

XProtect

Integration

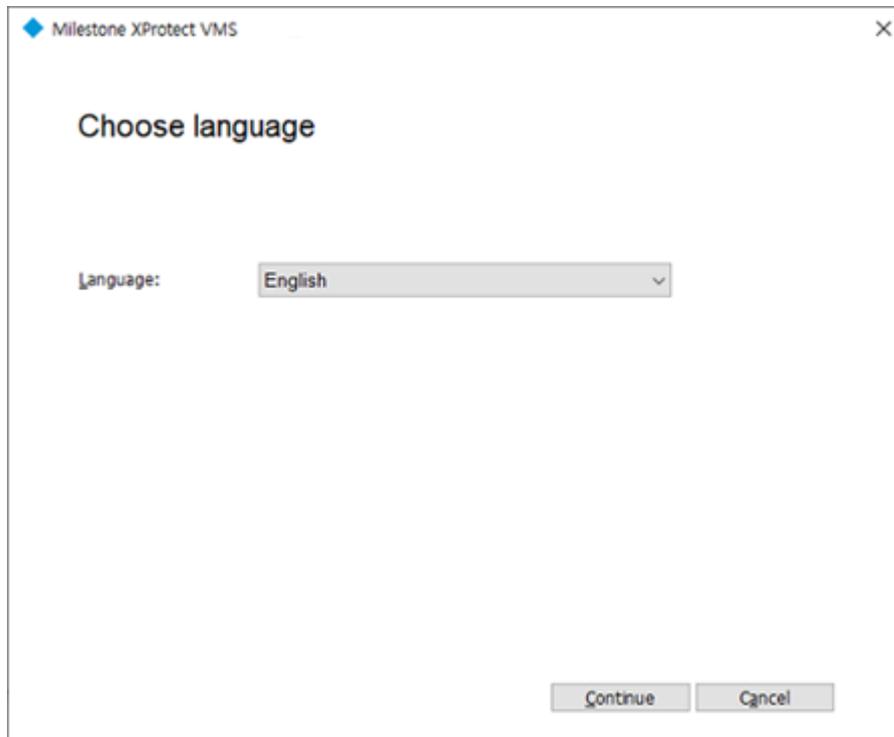
UNION biometrics CO., Ltd

Table of Contents

How to setup XProtect	3
UBio-Sync Alpeta integration.....	8
1. MIP Plug-ins.....	8
1.1. Install UBio-Sync Alpeta Admin Plugin.....	8
1.2 How to use XProtect Management Client	11
2. Access Control.....	17
2.1 Install UBio-Sync Alpeta Control Plugin.....	17
2.2 How to set XProtect Management Client	20
2.3 How to use Milestone XProtect Smart Client	266

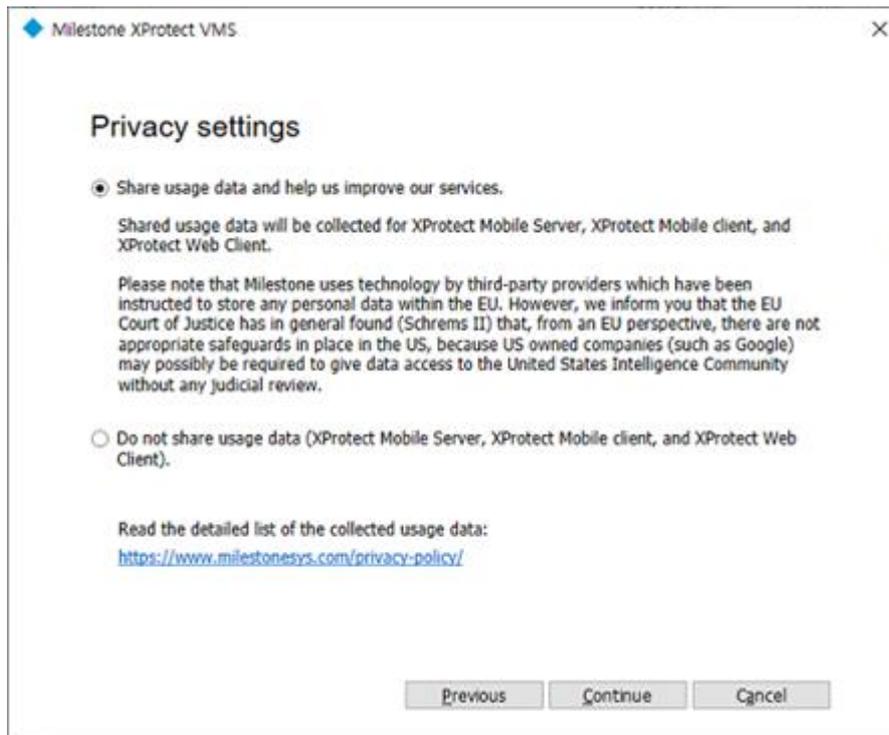
How to setup XProtect

1. Select the language.

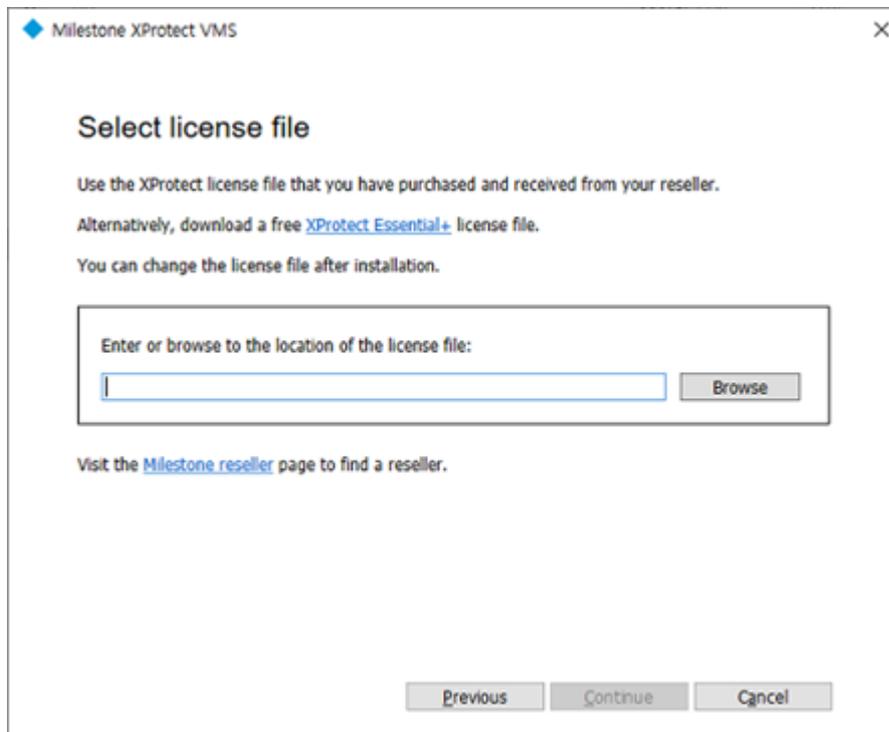


2. Read the agreement and select [Continue].

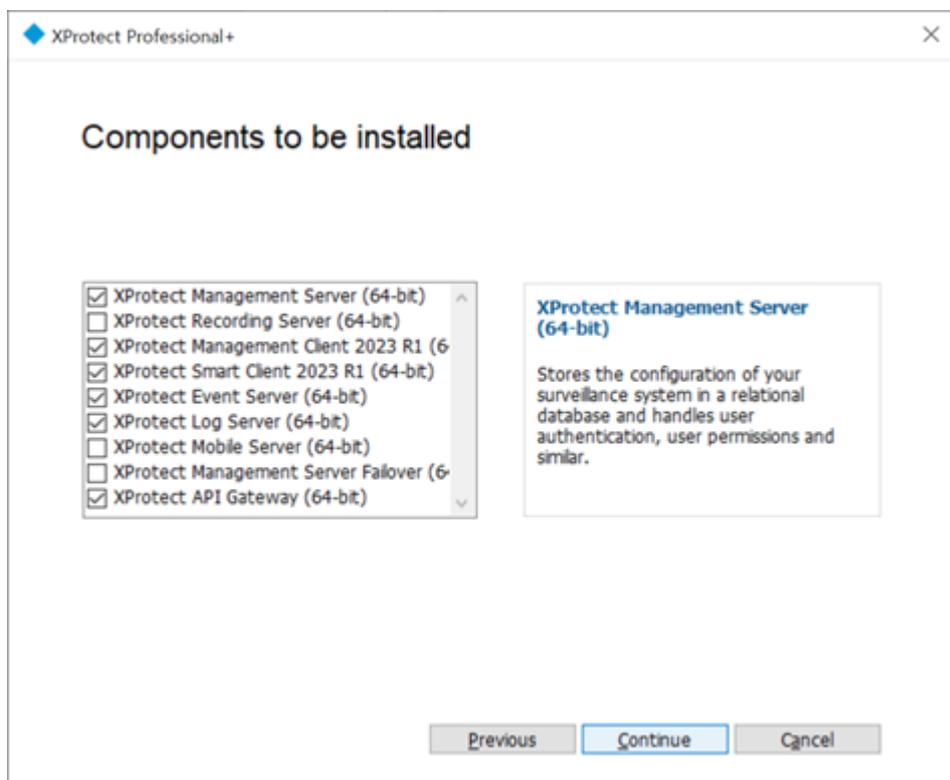
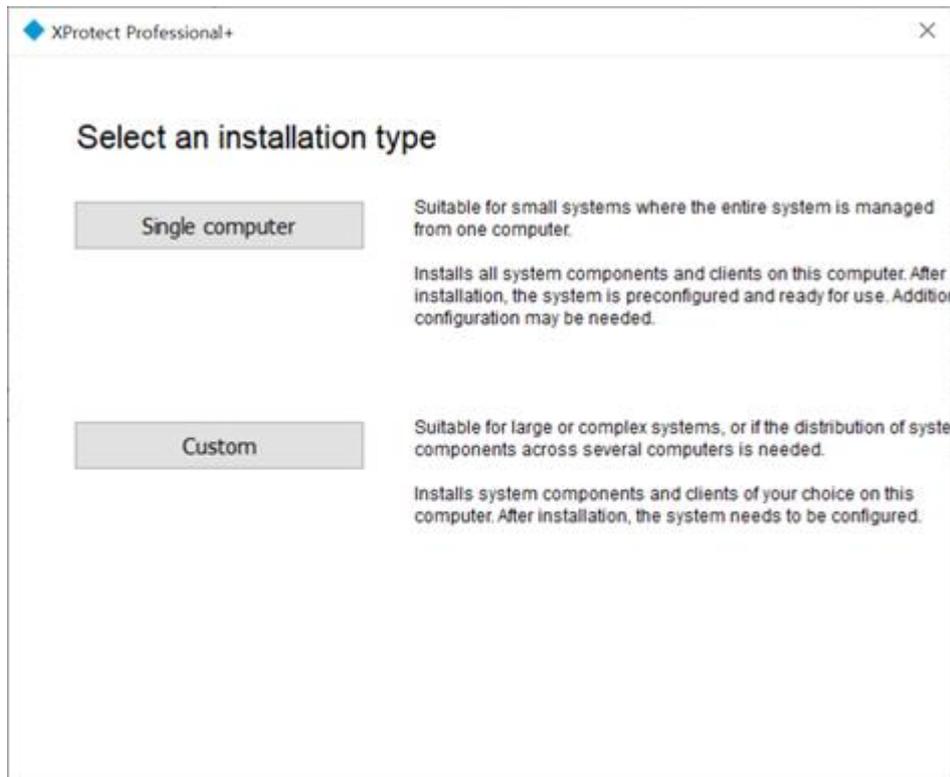




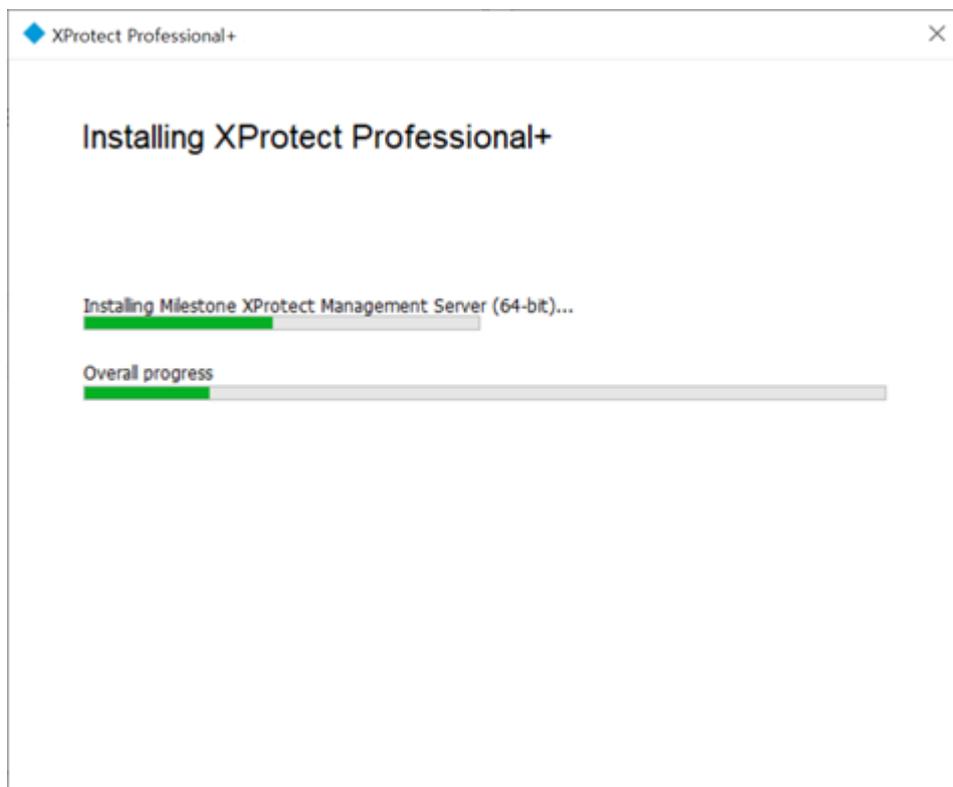
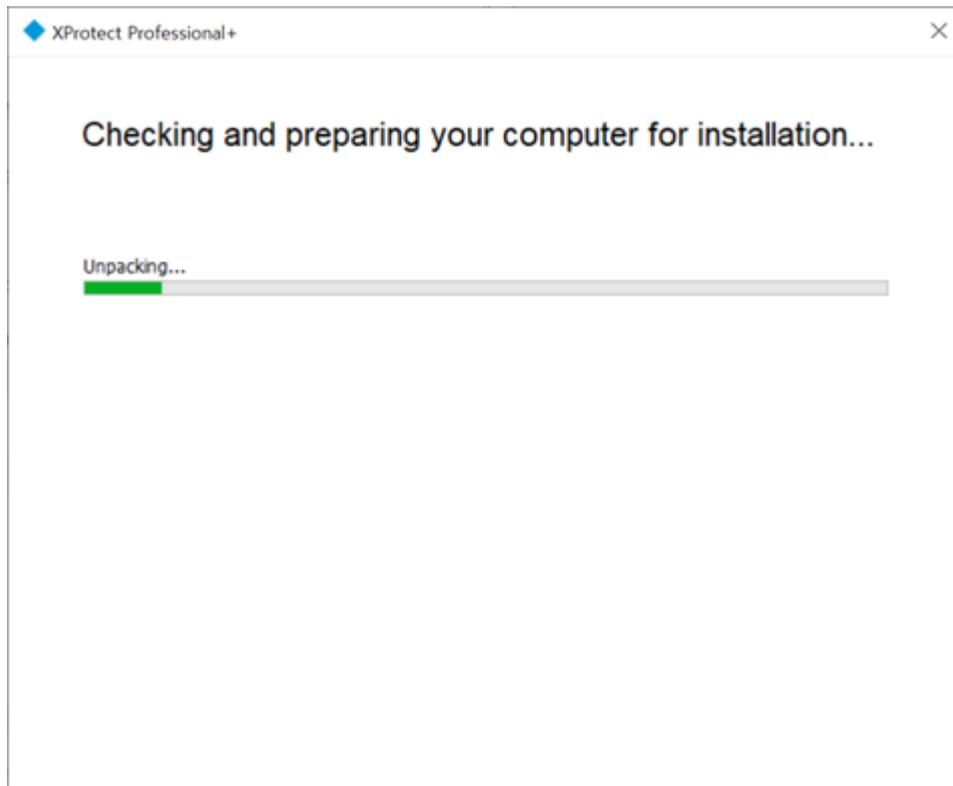
3. Select the path that the program is installed in and [Continue].



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

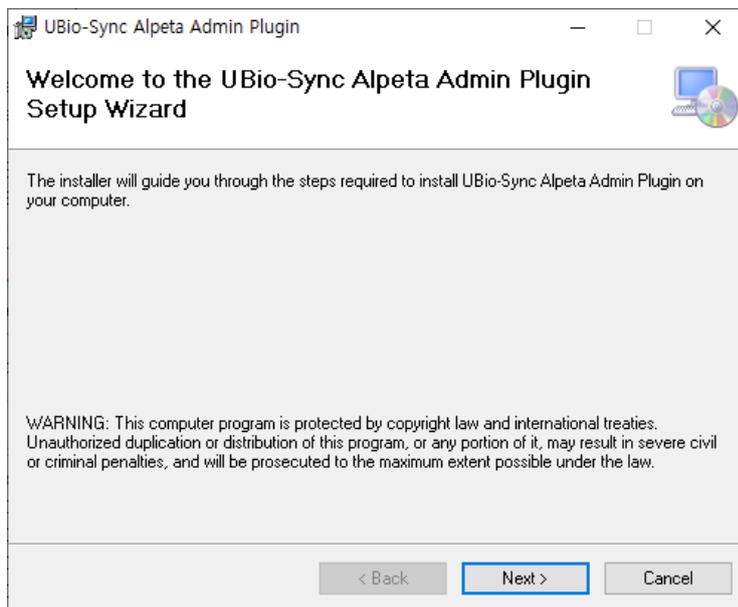
UBio-Sync Alpeta integration

1. MIP Plug-ins

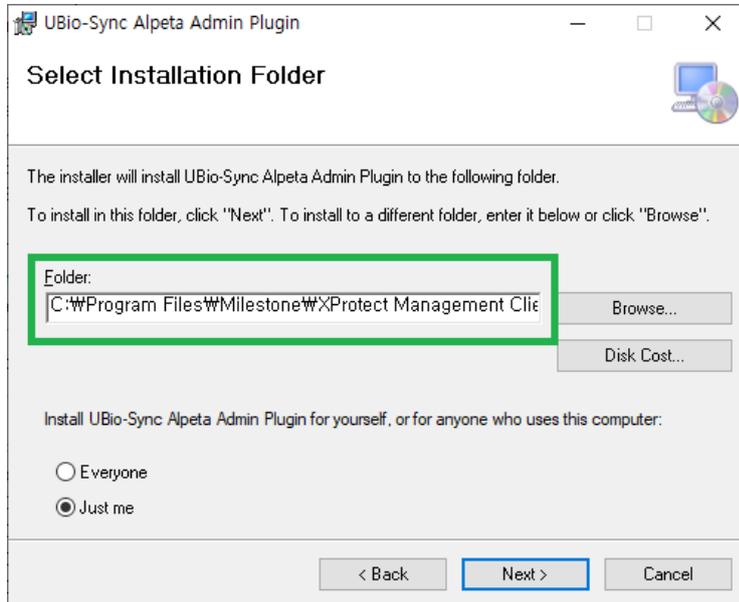
1.1. Install UBio-Sync Alpeta Admin Plugin

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

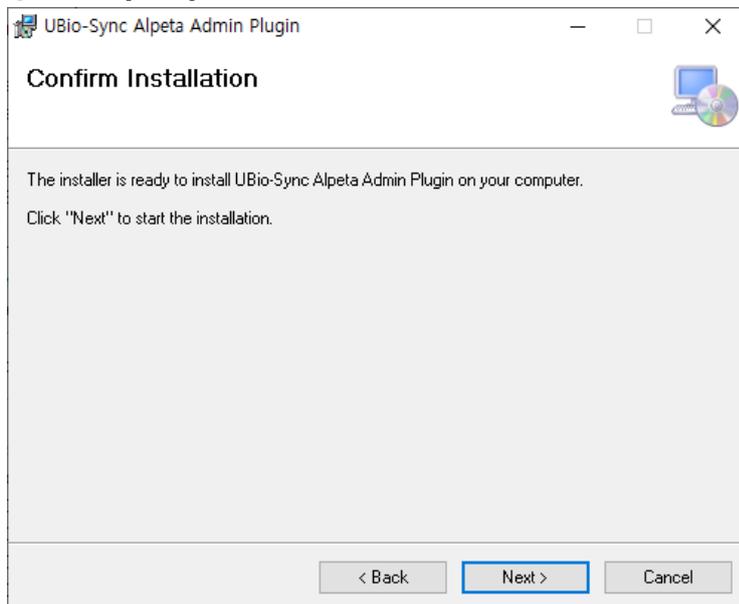
② Select [Next].



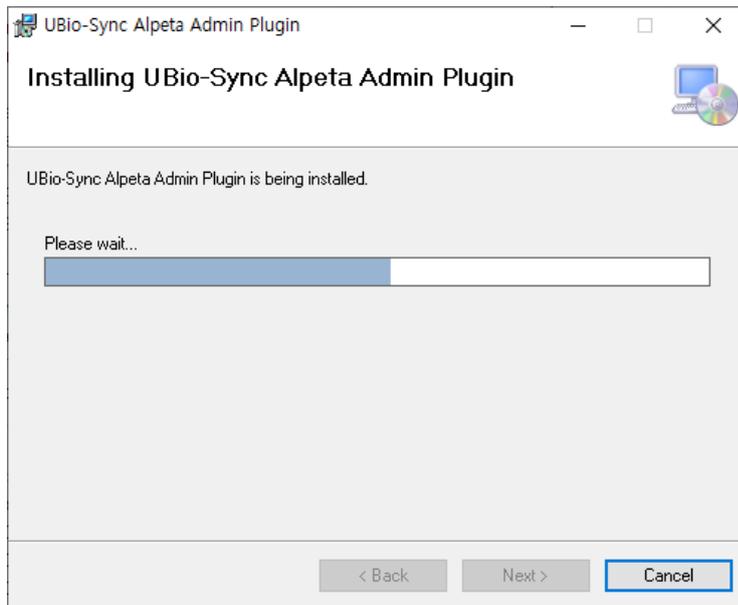
③ Check the installation path in green box. It should be saved in MIPPlugins folder where "VideoOS.Administration.exe" is installed on the path where Milestone is installed. Otherwise, when it is saved in other paths, the program would not operate properly.



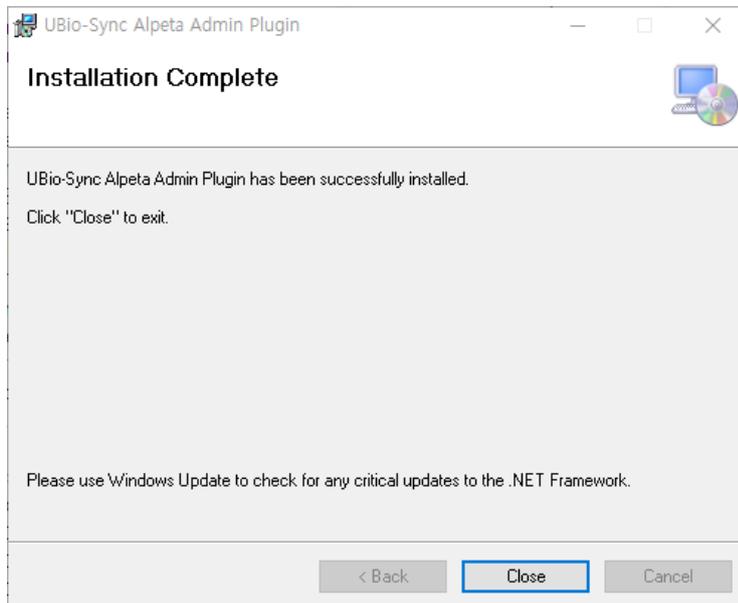
④ Select [Next].



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



⑥ The installation is completed

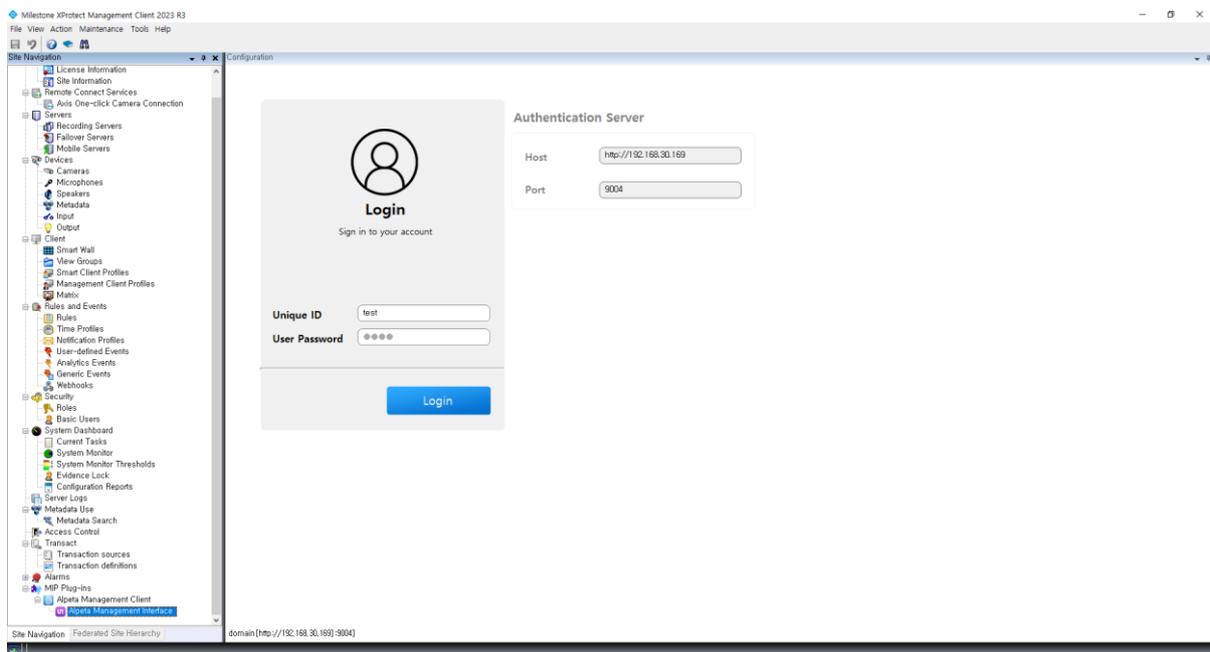


1.2 How to use XProtect Management Client

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



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



[Unique ID]: Alpeta Login Unique ID

[Users Password]: Alpeta Login Password

[Authentication Server]: Authentication server connection information

1. Alpeta login screen



Users, groups, terminals, authentication logs information

2. Users

ID	Name	Unique ID	Privilege	GroupName	Access Group	Title	Auth Info	FP 1:N	FA 1:N	BlackList
00000001			User	---	---			OFF	OFF	OFF
00000002	unique	1234	Display Board	ttt	---		PW	OFF	OFF	OFF
00000003	asdasdsda		User	ttt	---		PW	OFF	OFF	OFF
00000004	admin	admin	Admin	ttt	---		PW	OFF	OFF	OFF
00000005	aaaaa		User	ttt	---		PW	OFF	OFF	OFF
00000006	testAdmin	testadmin	Admin	ttt	---		PW	OFF	OFF	OFF
00000007	face	test	Admin	ttt	---		/ PW FAW	OFF	OFF	OFF
00000010	not	0010	User	---	---		PW	ON	ON	OFF
00000011	asdasdsadsa		User	---	---		FP	ON	ON	OFF
00000012	QRTEST	0012	User	---	---		/ PW FAW	ON	ON	OFF
00000013	test13	0013	User	---	---		PW	ON	ON	OFF

[Add] : Select if you want to add the new user

User Info (UBio Alpha)

Save

Basic | Auth | Access | Management | Etc

Auth Info: AND Auth, OR Auth, Modify

Privilege: User

Regulation period: No restriction period, Access allowed period, Restriction period

Expiration Date: Regist Date: 2025-03-28 00:00, Expired date: 2025-03-28 23:59

User Name:

User ID: 00000008 ✓

Unique ID: Duplicate Check

[Delete] : Check Delete selected user

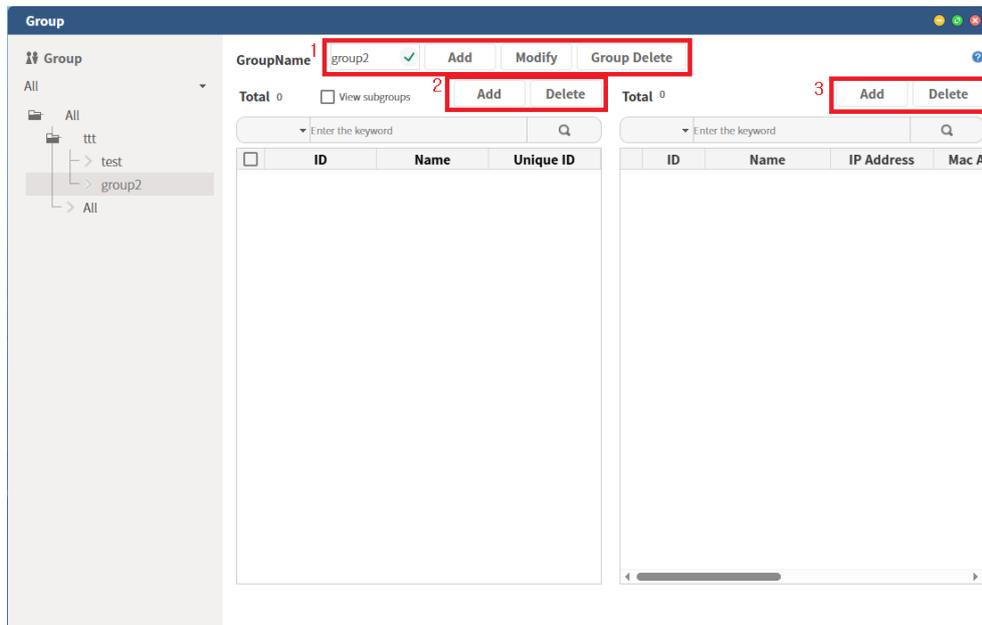
ID	Name	Unique ID	Privilege	GroupName	Access Group	Title	Auth Info	FP 1:N	FA 1:N	BlackList
00000001			User	---	---			OFF	OFF	OFF
00000002	unique	1234	Display Board	ttt	---		PW	OFF	OFF	OFF
00000003	asdasdsda		User	ttt	---		PW	OFF	OFF	OFF
00000004	admin	admin	Admin	ttt	---		PW	OFF	OFF	OFF
<input checked="" type="checkbox"/>	00000005	aaaaa	User	ttt	---		PW	OFF	OFF	OFF
00000006	testAdmin	testadmin	Admin	ttt	---		PW	OFF	OFF	OFF
00000007	face	test	Admin	ttt	---		/ PW FAW	OFF	OFF	OFF
00000010	not	0010	User	---	---		PW	ON	ON	OFF
00000011	asdasdsadsa		User	---	---		FP	ON	ON	OFF
00000012	QRTEST	0012	User	---	---		/ PW FAW	ON	ON	OFF
00000013	test13	0013	User	---	---		PW	ON	ON	OFF

confirm

Are you sure you want to delete it?

OK Cancel

3. Group

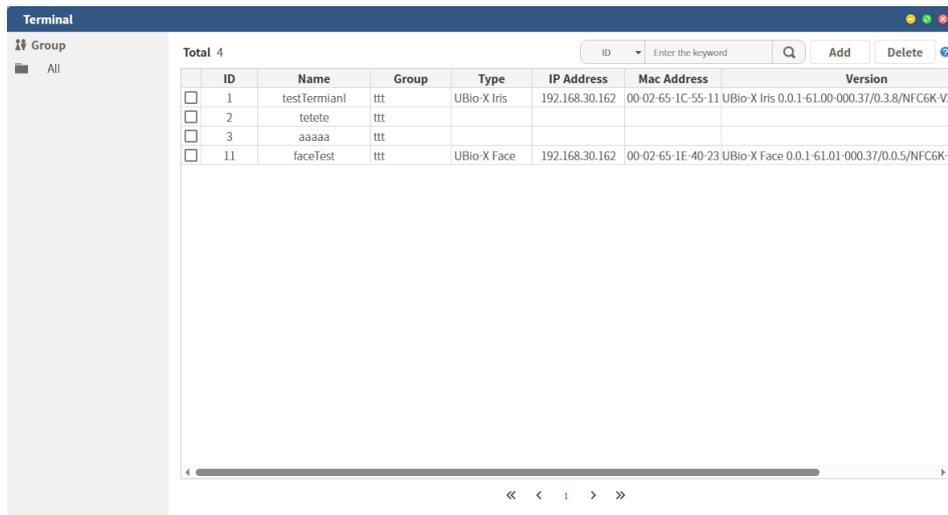


[1] : Group management

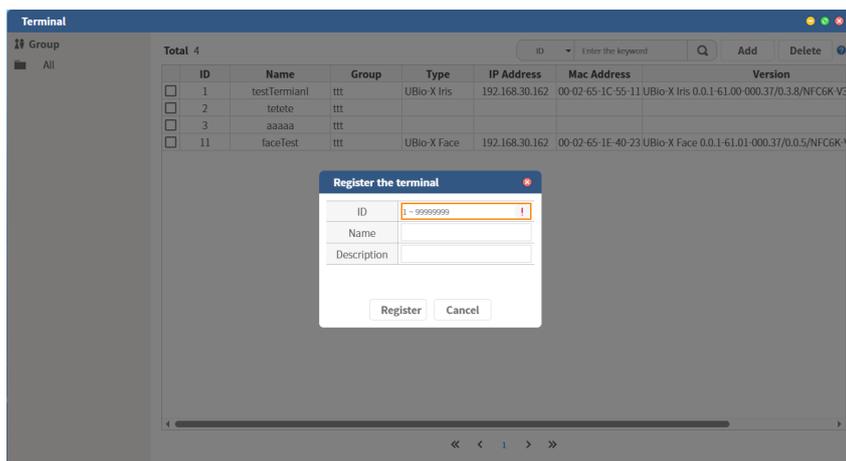
[2] : Users in group management

[3] : Terminals in group management

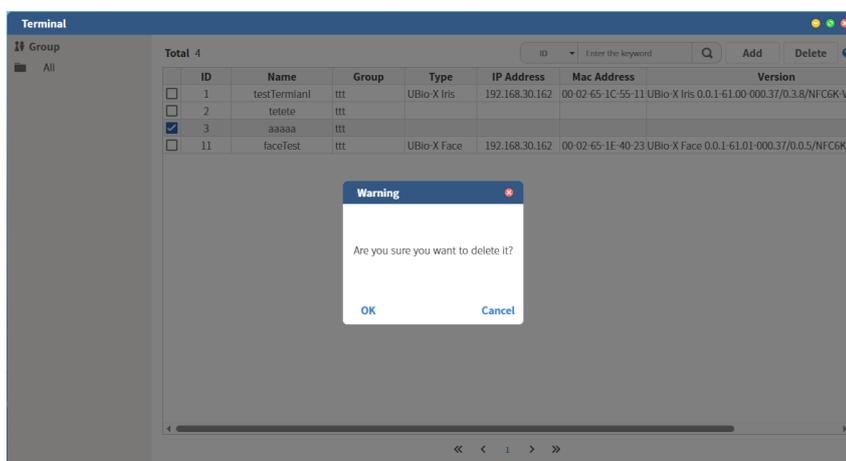
4. Terminal



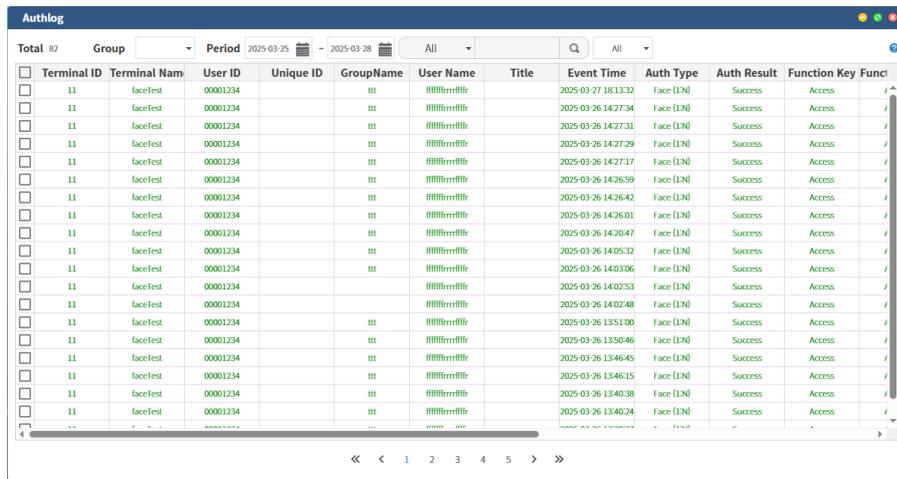
[Add] : Select if you want to add the terminal.



[Delete] : Delete the selected terminals.



5. Authlog



The screenshot shows the 'Authlog' application window. At the top, there is a header bar with the title 'Authlog'. Below the header, there is a toolbar with various controls: a 'Total' label showing '82', a 'Group' dropdown menu, a 'Period' section with date pickers for '2025-03-25' and '2025-03-28', a filter dropdown set to 'All', and a search input field. The main area is a table with the following columns: Terminal ID, Terminal Name, User ID, Unique ID, GroupName, User Name, Title, Event Time, Auth Type, Auth Result, and Function Key. The table contains 20 rows of data, all showing successful authentication events. The 'Auth Result' column consistently displays 'Success' and the 'Function Key' column displays 'Access'. The 'Event Time' column shows a sequence of timestamps from 2025-03-27 18:13:32 to 2025-03-26 13:40:24. At the bottom of the window, there is a pagination control with arrows and page numbers 1, 2, 3, 4, 5.

Terminal ID	Terminal Name	User ID	Unique ID	GroupName	User Name	Title	Event Time	Auth Type	Auth Result	Function Key	Funct
11	faceTest	00001234		tit	#####		2025-03-27 18:13:32	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:27:34	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:27:31	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:27:29	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:27:17	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:26:59	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:26:42	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:26:01	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:20:47	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:05:32	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:03:06	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:02:53	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 14:02:48	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 13:51:00	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 13:50:46	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 13:46:45	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 13:46:15	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 13:40:38	Face (LNO)	Success	Access	/
11	faceTest	00001234		tit	#####		2025-03-26 13:40:24	Face (LNO)	Success	Access	/

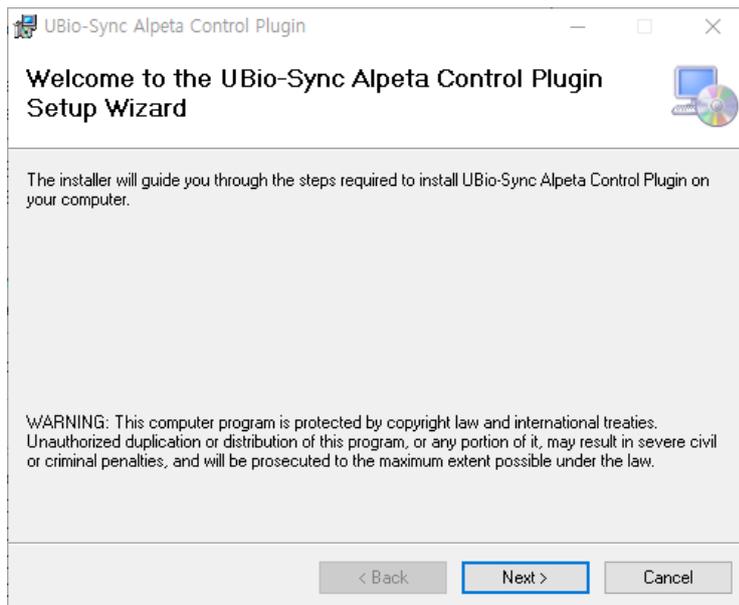
This window shows the access authentication record logs.

2. Access Control

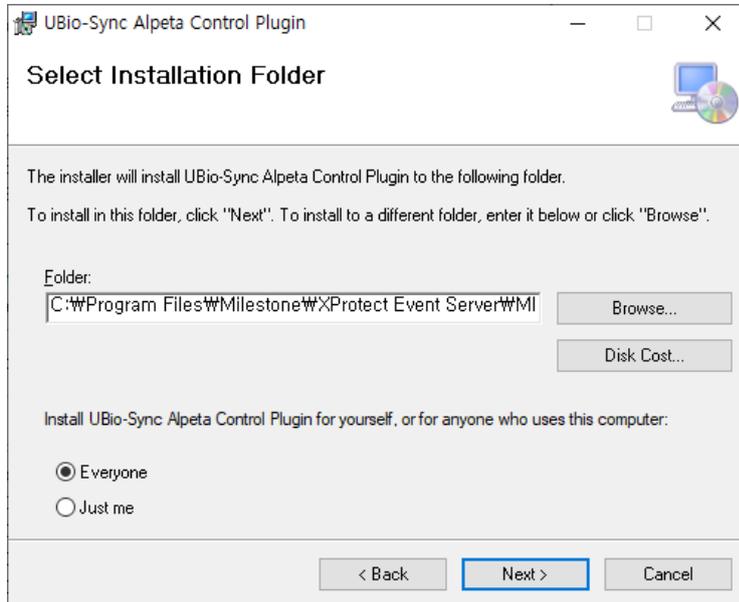
2.1 Install UBio-Sync Alpeta Control Plugin

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

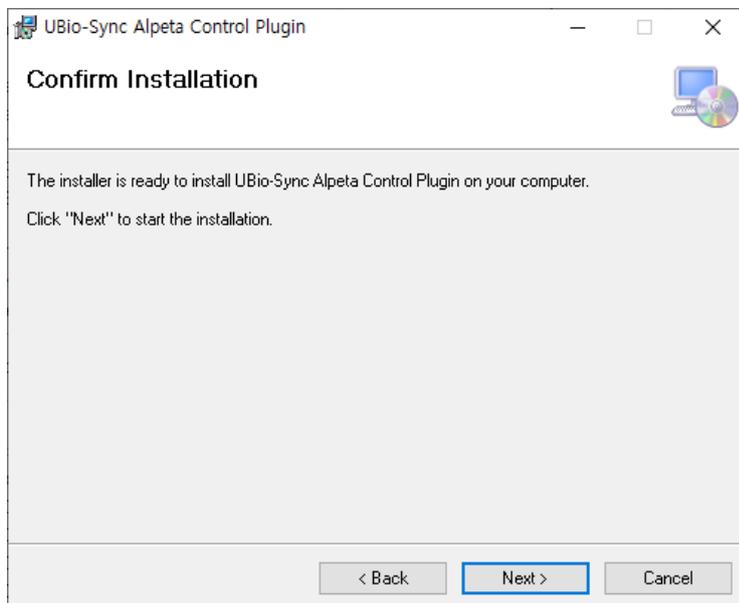
② Select [Next]



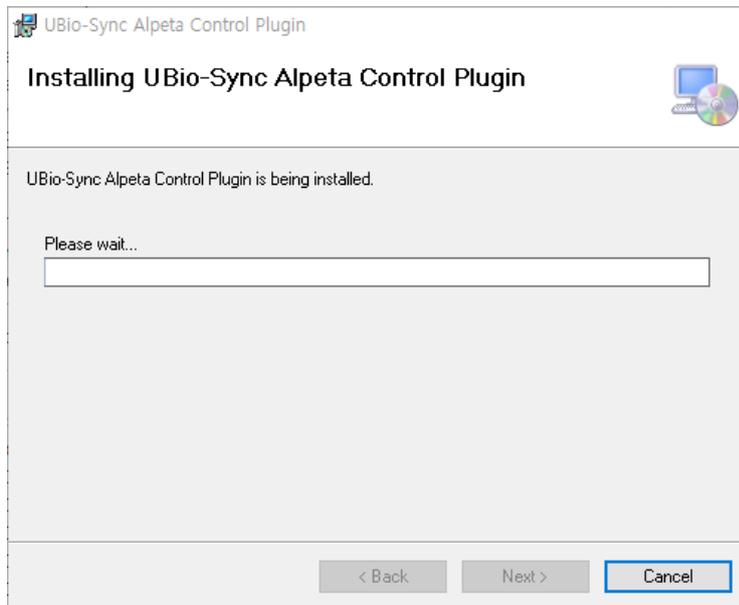
③ Check the installation path in green box. It should be saved in MIPPlugins folder where "XProtect Event Server" is installed on the path where Milestone is installed. Otherwise, when it is saved in other paths, the program would not operate properly



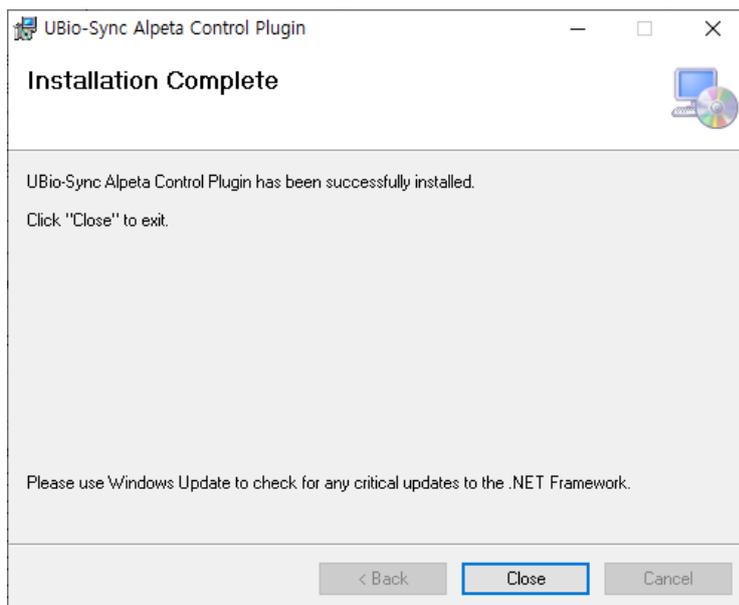
④ Select [Next].



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



⑥ The installation is completed.

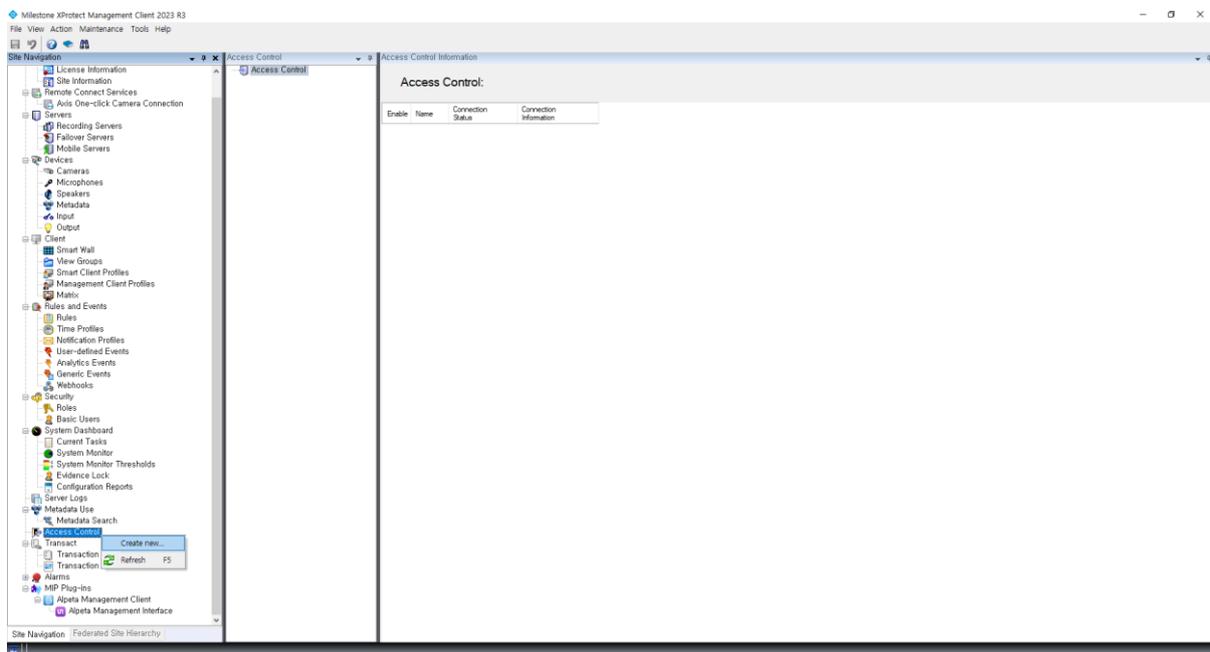


2.2 How to set XProtect Management Client

- 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 Alpetra System Integration window

Select [UBio-Sync Alpetra_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:

Integration plug-in:

Address:

Port:

Username:

Password:

[Name]: The name of access control

[Integration plug-in]: Plug-in types

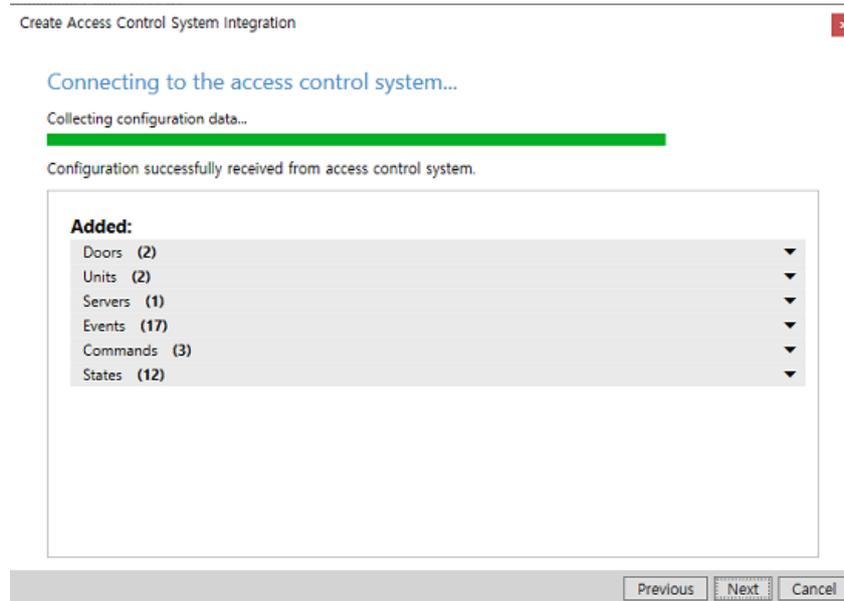
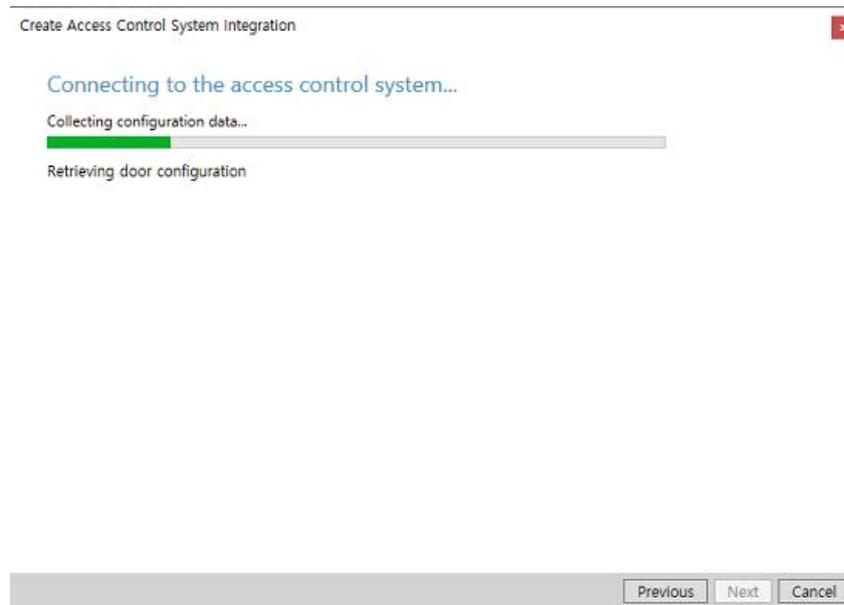
[Address]: Alpetra server domain address

[Port]: Alpetra Server connection port

[Username]: Alpetra user unique ID

[Password]: Alpetra user remote access 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

UBio-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.

Connecting to the access control system...

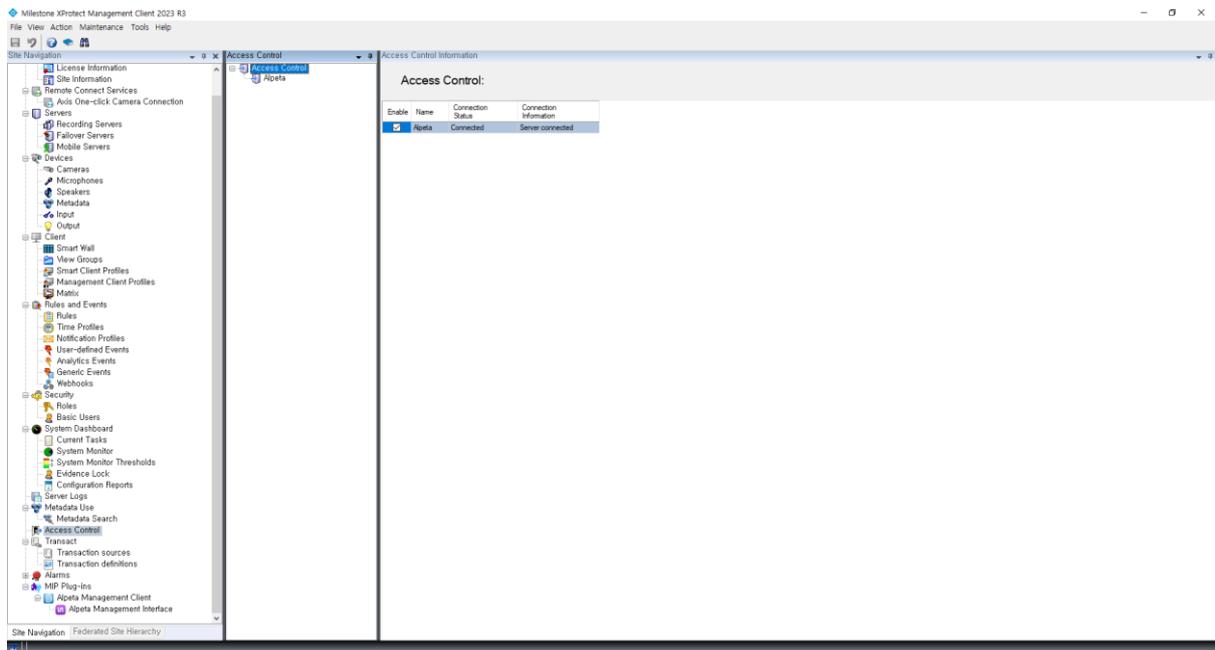
Collecting configuration data...

Unable to receive configuration from the access control system. Error message: Retrieving door configuration failed

Previous Next Cancel

⑧ You can see that Alpeta Access control is added.

Double click on [Alpeta] 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: 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"/>	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	Wifi Server	All categories
<input checked="" type="checkbox"/>	Server connecting	Wifi Server	All categories
<input checked="" type="checkbox"/>	Server disconnected	Wifi Server	All categories
<input checked="" type="checkbox"/>	Terminal Tamper	Access Point	All categories

User-defined Categories...

Site Navigation: Federated Site Hierarchy

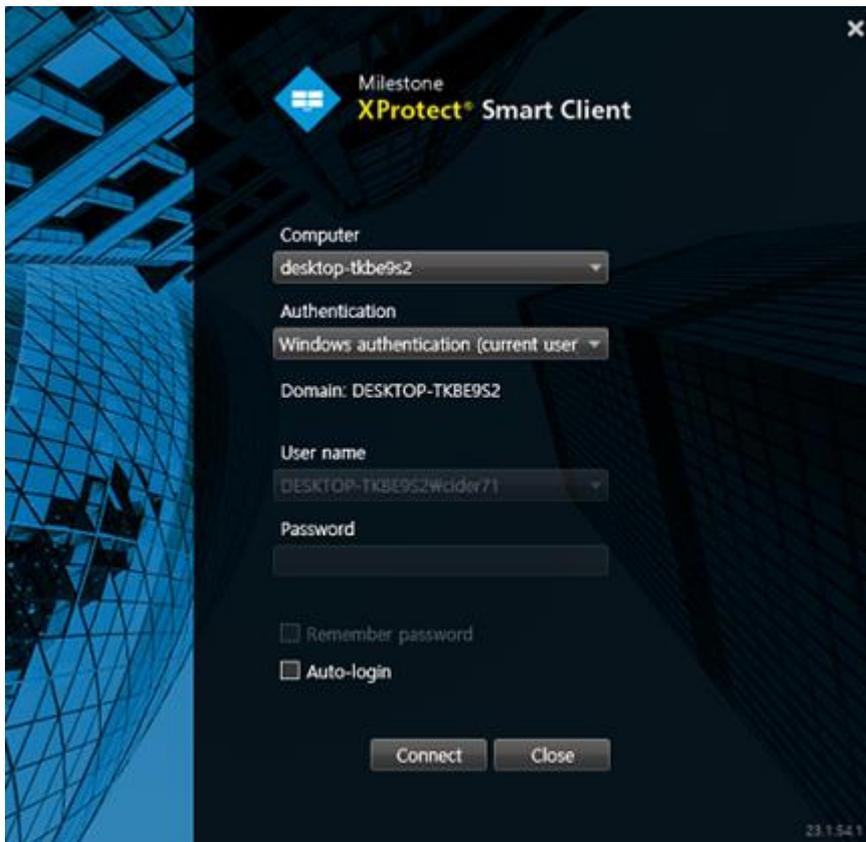
General Settings Doors and Associated Camera Access Control Events Access Request Notifications Cardholders

2.3 How to use Milestone XProtect Smart Client

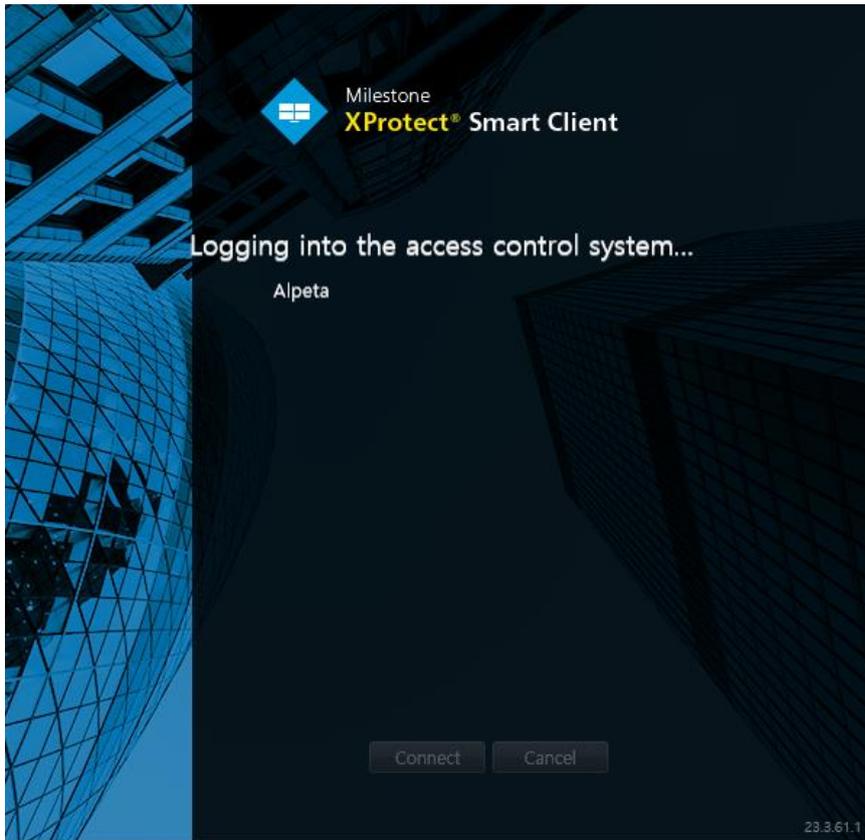
- ① Double click on "XProtect Smart Client" to execute.



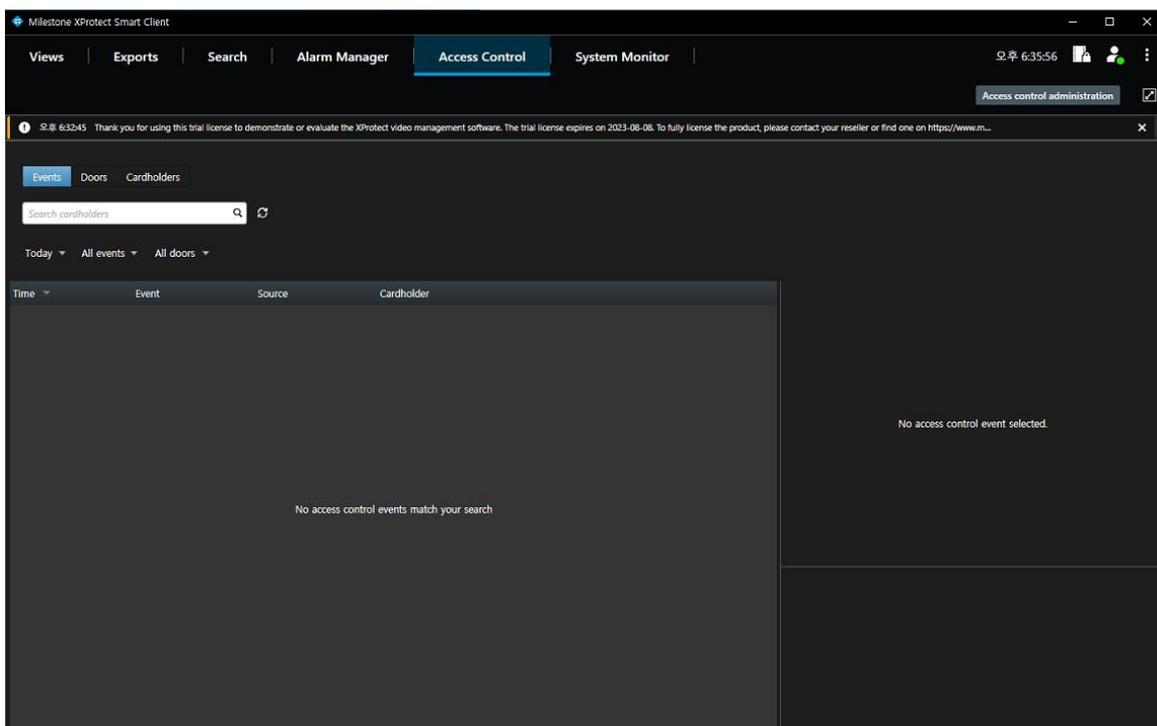
- ② Check the information and select [Connect].



③ It is logging into the access control system.



④ Select [Access Control Tab].

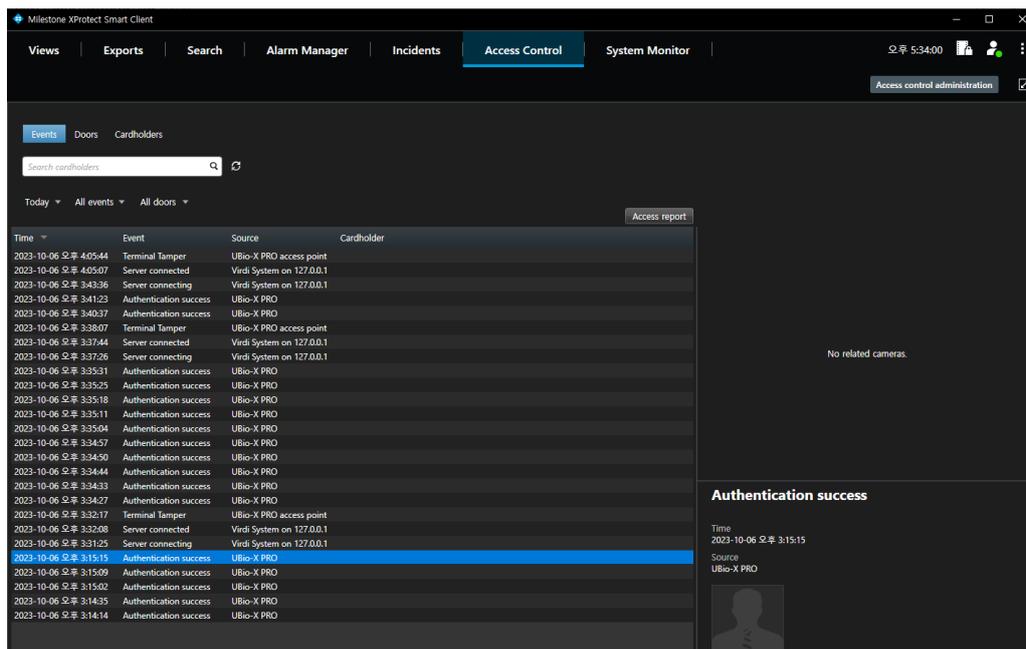


[Events]: Monitor the server connection status, terminal connection status, and user authentication event.

[Doors]: Monitor terminal status

[Cardholders]: User list

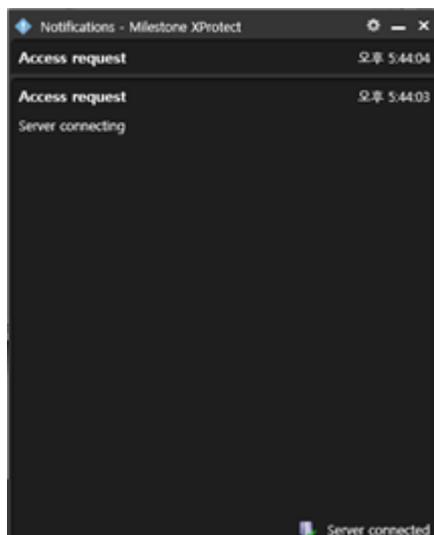
⑤ Click for  updating real-time list.



The screenshot shows the Milestone XProtect Smart Client interface. The 'Access Control' tab is active, displaying a list of events. The event list includes columns for Time, Event, Source, and Cardholder. A search bar and a refresh icon are visible above the list. A detailed view of an 'Authentication success' event is shown on the right, including the time (2023-10-06 오후 3:15:15) and source (UBio-X PRO).

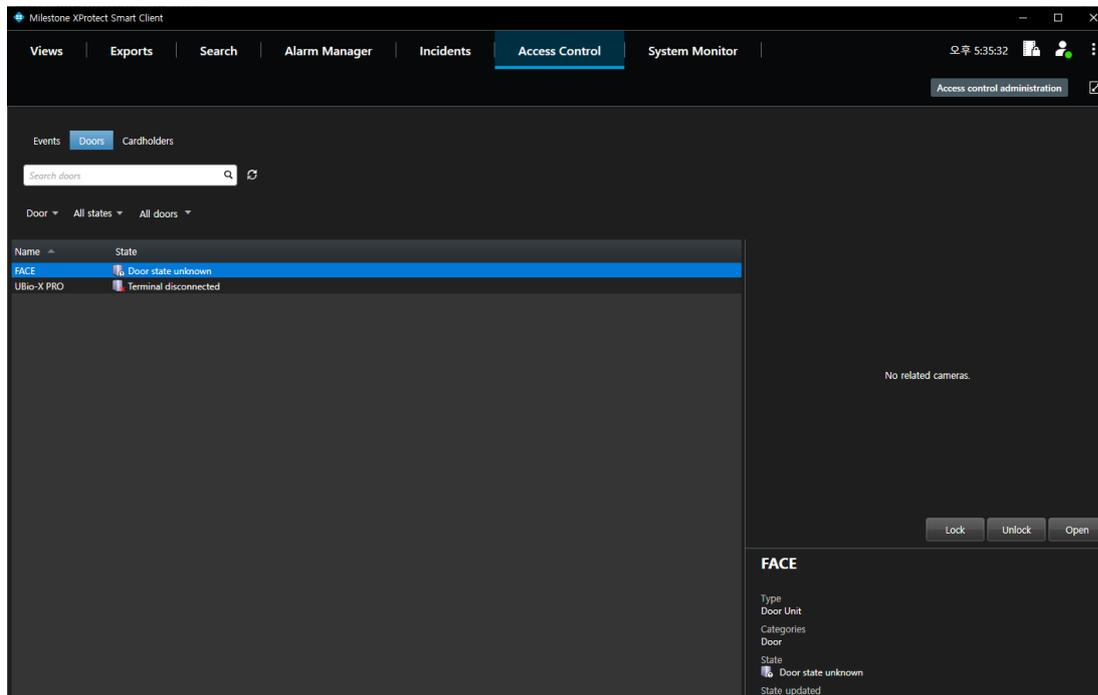
Time	Event	Source	Cardholder
2023-10-06 오후 4:05:44	Terminal Tamper	UBio-X PRO access point	
2023-10-06 오후 4:05:07	Server connected	Virdi System on 127.0.0.1	
2023-10-06 오후 3:43:36	Server connecting	Virdi System on 127.0.0.1	
2023-10-06 오후 3:41:23	Authentication success	UBio-X PRO	
2023-10-06 오후 3:40:37	Authentication success	UBio-X PRO	
2023-10-06 오후 3:38:07	Terminal Tamper	UBio-X PRO access point	
2023-10-06 오후 3:37:44	Server connected	Virdi System on 127.0.0.1	
2023-10-06 오후 3:37:26	Server connecting	Virdi System on 127.0.0.1	
2023-10-06 오후 3:35:31	Authentication success	UBio-X PRO	
2023-10-06 오후 3:35:25	Authentication success	UBio-X PRO	
2023-10-06 오후 3:35:18	Authentication success	UBio-X PRO	
2023-10-06 오후 3:35:11	Authentication success	UBio-X PRO	
2023-10-06 오후 3:35:04	Authentication success	UBio-X PRO	
2023-10-06 오후 3:34:57	Authentication success	UBio-X PRO	
2023-10-06 오후 3:34:50	Authentication success	UBio-X PRO	
2023-10-06 오후 3:34:44	Authentication success	UBio-X PRO	
2023-10-06 오후 3:34:33	Authentication success	UBio-X PRO	
2023-10-06 오후 3:34:27	Authentication success	UBio-X PRO	
2023-10-06 오후 3:32:17	Terminal Tamper	UBio-X PRO access point	
2023-10-06 오후 3:32:08	Server connected	Virdi System on 127.0.0.1	
2023-10-06 오후 3:31:25	Server connecting	Virdi System on 127.0.0.1	
2023-10-06 오후 3:15:15	Authentication success	UBio-X PRO	
2023-10-06 오후 3:15:09	Authentication success	UBio-X PRO	
2023-10-06 오후 3:15:02	Authentication success	UBio-X PRO	
2023-10-06 오후 3:14:35	Authentication success	UBio-X PRO	
2023-10-06 오후 3:14:14	Authentication success	UBio-X PRO	

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



The screenshot shows a notification window titled 'Notifications - Milestone XProtect'. It displays a list of notifications: 'Access request' at 5:44:04, 'Access request' at 5:44:03, and 'Server connecting'. At the bottom, a status bar indicates 'Server connected'.

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.

Milestone XProtect Smart Client

Views | Exports | Search | Alarm Manager | Incidents | **Access Control** | System Monitor

오후 5:52:18

Access control administration

오후 5:44:03 The configuration of the access control system 'VIRDI' has been changed. You can continue working.

Events | Doors | **Cardholders**

Search cardholders

Name	Type
1:	General User
2: kim	General User
3:	General User
30: test	General User

 **k**

Card id
1290000-102565

View cardholder events