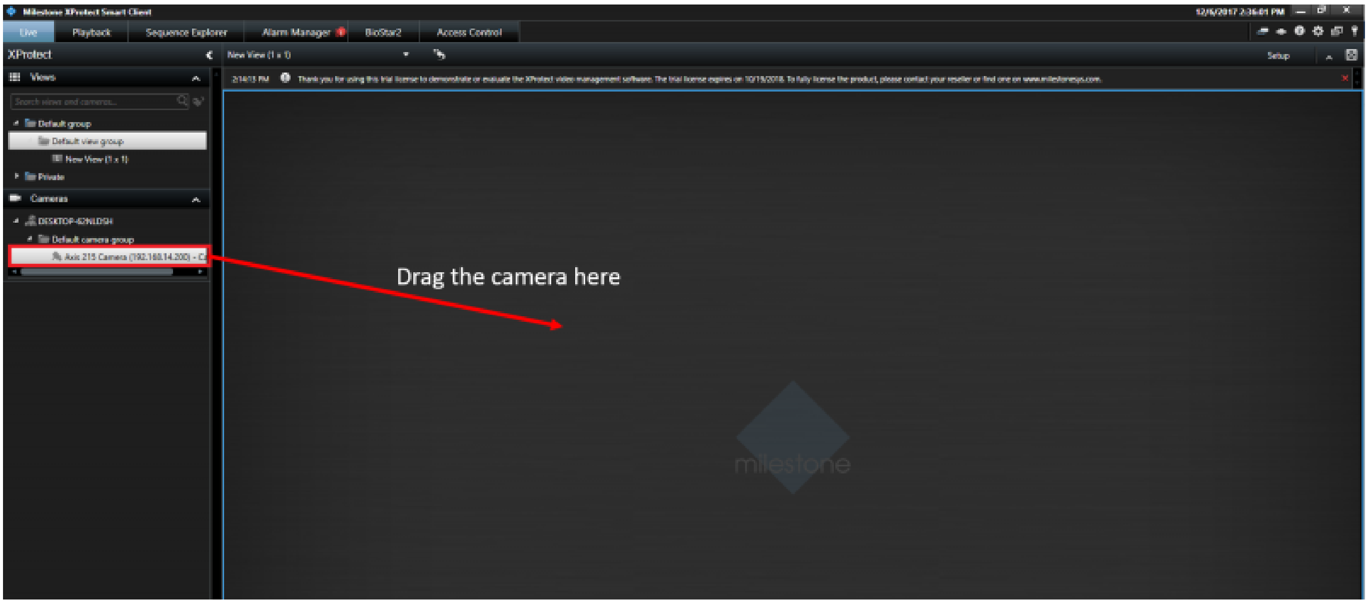
2:22:44 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 10/19/2018. To fully license the product, please contact your reseller or find one on www.milestonesys.com.

- Live
- Alarm Manager
- BioStar2
- Access Control

Major Features

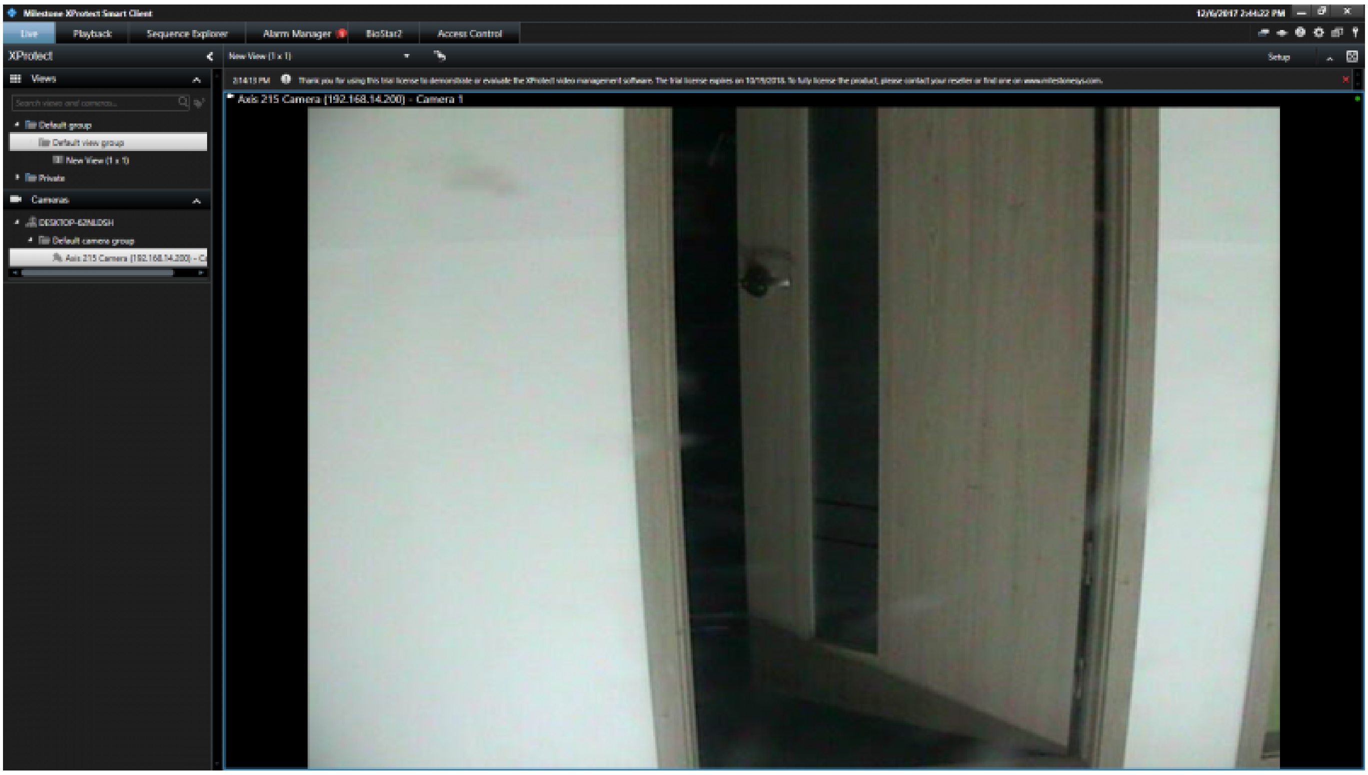
Feature 1: Live

In Milestone XProtect Smart Client, you can monitor real-time video recorded by IP camera. After you select the camera you associated in Milestone XProtect management, drag it into the right panel.



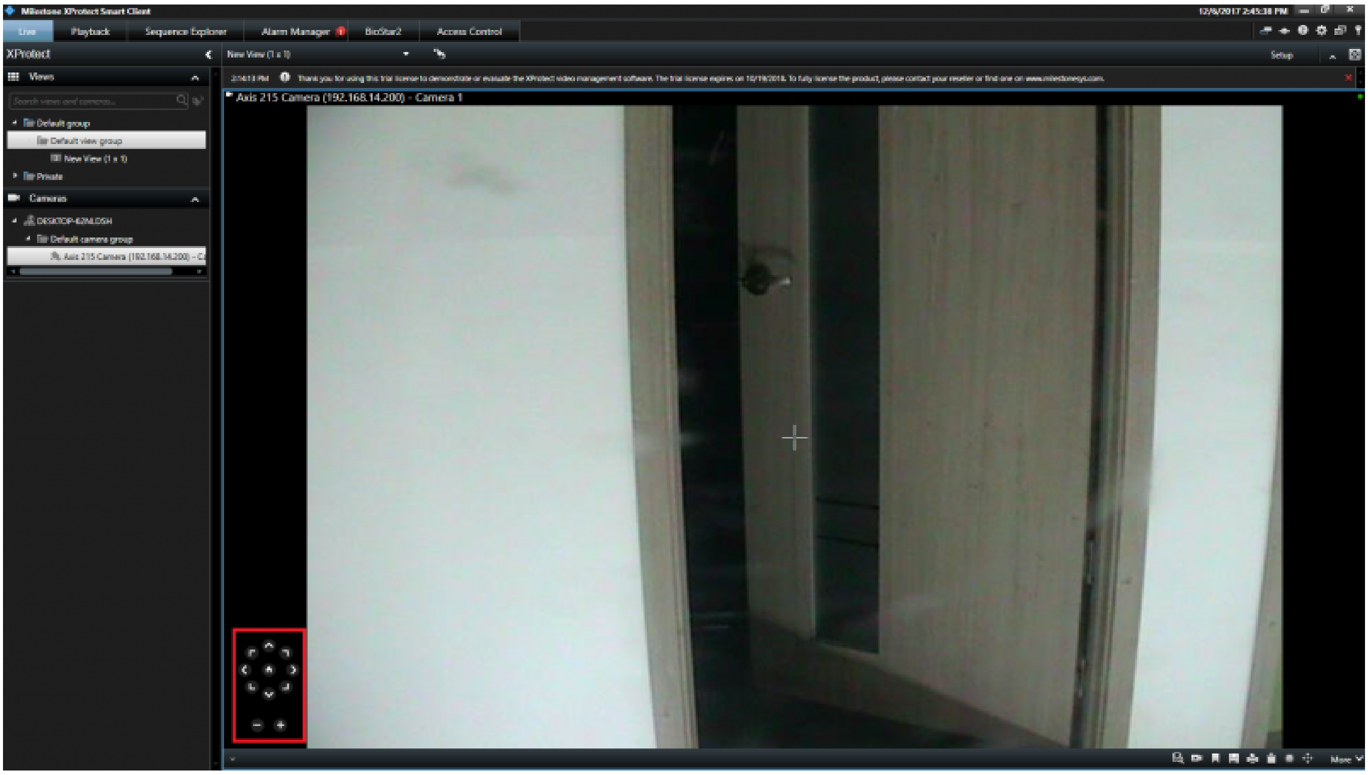
2:14:13 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 10/19/2018. To fully license the product, please contact your reseller or find one on www.milestonesys.com.

Then, you can see the real-time video recorded by IP camera.



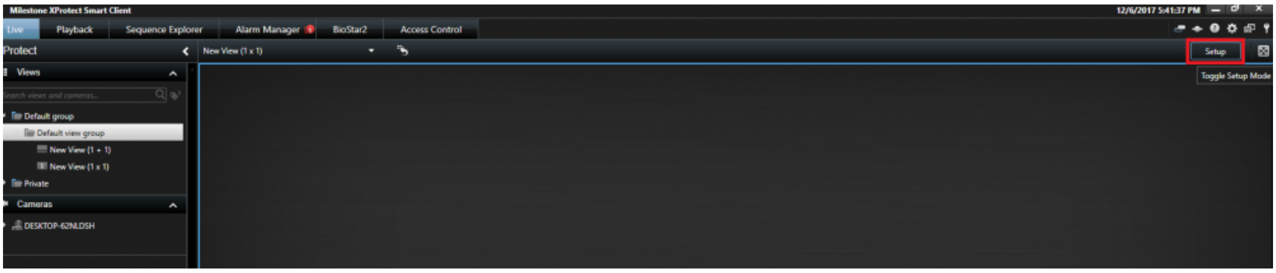
2:14:13 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 10/19/2018. To fully license the product, please contact your reseller or find one on www.milestonesys.com.

In addition, you can adjust direction or zoom in/out by clicking the icon located in left-bottom side.

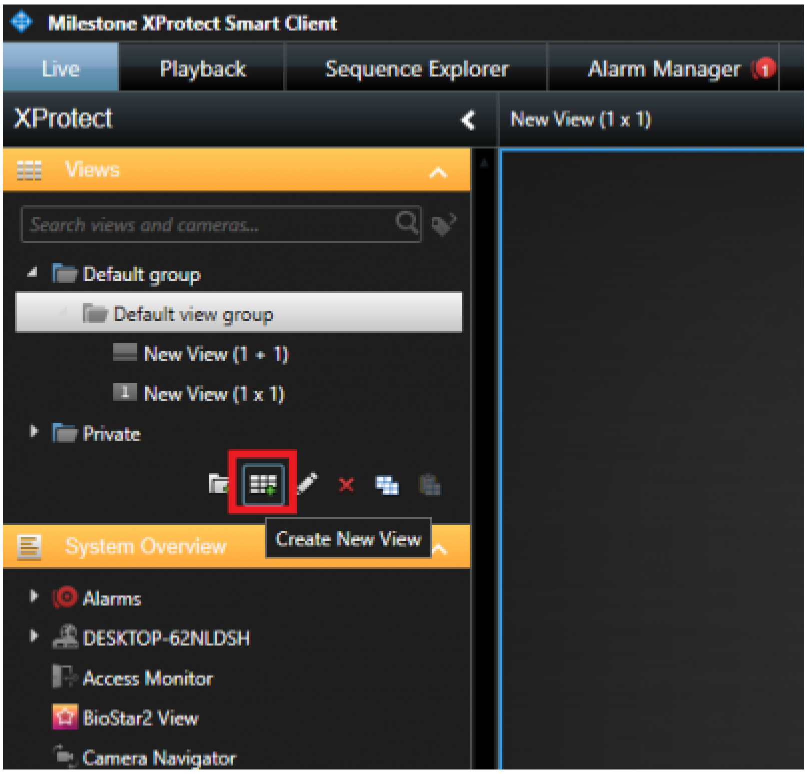


2:14:13 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 10/19/2018. To fully license the product, please contact your reseller or find one on www.milestonesys.com.

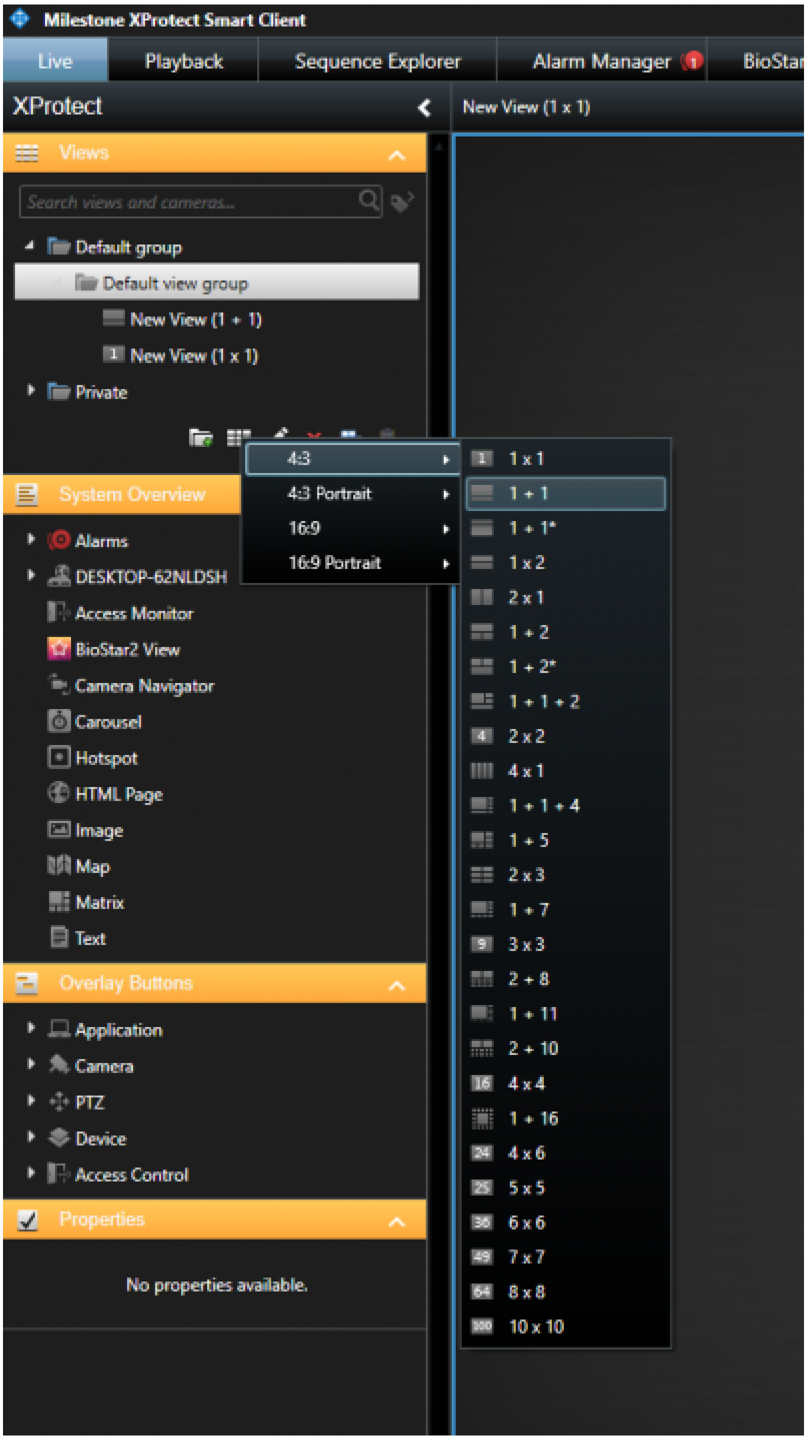
You can customize the View in Live tab.
For example, if you want to monitor video and check the information on users who authenticate their identity with PIN/Fingerprint template at the same time, click **Setup** button.



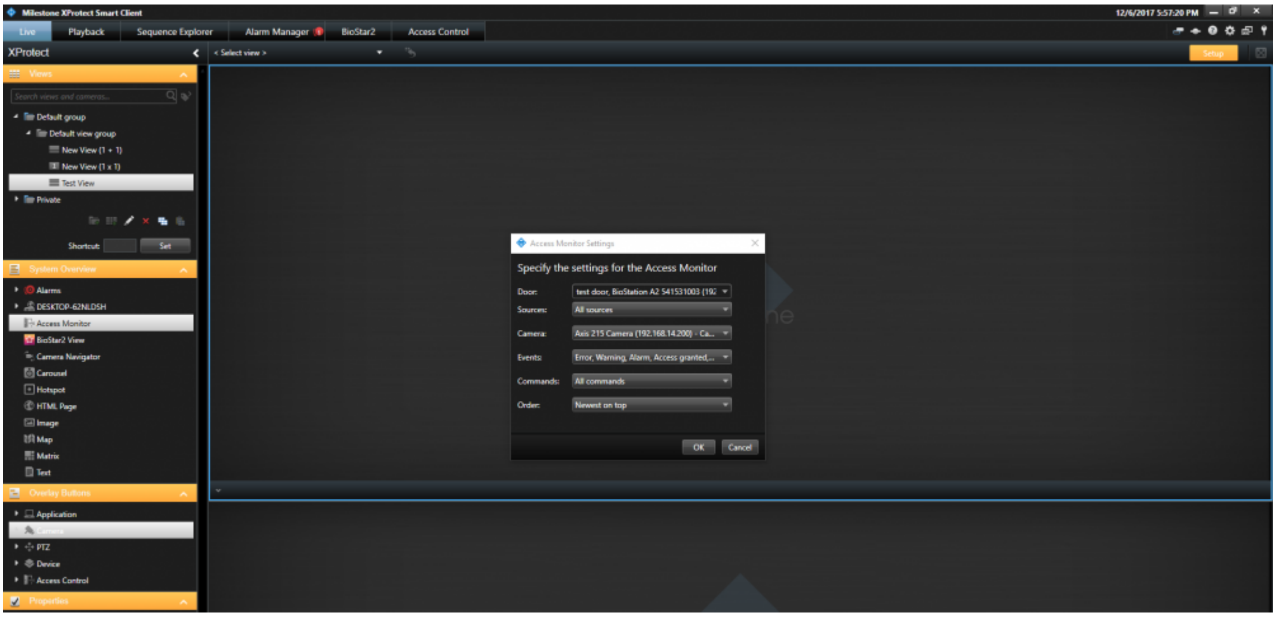
Then, you can see various options you can configure. First of all, click **Create New View** icon.



After that, you can select one option you want to customize in the view. By clicking the icon shaped pencil, you can modify the name. Then, Click **Set** button.



Next, drag **Access Monitor** in **System Overview**. In the Access Monitor Settings, you should specify the settings for the Access Monitor and click **OK** button.



Access Monitor Settings

Specify the settings for the Access Monitor

Door: test door, BioStation A2 541531003 (192

Sources: All sources

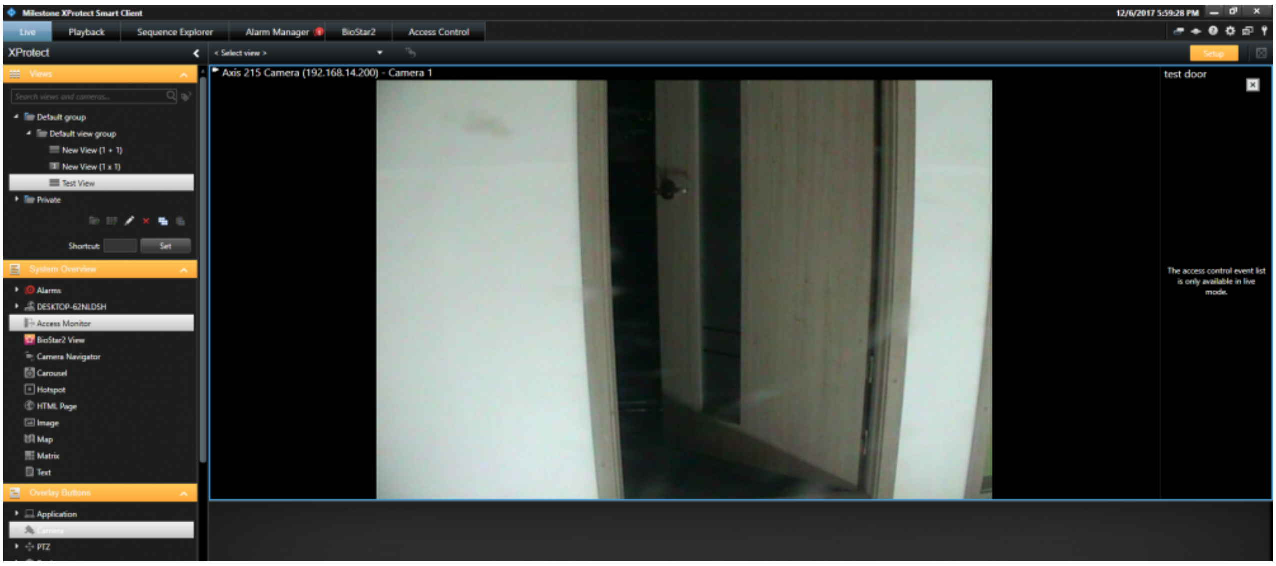
Camera: Axis 215 Camera (192.168.14.200) - Ca...

Events: Error, Warning, Alarm, Access granted,...

Commands: All commands

Order: Newest on top

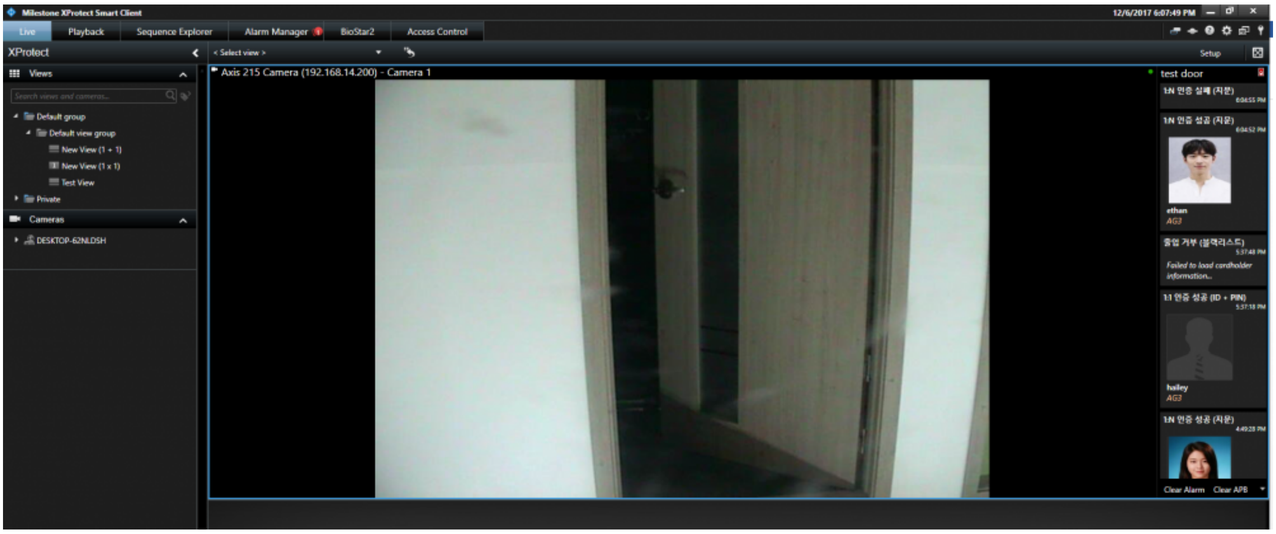
Once you click OK button, you can see the customized view. Please note that you should click Setup button again to escape the setting of View. If you see below screenshot, you can monitor video and the information on users who authenticate their identity to enter the door simultaneously.



Axis 215 Camera (192.168.14.200) - Camera 1

test door

The access control event list is only available in live mode.



1:N 인증 실패 (지문) 6:04:55 PM

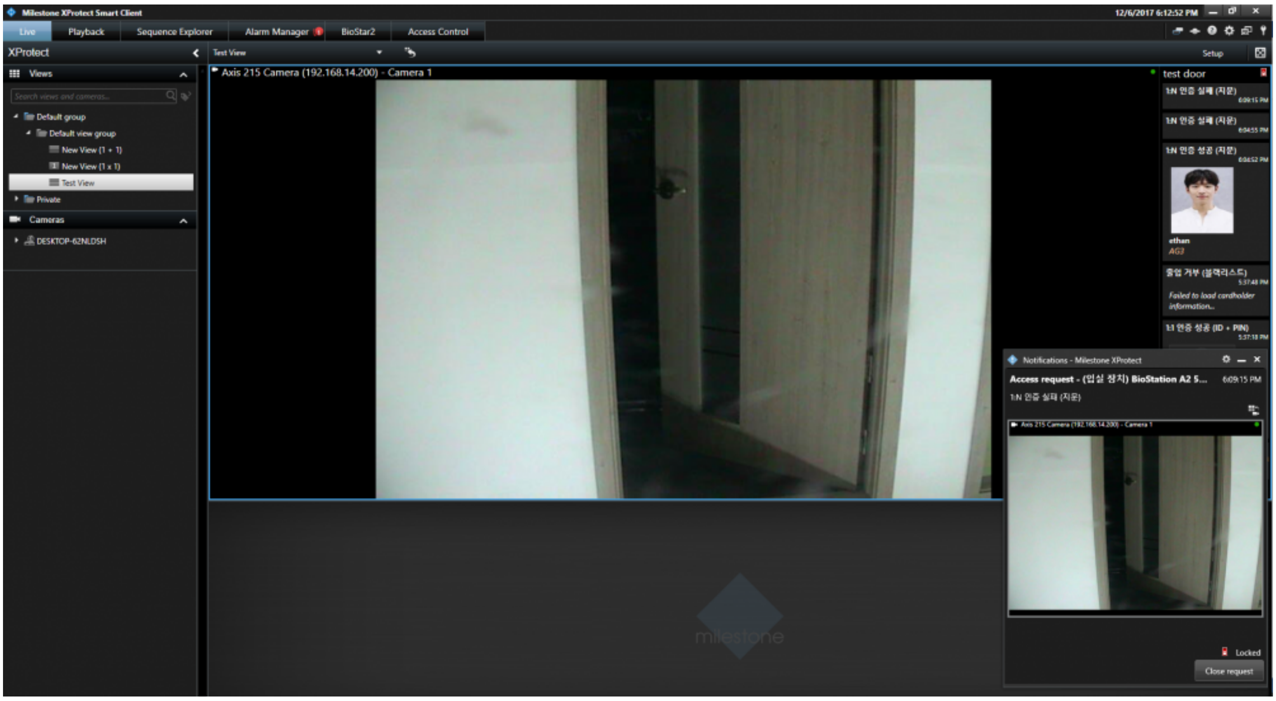
1:N 인증 성공 (지문) 6:04:52 PM
ethan
AG3

출입 거부 (블랙리스트) 5:37:48 PM
Failed to load cardholder information...

1:1 인증 성공 (ID + PIN) 5:37:18 PM
hailey
AG3

1:N 인증 성공 (지문) 4:49:28 PM

If someone fails to authenticate their identity, the notification will be displayed in the right-bottom side and display the real-time video.



1:N 인증 실패 (지문) 6:09:15 PM

1:N 인증 실패 (지문) 6:04:55 PM

1:N 인증 성공 (지문) 6:04:52 PM
ethan
AG3

출입 거부 (블랙리스트) 5:37:48 PM
Failed to load cardholder information...

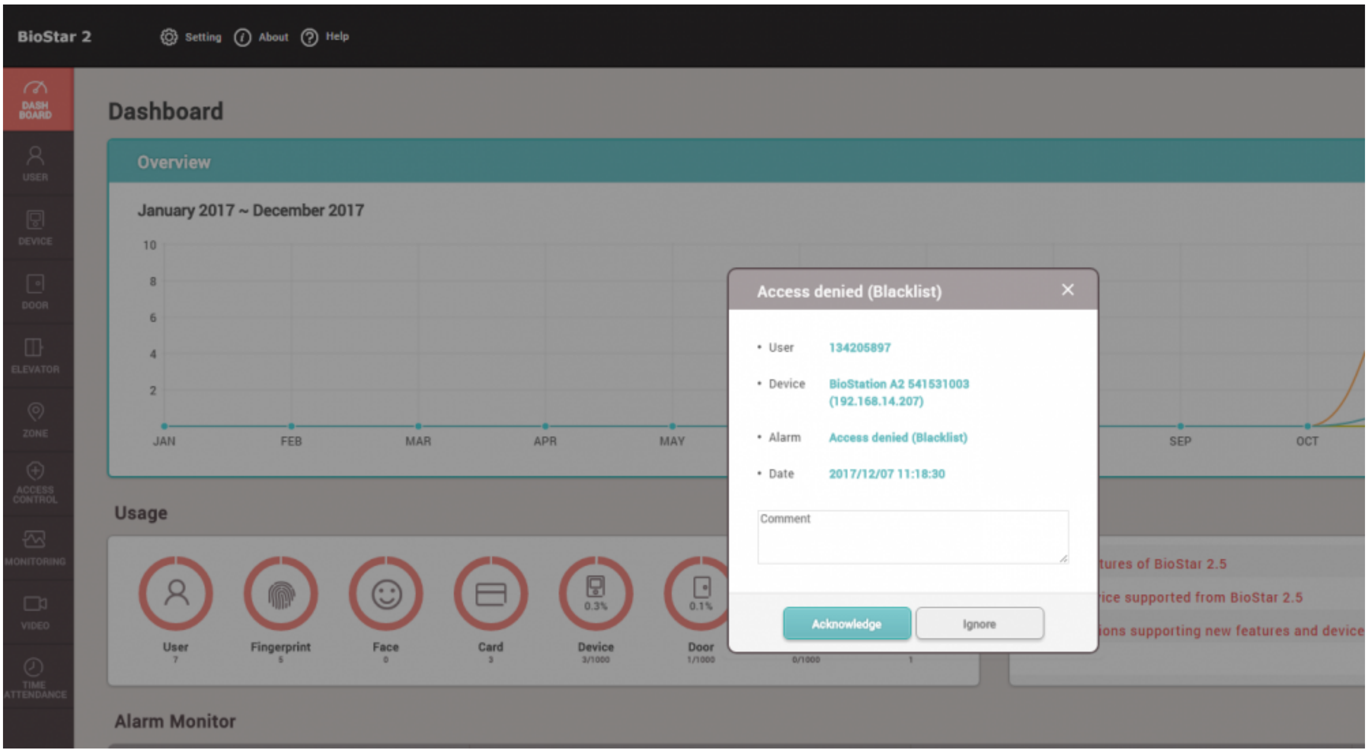
1:1 인증 성공 (ID + PIN) 5:37:18 PM

Access request - (입실 장치) BioStation A2 5... 6:09:15 PM
1:N 인증 실패 (지문)

Feature 2: Alarm Manager

If an alarm occurs in BioStar 2, the alarm message will be generated in Milestone.

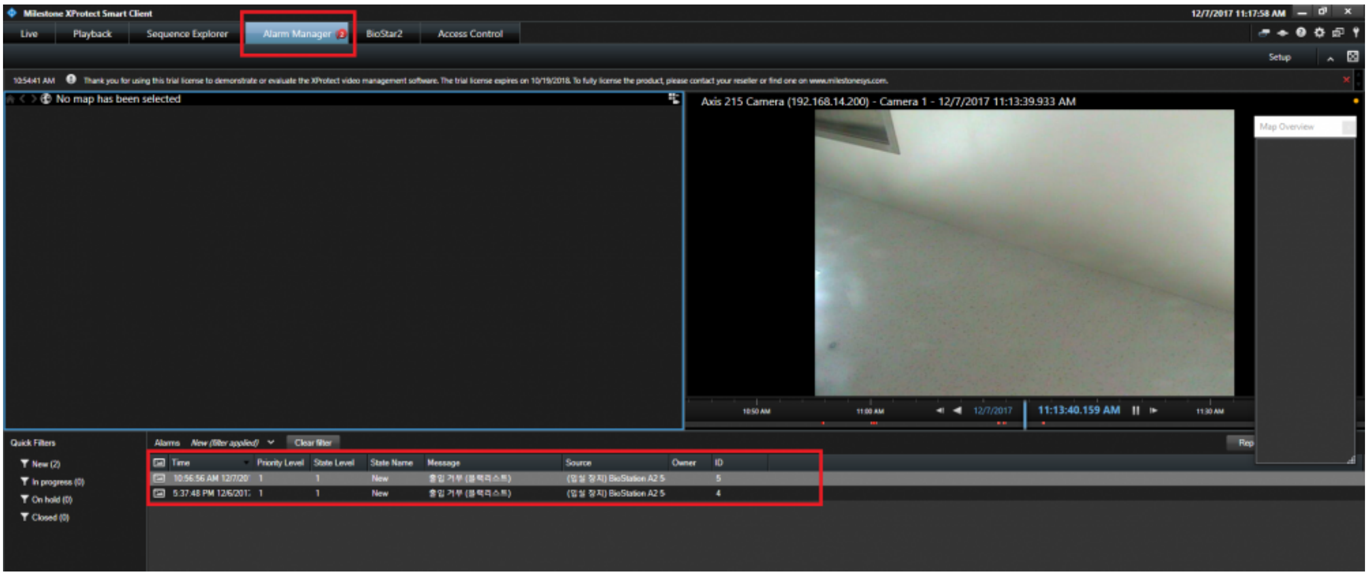
BioStar 2:



Access denied (Blacklist)

- User 134205897
- Device BioStation A2 541531003 (192.168.14.207)
- Alarm Access denied (Blacklist)
- Date 2017/12/07 11:18:30

Milestone:



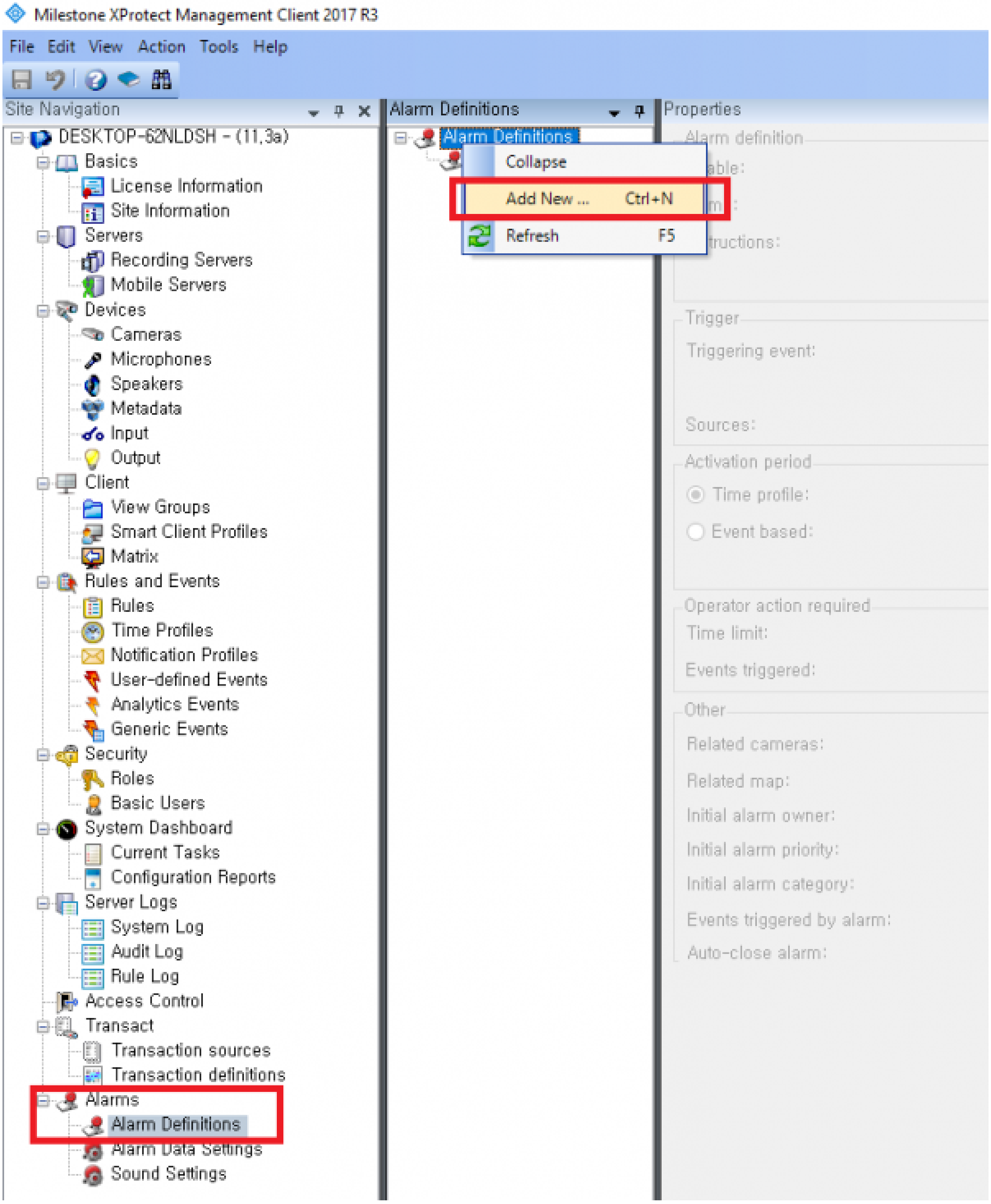
	Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
	10:56:56 AM 12/7/20	1	1	New	출입 거부 (블랙리스트)	(입실 장치) BioStation A2 5		5
	5:37:48 PM 12/6/201	1	1	New	출입 거부 (블랙리스트)	(입실 장치) BioStation A2 5		4

In Milestone, Alarm Manager will judge if generated event should be dealt with alarm based on Access Control Events tab and Alarm Definitions.

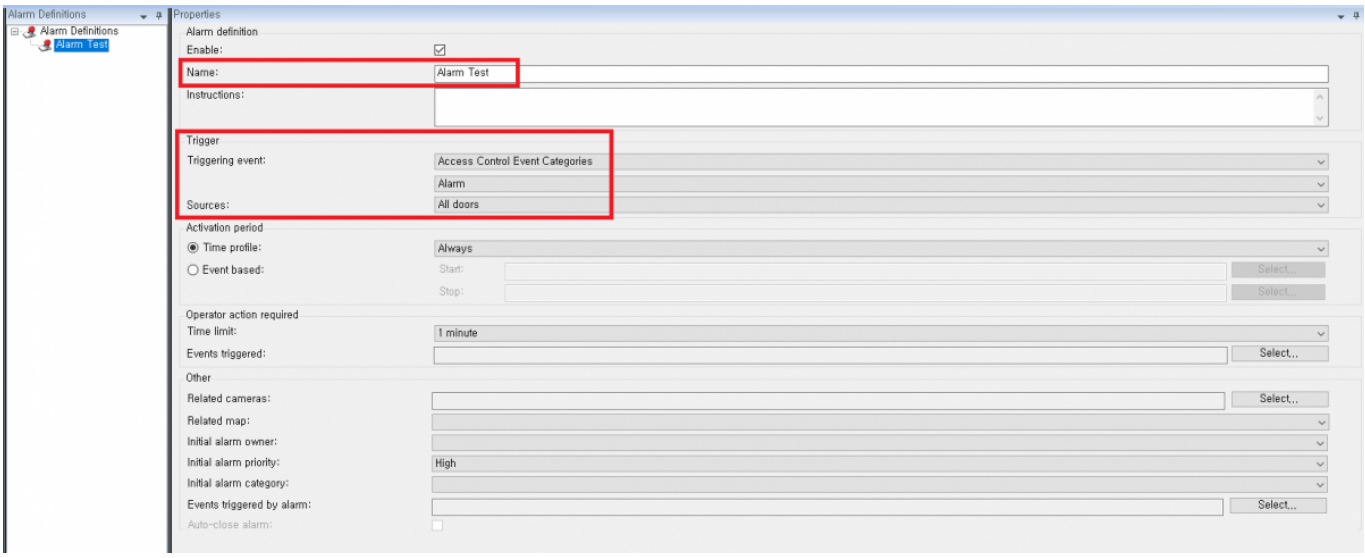
[How to configure the alarm]

This setting is required to view or acknowledge the access control event alarms of BioStar 2 in XProtect Smart Client. The alarm can be set in Setting menu of BioStar 2 and if the event alarm happens, XProtect Smart Client displays the alarm in Alarm Manager.

Go to Alarms in the Site Navigation and select **Alarm Definitions**. Then, right click **Alarm Definitions** and click **Add New**.



Enter **Name** in **Alarm definition** section.
Select **Access Control Event Categories** and one of Events you want to set in **Trigger** section. In below picture, I selected **Alarm**.
Selet one option for **Sources** in **Trigger** section. In below picture, I selected **All doors**.



Alarm Definitions
- Alarm Definitions
  - Alarm Test

Properties

Alarm definition

Enable: ☑

Name: Alarm Test

Instructions:

Trigger

Triggering event: Access Control Event Categories

Alarm

Sources: All doors

Activation period

● Time profile: Always

○ Event based: Start: Select... Stop: Select...

Operator action required

Time limit: 1 minute

Events triggered: Select...

Other

Related cameras: Select...

Related map:

Initial alarm owner:

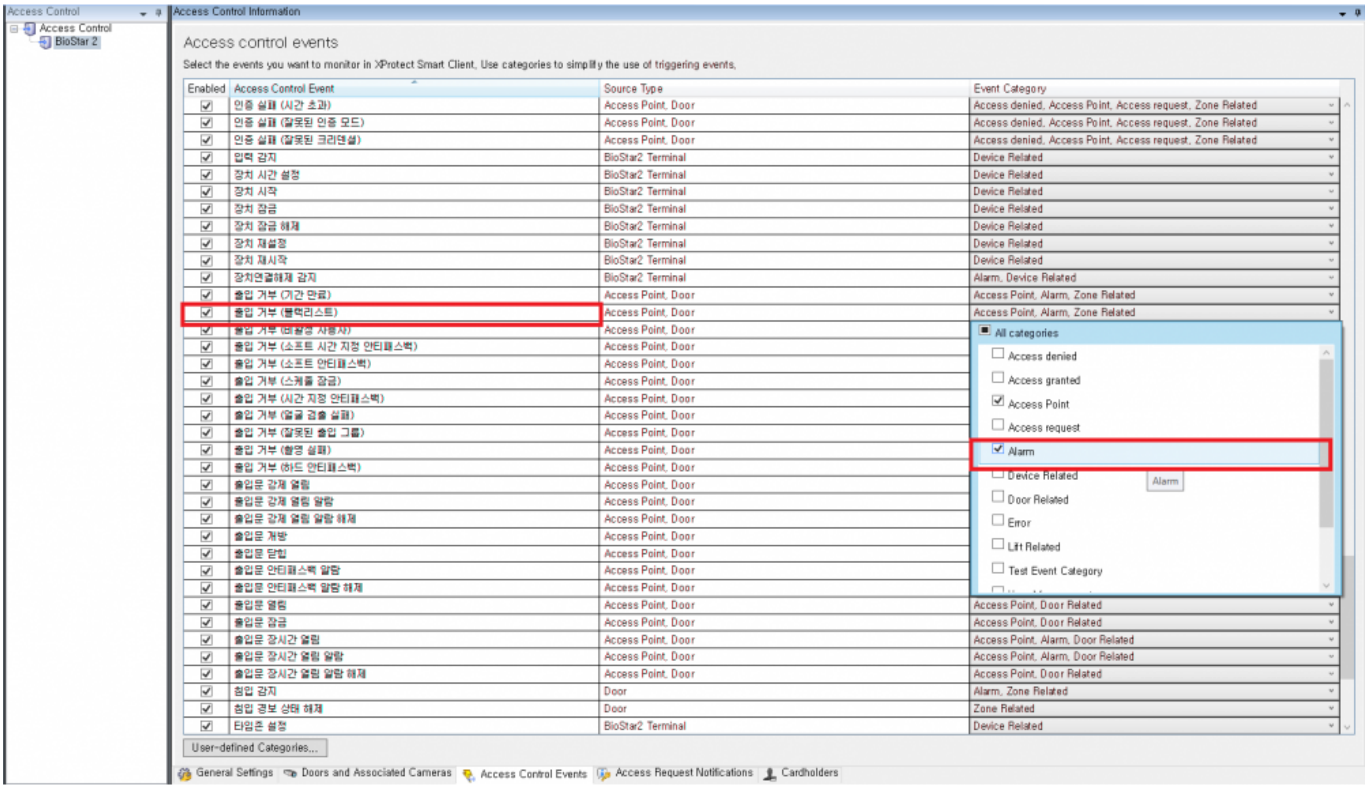
Initial alarm priority: High

Initial alarm category:

Events triggered by alarm: Select...

Auto-close alarm: □

At this point, please check Access Control Events which **Alarm** event is allocated. You can map Alarm event to certain Access Control Events. In below picture, I set Alarm event for the Access Control Event, **“Access denied (Blacklist)“**.



Access Control
- Access Control
  - BioStar 2

Access Control Information

Access control events

Select the events you want to monitor in XProtect Smart Client. Use categories to simplify the use of triggering events.

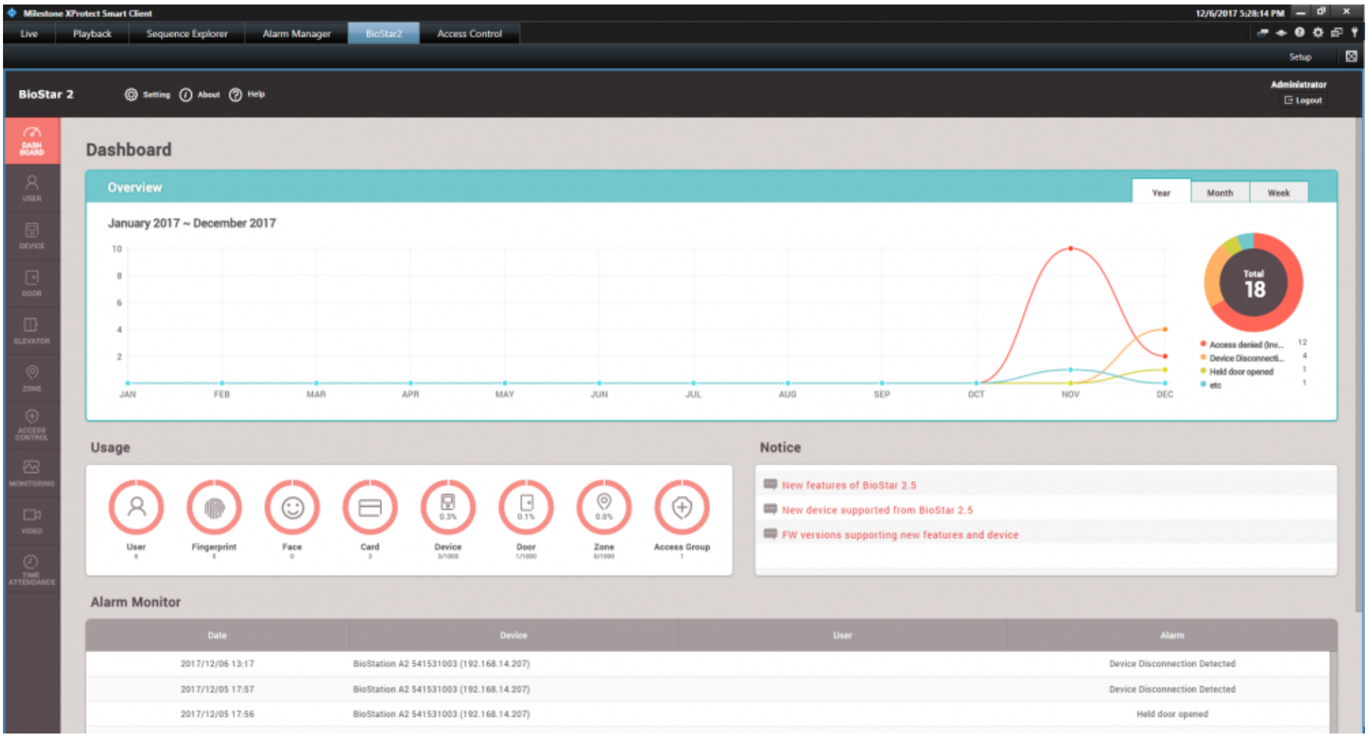
Enabled	Access Control Event	Source Type	Event Category
☑	인증 실패 (시간 초과)	Access Point, Door	Access denied, Access Point, Access request, Zone Related
☑	인증 실패 (잘못된 인증 모드)	Access Point, Door	Access denied, Access Point, Access request, Zone Related
☑	인증 실패 (잘못된 크리덴셜)	Access Point, Door	Access denied, Access Point, Access request, Zone Related
☑	입력 감지	BioStar2 Terminal	Device Related
☑	장치 시간 설정	BioStar2 Terminal	Device Related
☑	장치 시작	BioStar2 Terminal	Device Related
☑	장치 잠금	BioStar2 Terminal	Device Related
☑	장치 잠금 해제	BioStar2 Terminal	Device Related
☑	장치 재설정	BioStar2 Terminal	Device Related
☑	장치 재시작	BioStar2 Terminal	Device Related
☑	장치연결해제 감지	BioStar2 Terminal	Alarm, Device Related
☑	출입 거부 (기간 만료)	Access Point, Door	Access Point, Alarm, Zone Related
☑	출입 거부 (블랙리스트)	Access Point, Door	Access Point, Alarm, Zone Related
☑	출입 거부 (비활성 사용자)	Access Point, Door	
☑	출입 거부 (소프트 시간 지정 안티패스백)	Access Point, Door	
☑	출입 거부 (소프트 안티패스백)	Access Point, Door	
☑	출입 거부 (스케줄 잠금)	Access Point, Door	
☑	출입 거부 (시간 지정 안티패스백)	Access Point, Door	
☑	출입 거부 (얼굴 검출 실패)	Access Point, Door	
☑	출입 거부 (잘못된 출입 그룹)	Access Point, Door	
☑	출입 거부 (촬영 실패)	Access Point, Door	
☑	출입 거부 (하드 안티패스백)	Access Point, Door	
☑	출입문 강제 열림	Access Point, Door	
☑	출입문 강제 열림 알람	Access Point, Door	
☑	출입문 강제 열림 알람 해제	Access Point, Door	
☑	출입문 개방	Access Point, Door	
☑	출입문 닫힘	Access Point, Door	
☑	출입문 안티패스백 알람	Access Point, Door	
☑	출입문 안티패스백 알람 해제	Access Point, Door	
☑	출입문 열림	Access Point, Door	Access Point, Door Related
☑	출입문 잠금	Access Point, Door	Access Point, Door Related
☑	출입문 장시간 열림	Access Point, Door	Access Point, Alarm, Door Related
☑	출입문 장시간 열림 알람	Access Point, Door	Access Point, Alarm, Door Related
☑	출입문 장시간 열림 알람 해제	Access Point, Door	Access Point, Door Related
☑	침입 감지	Door	Alarm, Zone Related
☑	침입 경보 상태 해제	Door	Zone Related
☑	타임존 설정	BioStar2 Terminal	Device Related

■ All categories
- □ Access denied
- □ Access granted
- ☑ Access Point
- □ Access request
- ☑ Alarm
- □ Device Related
- □ Door Related
- □ Error
- □ Lift Related
- □ Test Event Category

Alarm
User-defined Categories...
General Settings
Doors and Associated Cameras
Access Control Events
Access Request Notifications
Cardholders

Feature 3: BioStar2

In Milestone XProtect Smart Client, you can access to BioStar 2 and add/modify the data (e.g. User, Device, Door) in BioStar 2.



New features of BioStar 2.5

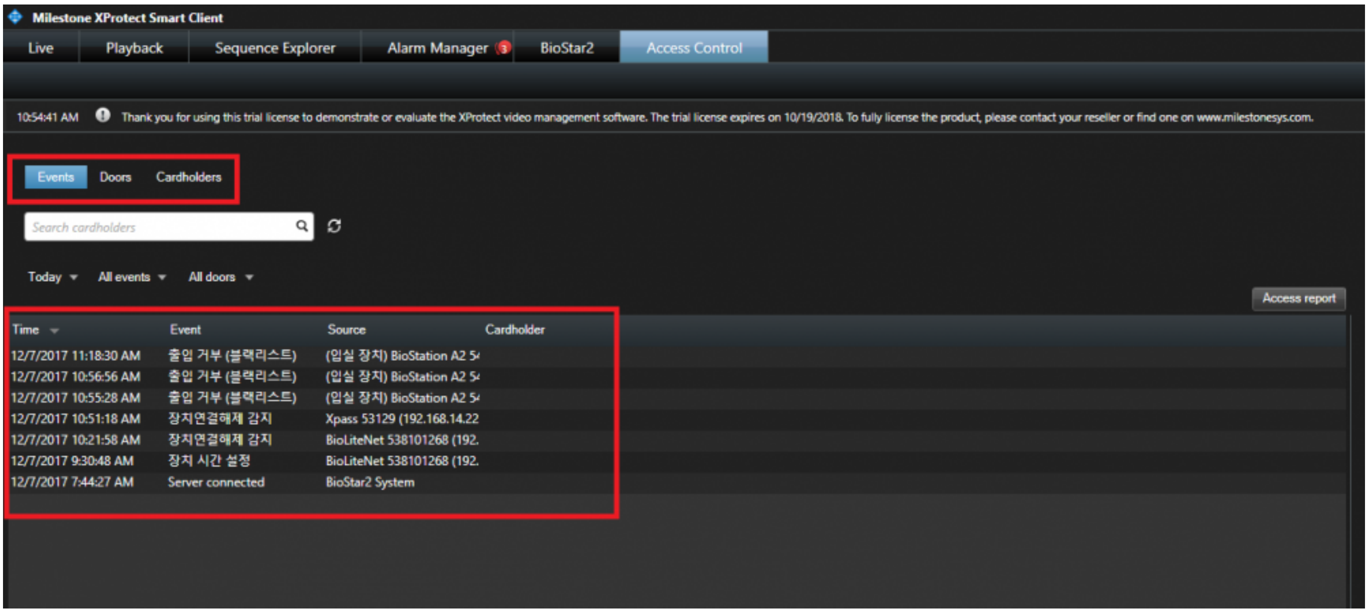
New device supported from BioStar 2.5

FW versions supporting new features and device

Date	Device	User	Alarm
2017/12/06 13:17	BioStation A2 541531003 (192.168.14.207)		Device Disconnection Detected
2017/12/05 17:57	BioStation A2 541531003 (192.168.14.207)		Device Disconnection Detected
2017/12/05 17:56	BioStation A2 541531003 (192.168.14.207)		Held door opened

Feature 4: Access Control

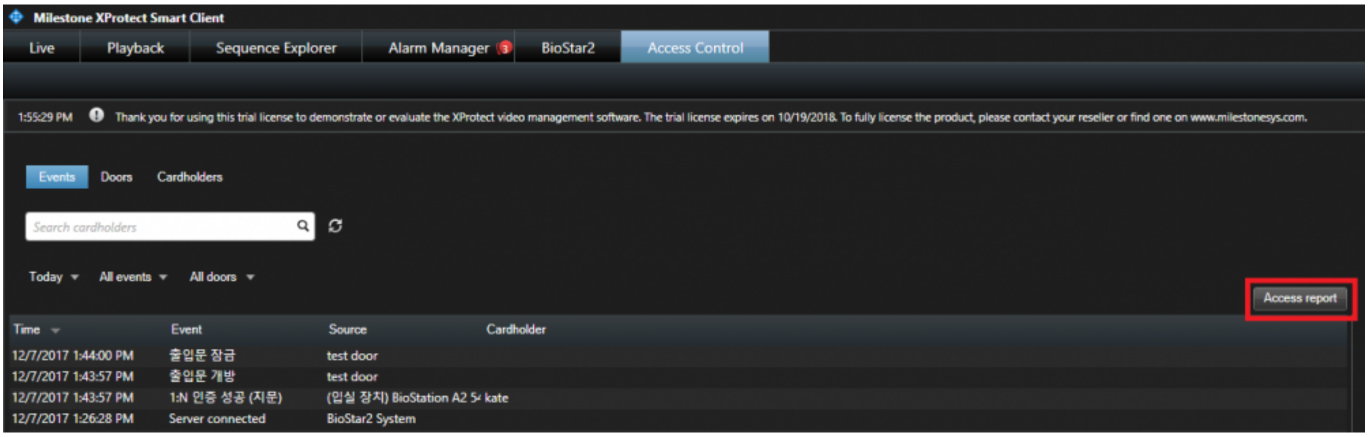
You can check Events, Doors and Cardholders for BioStar 2 in Milestone.



10:54:41 AM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 10/19/2018. To fully license the product, please contact your reseller or find one on www.milestonesys.com.

Time	Event	Source	Cardholder
12/7/2017 11:18:30 AM	출입 거부 (블랙리스트)	(입실 장치) BioStation A2 5	
12/7/2017 10:56:56 AM	출입 거부 (블랙리스트)	(입실 장치) BioStation A2 5	
12/7/2017 10:55:28 AM	출입 거부 (블랙리스트)	(입실 장치) BioStation A2 5	
12/7/2017 10:51:18 AM	장치연결해제 감지	Xpass 53129 (192.168.14.22	
12/7/2017 10:21:58 AM	장치연결해제 감지	BioLiteNet 538101268 (192.	
12/7/2017 9:30:48 AM	장치 시간 설정	BioLiteNet 538101268 (192.	
12/7/2017 7:44:27 AM	Server connected	BioStar2 System	

You can also create the PDF report for Event records by clicking **Access report** button.



1:55:29 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 10/19/2018. To fully license the product, please contact your reseller or find one on www.milestonesys.com.

Time	Event	Source	Cardholder
12/7/2017 1:44:00 PM	출입문 잠금	test door	
12/7/2017 1:43:57 PM	출입문 개방	test door	
12/7/2017 1:43:57 PM	1:N 인증 성공 (지문)	(입실 장치) BioStation A2 5	kate
12/7/2017 1:26:28 PM	Server connected	BioStar2 System	