

Table of Contents

How to utilize BioStar 2 integrating with Milestone	1
The summary of Procedure	1
Step 1: Install BioStar 2	2
Step 2: Install one of Milestone XProtect VMS (with professional license or higher)	3
Step 3: Install BioStar 2 Integration for Milestone XProject	4
Step 4: Add IP Camera in Milestone XProtect VMS	4
Step 5: Create new Access Control to connect Milestone to BioStar 2	8
Major Features	15
Feature 1: Access Control Events	15
Feature 2: Cardholders	17
Step 6: Utilize XProtect Smart Client	19
Major Features	20
Feature 1: Live	20
Feature 2: Alarm Manager	26
Feature 3: BioStar2	29
Feature 4: Access Control	30

[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 higher version.
- XProtect VMS and BioStar 2 must be installed first.
- All access control configuration settings of BioStar 2 must be completed.
- System requirements
 - 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

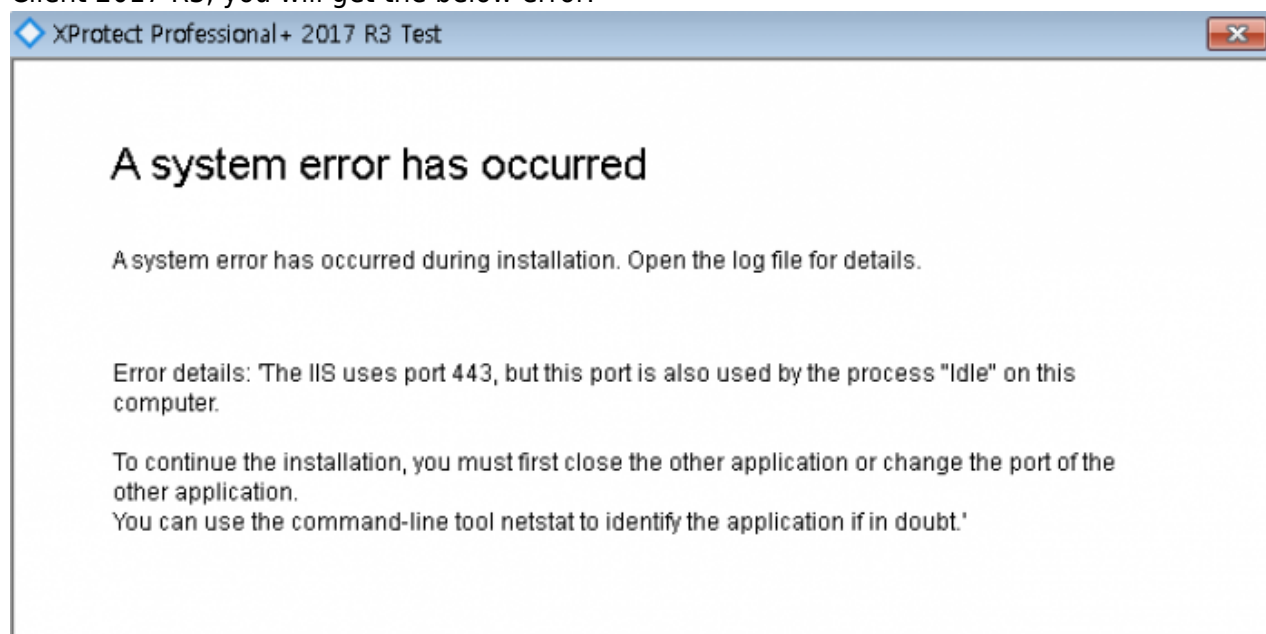
Step 1: Install BioStar 2

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

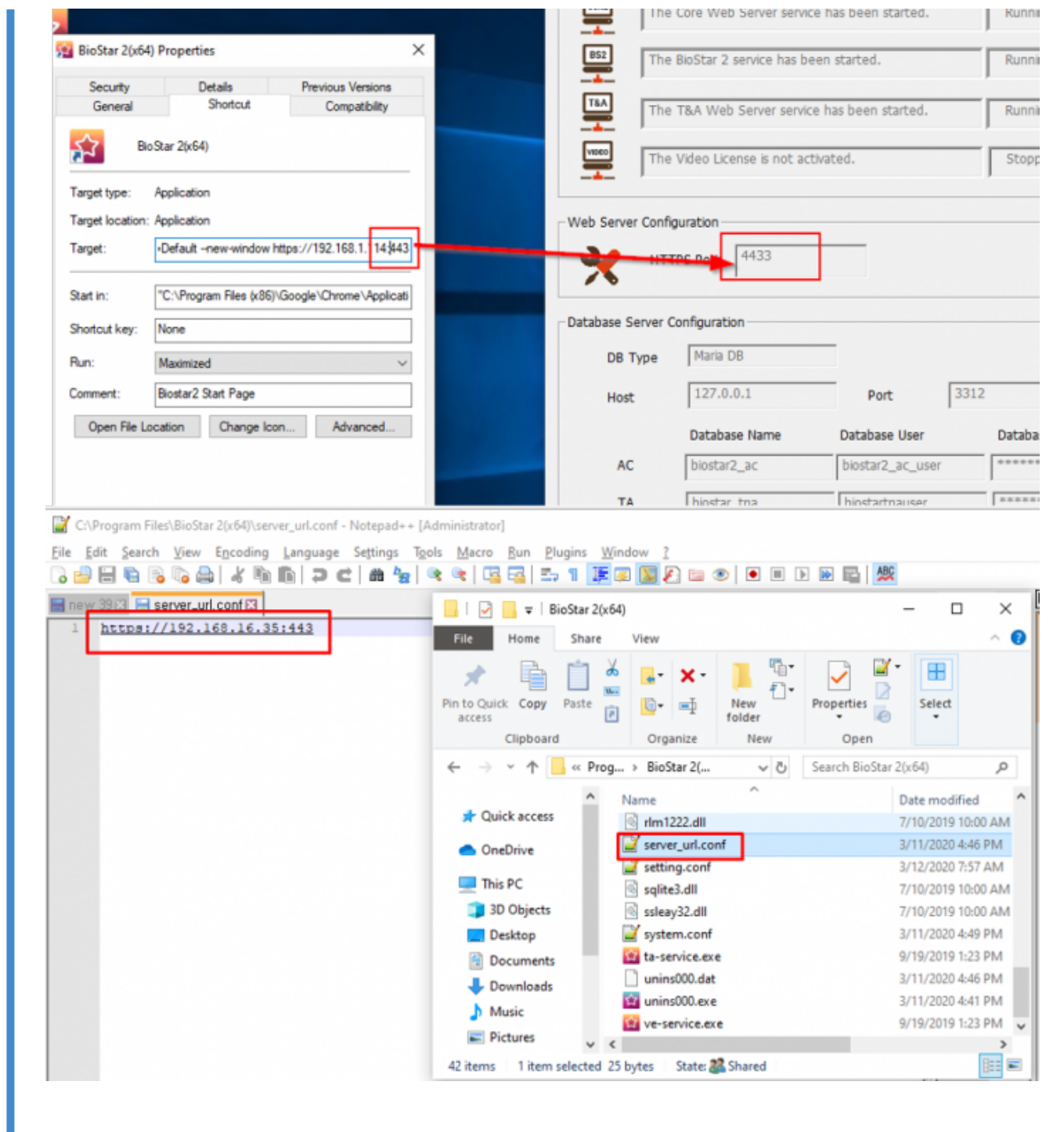
[BioStar 2 Installation](#)

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.



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.



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

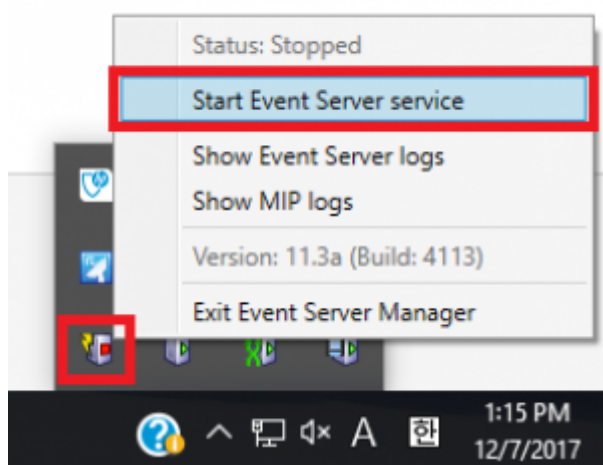
You should install two installation files below.

-  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.

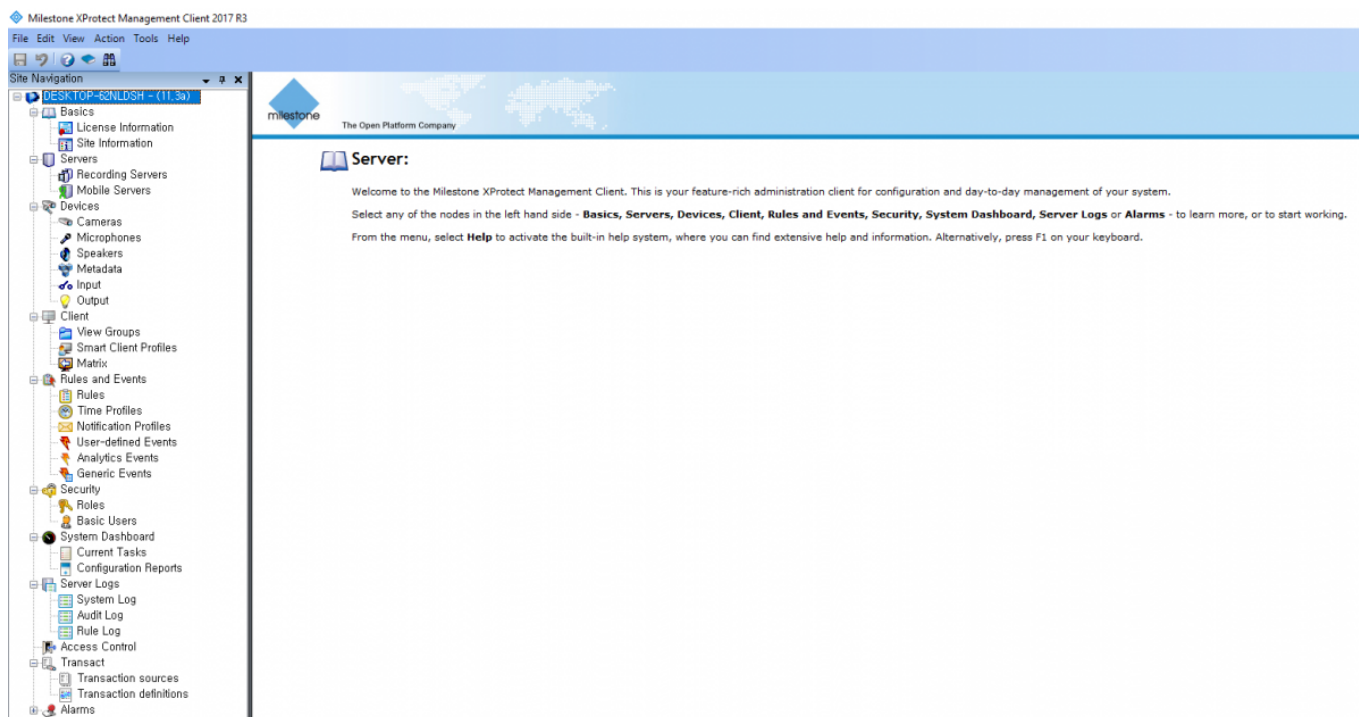
You can refer to BioStar2 Integration for Milestone XProtect Setup Guide to install them.

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.



Step 4: Add IP Camera in Milestone XProtect VMS

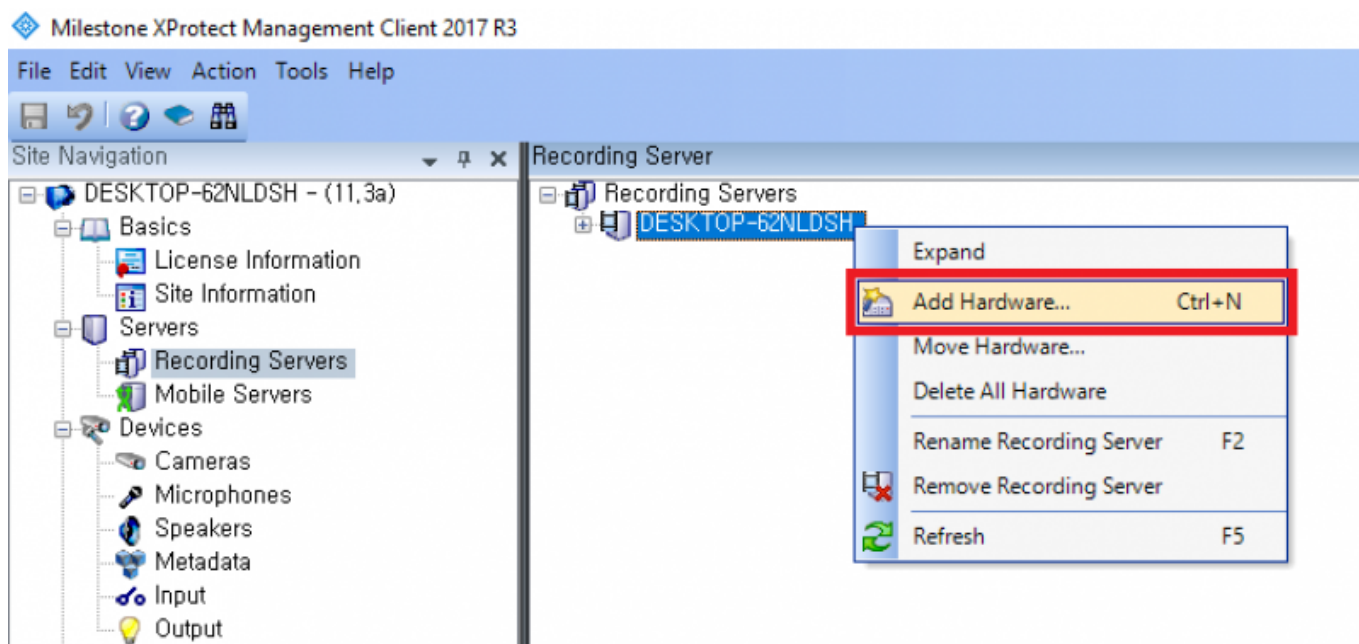
When you run XProtect Management Client 2017 R3 and connect to your PC, you can see the below screen.



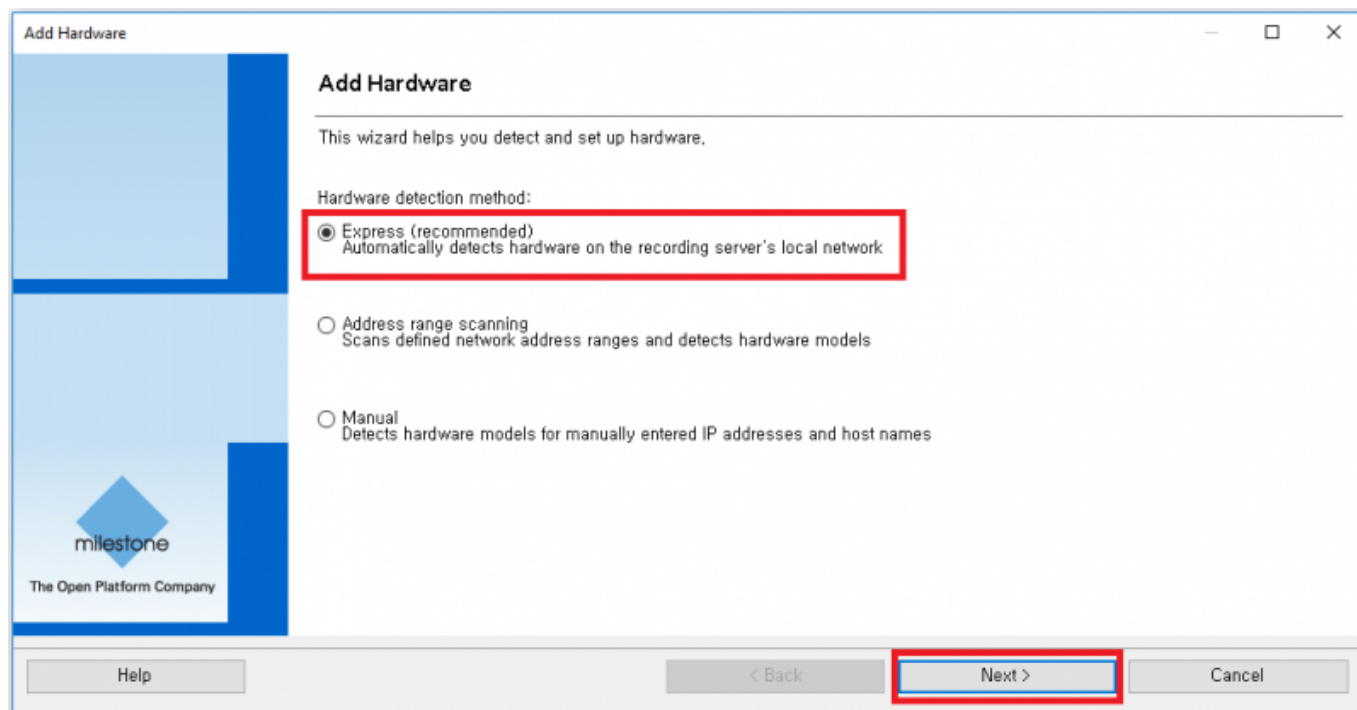
Prepare IP camera.

Go to **Servers > Recording Servers**.

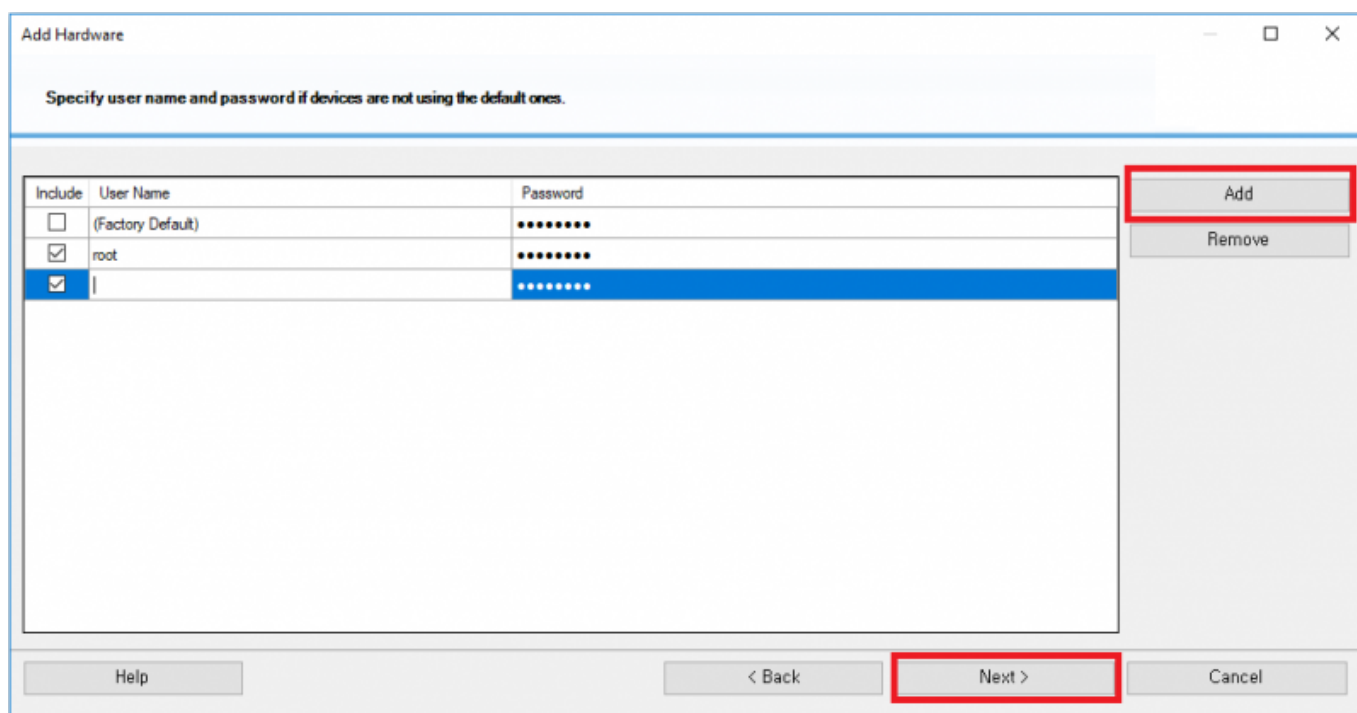
Right click one of **Recording Servers** and select **Add Hardware**.



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



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



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 will be added.

Stop

Collected hardware information:

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

Help < Back **Next >** Cancel

Click **Next** button.

Add Hardware

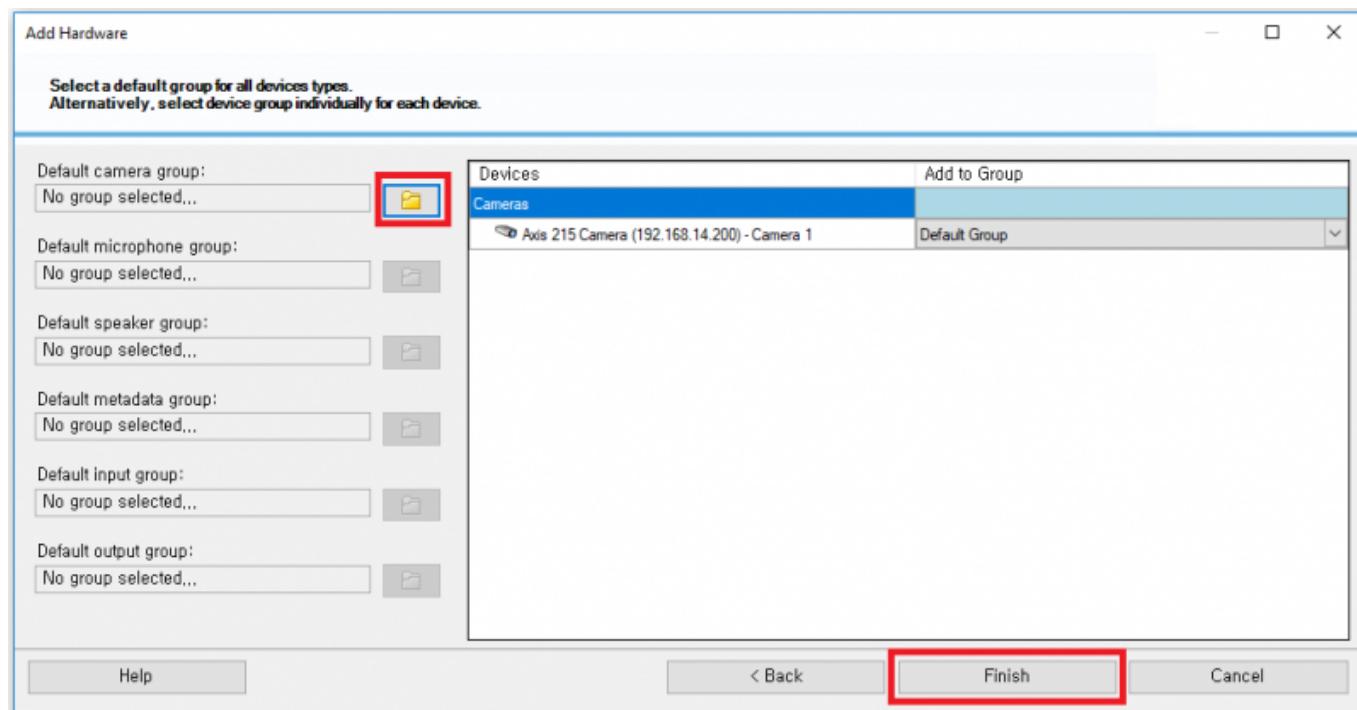
Hardware and cameras are enabled per default. Manually enable additional devices to be used.
The hardware and its devices will be assigned auto-generated names. Alternatively, enter names manually.

Hardware name template: Default Device name template: Default

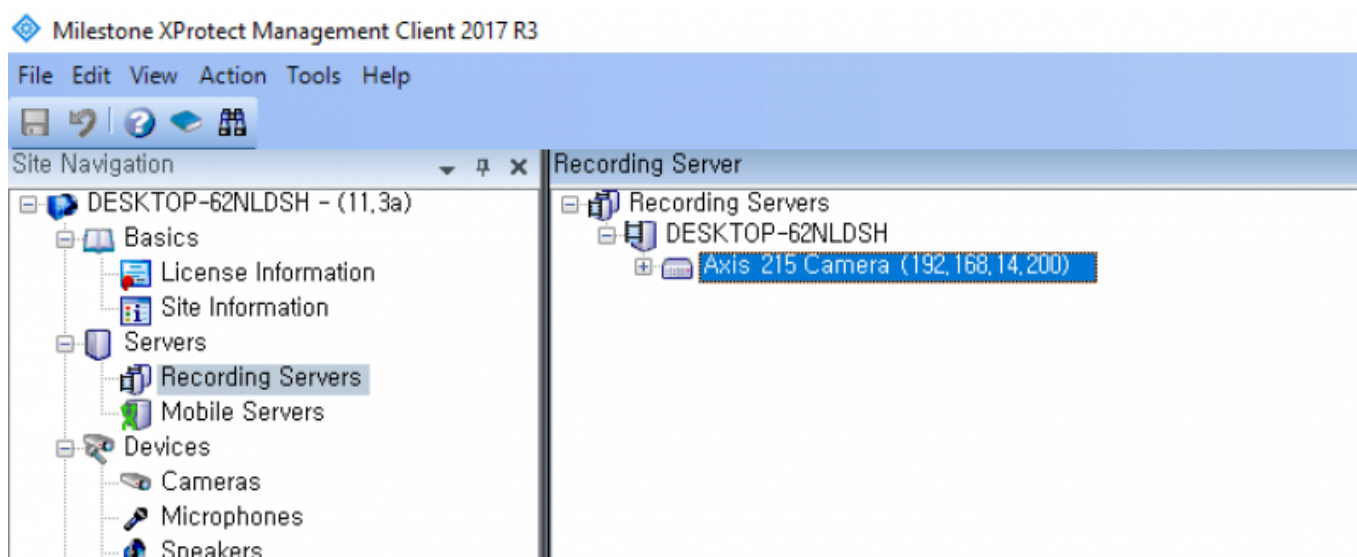
Hardware to Add	Enabled	Name
Axis 215 Camera - 192.168.14.200		
Hardware:	<input checked="" type="checkbox"/>	Axis 215 Camera (192.168.14.200)
Camera port 1:	<input checked="" type="checkbox"/>	Axis 215 Camera (192.168.14.200) - Camera 1
Microphone port 1:	<input type="checkbox"/>	Axis 215 Camera (192.168.14.200) - Microphone 1
Speaker port 1:	<input type="checkbox"/>	Axis 215 Camera (192.168.14.200) - Speaker 1
Input port 1:	<input type="checkbox"/>	Axis 215 Camera (192.168.14.200) - Input 1
Output port 1:	<input type="checkbox"/>	Axis 215 Camera (192.168.14.200) - Output 1

Help < Back **Next >** Cancel

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

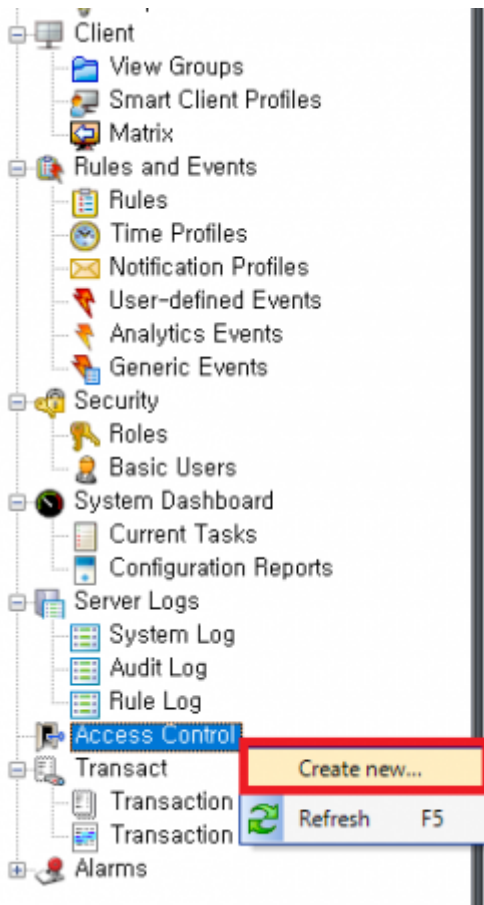


If you succeed in add IP camera, you can see your camera in the Recording Servers's tree.



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:

Integration plug-in:

Address:

User:

Password:

Use HTTP encryption: ☐

Next Cancel

The image shows the 'BioStar Setting' window. It has three main sections: 'Service Status', 'Web Server Configuration', and 'Database Server Configuration'.

Service Status: This section contains four rows of service status information. Each row has an icon, a status message, a 'Running' button, and a 'Stop' button.

Service	Status Message	Running	Stop
CORE	The Core Web Server service has been started.	Running	Stop
BS2	The BioStar 2 service has been started.	Running	Stop
T&A	The T&A Web Server service has been started.	Running	Stop
VIDEO	The Video Server service has been started.	Running	Stop

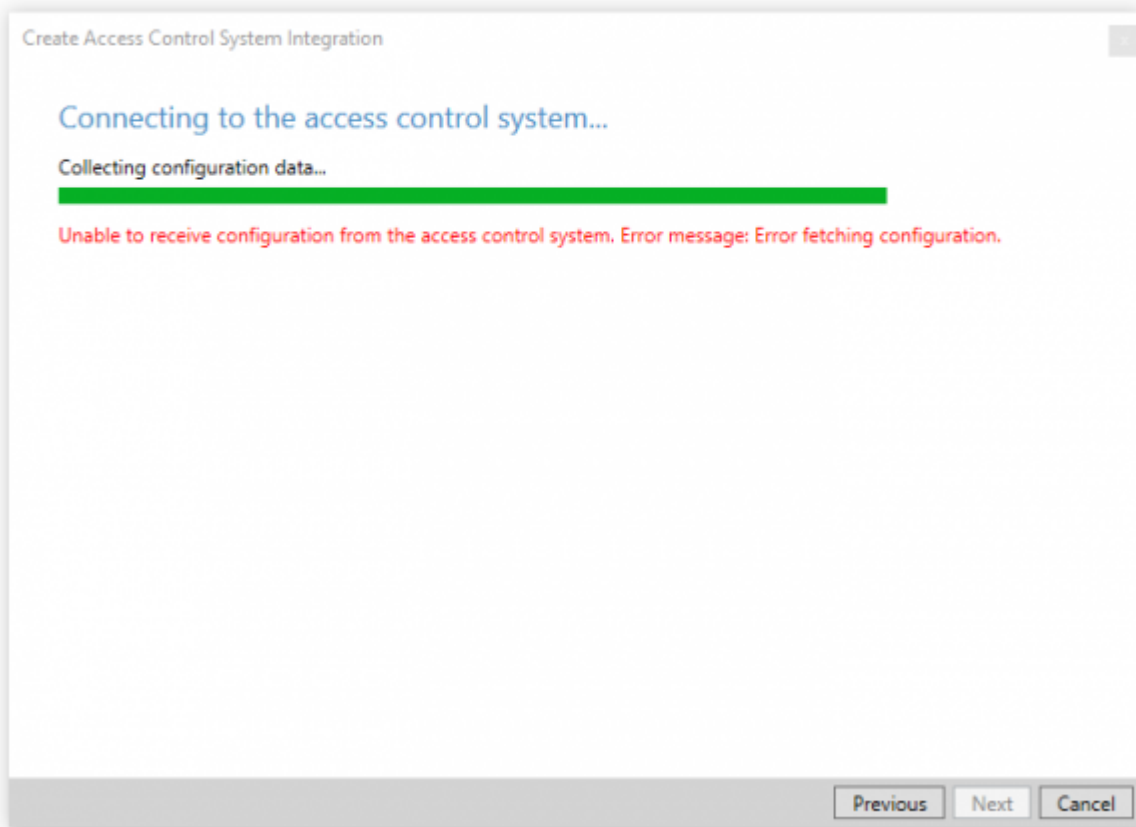
Web Server Configuration: This section contains a 'Wrench and Screwdriver' icon, the label 'HTTPS Port', and a text input field containing the value '456'.

Database Server Configuration: This section contains several input fields for database configuration.

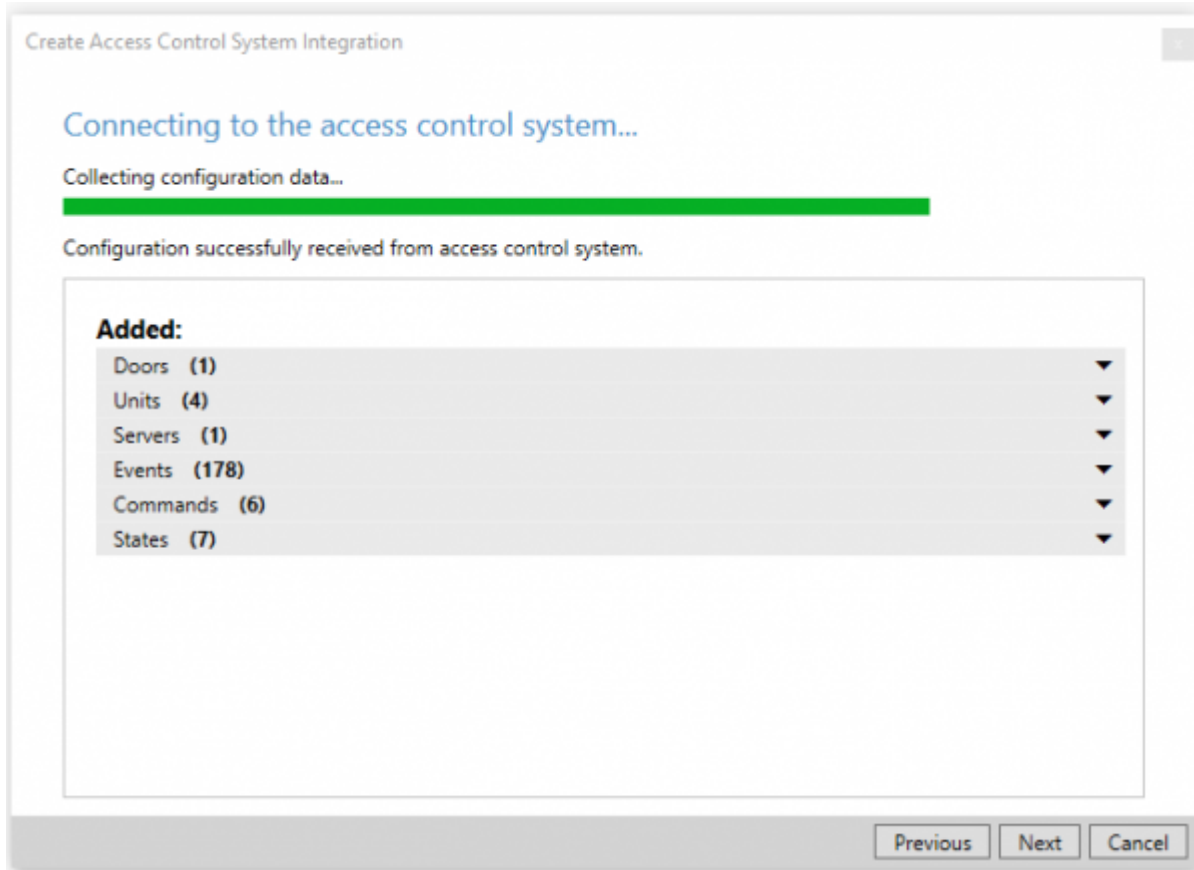
DB Type	Host	Port	Database Name	Database User	Database Password
Maria DB	127.0.0.1	3312	biostar2_ac	biostar2_ac_user	*****
AC			biostar_tna	biostartnauser	*****
TA			biostar_ve	biostarveuser	*****
Video					

At the bottom of the 'Database Server Configuration' section, there are two buttons: 'Test Connection' and 'Save'.

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.

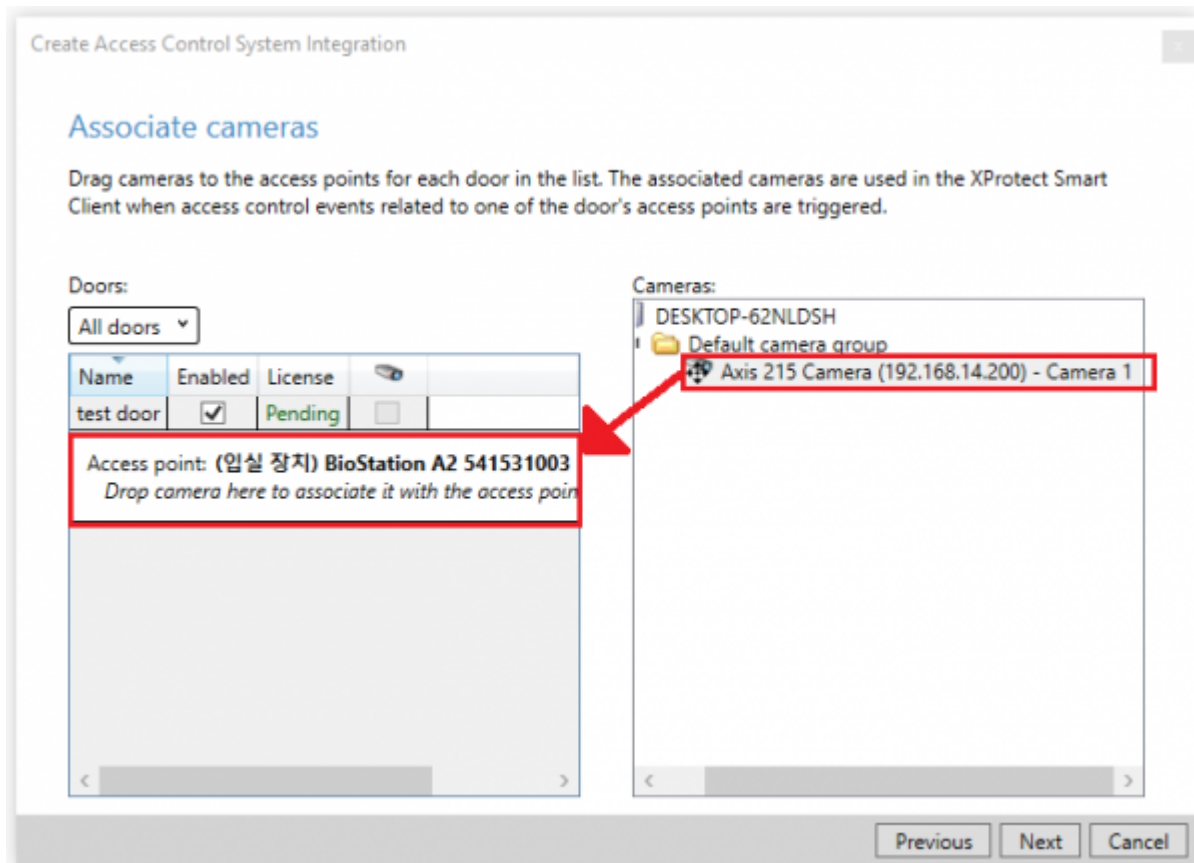


If you succeed in connection to the access control system (BioStar 2 AC), you can see below picture.

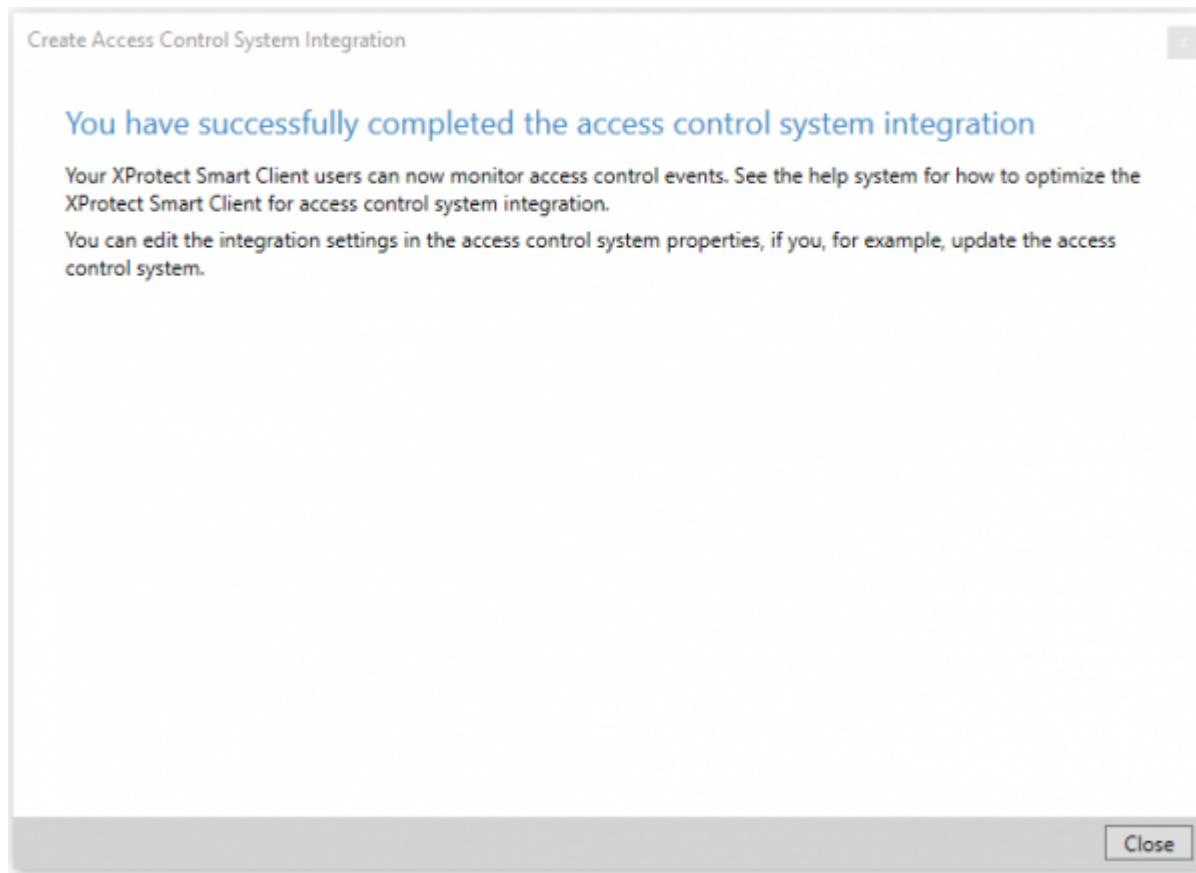


If BioStar 2 connected to Milestone successfully, the below screen will appear.

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.



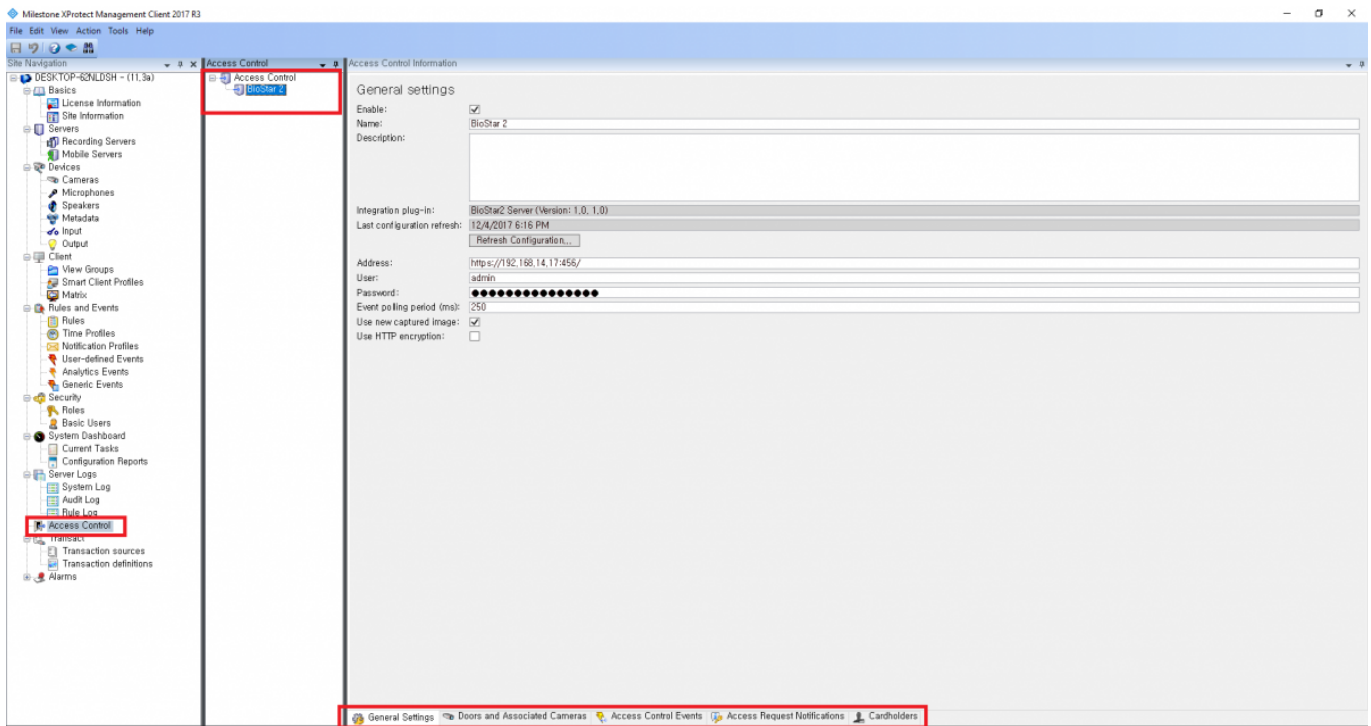
If you succeeded in integrate Milestone with BioStar2 with IP camera, you can see below picture.



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:** 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
<input checked="" type="checkbox"/>	1:1 인증 성공 (ID + PIN)	Access Point	Access granted, Access Point
<input checked="" type="checkbox"/>	1:1 인증 성공 (ID + 얼굴 + PIN)	Access Point	Access granted, Access Point
<input checked="" type="checkbox"/>	1:1 인증 성공 (ID + 얼굴)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (ID + 지문 + PIN)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (ID + 지문)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (엑세스카드 + PIN)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (엑세스카드 + 지문 + PIN)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (엑세스카드 + 지문)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (엑세스카드)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (카드 + PIN)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (카드 + 얼굴 + PIN)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (카드 + 얼굴)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (카드 + 지문 + PIN)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (카드 + 지문)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 성공 (카드)	Access Point	
<input checked="" type="checkbox"/>	1:1 인증 실패 (ID)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (PIN)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (엑세스카드 + PIN)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (엑세스카드 + 지문)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (얼굴)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (지문)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (카드)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드 + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드 + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드)	Access Point	Access granted, Access Point, Alarm, Warning

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

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
<input checked="" type="checkbox"/>	1:1 인증 실패 (ID)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (PIN)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (엑세스카드 + PIN)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (엑세스카드 + 지문)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (얼굴)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (지문)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 인증 실패 (카드)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (ID + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드 + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드 + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (엑세스카드)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드 + 지문)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:1 협박 지문 인증 (카드)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:N 인증 성공 (얼굴 + PIN)	Access Point	Access granted, Access Point
<input checked="" type="checkbox"/>	1:N 인증 성공 (얼굴)	Access Point	Access granted, Access Point
<input checked="" type="checkbox"/>	1:N 인증 성공 (지문 + PIN)	Access Point	Access granted, Access Point
<input checked="" type="checkbox"/>	1:N 인증 성공 (지문)	Access Point	Access granted, Access Point
<input checked="" type="checkbox"/>	1:N 인증 실패 (PIN)	Access Point	Access granted, Access Point
<input checked="" type="checkbox"/>	1:N 인증 실패 (엑세스카드 + PIN)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:N 인증 실패 (엑세스카드 + 지문)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:N 인증 실패 (얼굴)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:N 인증 실패 (지문)	Access Point	Access denied, Access Point, Access request
<input checked="" type="checkbox"/>	1:N 협박 지문 인증 성공 (얼굴 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:N 협박 지문 인증 성공 (얼굴)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:N 협박 지문 인증 성공 (지문 + PIN)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	1:N 협박 지문 인증 성공 (지문)	Access Point	Access granted, Access Point, Alarm, Warning
<input checked="" type="checkbox"/>	AC Power 성공	BioStar2 Terminal	Alarm, Device Related
<input checked="" type="checkbox"/>	AC Power 실패	BioStar2 Terminal	Alarm, Device Related

User-defined Categories...

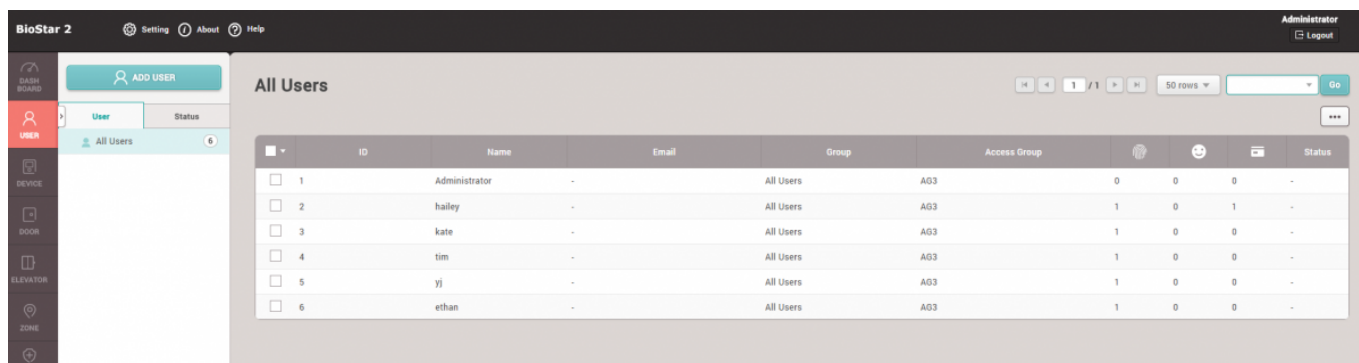
General Settings | Doors and Associated Cameras | Access Control Events | Access Request Notifications | Cardholders

Feature 2: Cardholders

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

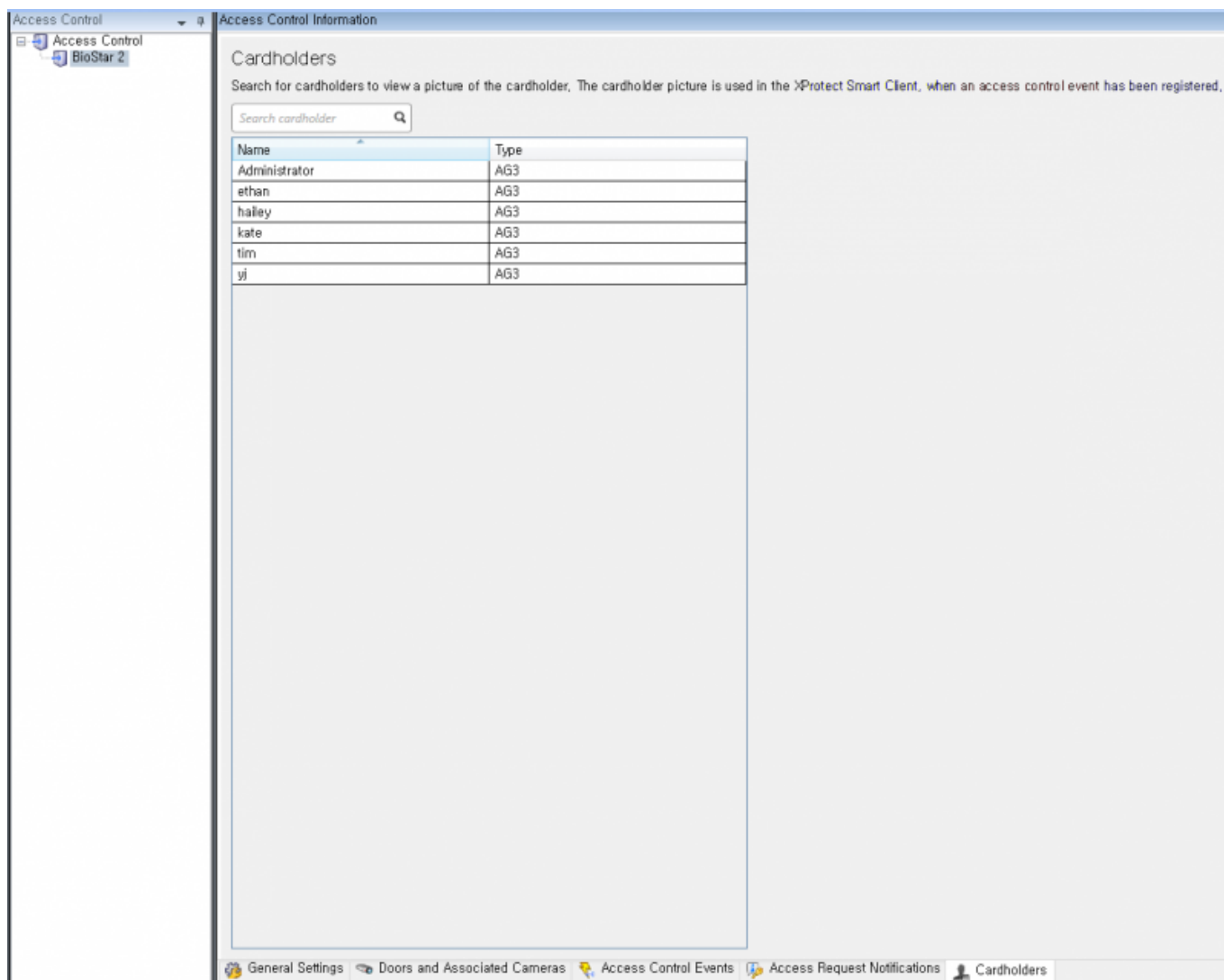
List of all Users

BioStar 2:



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

Milestone:



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

User Details

BioStar 2:

The screenshot shows the 'kate' user profile in BioStar 2. The window is divided into 'Information' and 'Credential' sections.

Information Section:

- Name: kate
- ID: 3
- Group: All Users
- Period: 2001/01/01 00:00 ~ 2030/12/31 23:59
- Operator Level: User
- Login ID: kate
- Password: [masked]
- Email: [empty field]
- Telephone: [empty field]
- Status: Active (toggle switch)
- Access Group: AG3

Credential Section:

- PIU: [masked]
- Auth Mode: Device Default
- Credential: + Fingerprint, + Face, + Card
- 1:1 Security Level: Device Default

Card Data Table:

Type	Card Data Format	Summary
Fingerprint	-	1

Buttons: Apply, Cancel

Milestone:

The screenshot shows the 'Access Control Information' window in Milestone. The 'Cardholders' section is active, displaying a list of users and their details.

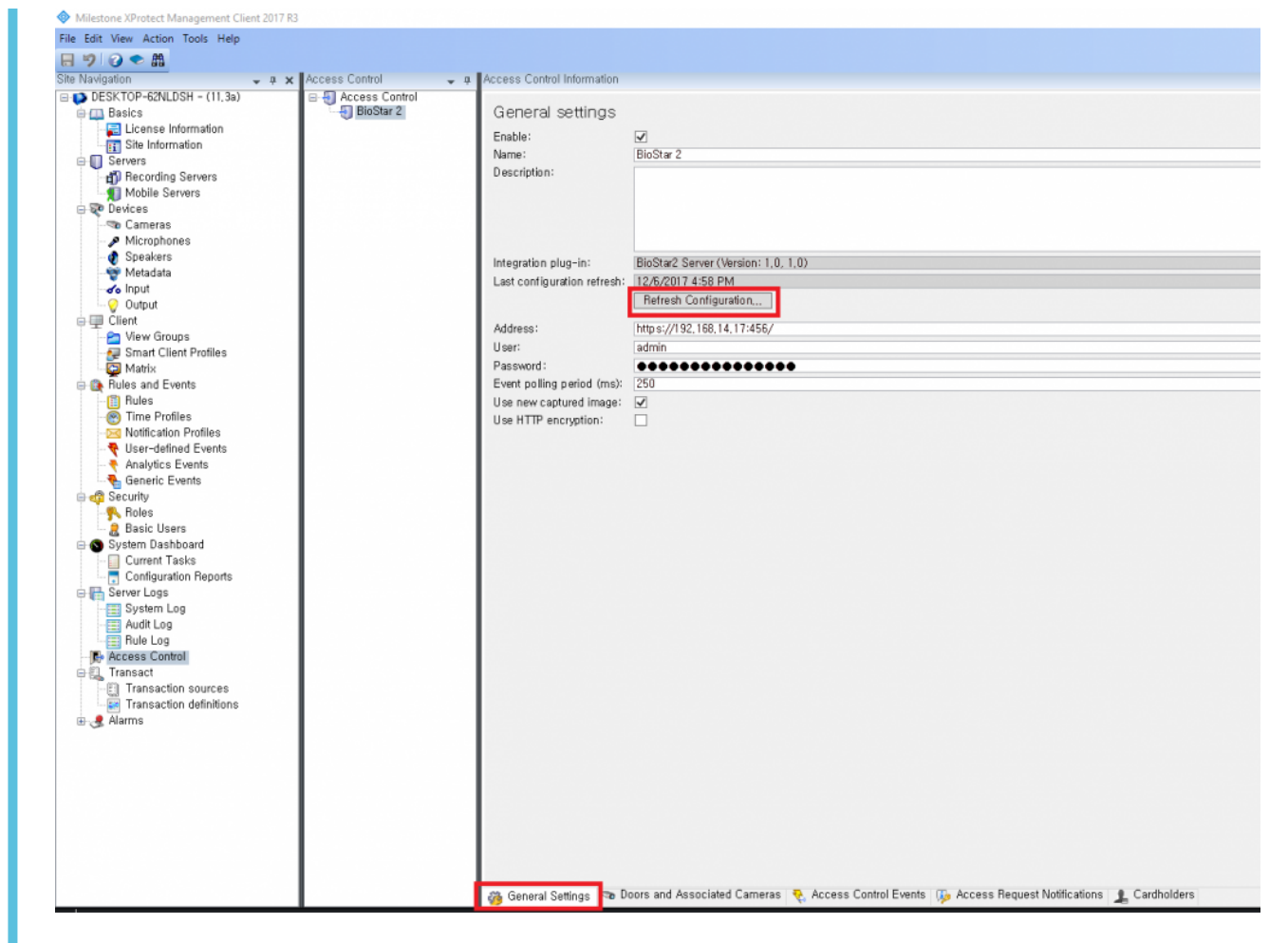
Cardholders List:

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

User Details for 'kate':

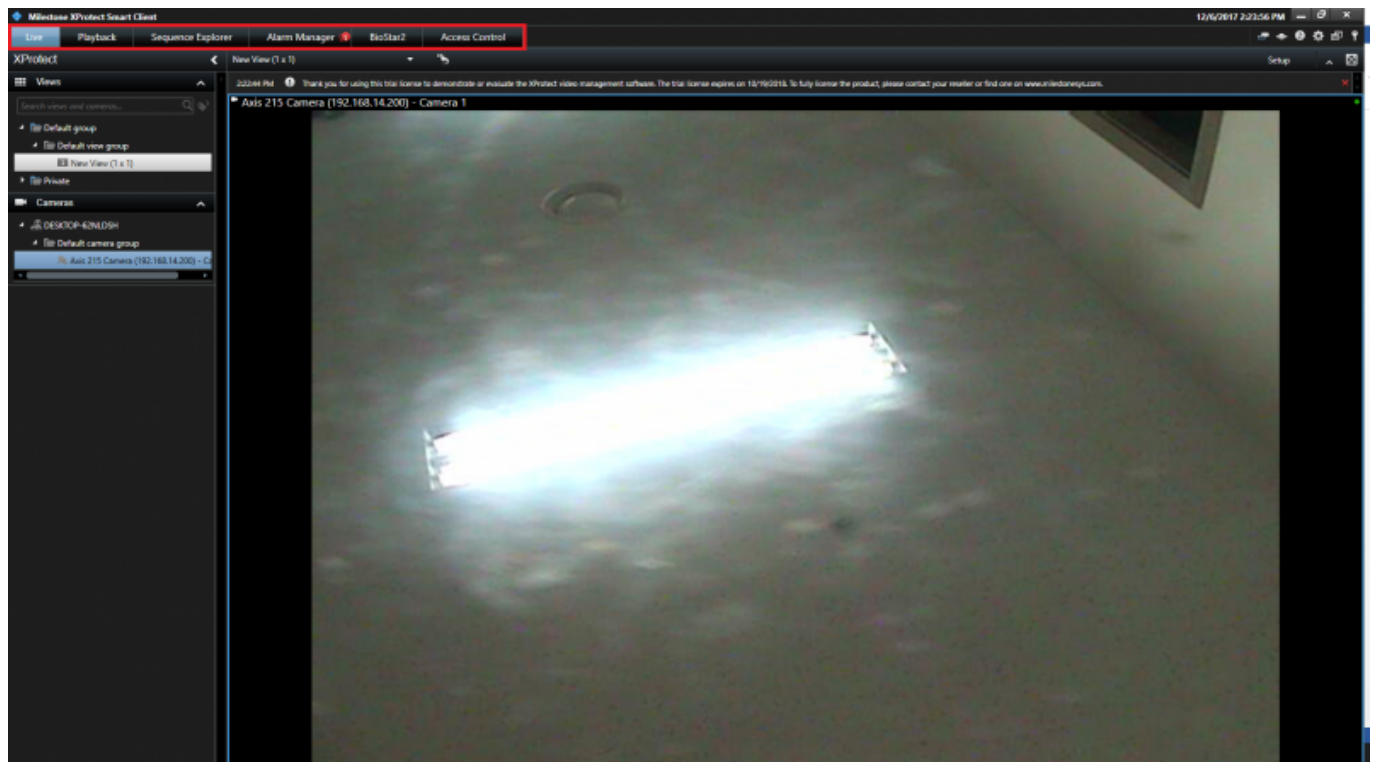
- Name: kate
- Type: AG3
- 사용자 ID: 3
- 사용자 그룹: All Users
- 비활성: false
- 시작 날짜: 2001-01-01 오전 12:00:00
- 만료 날짜: 2030-12-31 오후 11:59:00
- PIN: true
- 지문: 1
- 얼굴: 0
- 카드: 0

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.



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.

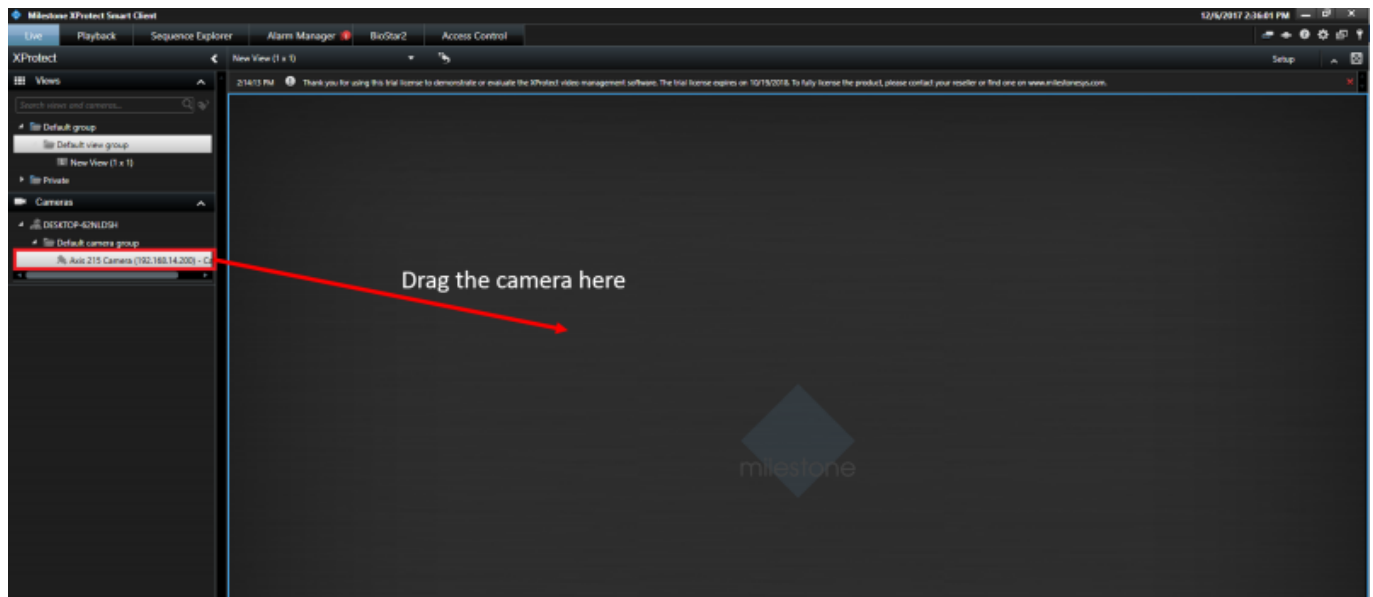


- Live
- Alarm Manager
- BioStar2
- Access Control

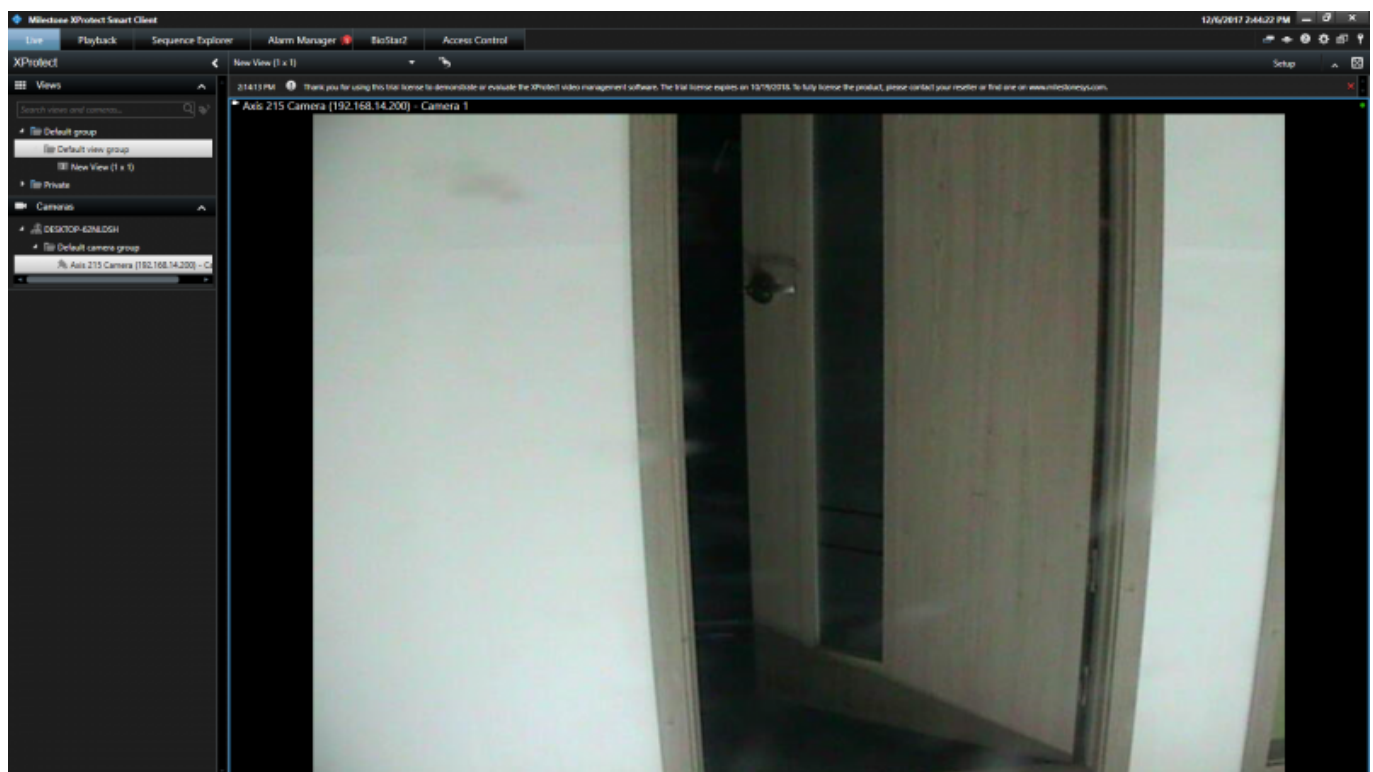
Major Features

Feature 1: Live

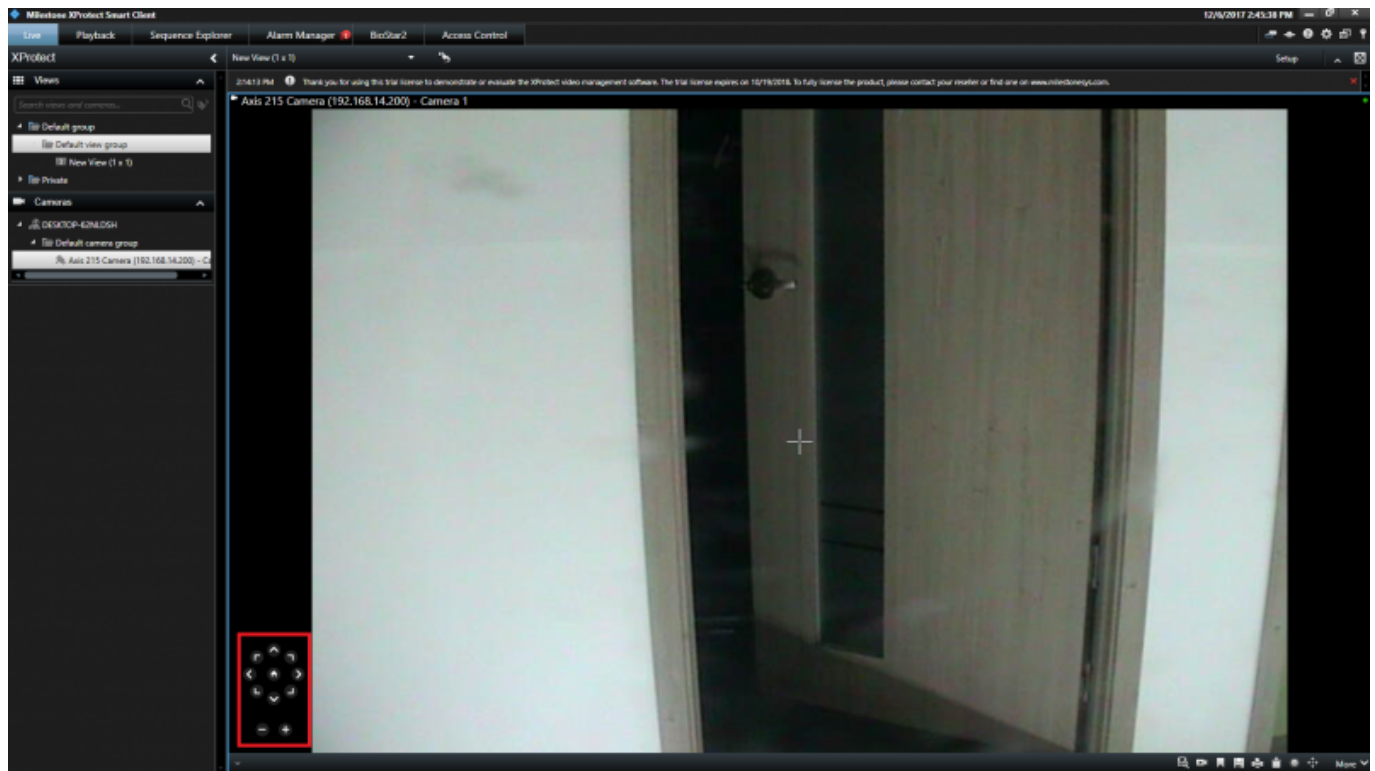
In Milestone XProtect Smart Client, you can monitor real-time video recorded by IP camera. After you select the camera you associated in Milestone XProtect management, drag it into the right panel.



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

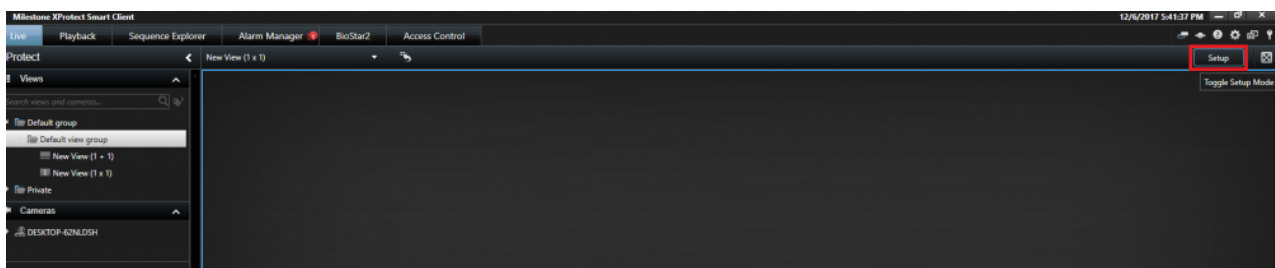


In addition, you can adjust direction or zoom in/out by clicking the icon located in left-bottom side.

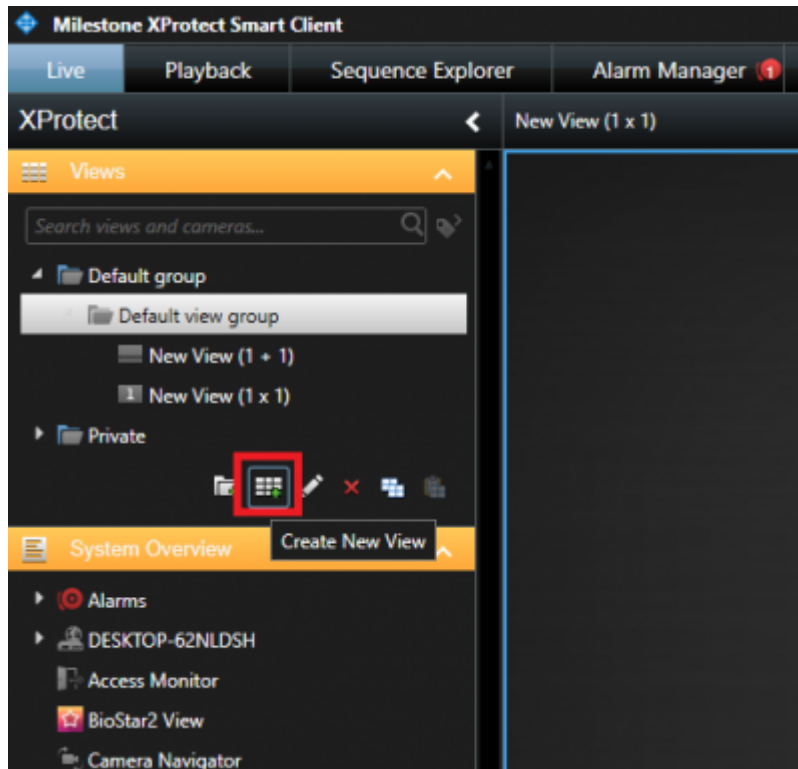


You can customize the View in Live tab.

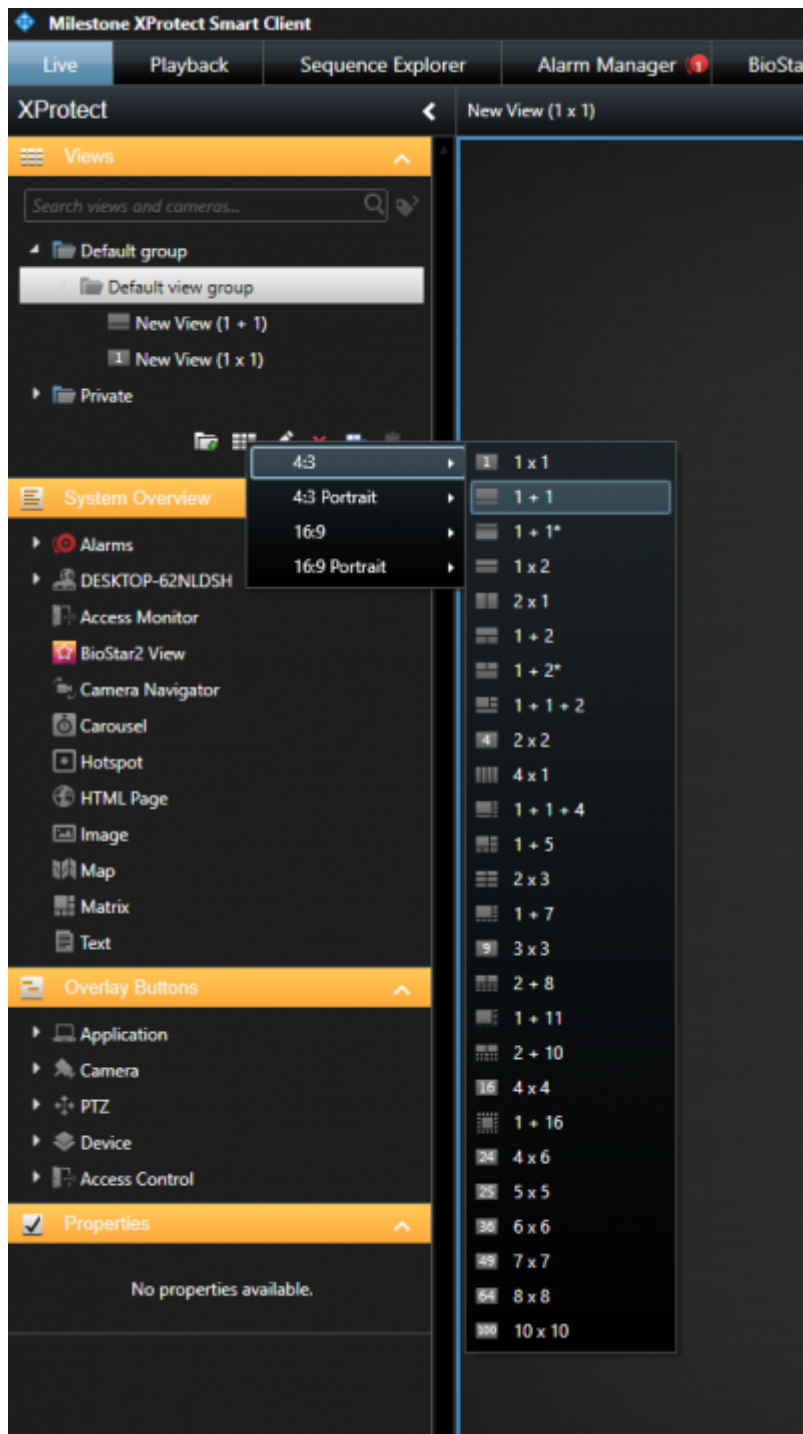
For example, if you want to monitor video and check the information on users who authenticate their identity with PIN/Fingerprint template at the same time, click **Setup** button.



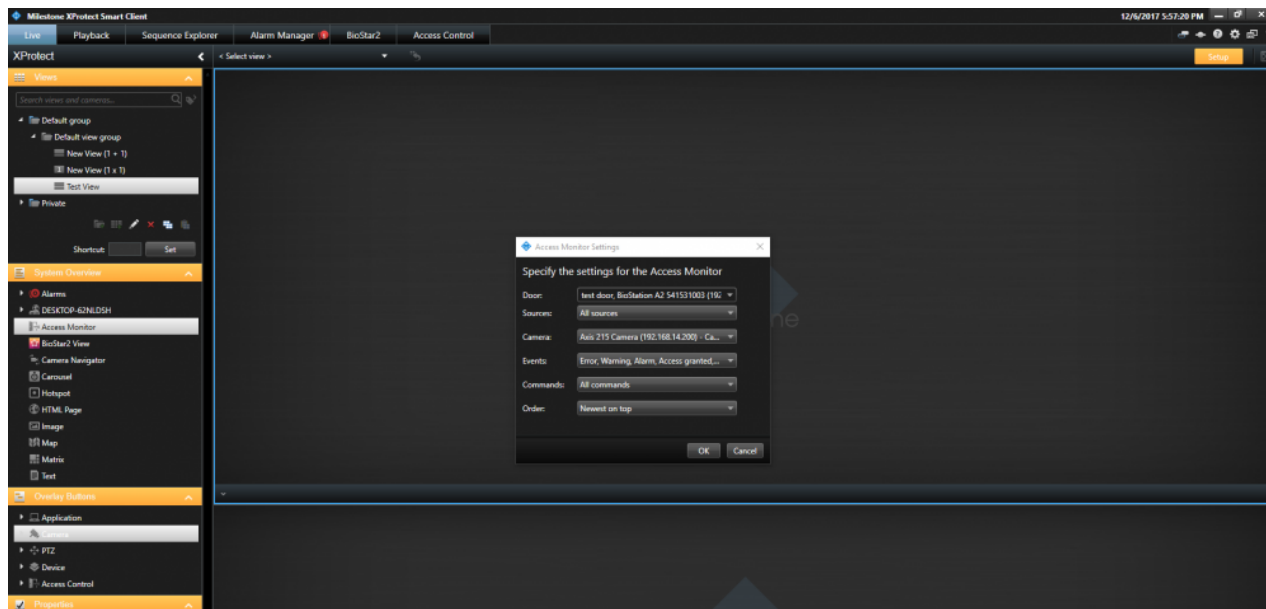
Then, you can see various options you can configure. First of all, click **Create New View** icon.



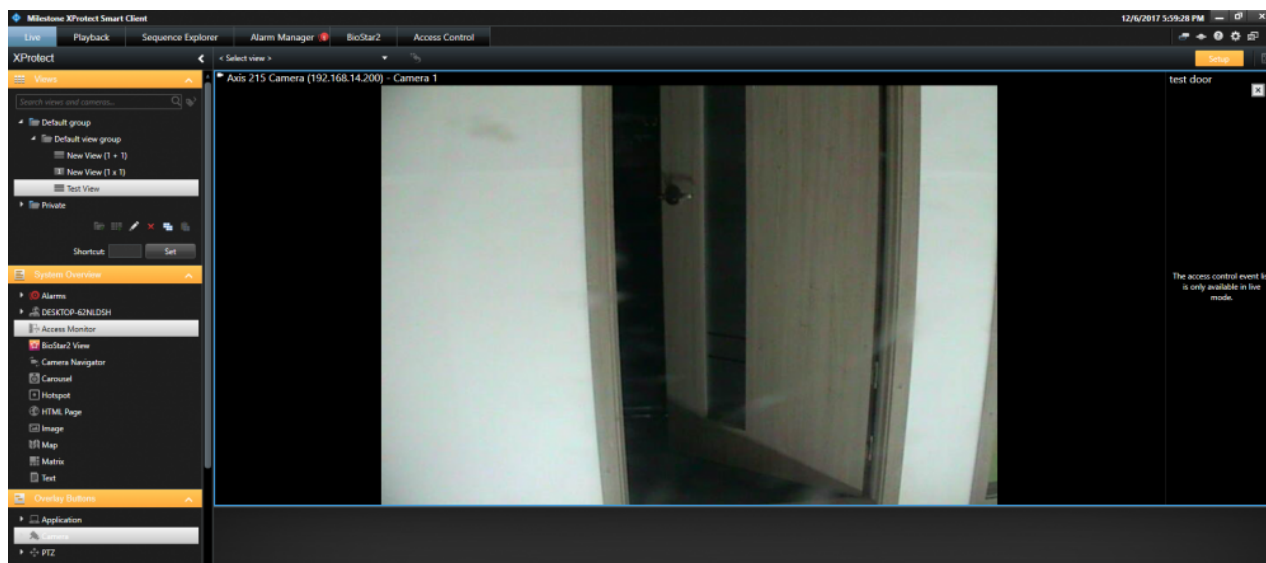
After that, you can select one option you want to customize in the view. By clicking the icon shaped pencil, you can modify the name. Then, Click **Set** button.

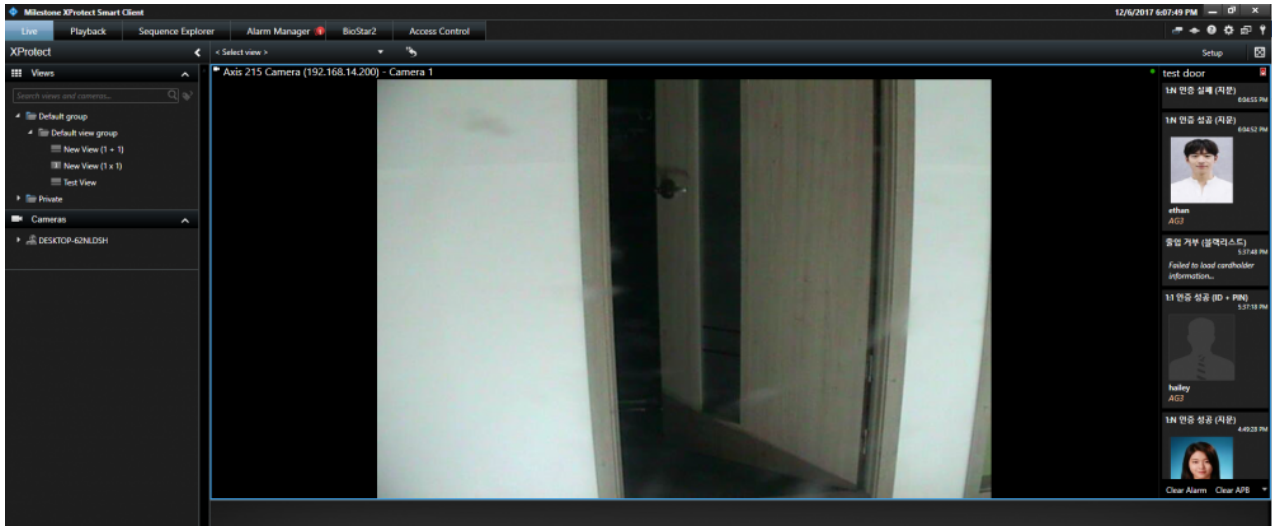


Next, drag **Access Monitor** in **System Overview**. In the Access Monitor Settings, you should specify the settings for the Access Monitor and click **OK** button.

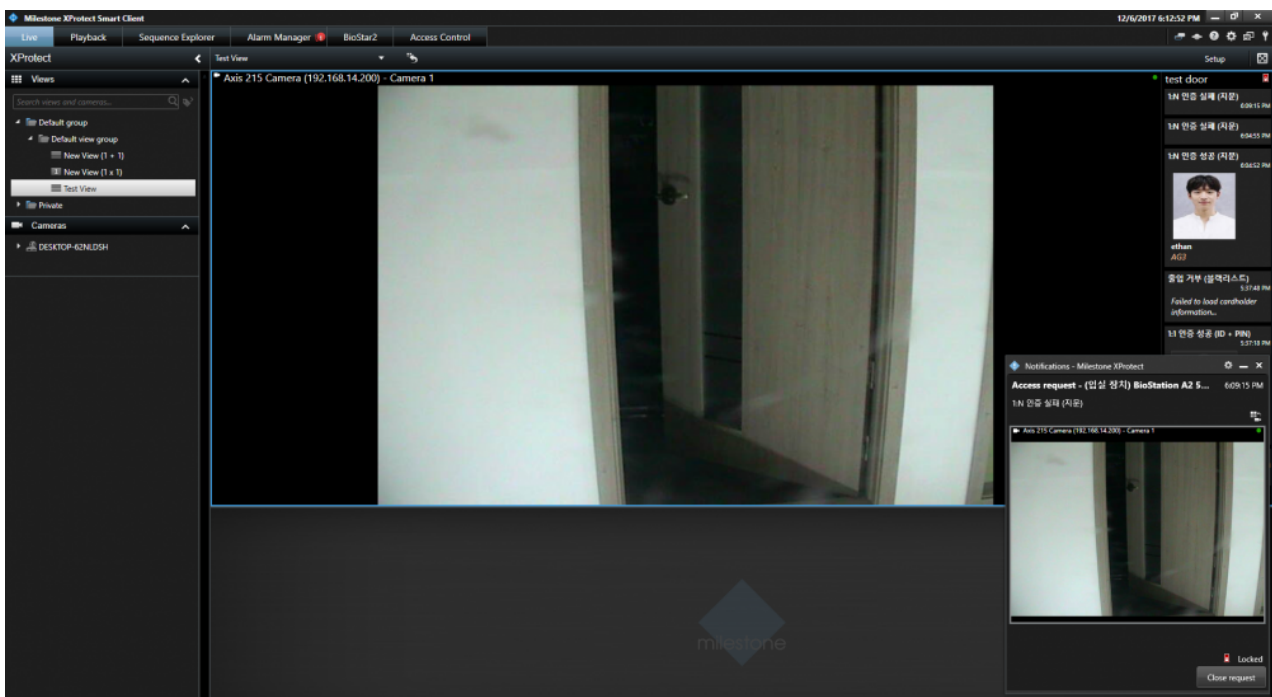


Once you click OK button, you can see the customized view. Please note that you should click Setup button again to escape the setting of View. If you see below screenshot, you can monitor video and the information on users who authenticate their identity to enter the door simultaneously.





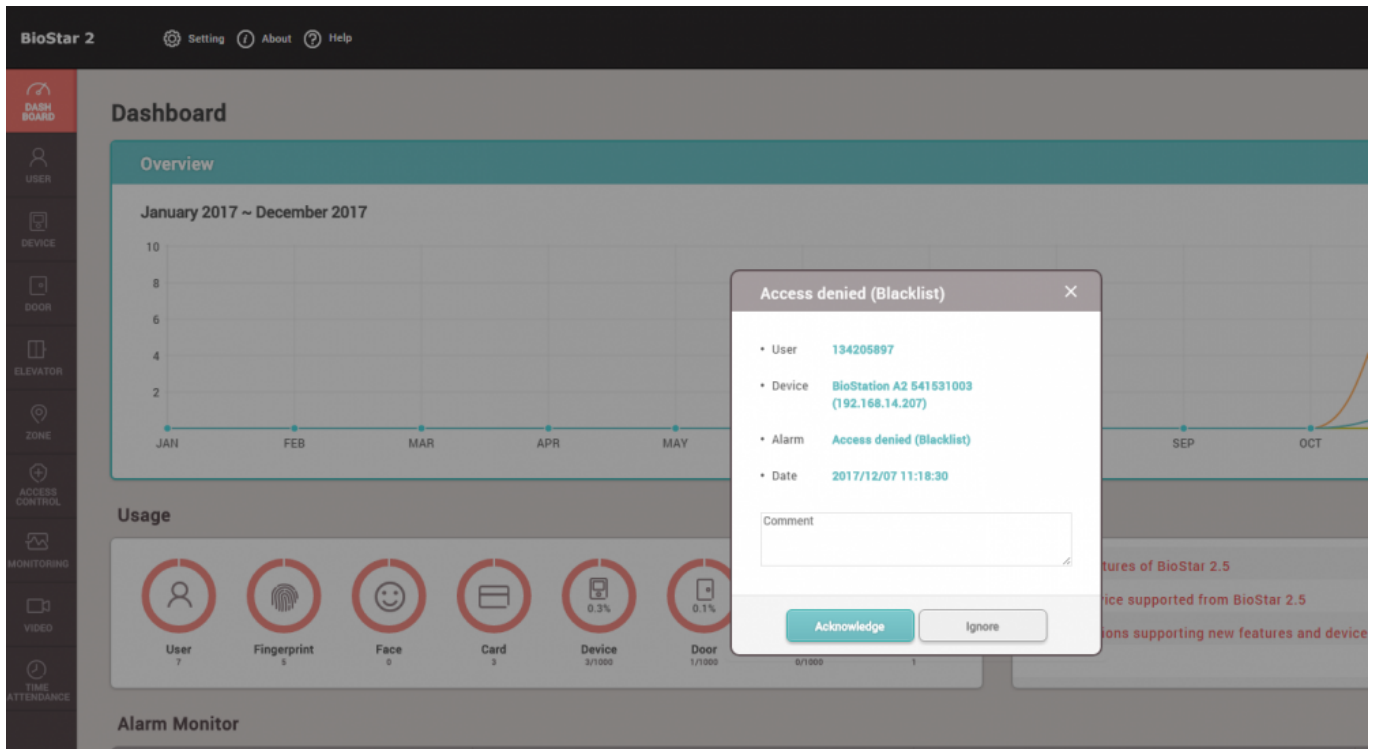
If someone fails to authenticate their identity, the notification will be displayed in the right-bottom side and display the real-time video.



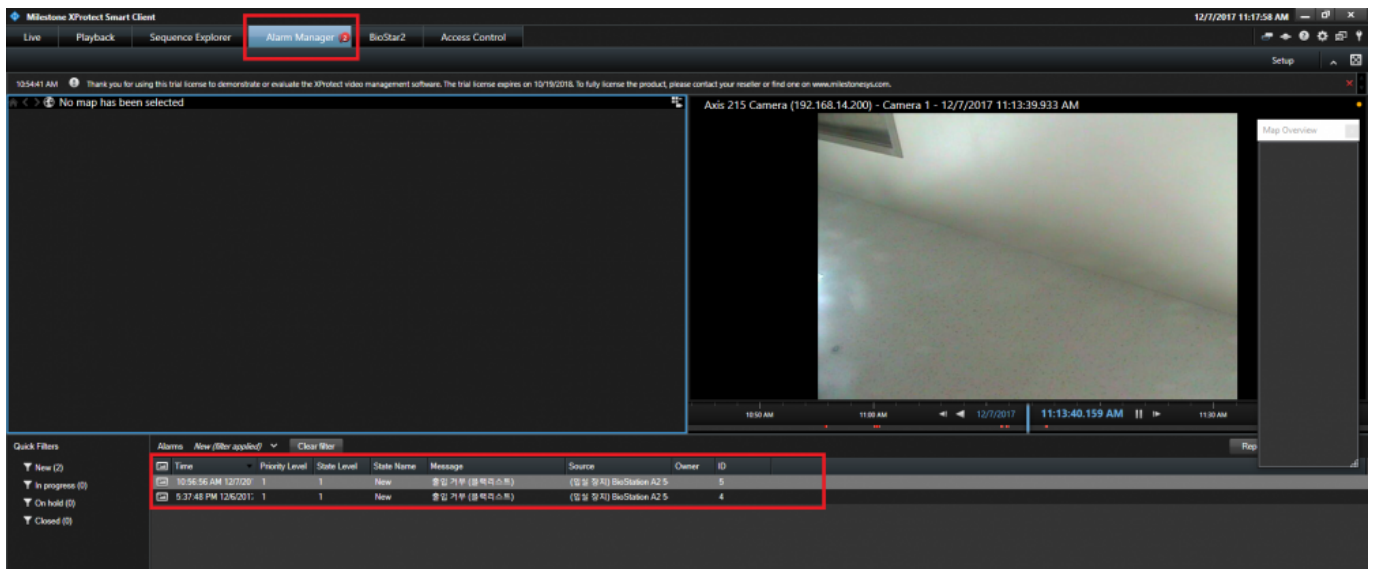
Feature 2: Alarm Manager

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

BioStar 2:



Milestone:

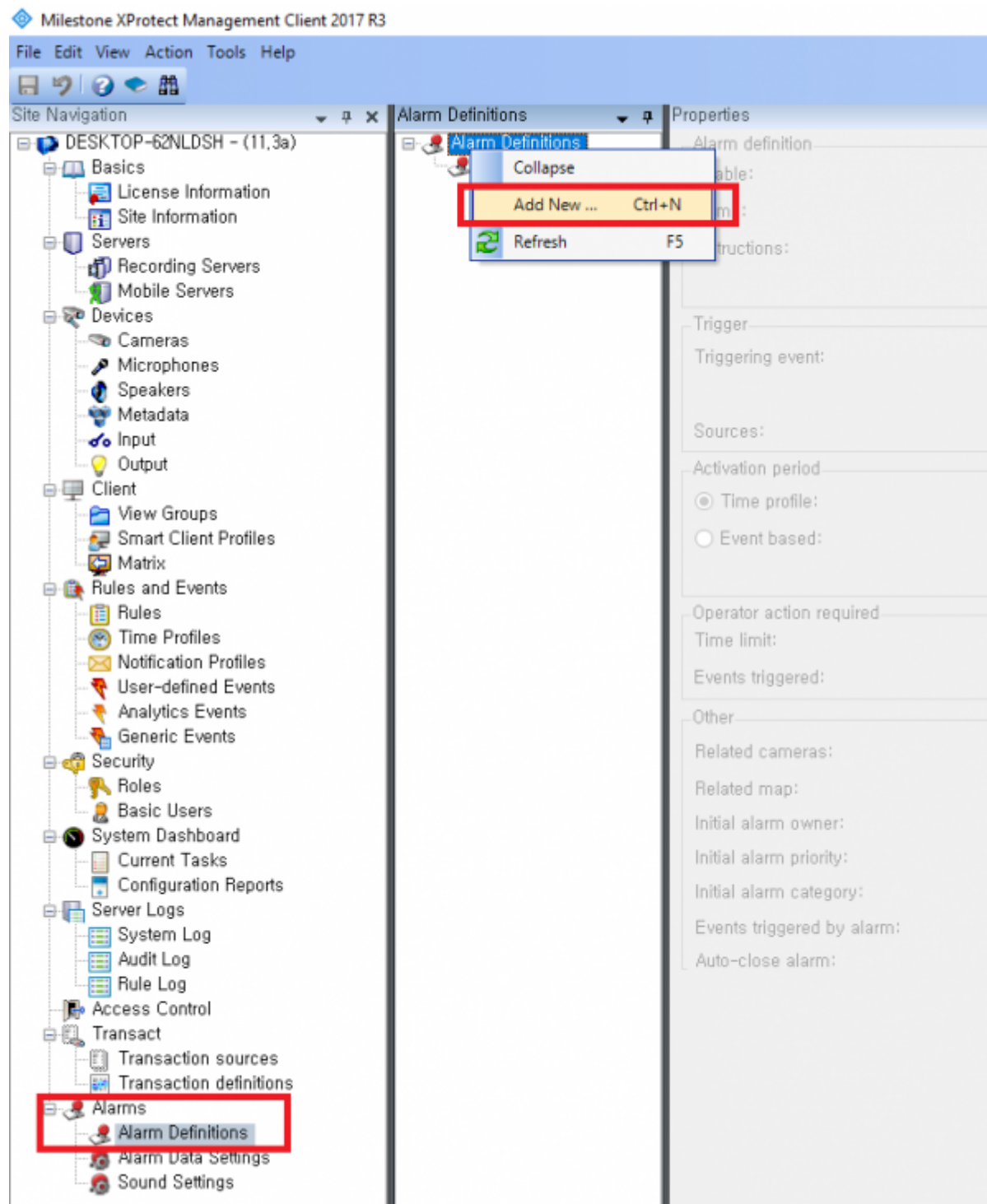


In Milestone, Alarm Manager will judge if generated event should be dealt with alarm based on Access Control Events tab and Alarm Definitions.

[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**.

Select one option for **Sources** in **Trigger** section. In below picture, I selected **All doors**.

Alarm Definitions

Properties

Alarm definition

Enable: ☒

Name:

Instructions:

Trigger

Triggering event:

Sources:

Activation period

Time profile: ☒ Always

Event based: ☐

Start:
Stop:

Operator action required

Time limit:

Events triggered:

Other

Related cameras:

Related map:

Initial alarm owner:

Initial alarm priority:

Initial alarm category:

Events triggered by alarm:

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 Information

Access control events

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

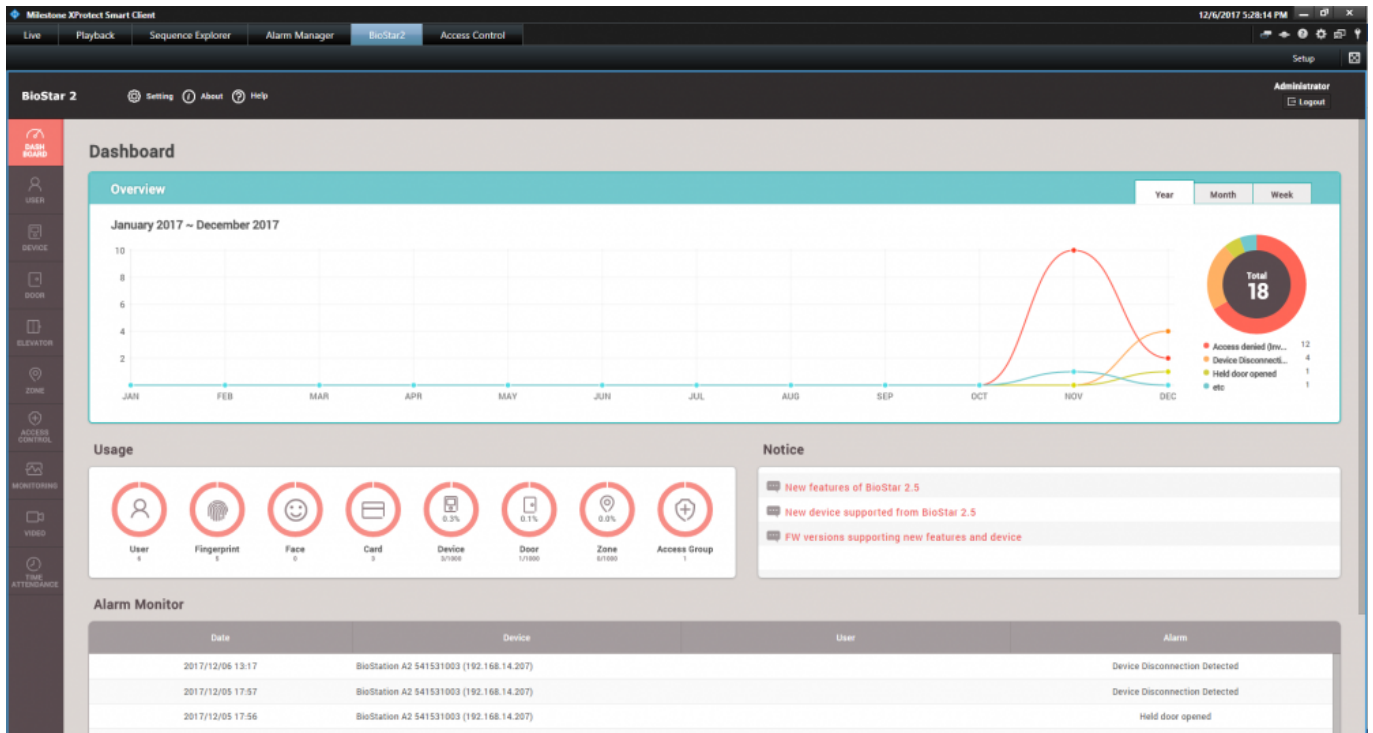
Enabled	Access Control Event	Source Type	Event Category
<input checked="" type="checkbox"/>	인출 실패 (시간 초과)	Access Point, Door	Access denied, Access Point, Access request, Zone Related
<input checked="" type="checkbox"/>	인출 실패 (일부된 인출 모드)	Access Point, Door	Access denied, Access Point, Access request, Zone Related
<input checked="" type="checkbox"/>	인출 실패 (일부된 크라덴셜)	Access Point, Door	Access denied, Access Point, Access request, Zone Related
<input checked="" type="checkbox"/>	입력 감지	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	장치 시간 설정	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	장치 시작	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	장치 잠금	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	장치 잠금 해제	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	장치 재설정	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	장치 재시작	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	장치연결해제 감지	BioStar2 Terminal	Device Related
<input checked="" type="checkbox"/>	출입 거부 (시간 만료)	Access Point, Door	Access Point, Alarm, Zone Related
<input checked="" type="checkbox"/>	출입 거부 (블랙리스트)	Access Point, Door	Access Point, Alarm, Zone Related
<input checked="" type="checkbox"/>	출입 거부 (비활성 사용자)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (소프트 시간 지정 안티패스)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (소프트 안티패스)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (스케줄 잠금)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (시간 지정 안티패스)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (일부된 출입 실패)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (일부된 출입 그룹)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (활동 실패)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입 거부 (하드 안티패스)	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 강제 열림	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 강제 열림 알람	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 강제 열림 해제	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 개방	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 안티패스	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 안티패스 해제	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 열림	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 잠금	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	출입문 잠시간 열림	Access Point, Door	Access Point, Alarm, Door Related
<input checked="" type="checkbox"/>	출입문 잠시간 열림 알람	Access Point, Door	Access Point, Alarm, Door Related
<input checked="" type="checkbox"/>	출입문 잠시간 열림 해제	Access Point, Door	Access Point, Door Related
<input checked="" type="checkbox"/>	침입 감지	Door	Alarm, Zone Related
<input checked="" type="checkbox"/>	침입 경보 상태 해제	Door	Zone Related
<input checked="" type="checkbox"/>	타입은 설정	BioStar2 Terminal	Device Related

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.



Feature 4: Access Control

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

Access Control

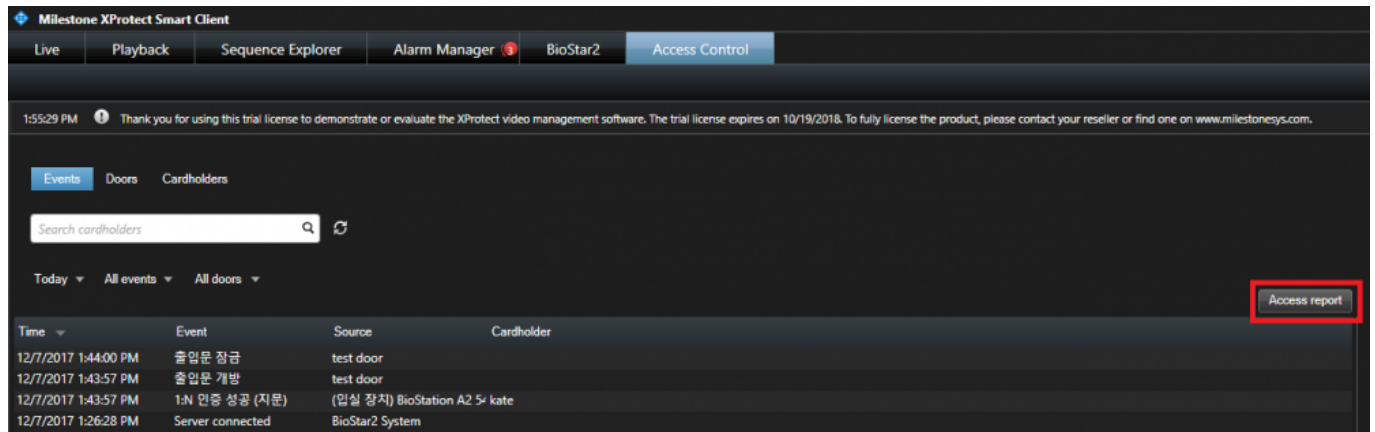
Search cardholders

Today All events All doors

Access report

Time	Event	Source	Cardholder
12/7/2017 11:18:30 AM	출입 거부 (블랙리스트)	(임실 장치) BioStation A2 541531003	
12/7/2017 10:56:56 AM	출입 거부 (블랙리스트)	(임실 장치) BioStation A2 541531003	
12/7/2017 10:55:28 AM	출입 거부 (블랙리스트)	(임실 장치) BioStation A2 541531003	
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 (192.168.14.22)	
12/7/2017 9:30:48 AM	장치 시간 설정	BioLiteNet 538101268 (192.168.14.22)	
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.



Milestone XProtect Smart Client

Live Playback Sequence Explorer Alarm Manager BioStar2 Access Control

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.

Events Doors Cardholders

Search cardholders

Today All events All doors

Access report

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 5x kate	
12/7/2017 1:26:28 PM	Server connected	BioStar2 System	

From:

<http://kb.supremainc.com/knowledge/> -

Permanent link:

http://kb.supremainc.com/knowledge/doku.php?id=en:how_to_integrate_milestone_with_biostar_2&rev=1583994744

Last update: **2020/03/12 15:32**