

XProtect

Integration

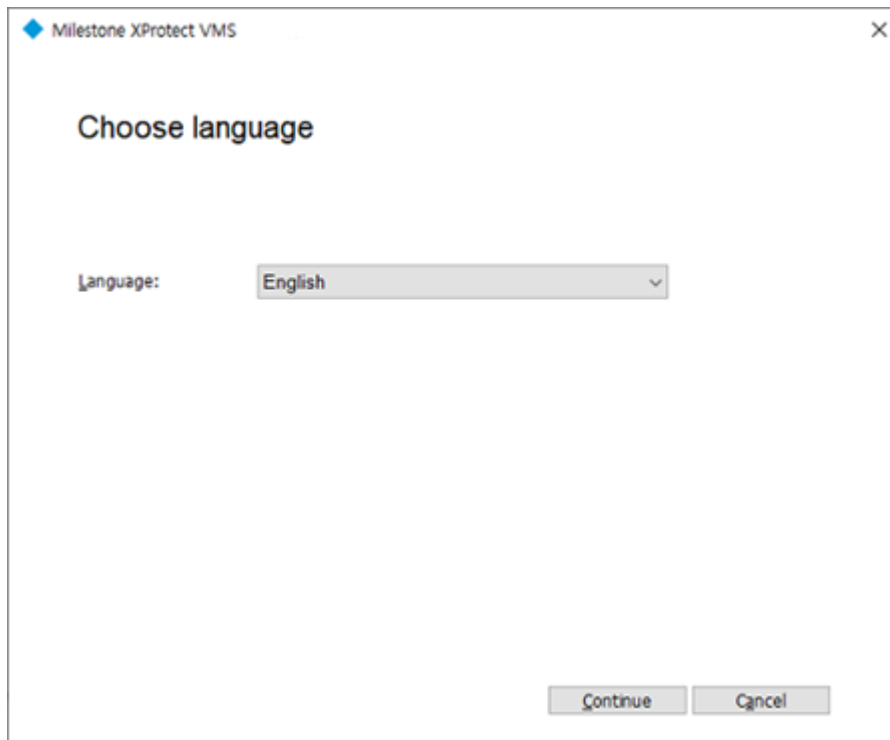
UNION biometrics CO., Ltd

Table of Contents

How to setup XProtect	3
UBio-Sync UNIS integration.....	8
1. MIP Plug-ins.....	8
1.1. Install UBio-Sync UNIS Admin Plugin	8
1.2 How to use XProtect Management Client	11
2. Access Control.....	17
2.1 Install UBio-Sync UNIS Control Plugin.....	17
2.2 How to set XProtect Management Client	20
2.3 How to use Milestone XProtect Smart Client	26

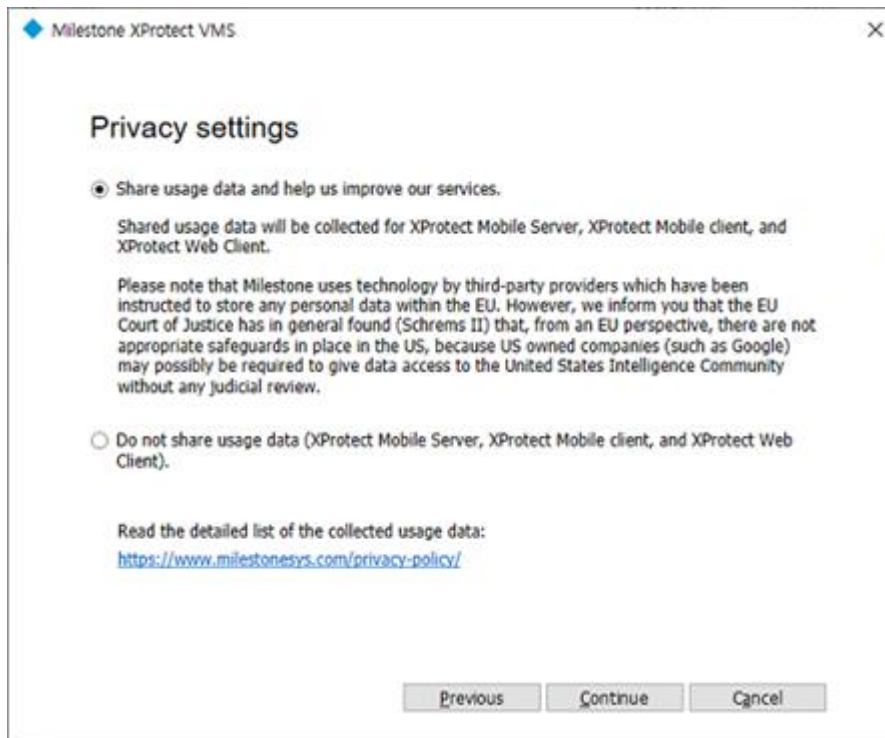
How to setup XProtect

1. Select the language.

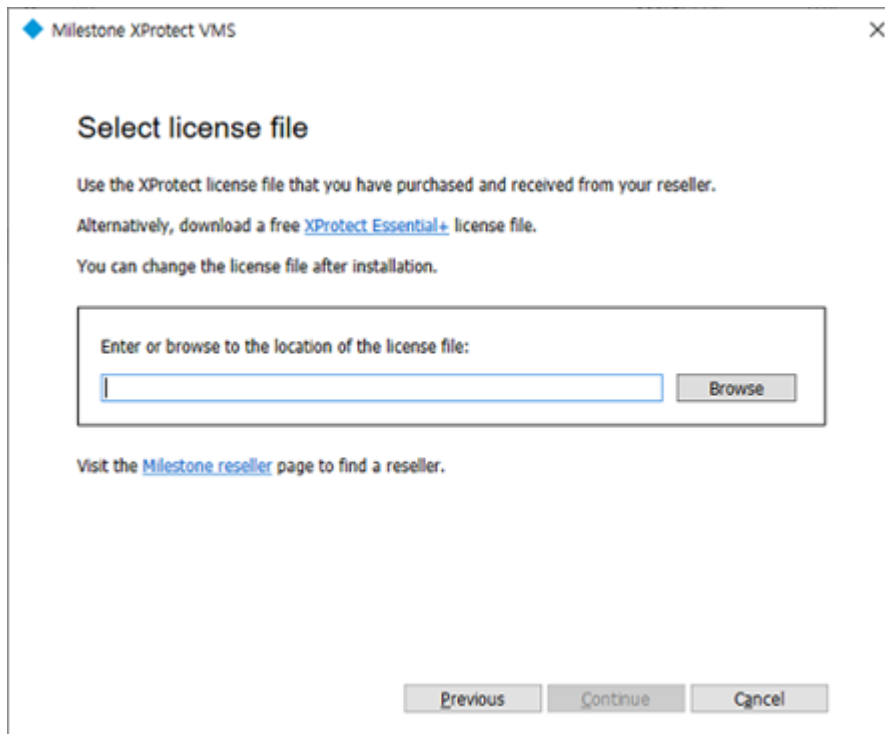


2. Read the agreement and select [Continue].

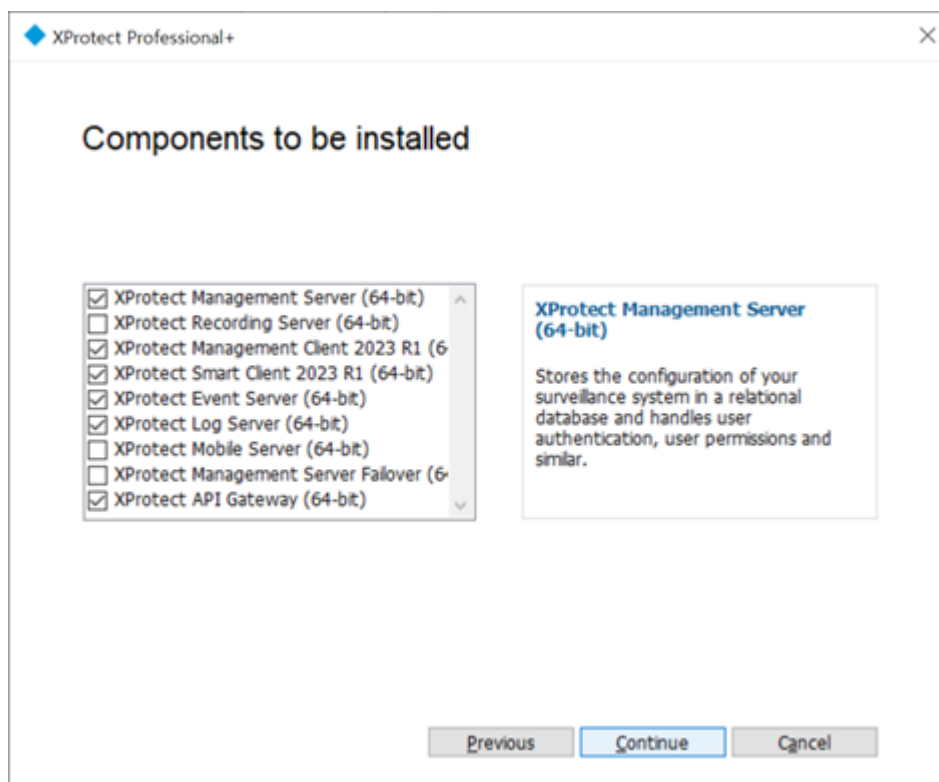
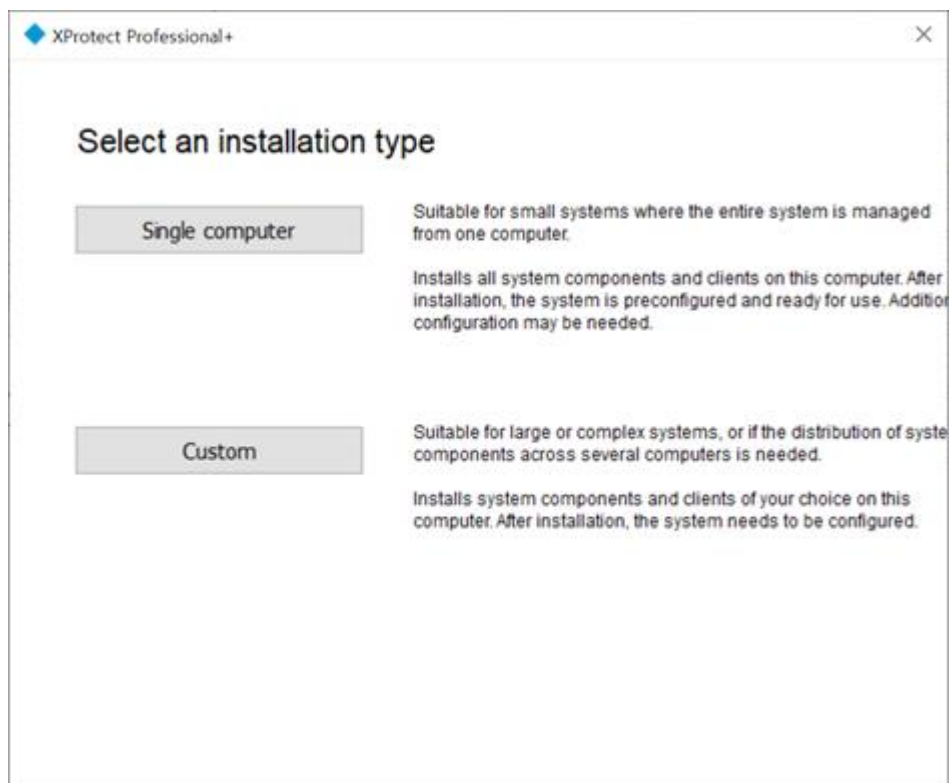




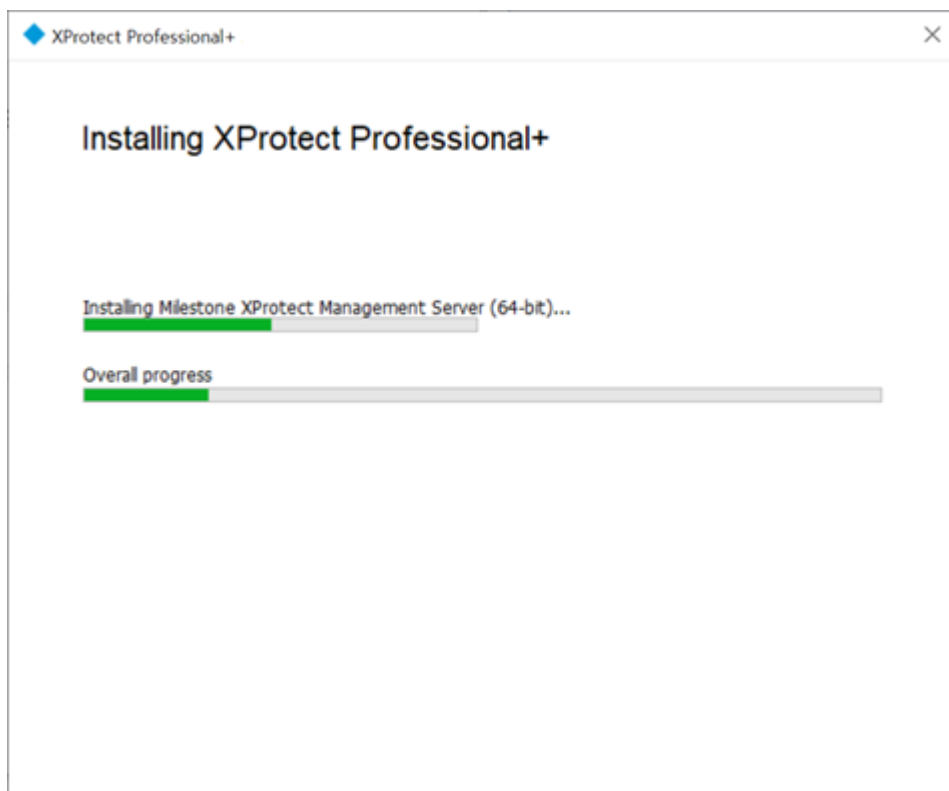
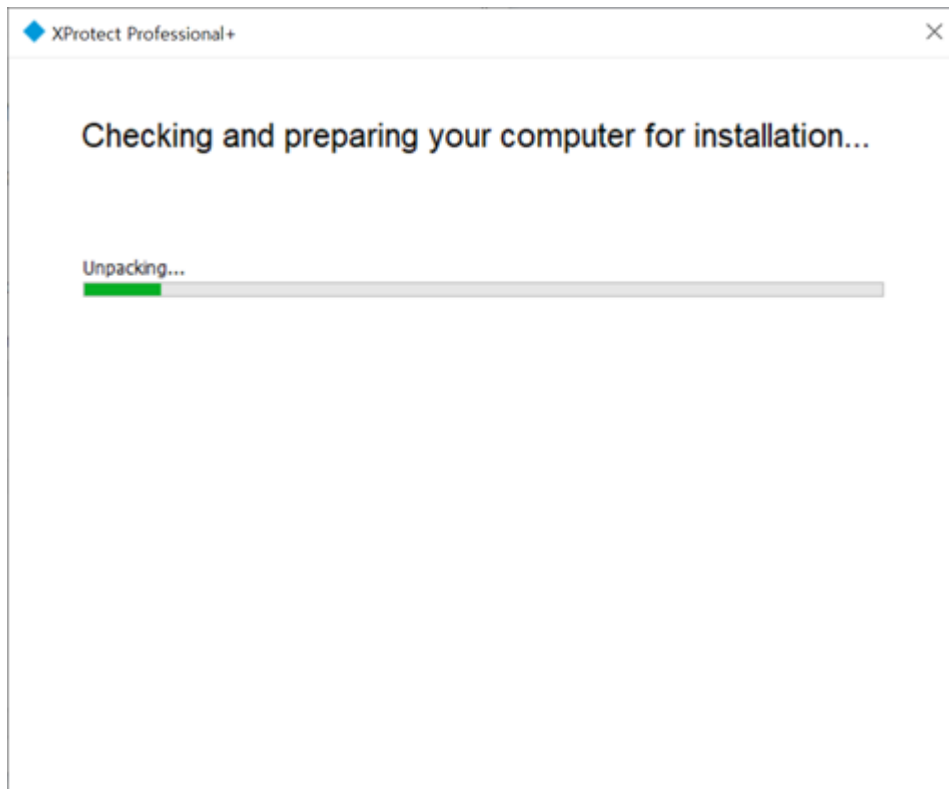
3. Select the path that the program is installed in and [Continue].



4. Select the installation type.



5. You can find that it is installing as below.



6 The installation is completed.

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 API Gateway (64-bit)
XProtect Event Server (64-bit)
XProtect Log Server (64-bit)
XProtect Management Client 2023 R1 (64-bit)
XProtect Smart Client 2023 R1 (64-bit)

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

Web Client address:

<http://desktop-tkbe9s2:8081/>

Mobile Client address:

<http://desktop-tkbe9s2/>

Continue

Close

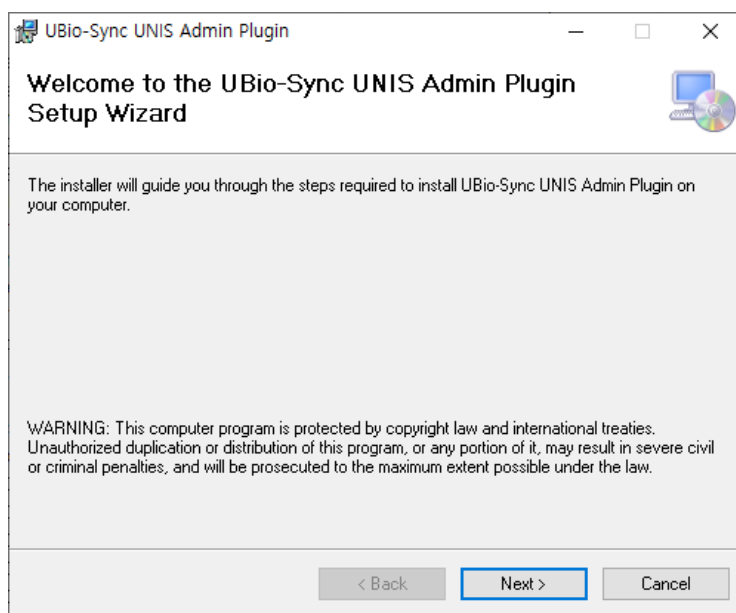
UBio-Sync UNIS integration

1. MIP Plug-ins

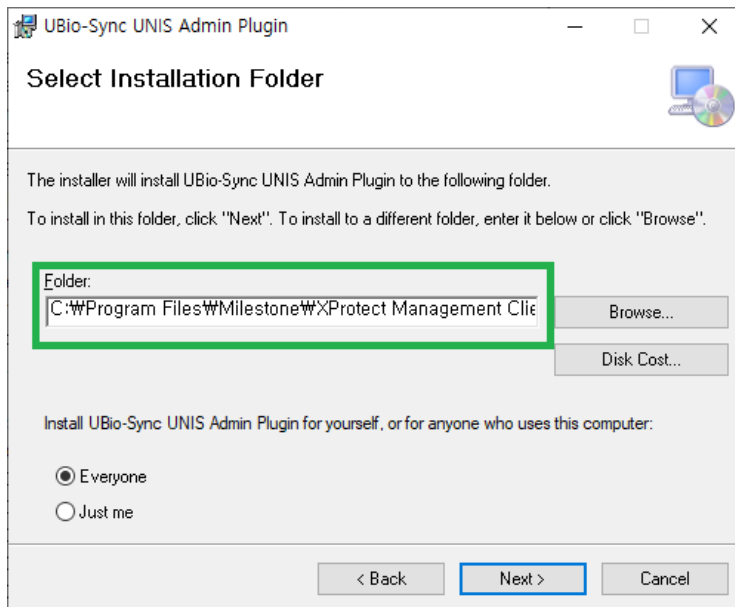
1.1. Install UBio-Sync UNIS Admin Plugin

① Execute "UBio-Sync UNIS Admin Plugin.msi".

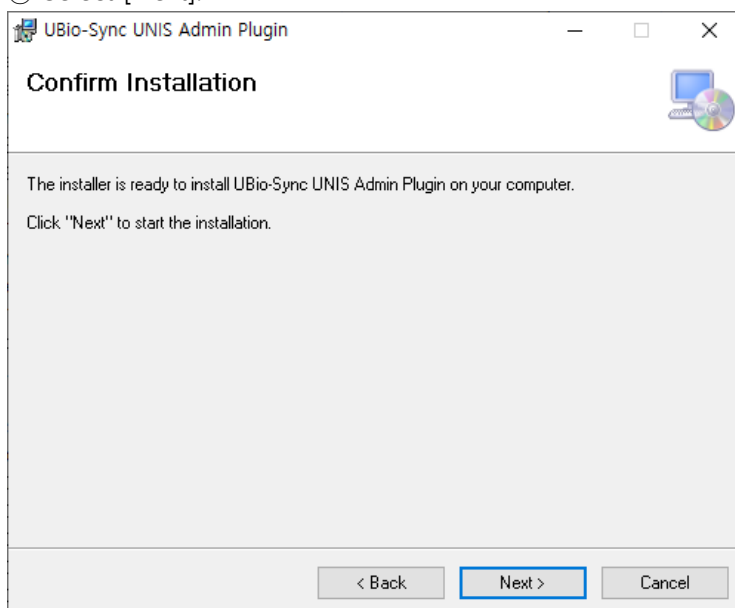
② Select [Next].



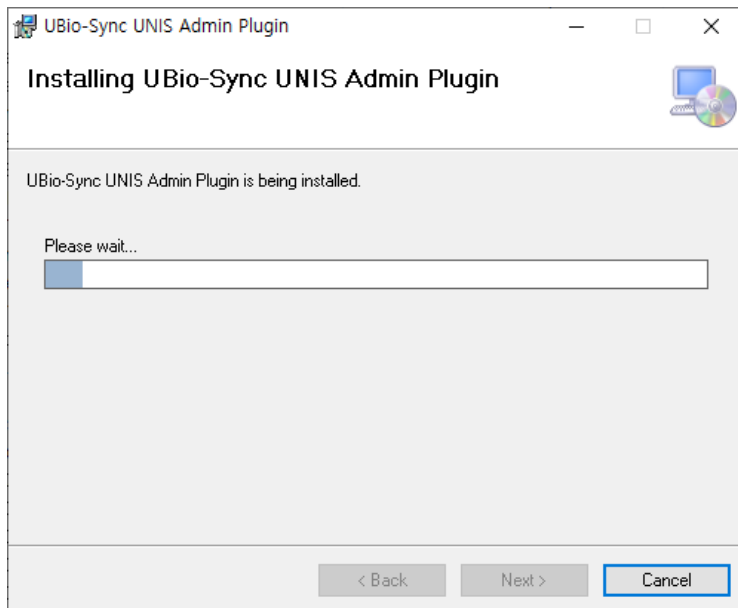
③ Check the installation path in green box. It should be saved in MIPPlugins folder where "VideoOS.Administration.exe" is installed on the path where Milestone is installed. Otherwise, when it is saved in other paths, the program would not operate properly.



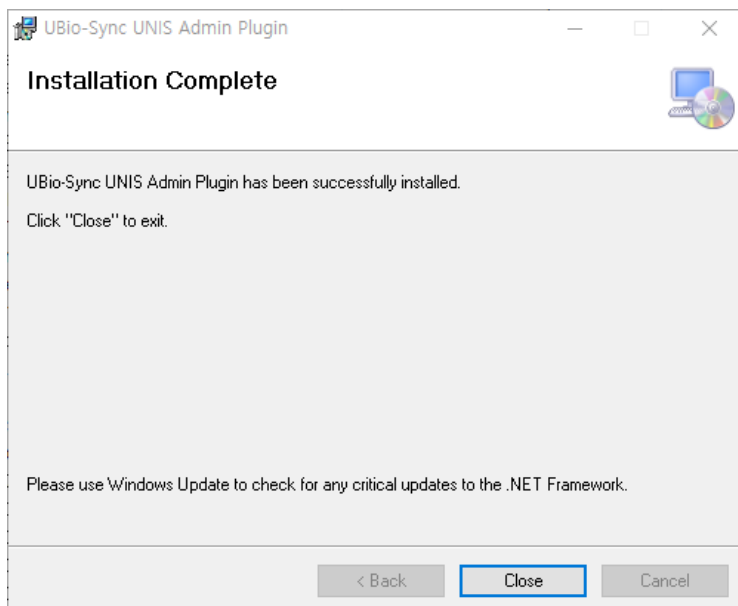
④ Select [Next].



⑤ You can see the window below that it is installing.



⑥ The installation is completed

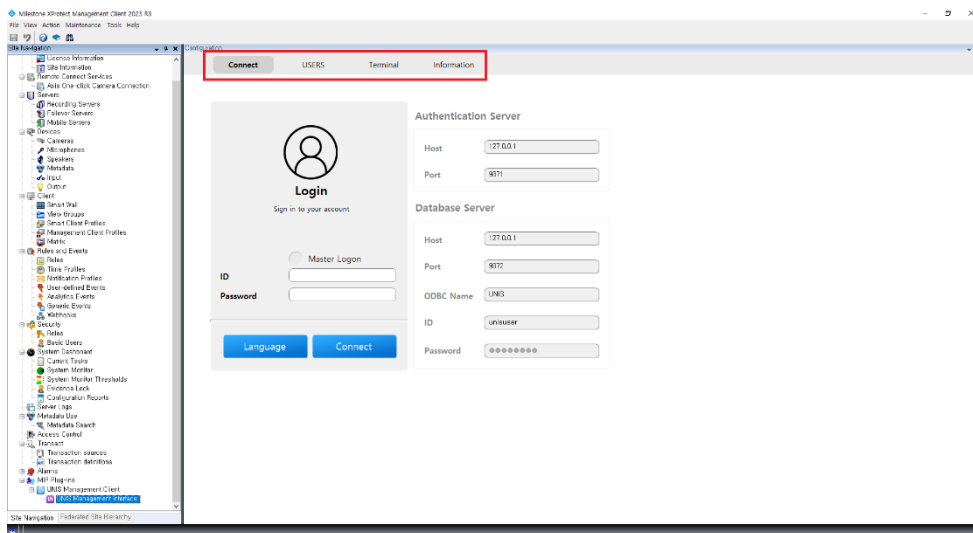


1.2 How to use XProtect Management Client

- ① Double click on "XProtect Management Client" icon to execute.



- ② Click "UNIS Management Interface" from MIP Plug-ins in left Tree view.



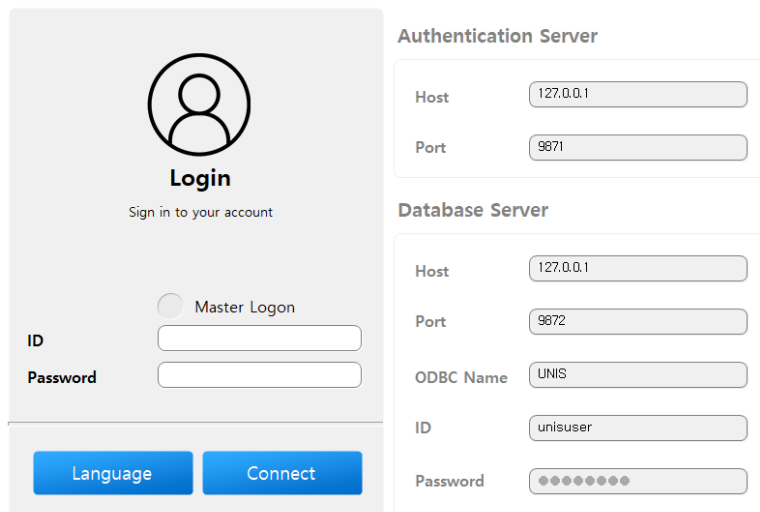
[Connection]: UNIS connection information

[Users]: User management

[Terminal]: Terminal management

[Information]: Log information

1. Connection



Login
Sign in to your account

☐ Master Logon

ID

Password

[Language](#) [Connect](#)

Authentication Server

Host

Port

Database Server

Host

Port

ODBC Name

ID

Password

[Master]: Select if you log in with UNIS master administrator.

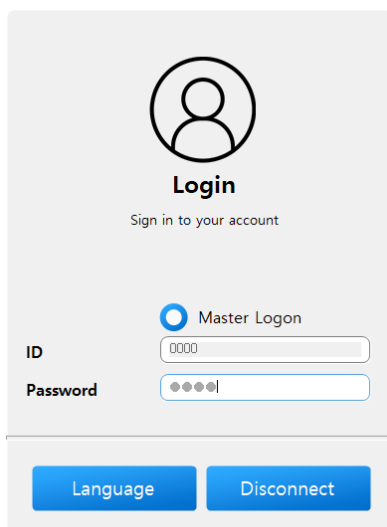
[User ID]: Login ID

[User Password]: Login Password

[Connect]: Try for connection

[Authentication Server]: Authentication server connection information

[Database Server]: Database server connection information



Login
Sign in to your account

☒ Master Logon

ID

Password

[Language](#) [Disconnect](#)

The first password for Master administrator is 1.

2. Users

Add User

Delete User

Send to Terminals

Terminal User

C	ID	Name	Employee ID	Location	Branch	Department	Title	Authority	Access Group
<input type="checkbox"/>	0001	user1	0001	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0002	user2	0002	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0003	test	0003	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0004	asdsa	0004	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0006	asdsadsa	0006	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0010	not	0010	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0011	asdasdsadsa		****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0012	QRTEST	0012	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0013	test13	0013	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0017	dsa	0017	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0018	dfgg		****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0019	tt	0019	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0020	das	0020	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0021	FaceTest	0021	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0022	qq	0022	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned
<input type="checkbox"/>	0005		0005	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned	****: Not Assigned

[illegible]

3. Terminal

**** : Not Assigned

- 0001 terminal1
- 0002 test
- 0003 test3
- 0004 test4
- 0005 test5
- 0011 1234
- 4444 QRTEST

Add Terminal

Delete Terminal

ID	1
Name	terminal1
IP Address	192.168.21.163
Version	UBio-X Face Pro 0.0.0-61.01-000.49//NFC9K-V1.3N/
Type	Normal

[Add Terminal] : Select if you want to add the terminal.

Modify Terminal's Information

Modify Terminal

Basic Information

ID	<input type="text" value="0002"/>
Name	<input type="text" value="FACE"/>
Branch	**** : Not Assigned
Install Type	Fixed
Location	<input type="text"/>
Reg. Date	2023/07/05 15:49:14
Door Control	Allow all Functions
Type	Normal

☒ Time Zone (UTC+09:00) 오사카, 삿포르, 도쿄
2023-10-06 20:50:24

Function

☒ TNA ☒ MEAL

Anti Pass Back

Enter Zone **** : Not Assigned

Exit Zone **** : Not Assigned

☒ Soft Passback

Other

DVR Configuration

DVR ID	Not Defined	DVR IP	<input type="text"/>	CH1	Not Defined	CH2	Not Defined
--------	-------------	--------	----------------------	-----	-------------	-----	-------------

Unassigned Admin

Admin...	Name

Assigned Admin

Admin...	Name

Modify
Close

[Delete Selected Terminal] : Delete the selected terminals.

[illegible]

4. Information

Information	
Type	Message
Information	Main UDB Version : Standard v4.5.0.2
Information	UDB_Server connection!
Information	UNIS_Server connection!

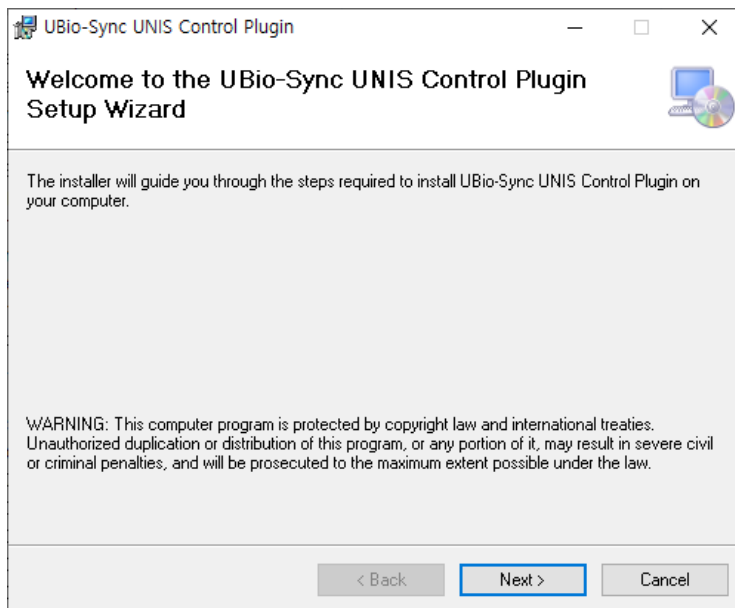
This window shows the status logs.

2. Access Control

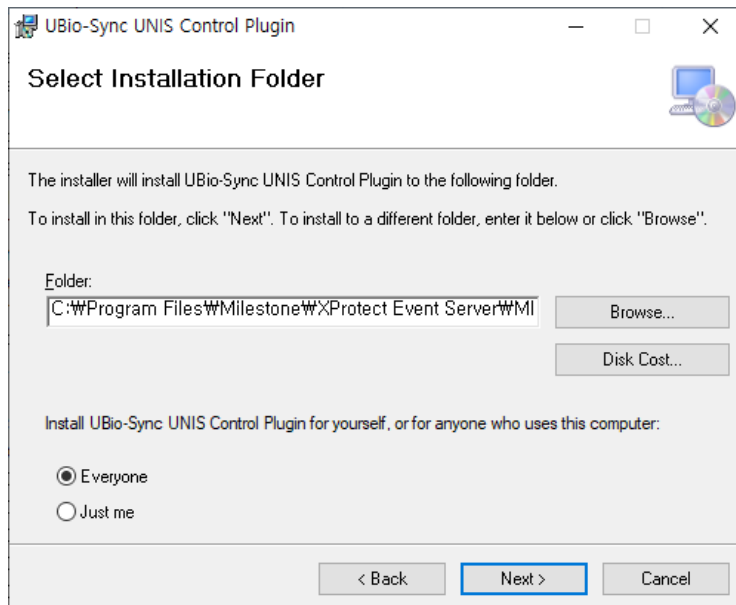
2.1 Install UBio-Sync UNIS Control Plugin

① Execute "UBio-Sync UNIS Control Plugin.msi".

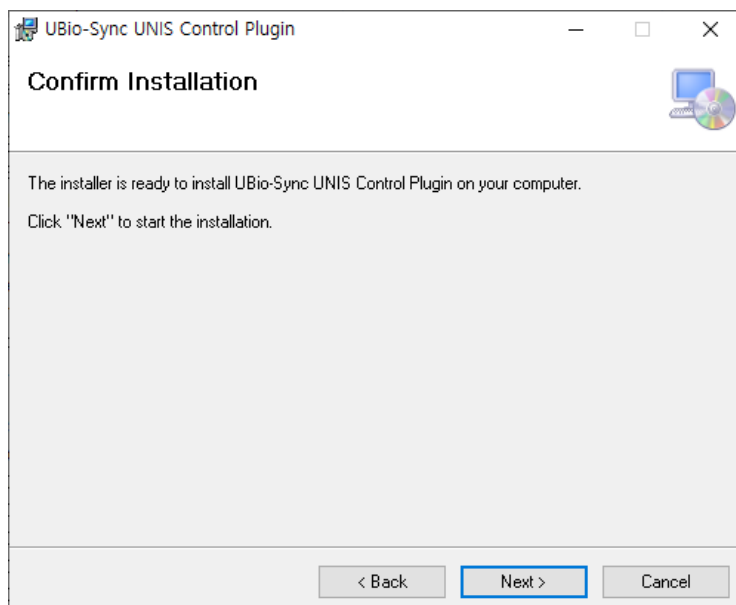
② Select [Next]



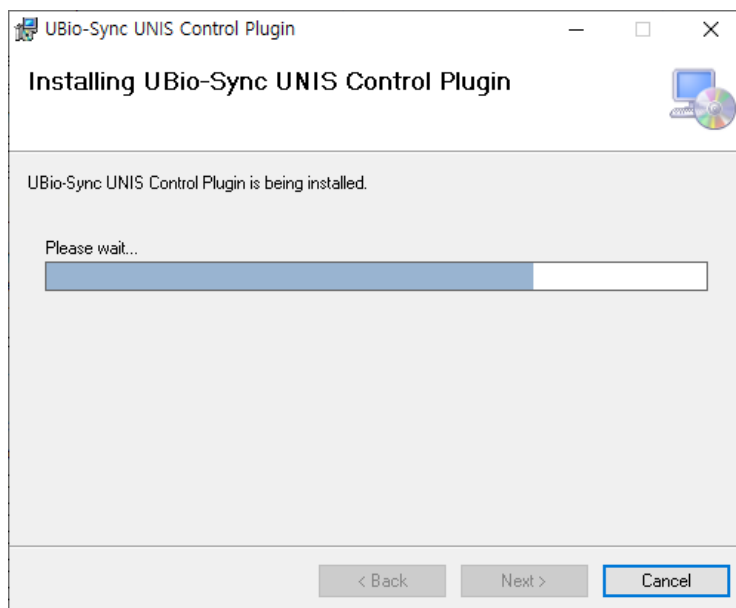
③ Check the installation path in green box. It should be saved in MIPPlugins folder where "XProtect Event Server" is installed on the path where Milestone is installed. Otherwise, when it is saved in other paths, the program would not operate properly



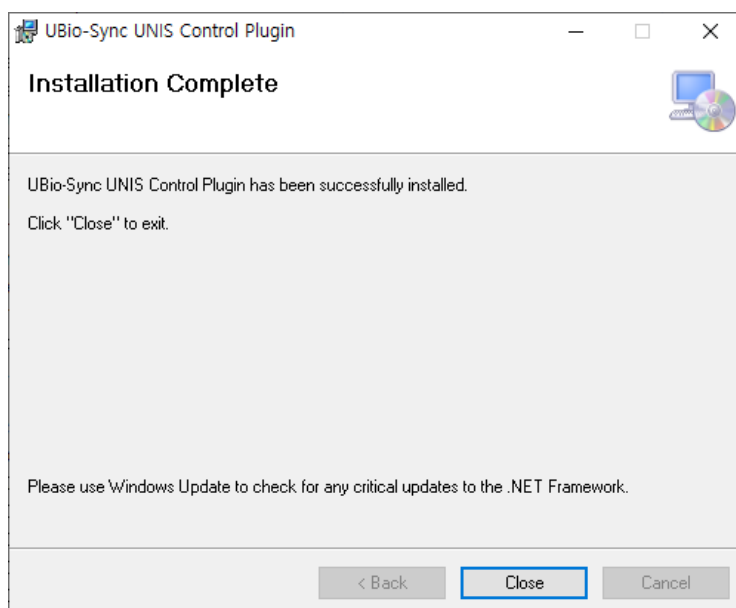
④ Select [Next].



⑤ You can see the window below that it is installing.



⑥ The installation is completed.

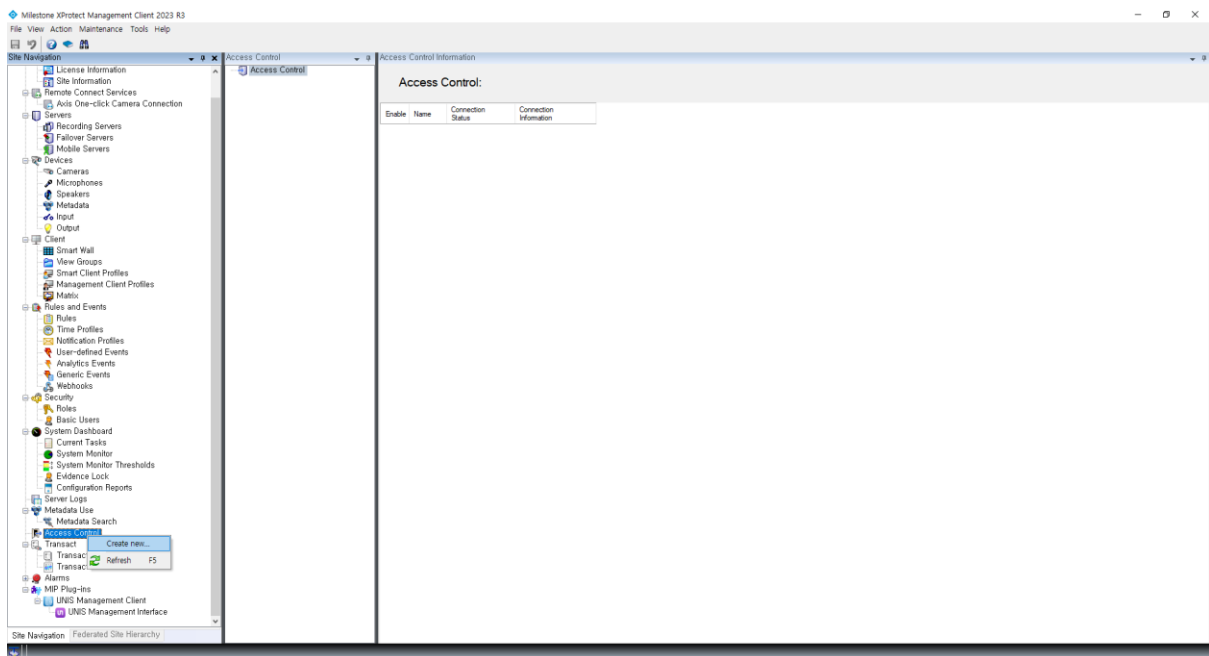


2.2 How to set XProtect Management Client

- ① Double click on "XProtect Management Client" icon to execute.



- ② Right click on [Access Control] and select [Create New] in the left Tree view.



③ You can see UNIS System Integration window

Select [UBio-Sync UNIS_AccessControl] in [Integration plug-in]

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:

UNIS

Integration plug-in:

UBio-Sync UNIS_AccessControl

Address:

127.0.0.1

Port:

9871

Username:

admin

Password:

●●●●

Next

Cancel

[Name]: The name of access control

[Integration plug-in]: Plug-in types

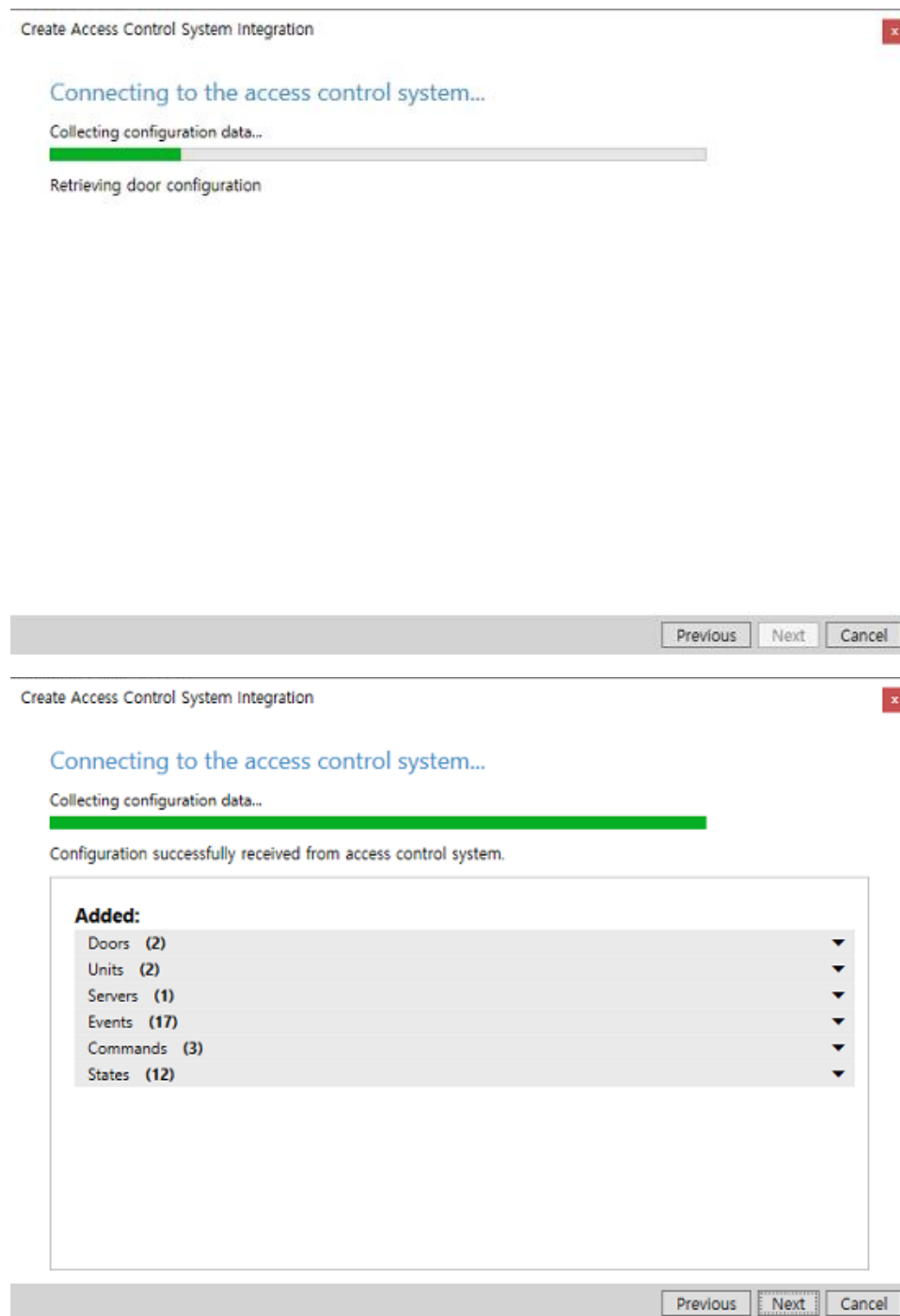
[Address]: IP host where UNIS server is installed

[Port]: UNIS Server connection port

[Username]: ID

[Password]: Master password

- ④ It is connecting to the access control system.



*() shows the value of system configuration status that is set.

- ⑤ Connect the terminal and camera.

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		
FACE	<input checked="" type="checkbox"/>	Pending	<input type="checkbox"/>	
Access point: FACE access point Drop camera here to associate it with the access point				
UBlo-X PRO	<input checked="" type="checkbox"/>	Pending	<input type="checkbox"/>	

Cameras:

DESKTOP-TKBE9S2

Previous

Next

Cancel

- ⑥ The installation for access control connection has been completed.

You have successfully completed the access control system integration

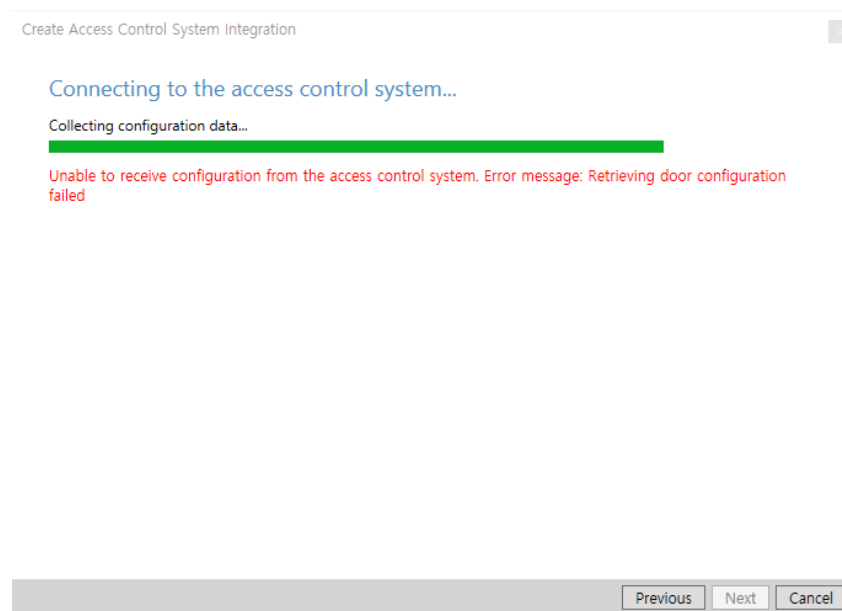
Your XProtect Smart Client users can now monitor access control events. See the help system for how to optimize the XProtect Smart Client for access control system integration.

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

Close

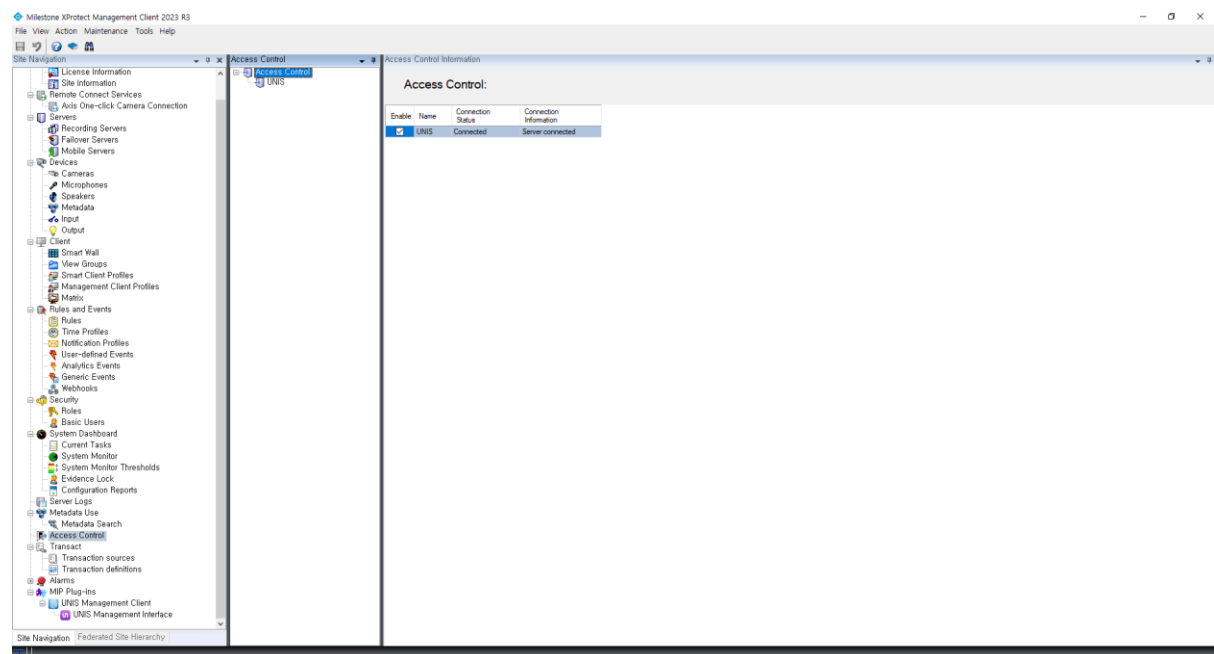
- ⑦ If you get a Retrieving door configuration failed error, please register at least one terminal and

try again.



⑧ You can see that UNIS Access control is added.

Double click on [UNIS] in the list.



⑨ After selecting on [Access Control Events], select [All categories] in [Event Category].

Milestone XProtect Management Client 2023 R3
File View Action Maintenance Tools Help

Site Navigation

License Information

Site Information

Remote Connect Services

Axis One-click Camera Connection

Servers

Recording Servers

Follower Servers

Mobile Servers

Devices

Cameras

Microphones

Speakers

Metadata

Input

Output

Client

Smart Wall

View Groups

Smart Client Profiles

Management Client Profiles

Matrix

Rules and Events

Rules

Time Profiles

Notification Profiles

User-defined Events

Analytics Events

Generic Events

Webhooks

Security

Roles

Basic Users

System Dashboard

Current Tasks

System Monitor

System Monitor Thresholds

Evidence Lock

Configuration Reports

Server Logs

Metadata Use

Metadata Search

Access Control

Transact

Transaction sources

Transaction definitions

Alarms

MP Plug-ins

UWS Management Client

UWS Management Interface

Access Control

Access Control Information

Access control events

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

Enable all

Disable all

Enabled	Access Control Event	Source Type	Event Category
<input checked="" type="checkbox"/>	Access Control Event	Door Unit	All categories
<input checked="" type="checkbox"/>	Authentication failure	Door Unit	All categories
<input checked="" type="checkbox"/>	Authentication success	Door Unit	All categories
<input checked="" type="checkbox"/>	Door Forced open	Door Unit	All categories
<input checked="" type="checkbox"/>	Door open too long	Door Unit	All categories
<input checked="" type="checkbox"/>	External Sensor 1 Start	Door Unit	All categories
<input checked="" type="checkbox"/>	External Sensor 2 Start	Door Unit	All categories
<input checked="" type="checkbox"/>	External Sensor 3 Start	Door Unit	All categories
<input checked="" type="checkbox"/>	External Sensor 4 Start	Door Unit	All categories
<input checked="" type="checkbox"/>	Fire Sensor Start	Access Point	All categories
<input checked="" type="checkbox"/>	Invalid User	Door Unit	All categories
<input checked="" type="checkbox"/>	Lock Error	Door Unit	All categories
<input checked="" type="checkbox"/>	No Permission	Door Unit	All categories
<input checked="" type="checkbox"/>	Panic Sensor Start	Door Unit	All categories
<input checked="" type="checkbox"/>	Server connected	VMD Server	All categories
<input checked="" type="checkbox"/>	Server connecting	VMD Server	All categories
<input checked="" type="checkbox"/>	Server disconnected	VMD Server	All categories
<input checked="" type="checkbox"/>	Terminal Tamper	Access Point	All categories

User-defined Categories...

General Settings

Doors and Associated Cameras

Access Control Events

Access Request Notifications

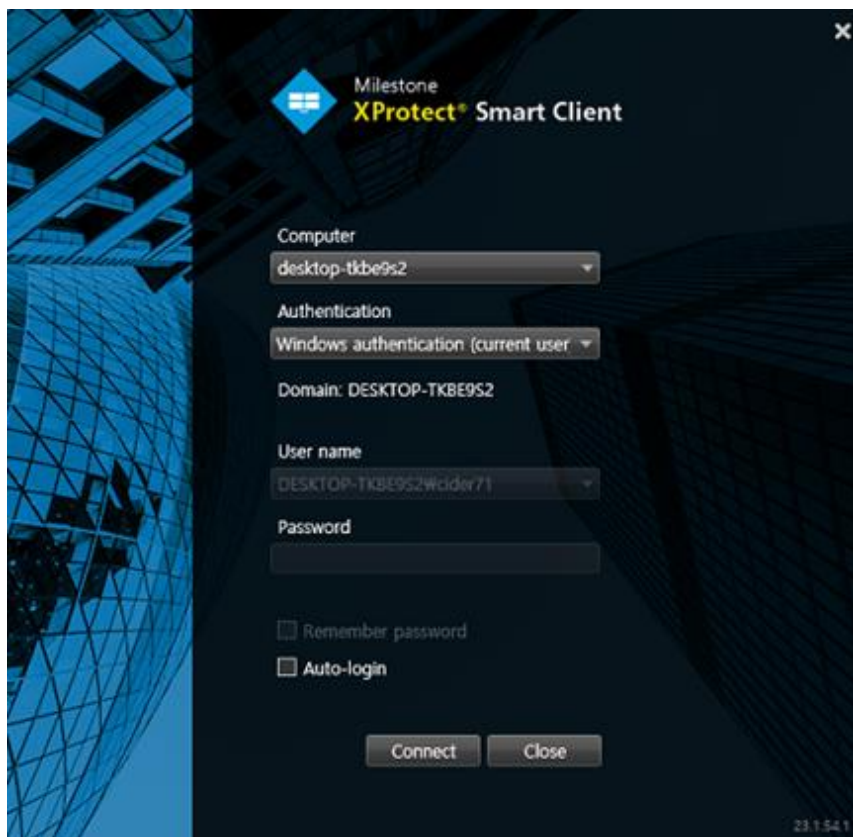
Cardholders

2.3 How to use Milestone XProtect Smart Client

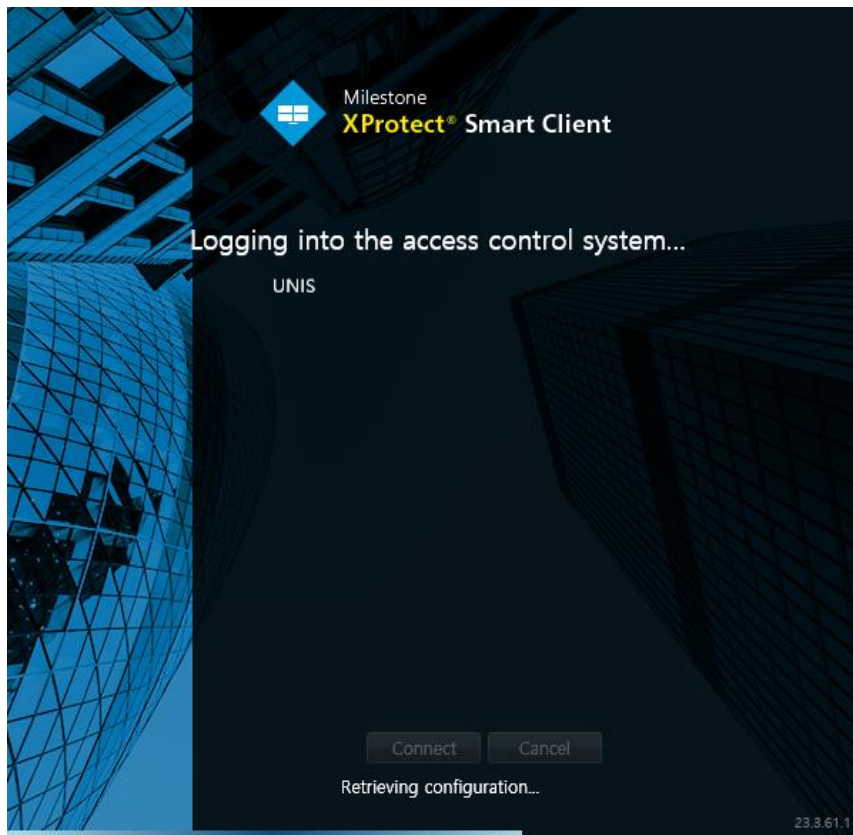
- ① Double click on "XProtect Smart Client" to execute.



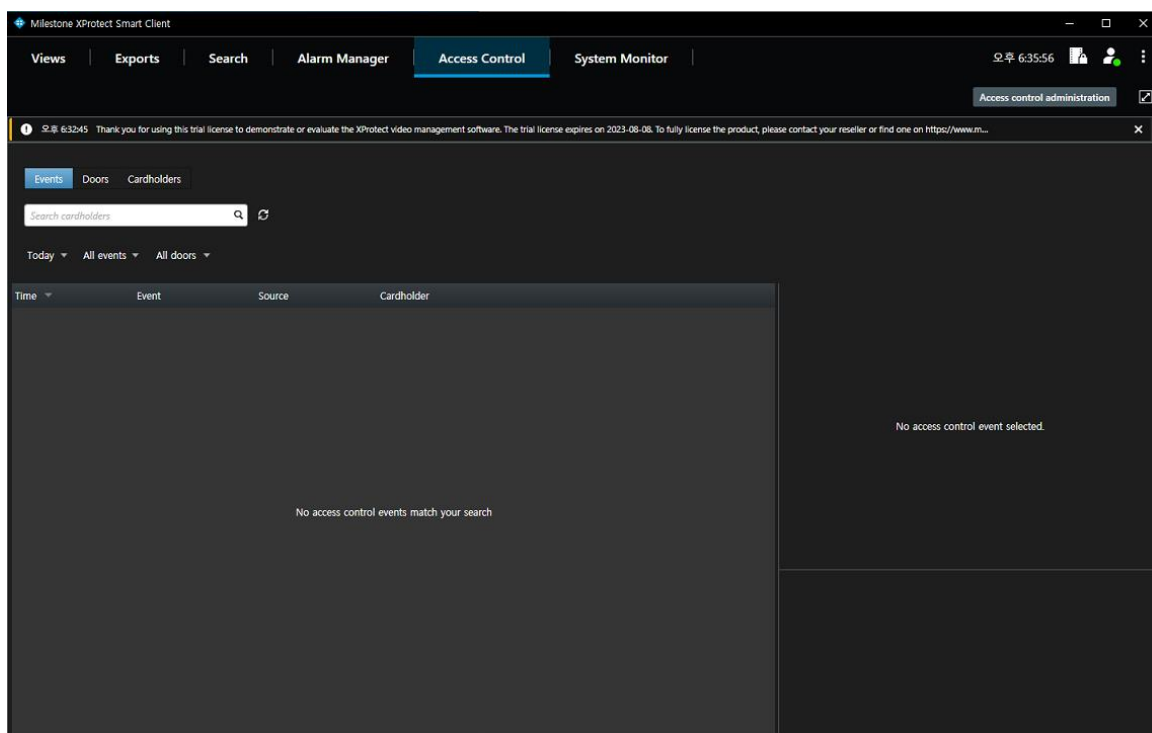
- ② Check the information and select [Connect].



③ It is logging into the access control system.



④ Select [Access Control Tab].

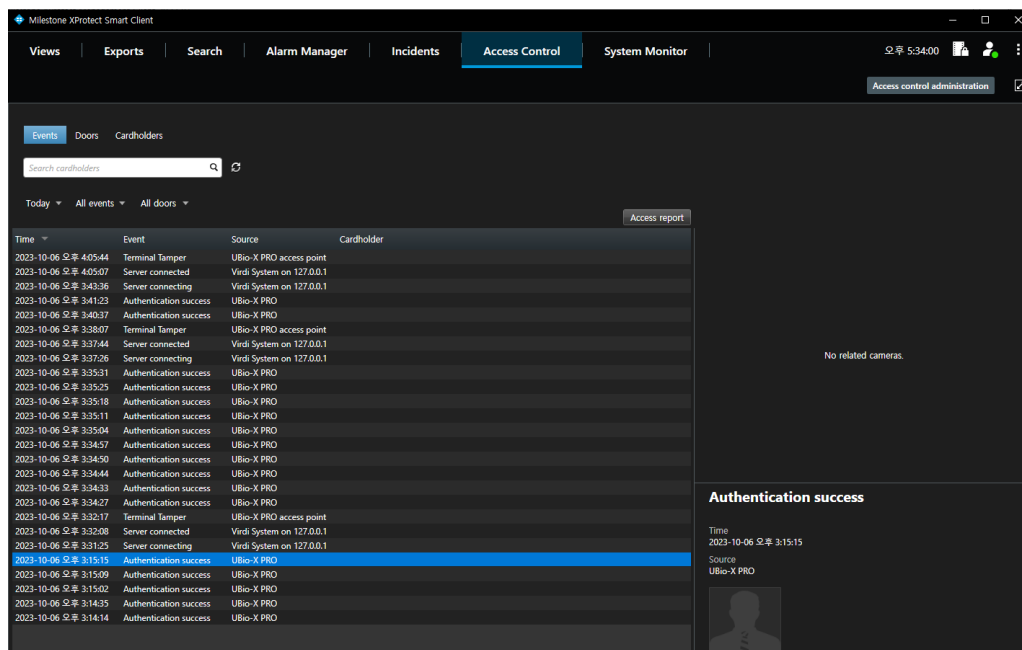


[Events]: Monitor the server connection status, terminal connection status, and user authentication event.

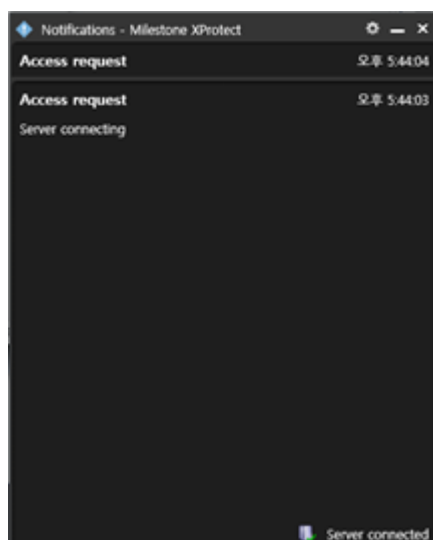
[Doors]: Monitor terminal status

[Cardholders]: User list

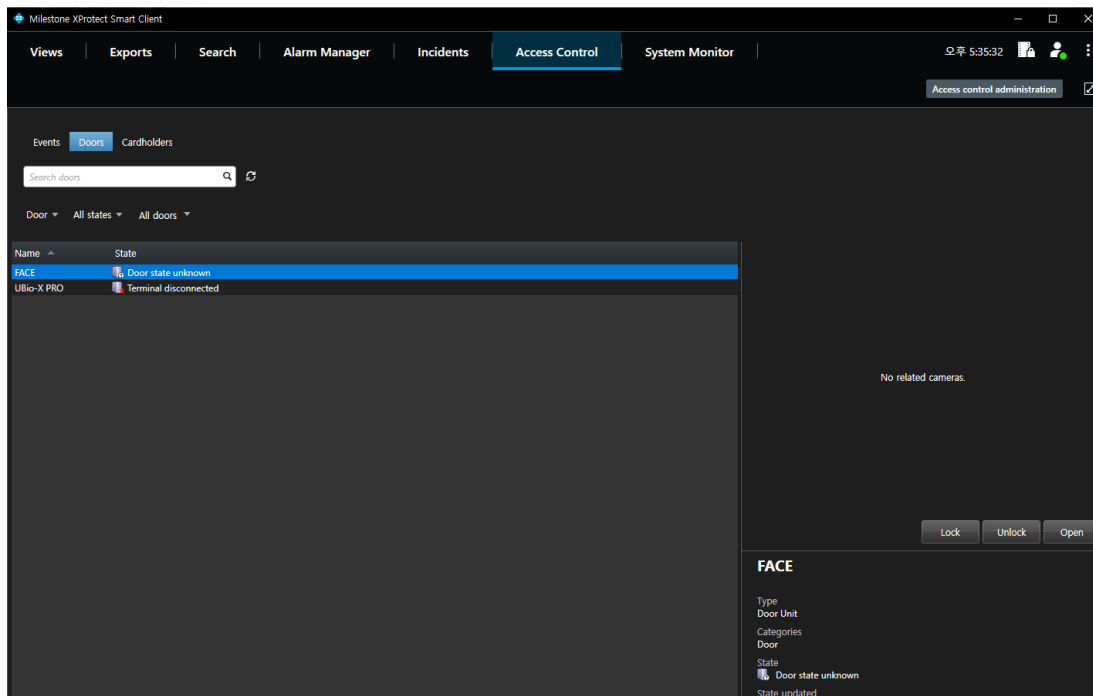
⑤ Click for  updating real-time list.



⑥ After completing all procedure, if the authentication succeeds, you can see the window below.



⑦ After authentication, you can control the status of door.



[Lock] : Locks the terminal status.

[Unlock] : Unlocks the terminal status.

[Open] : Opens the door status during the period of lock setting on the terminals.

⑧ view cardholder events.

