



Fiber Sensys Integration Module Setup and User Guide

ACFA PSIM 1.1

Last update 05/03/2024

Table of Contents

1	Introduction into Fiber Sensys Integration Module Setup and User Guide	3
1.1	Purpose and Structure of the Guide	3
1.2	General information about the Fiber Sensys integration module	3
2	Hardware compatibility and licensing of the Fiber Sensys module	4
3	Configuring Fiber Sensys integration module	5
3.1	Connection of the Fiber Sensys PIDs to ACFA PSIM software package	5
3.2	Configuration management of the PIDs Fiber Sensys	6
3.3	Fiber Sensys APU channel Setting	7
4	Working with the Fiber Sensys integration module	8
4.1	General information about working with the Fiber Sensys integration module	8
4.2	Managing the Fiber Sensys channel	8

1 Introduction into Fiber Sensys Integration Module Setup and User Guide

On the page:

- [Purpose and Structure of the Guide](#)
- [General information about the Fiber Sensys integration module](#)

1.1 Purpose and Structure of the Guide

The *Fiber Sensys* Module Settings Guide is a reference manual designed for *Fiber Sensys* Module users. This module functions as a part of perimeter intrusion detection system based on the *ACFA PSIM* software package.

This Guide presents the following materials:

1. General information about the *Fiber Sensys* integration module;
2. Configuration of the *Fiber Sensys* integration module;
3. Working with the *Fiber Sensys* integration module.

1.2 General information about the Fiber Sensys integration module

The *Fiber Sensys* integration module is part of the perimeter intrusion detection system (PIDs) built on the basis of the *ACFA PSIM* Software System. It is designed to monitor and control channels of the *Fiber Sensys* PIDs. Partial configuration of *Fiber Sensys* channels is available.

Before start the working of the *Fiber Sensys* integration module install hardware on the secured object and configure the system in the vendor's software.

Note.

Detailed information about the *Fiber Sensys* PIDs is presented in the official documentation for that system (manufacturer: Fiber SenSys, Inc.).

2 Hardware compatibility and licensing of the Fiber Sensys module

Manufacturer	Fiber SenSys, Inc. 6175 NE Century Blvd. Hillsboro, OR 97124 USA Phone: +1 503.692.4430 Fax: +1 503.692.4410 https://fibersensys.com/
Integration type	SDK
Hardware connections	Ethernet

Supported equipment

Equipment	Function
All 300 Series APUs (Alarm Processor Units)	Alarm Processor Unit

Protection

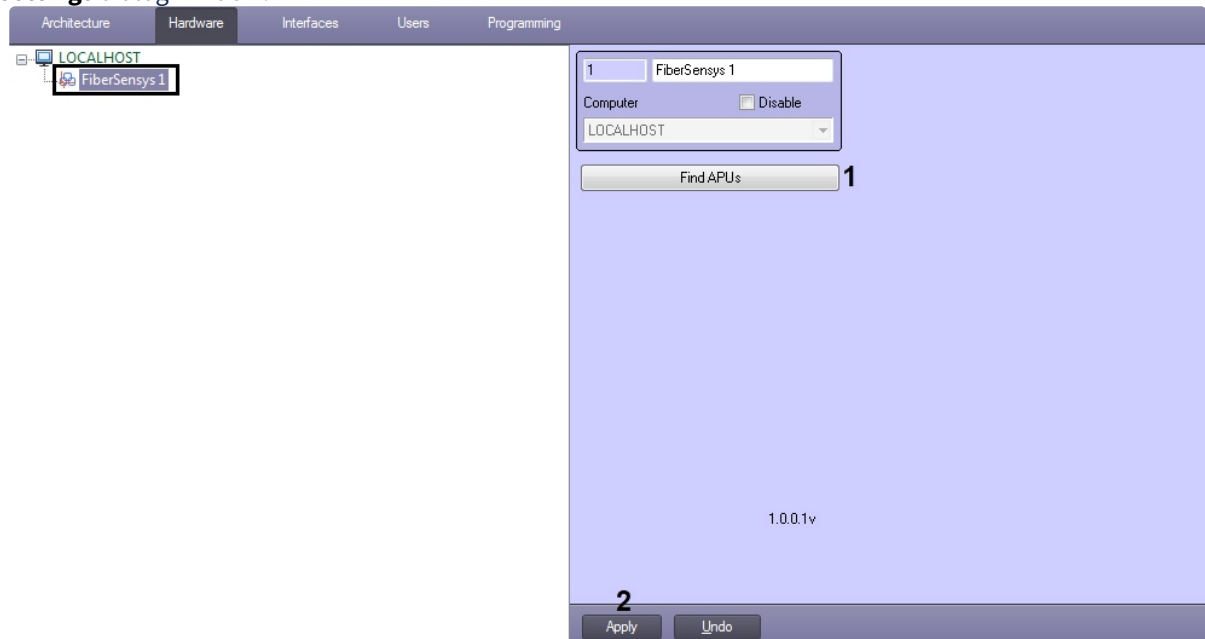
For 1 APU.

3 Configuring Fiber Sensys integration module

3.1 Connection of the Fiber Sensys PIDs to ACFA PSIM software package

To automatically connect the *Fiber Sensys* PIDs to the *ACFA PSIM* software package, do the following:

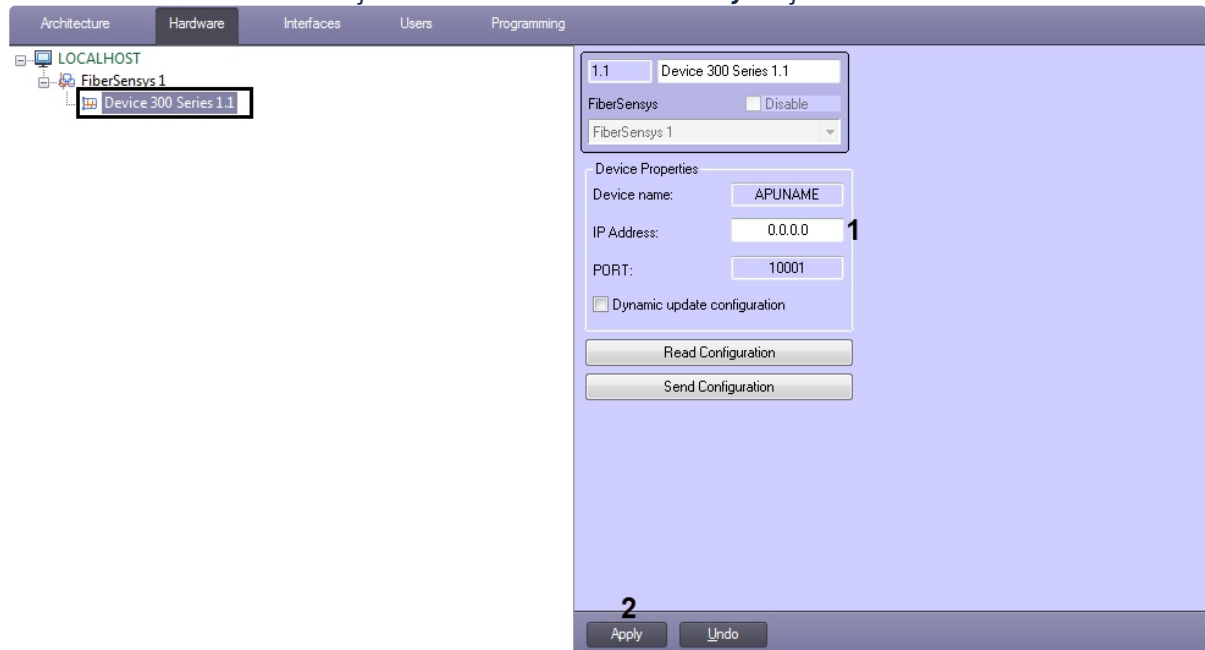
1. Create the **FiberSensys** object on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog window.



2. Click on the **Find APUs** button (1) to search for APUs in the network. As a result, a tree of objects will be built for each device found.
3. Click the **Apply** button (2).

To manually connect the *Fiber Sensys* PIDs to the *ACFA PSIM* software package, do the following:

1. Create the **Device 300 Series** object on the basis of the **FiberSensys** object.

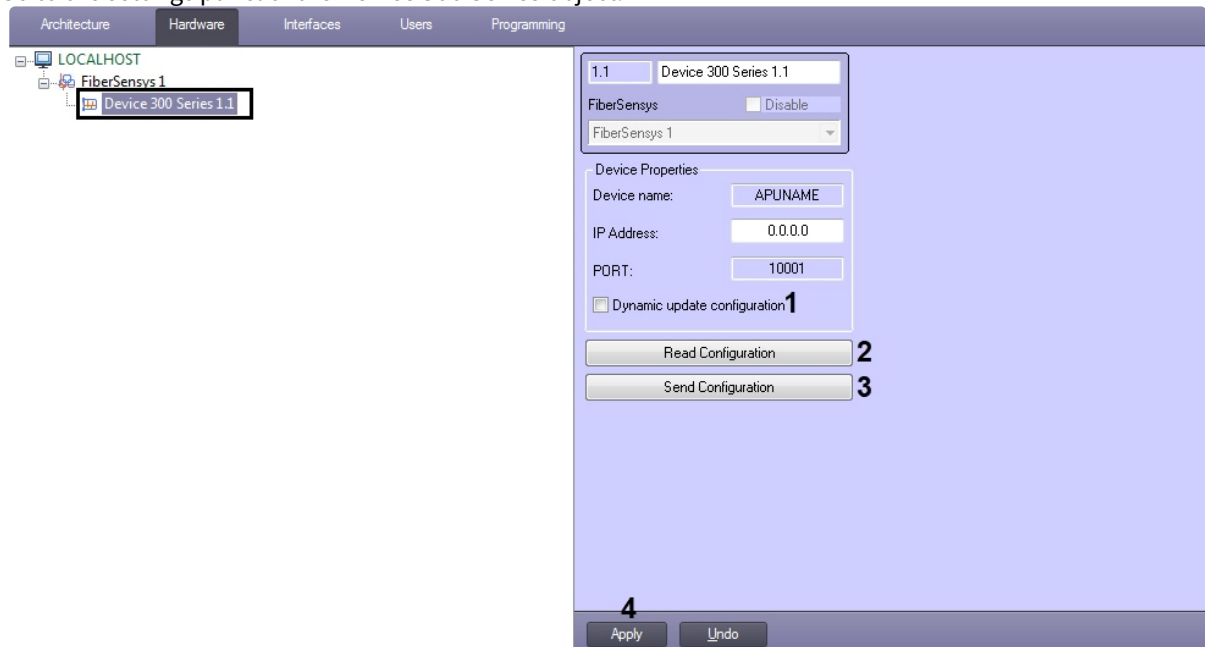


2. In the **IP Address** field (1) specify the IP address of the APU.
3. Click the **Apply** button (2).

3.2 Configuration management of the PIDs Fiber Sensys

Configuration management of the *Fiber Sensys* PIDs as follows:

1. Go to the settings panel of the **Device 300 Series** object.



2. Set the **Dynamic update configuration** checkbox (1) to dynamically read the configuration from the APU.
3. Press the **Read Configuration** button (2) to read the configuration from the APU.
4. Press the **Send Configuration** button (3) to write the current configuration to the APU.

- Click the **Apply** button (4).

3.3 Fiber Sensys APU channel Setting

The *Fiber Sensys* APU channel is configured as follows:

- Go to the settings panel of the **Channel** object.



- In the **Gain (1)** field, specify the overall sensitivity of the system. A higher value means a higher sensitivity.
- Use the **Enable wind rejection** drop-down list (2) to enable or disable wind rejection function. If this parameter is enabled, the APU will track the effect of wind on the channel and compensate for it based on the detected load.
- In the **Comb Reject Filter (db) [1 to 300] (3)** field, specify the signal gain in decibels to implement the comb filter.
- In the **Sensitivity Factor [1 to 100] (4)** field, specify the gain of the dry signal from the protected area. Typically used to increase the amplitude of a signal in spectrum view to improve signal visibility.
- If XML mode is enabled, in the **XML report interval (0.1s) [1 to 600] (5)** field specify the maximum frequency in seconds for outputting XML reports.
- Use the **Enable CPU-1** drop-down list (6) to enable or disable processor 1 (climb detection).
- Use the **Enable CPU-2** drop-down list (7) to enable or disable processor 2 (cut detection).
- Click the **Apply** button (8).

4 Working with the Fiber Sensys integration module

4.1 General information about working with the Fiber Sensys integration module

The following interface objects are used for working with *Fiber Sensys* integration module:

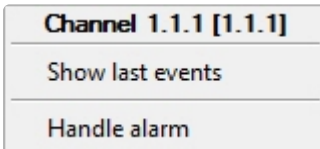
1. **Map.**
2. **Events protocol.**

Information about **Map** and **Events protocol** interface objects configuration is given in [Axxon PSIM Software Package: Administrator's Guide](#).

Working with these interface objects is given in details in [Axxon PSIM Software Package: Operator's Guide](#).

4.2 Managing the Fiber Sensys channel





The *Fiber Sensys* channel is managed in the **Map** interactive window using the **Channel** object functional menu:



The *Fiber Sensys* channel functional menu commands description is given in the table:

Menu command	Function performed
Handle alarm	Operator acknowledge alarm

The *Fiber Sensys* channel can have the following states:

	Alarm
	Control
	Error
	Intrusion