suprema

BioStar 2 Integration for Milestone XProtect

SETUP GUIDE

Version 1.2 English

Contents

Target Audience	3
Introduction	4
System diagram	4
Structural differences between BioStar 2 and XProtect	5
Functionalities	5
Installation	6
Prereguisites	
Configuration procedure	7
Installing the BioStar 2 Integration for Milestone XProtect	
AC Plugin for BioStar 2	
Workspace Plugin for BioStar 2	
Configuration	
Connecting to BioStar 2	
Connecting to BioStar 2 Associating the camera	
Connecting to BioStar 2 Associating the camera Managing the access control properties	
Connecting to BioStar 2 Associating the camera Managing the access control properties Configuring the alarm	
Connecting to BioStar 2 Associating the camera Managing the access control properties Configuring the alarm	
Connecting to BioStar 2 Associating the camera Managing the access control properties Configuring the alarm Troubleshooting Fail to get settings from BioStar 2 when using HTTPS connection	
Connecting to BioStar 2 Associating the camera Managing the access control properties Configuring the alarm Troubleshooting Fail to get settings from BioStar 2 when using HTTPS connection Fail to access BioStar 2 when using HTTP connection	
Connecting to BioStar 2 Associating the camera Managing the access control properties Configuring the alarm Troubleshooting Fail to get settings from BioStar 2 when using HTTPS connection Fail to access BioStar 2 when using HTTP connection Appendices	
Connecting to BioStar 2 Associating the camera Managing the access control properties Configuring the alarm Troubleshooting Fail to get settings from BioStar 2 when using HTTPS connection Fail to access BioStar 2 when using HTTP connection Fail to access BioStar 2 when using HTTP connection Event list	

Target Audience

This document is intended for system operators as well as system administrators and describes the integration between Suprema BioStar 2 and Milestone XProtect.

The system operators/administrators require basic knowledge of the Milestone XProtect system and high knowledge of the Suprema BioStar 2.

Introduction

Suprema's BioStar 2 is the powerful web-based security platform that provides the ability to integrate with third-party systems easily. This integration is based on Suprema's BioStar 2 server and enables operators to display the access control events and alarm on the XProtect Smart Client.

With the full features of BioStar 2, XProtect VMS creates a comprehensive access control solution. Furthermore, by coupling video and access control events, operators can control cameras and view real-time video and recorded video from one easy-to-use interface.

- Management and administration for users, doors, zones, and elevators with XProtect Smart Client.
- View live and historical access control events from within Milestone software and allows the operator to search for historical events with a range of parameters.
- Acknowledge the access control alarm of BioStar 2 in XProtect Smart Client.
- Real-time control the doors to unlock, lock and release the alarm.
- Open and close the doors through the Maps function of the XProtect Smart Client.

NOTE

• For more details on the functionality of XProtect VMS and XProtect Smart Client, see the manuals for Milestone software.

System diagram



Structural differences between BioStar 2 and XProtect

BioStar 2 is a security platform which can manage all components for access control, but XProtect uses the simple ACUbased topology. Therefore, there are few differences between BioStar 2 and XProtect. For examples, BioStar 2's Door, Zone, Elevator has the same level with XProtect's Door, but BioStar 2's element has more specified items. See below image.



Milestone XProtect



Functionalities

In XProtect Smart Client, you can use below functionalities with this plug-in;

- Retrieves the user(cardholder) from BioStar 2.
- Retrieves the door from BioStar 2.
- Retrieves the zone from BioStar 2.
- Retrieves the elevator from BioStar 2.
- Displays the status of the door in real-time.
- Displays the access control event in real-time.
- Displays the access control alarm of BioStar 2.
- Acknowledges the access control alarm of BioStar 2.
- Controls the door status of BioStar 2. (Clear Alarm, Clear APB, Open, Lock Door, Unlock Door, Release Door)
- Controls the zone status of BioStar 2. (Clear Alarm, Clear APB)
- Controls the elevator status of BioStar 2. (Clear Alarm)
- Links doors and camera and monitors them together.
- Allocates and monitors the door, zone, and elevator with Maps.
- Generates a report for access control events.

Installation

Prerequisites

- Must install the one of Milestone XProtect VMS.
 - XProtect Professional 2017 R2 or higher version
 - 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 7 Pro (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



Installing the BioStar 2 Integration for Milestone XProtect

BioStar 2 Integration for Milestone XProtect has two components;

- AC Plugin for BioStar 2.exe
- WorkspacePluginforBioStar2.exe

AC Plugin for BioStar 2.exe is used to connect the access control system and XProtect VMS. In other words, it works as a middleware to exchange the data between BioStar 2 and XProtect VMS.

WorkspacePluginforBioStar2.exe provides the functionality for using BioStar 2 in the XProtect Smart Client. This component must be installed on the PC where XProtect Smart Client is installed.

NOTE

• These plug-ins were built with MIP SDK 2016 and tested for Milestone XProtect Professional 2017 R2. For other versions of XProtect, please contact suprema technical support team(support.supremainc.com).

AC Plugin for BioStar 2

- 1 Run AC Plugin for BioStar 2.exe file.
- 2 Select a language and click **OK**.
- **3** To continue the intallation, select **I accept the agreement** and click **Next**.



4 After setting a path for plug-in to be installed, click **Next**.



5 Select Full installation and click Next. If XProtect Smart Client is installed separately with XProtect Professional, uncheck Workspace Plugin for BioStar 2.

😭 Setup - AC Plugin for BioStar2		x
Select Components Which components should be installed?	S	不
Select the components you want to install; clear the components you do n install. Click Next when you are ready to continue.	ot want to	
Full installation		
AC Plugin for BioStar2	13.1 MB	
Workspace Plugin for BioStar2	145.8 MB	
Current selection requires at least 201.1 MB of disk space.		
< <u>B</u> ack Next >	Cancel	

6 If a "Milestone XProtect Event Server Service is running. Do you want to stop this service?" window appears, click Yes.



7 If ready to install, click Install.



- 8
 - To complete the plug-in installation, click **Finish**.

🔯 Setup - AC Plugin for BioS	tar2
CC-	Completing the AC Plugin for BioStar2 Setup Wizard Setup has finished installing AC Plugin for BioStar2 on your computer. Click Finish to exit Setup.
	Einish

Workspace Plugin for BioStar 2

- 1 Run WorkspacePluginforBioStar2.exe file.
- 2 Select a language and click **OK**.
- 3 To continue the intallation, select I accept the agreement and click Next.



4 After setting a path for plug-in to be installed, click **Next**.







6

If ready to install, click **Install**.



7 If a warning message appears, select Automatically close the applications and click Next.



8 To complete the Workspace Plugin for BioStar 2 installation, click **Finish**.

🔯 Setup - Workspace Plugin f	for BioStar2	
B	Completing the Workspa for BioStar2 Setup Wizar Setup has finished installing Workspace Plugi your computer. Click Finish to exit Setup.	rce Plugin rd
	Einish	

9 When the installation is completed successfully, start the **Milestone XProtect Event Server** manually. To do this, go to the system tray and right-click on the **Milestone XProtect Event Server** icon and then click **Start Event Server** service.



Configuration

Connecting to BioStar 2

- 1 Run Milestone XProtect Professional 2017 R2 Management Application.
- 2 Navigate to the Access Control node. Righ-click on it and click Create new.



NOTE

• If the plug-in is not found, restart the Milestone Event Server Service. To do this, go to the system tray and right-click on the Milestone XProtect Event Server icon and then click Restart Event Server service.

3 Select **Integration plug-in** as **BioStar 2 Server**.

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:	BioStar2 Server ~
Address:	https://192.168.16.38/
User:	admin
Password:	
Use HTTP encryption:	

4 If the plug-in is found, **Create Access Control System Integration** window is appear. Enter or edit the each field.

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://192.168.16.38/
User:	admin
Password:	••••••
Use HTTP encryption:	

- Name: Enter the desired name of the plug-in.
- Integration plug-in: Select BioStar 2 Server from the list.
- Address: IP address of BioStar 2 server.
- **User**: Enter the login ID for BioStar 2.
- **Password**: Enter the password for BioStar 2.

5 To connect the Biostar 2, click **Next**.

Associating the camera

If BioStar 2 connected correctly, the **Associate cameras** screen appear. In this step, you can associate the cameras with access points.

1 Find the camera in the **Cameras** pane and drag it to the associated access points.

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 doo	ors 💙				Cameras:
Name DR-1	Enabled	License Pending	8		Camera 1
Acces Dro Acces Dro	s point: (E <i>p camera</i> s point: (E <i>p camera</i>	Entry Devi <i>here to a</i> Exit Device <i>here to a</i> :	ce) BioSt ssociate i e) BioSta ssociate i	tation A2 541530 t with the access (tion 2 54773264! t with the access (
	, 				
<					

2 When all access points associated with cameras, click **Next** to complete the settings. 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:					Cameras:
All doo	ors Y				▲ U Server ▲ All Cameras (Server)
Name	Enabled	License	9		Camera 1 Al Slaves (Server)
DR-1	>	Pending	\checkmark		
Access Cam Droj Access Cam Droj	s point: (E nera 1 <i>p camera</i> s point: (E nera 1 <i>p camera</i>	Entry Devic <i>here to as</i> Exit Device <i>here to as</i>	e) BioS sociate) BioSta sociate	tation A2 541530 it with the access p ation 2 547732649 it with the access p	
<				>	

3 When the success confirmation window appears, click **Close**.

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.

Managing the access control properties

After configuring the plug-in properly, you can add/edit the access control properties at any time.

1 Run Milestone XProtect Professional 2017 R2 Management Application.

2 Navigate to the Access Control node. Righ-click on it and click Properties.

Access Control					~
Ceneral Settings					
Depresent Apportated Cam	General settings				
	Enable:	\checkmark			
🗞 Access Control Events	Name:	BioStar 2			
Access Control Actions	Description:				
🤱 Cardholders					
	Integration plug-in:	BioStar2 Server (Version: 1.0. 1.0)			_
	Last configuration refresh:	2017-10-16 오후 4:18			
		Refresh Configuration			
	A d d	[http://100.100.10.00/			
	Address:	nttps://192,166,16,36/			_
	Password:				_
	Event polling period (ms):	250			_
	Use new captured image:	✓			
	Use HTTP encryption:				
< >					
			OK	Can	cel

- 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. See Associating the Camera.
- Access Control Events: You can activate or deactivate the access control event from BioStar 2, also create and assign the userdefined categories.
- Access Control Actions: You can create an access control action or command which is performed by the operator on the
 associated access points. For example, when a cardholder 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.

Configuring 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 occurs, XProtect Smart Client displays the alarm in **Alarm Manager**.

- 1 Run Milestone XProtect Professional 2017 R2 Management Application.
- 2 Navigate to the Alarm Definitions node. Righ-click on it and click Add New.



3 Change the alarm name in **Name** field.

4 1

In **Trigger** section, set **Triggering event** as **Access Control Event Categories** and then select **Alarm**.

5 In Trigger section, set Sources as All doors.

Ingger		
Triggering event:	Access Control Event Categories	•
	Alarm ~	•
Sources:	All doors ~	
Activation period	All deors DR-1	
Time profile:	Always	

Troubleshooting

Fail to get settings from BioStar 2 when using HTTPS connection

Environment

- OS: Windows Server 2012 / Windows 7(SP1) / Windows Server 2008 R2
- BioStar 2 Version: BioStar 2.5.0

Symptom

An error occurs during install the Workspace Plugin for BioStar 2.

Cause

BioStar 2.5.0 is designed to use TLS 1.1 or TLS 1.2 as a default. However, applications and services that are written by using WinHTTP for Secure Sockets Layer (SSL) connections that use the WINHTTP_OPTION_SECURE_PROTOCOLS flag can't use TLS 1.1 or TLS 1.2 protocols. This is because the definition of this flag doesn't include these applications and services.

Solution

Install Easy Fix which is provided by Microsoft and then rebstart the system. To do this, visit; https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-defaultsecure-protocols-in

Fail to access BioStar 2 when using HTTP connection

Environment

Upgrade BioStar 2 from BioStar 2.4.1 to BioStar 2.5.0

Symptom

An error occurs during login to BioStar 2.

Cause

When using HTTP connection, BioStar 2.4.1 uses the payload encryption to log in. However, BioStar 2.5.0 does not use the payload encryption.

Solution

After upgrading to BioStar 2.5.0, Run **Milestone XProtect Professional 2017 R2 Management Application**. Navigate to the **Access Control node**. Right-click on it and click **Properties**. Uncheck **Use HTTP encryption**.

Appendices

Event list

Here is an event list of BioStar 2 that can be handled by XProtect system. This list is part of BioStar 2 event list.

- 1:1 duress authentication succeeded (Access-on-card + Fingerprint + PIN)
- 1:1 duress authentication succeeded (Access-on-card + Fingerprint)
- 1:1 duress authentication succeeded (Access-on-card + PIN)
- 1:1 duress authentication succeeded (Access-on-card)
- 1:N authentication failed
- 1:N authentication failed (Access-on-card + Fingerprint)
- 1:N authentication failed (Access-on-card + PIN)
- 1:N authentication failed (Face)
- 1:N authentication failed (Fingerprint)
- 1:N authentication failed (PIN)
- 1:N authentication succeeded
- 1:N authentication succeeded (Face + PIN)
- 1:N authentication succeeded (Face)
- 1:N authentication succeeded (Fingerprint + PIN)
- 1:N authentication succeeded (Fingerprint)
- 1:N duress authentication succeeded
- 1:N duress authentication succeeded (Face + PIN)
- 1:N duress authentication succeeded (Face)
- 1:N duress authentication succeeded (Fingerprint + PIN)
- 1:N duress authentication succeeded (Fingerprint)
- Access denied
- Access denied (Blacklist)
- Access denied (Capture failure)
- Access denied (Disabled user)
- Access denied (Expired)
- Access denied (Face detection failure)
- Access denied (Forced lock schedule)
- Access denied (Hard Anti-passback)
- Access denied (Invalid access group)
- Access denied (Soft anti-passback)

- Access denied (Soft timed anti-passback)
- Access denied (Timed anti-passback)
- Access-on-card issue succeeded
- All user deletion succeeded
- Authentication failed
- Authentication failed (Bad fingerprint placement)
- Authentication failed (Invalid authentication mode)
- Authentication failed (Invalid credential)
- Authentication failed (Timeout)
- Authentication failed. (Server matching is off)
- Dual authentication failed
- Dual authentication failed (Invalid access group)
- Dual authentication failed (Timeout)
- Dual authentication succeeded
- Elevator activated
- Elevator deactivated
- Fake Fingerprint Detected
- Lock by emergency
- Lock by operator
- Lock by schedule
- Release by emergency
- Release by operator
- Release by schedule
- Unlock by emergency
- Unlock by operator
- Unlock by operator
- User deletion failed
- User deletion succeeded
- User enrollment failed
- User enrollment succeeded
- User update failed
- User update succeeded

Command list

Command	Components			
Commanu	Door	Zone	Elevator	
Clear Alarm	0	0	0	
Clear APB	0	O (APB only)	Х	
Open	0	Х	Х	
Lock Door	0	х	х	
Unlock Door	0	Х	Х	
Release Door	0	Х	Х	

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang- gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

©2020 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc. All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies. Product appearance, build status and/or specifications are subject to change without notice.