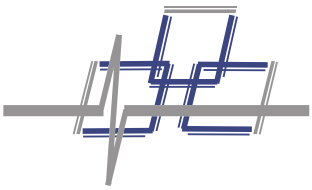
Fiber SenSys

HIGH PERFORMANCE
HIGH RELIABILITY
HIGH SECURITY

# Fiber SenSys XProtect Integrator

*How to integrate Fiber SenSys Fiber Defender® Alarm Processing Units with Milestone XProtect®*

## Application Note



**Fiber SenSys Inc.**
2925 NW Aloclek Dr.
Suite 120
Hillsboro, OR 97124
USA

Tel: 1-503-692-4430
Fax: 1-503-692-4410
info@fibersensys.com
www.fibersensys.com

## Contents

## Introduction

This application note provides an overview on how to add support for Fiber SenSys Inc. (FSI) Alarm Processing Units (APUs) to a Milestone XProtect® system (XProtect). The Fiber SenSys XProtect Integrator (Integrator) is responsible for communicating with Fiber SenSys APUs and forwarding alarms and other messages to XProtect.

This document will explain how to set up the integration software to send Generic Events to XProtect. It will also describe in general terms how to set up XProtect to handle the Generic Events. Finally, it will describe how to verify that communication is occurring between the APUs and XProtect.

Each installed site has its own requirements for XProtect configuration and you will need to design the configuration based on your site's requirements. This guide is not a substitute for experience with and understanding of the details of configuring XProtect.

This document was written based on XProtect Advanced VMS Products 2016 R2 and Fiber SenSys XProtect Integrator version 2.3.2.

**NOTE:** This is a basic guide for XProtect Advanced, which includes XProtect Expert and XProtect Corporate. Your specific configuration and steps may differ from what is shown. For more information about XProtect, refer to the *XProtect Administrator's Manual*.

## Before You Get Started

This guide assumes that XProtect has been installed, that at least one camera has been added to the system, and that you are familiar with how to configure XProtect to obtain the behavior you desire.

It also assumes that the Fiber SenSys APUs have been installed and are ready to integrate. For more information about setting up Fiber SenSys APUs, refer to each APU's documentation.

You will need to set each APU's IP address and configure the APU for incoming connections. Refer to the *APU Networking Application Note* (AN-SM-009) for instructions. Keep track of the IP addresses you are setting, because you will need to know them later when configuring Integrator.

## Configuring the software

This section will describe how to prepare XProtect and the Integrator software for integration.

Normally, Integrator is installed on the same computer as the XProtect Event Server. If you are planning to install Integrator on a separate computer, there are additional steps you must perform. See Appendix A for more information.

### Configuring XProtect

The XProtect Event server, the XProtect Management Client, and the XProtect Smart Client must all be installed and running on Windows computers. See the XProtect Adminstrator's Manual for more information about properly setting up your XProtect system.

Integrator integrates with XProtect via the Generic Event interface. As such, no add-on or special license is needed. However, the XProtect Event server must be configured to receive the Generic Events.

To begin, start the XProtect Management Client software and log in.


**Figure 1. The XProtect Management Client icon.**

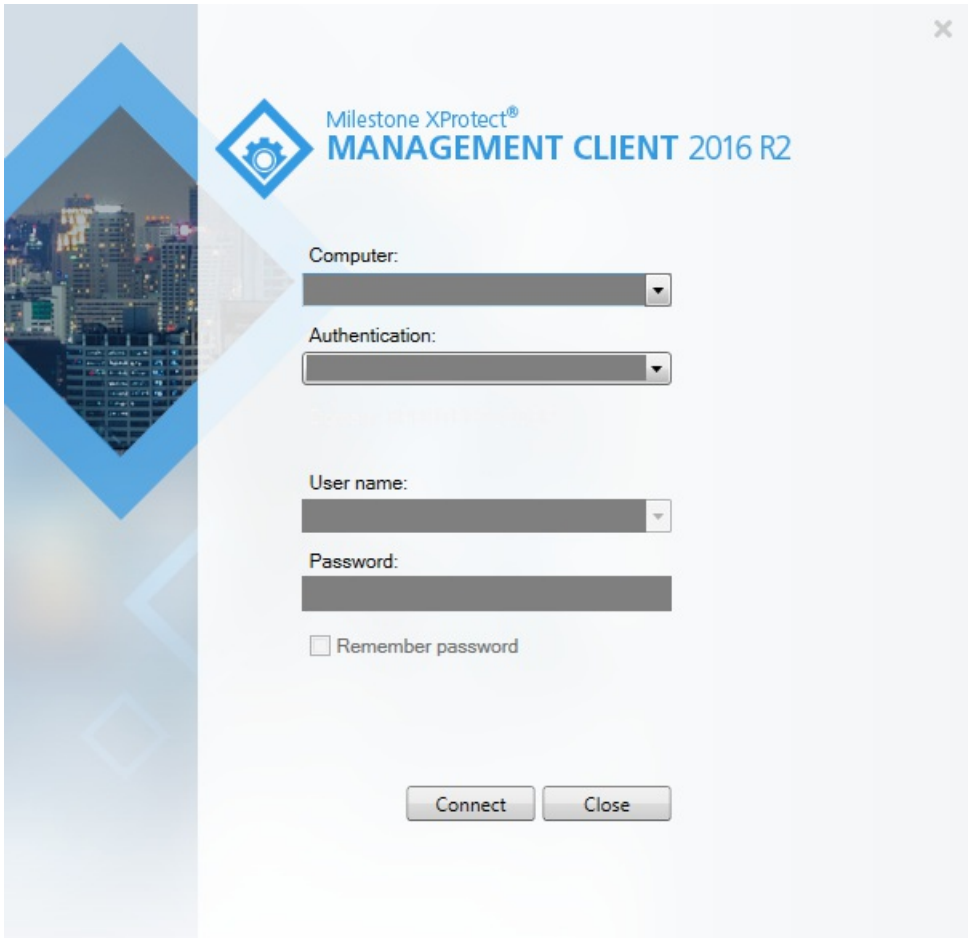



Figure 2. The Management Client login screen.

In Management Client, select the **Tools** menu and then the **Options...** item.

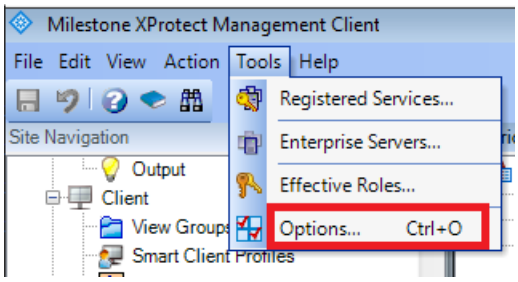



Figure 3. XProtect Tools menu.

The **Options** dialog window should appear. Select the **Generic Events** tab (at the right end of the tab list), then press the **New** button.

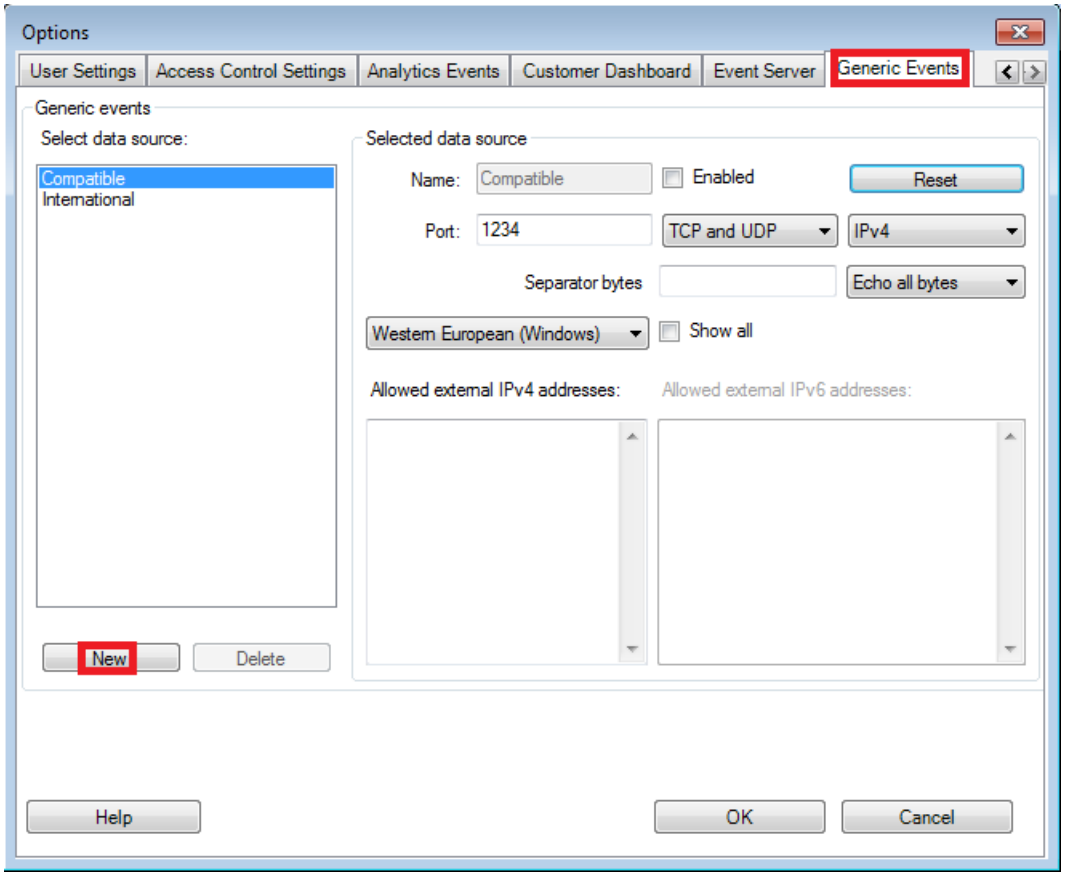



Figure 4. Generic Events tab on the XProtect Options dialog window.

Change the name of the data source to “Fiber SenSys”. Check the **Enabled** box. Make sure the other fields match the image below. Write down the number in the **Port** field; you will need this later to configure the Integrator to use the same port number.

Then click **OK** to activate the server.

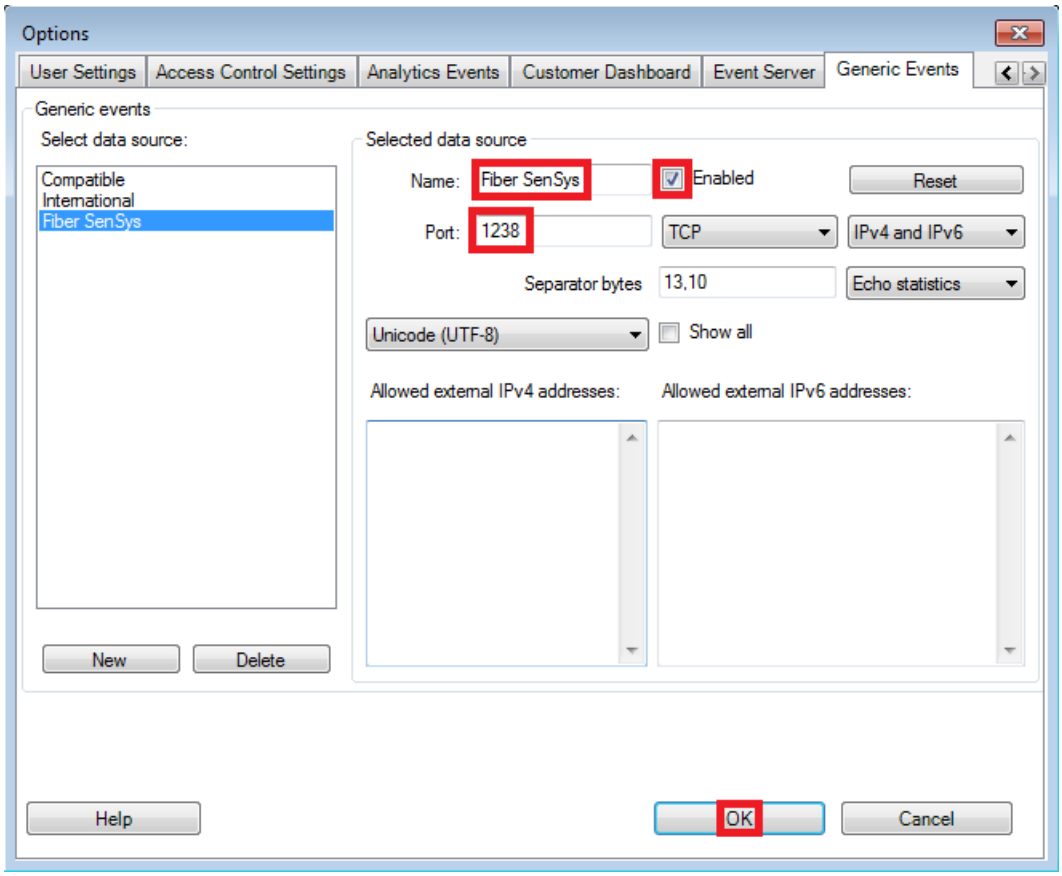


Figure 5. Configuring a new type of Generic Event.

## Configuring Fiber SenSys XProtect Integrator

Install the Fiber SenSys XProtect Integrator software using the provided installer executable. If you do not already have the installer executable, you can download it from the Fiber SenSys website.

**NOTE:** Integrator must be running at all times for alarms to be reported to XProtect. This is why the installer's default setting is to install the application to be run on computer startup. Do not switch off this setting unless you are sure that you do not want the service running continuously.

Open the Integrator software. It can be opened by clicking its icon on the desktop or the start menu.

Figure 6. The Fiber SenSys XProtect Integrator icon.

On the **File** menu, select the **Configuration...** item. This will raise the **Configuration** dialog window.

Change the **Port number** value to match the port number that you wrote down when creating the “Fiber SenSys” Generic Event type.

Then click **OK** to complete the configuration.

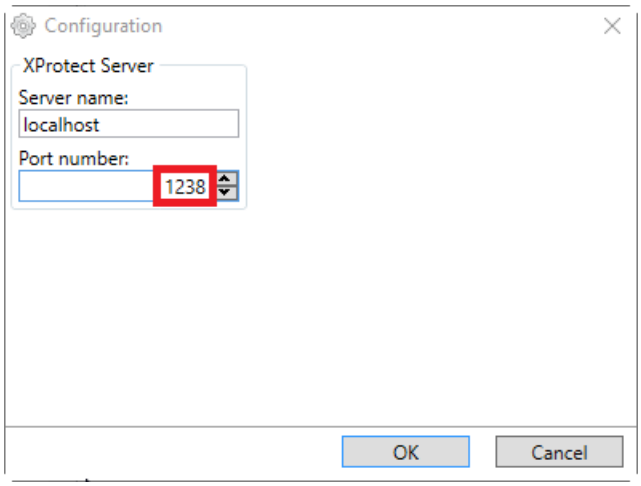



Figure 7. Configuration dialog window.

The connection to XProtect will be tested as part of the process of adding APUs. Unfortunately, there is no good technique for testing the connection without configuring XProtect to receive specific Generic Event messages.

## Adding APUs to Fiber SenSys XProtect Integrator

Now that the software has been set up, Integrator needs to be told about each APU that should be monitored.

Click the **Add** button to add a new APU to Integrator. This will raise the **Add Device** dialog window.

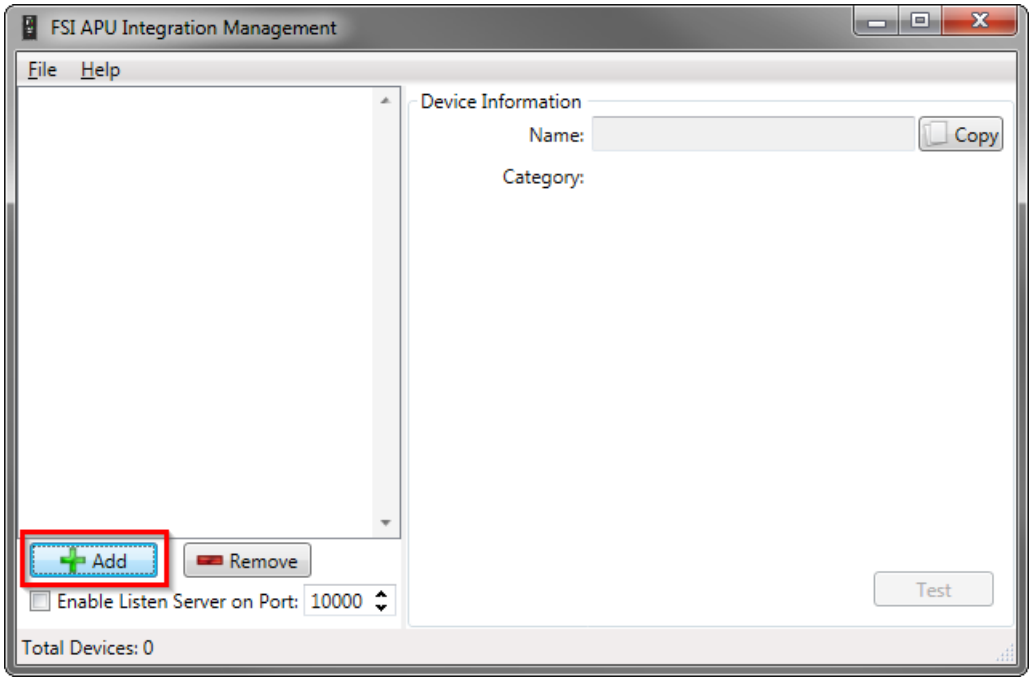



Figure 8. The main Integrator window.

In the **Add Device** dialog window, type the APU's IP address in the **Host** box; then click the **Add** button.

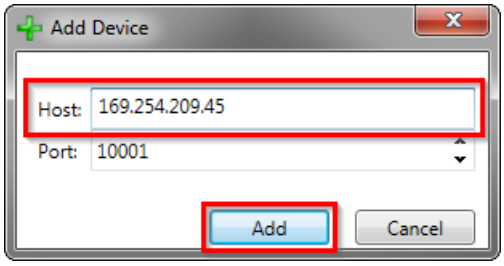



Figure 9. The Add Device dialog window.

The main Integrator window shows the connection state of the APU. There are three possible states:

Disconnected
: There is not a network connection to the APU. Check that the APU is powered, is connected to the network, and the IP address entered into Integrator is correct. Integrator may show a message providing more details about the connection problem.

Waiting for Handshake
: Integrator has established a TCP/IP connection to the APU and is waiting for the APU to report its device name and other information. The handshake process may take up to two minutes to complete. Alarms will not be reported while waiting for the handshake to complete.

Connected
: The APU is communicating with Integrator. Alarms and other events will be forwarded to XProtect.

The following images show the handshake and connected states.

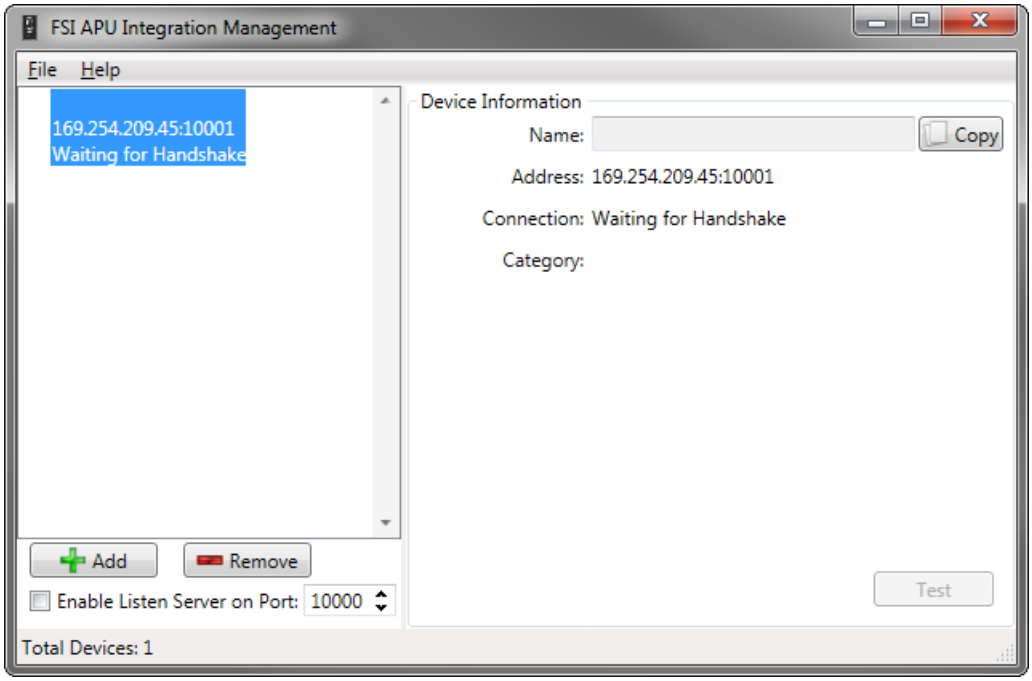



Figure 10. Waiting for the handshake to complete.

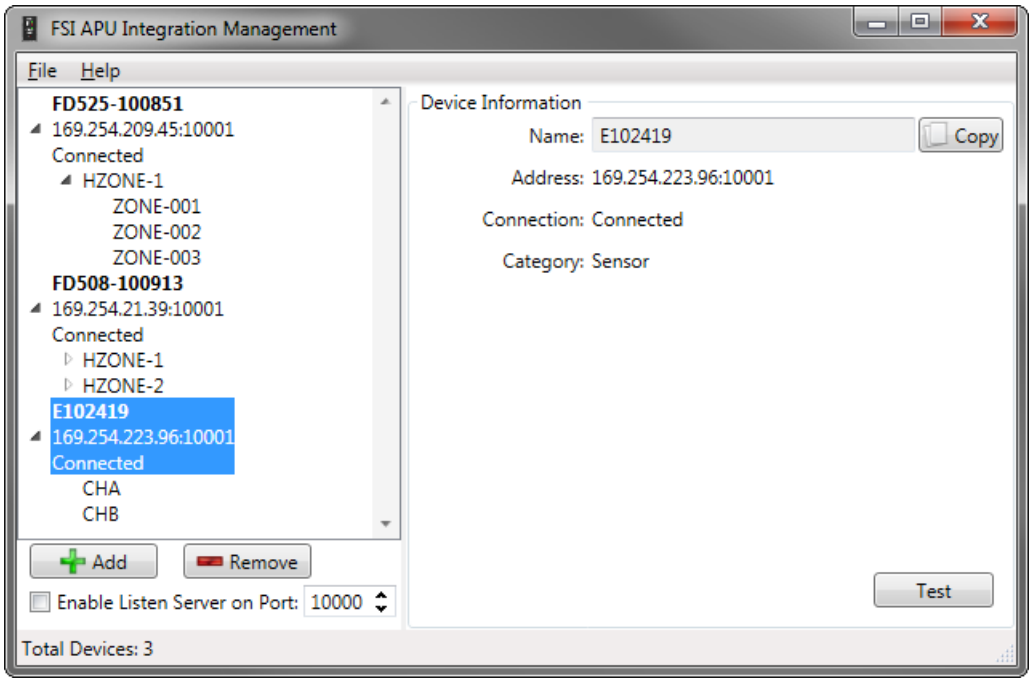



Figure 11. The APUs are connected Integrator. Note the zones underneath the APUs in the tree view.

Verify that each APU is connected to Integrator before proceeding to the next step.

## Integrating Fiber SenSys Generic Events into XProtect

The rest of the integration process consists of adding Generic Events, Alarm Definitions, Rules, and Outputs to XProtect. You will need to start the XProtect Management Client and add entries for each event in order for them to be visible within the XProtect Smart Client.

This section describes the particular aspects of Generic Events that are relevant for Fiber SenSys APUs.

Integrator forwards intrusions and other events to XProtect using Generic Event messages. The messages are in the Fiber SenSys SimpleMessage format and have the following form:

APUNAME:ZONENAME:EVENT

A message indicates that an event of interest has occurred on an APU's zone or the APU itself. APUNAME is the name of the APU; the default name is based on the serial number of the APU. If the event is about an APU itself, then ZONENAME will be empty. Otherwise, it will be the name of the zone.

**NOTE:** For historical reasons, the ZONENAME is hierarchically constructed. For 300 series APUs the ZONENAME will look something like E009999.CHA. For 500 series APUs the ZONENAME will look something like E009999.HZONE1.ZONE1.

The following table describes the events that are sent to XProtect:

| Event Text | Description |
|---|---|
| ALARM | A zone reported that an intrusion has been detected. |
| FAULTON | A zone reported loss or significant degradation of returning optical power. This condition exists until FAULTOFF is reported for that zone. |
| FAULTOFF | A zone reported normal conditions after a previous FAULTON report. |
| TAMPERON | The APU reported a tamper condition. This is an optional condition that is not reported by default. The APU must be configured to report it. This condition exists until TAMPEROFF is reported on the APU itself. |
| TAMPEROFF | The APU reported normal conditions after a previous TAMPERON report. |
| COMMFAILON | Integrator has lost communication with the APU. The APU will not report alarms or other events until communications is restored. |
| COMMFAILOFF | The APU reported normal conditions after a previous COMMFAILON report. |

Table 1. Description of events reported to XProtect.

### Identifying the events to add to XProtect

Each site will have its own requirements and you will need to design an XProtect configuration that matches those requirements. Refer to the *XProtect Administrator's Manual* to design a proper configuration. Understanding how to configure XProtect to meet your particular site's requirements is beyond the scope of this document.

To obtain the list of events that can be added, choose the **Export Event List...** item from the **File** menu of Integrator. Choose a location to save the file. After saving, a window containing the event list should appear; if not, then open the file using Windows Explorer.

You can see an example event list in Appendix C.

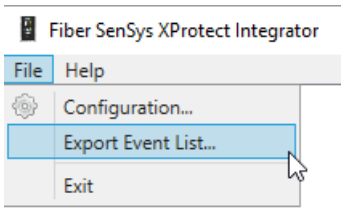



Figure 12. The Export Event List... menu item.

### Completing the integration

Using XProtect Management Client, please verify that all of the Generic Events and Alarm Definitions for your Fiber SenSys APUs have been added.

## Testing the integration

At this point, your site's XProtect configuration should be complete. This section describes how to test the integration. First it describes to how test each Generic Event in XProtect using a test function built into Integrator. Then it describes in general how to perform a system test.

### Testing XProtect's Generic Events and Alarm Definitions

The Integrator contains a test function that can assist you with verifying that the Generic Events and Alarm Definitions for each APU and zone have been set up in XProtect. This section describes how to use the test function.

If you are having difficulty troubleshooting your Generic Events and Alarm Definitions, Appendix C walks through setting up an integration for a fictional installation site. This integration is unlikely to meet your needs, but can be useful for troubleshooting.

To begin, open both the Fiber SenSys XProtect Integrator software and the XProtect Smart Client software.

In Integrator, you will need to select and test each APU and each zone. To begin, select the APU or zone to be tested, then click the **Test** button.

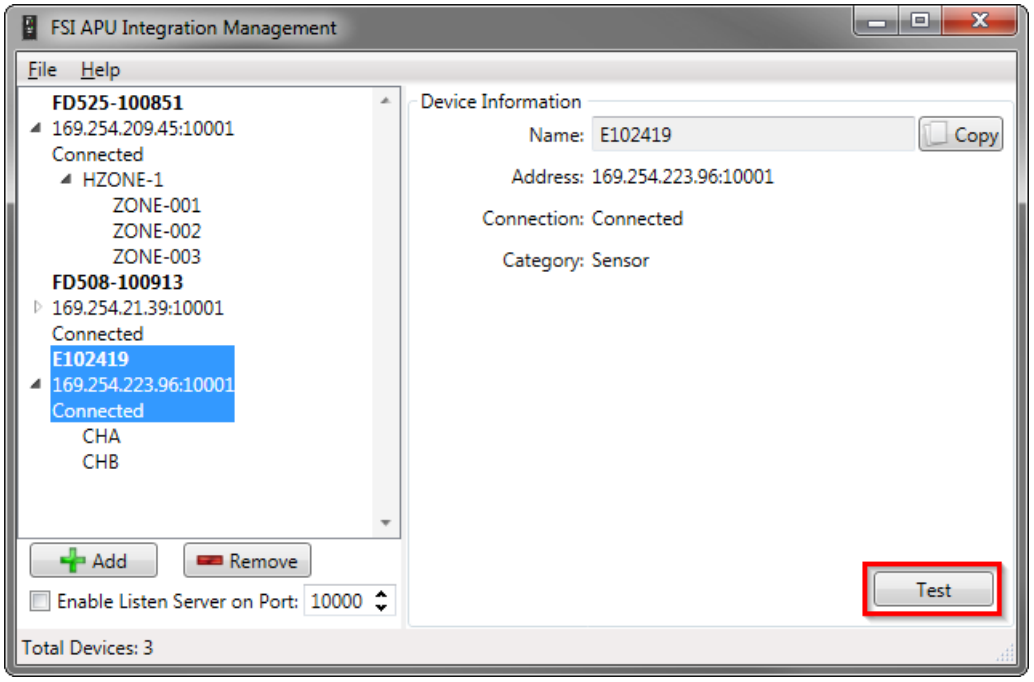



Figure 13. Integrator Test button.

Alarms should appear in the Smart Client for each enabled Alarm Definition that is based on a Generic Event that has been properly created and enabled in XProtect. The exact number and description of these alarms will depend on how you integrated in the Generic Events into XProtect.

The following are the Generic Events that are sent when the **Test** button is pressed.

When pressing the **Test** button for an APU, the `TAMPERON`, `TAMPEROFF`, `COMMFAILON`, and `COMMFAILOFF` test events will be sent for that APU. When pressing the **Test** button for a zone, the `ALARM`, `FAULTON`, and `FAULTOFF` test events will be sent for that zone.

### Testing Rules, Outputs, and other XProtect functionality

Before you begin your system validation testing, you will want to verify that XProtect has been configured to react according to your site's requirements. This may require adjusting the Rules, Outputs, and other aspects of XProtect that you have configured. The details depend on your site requirements. Refer to the *XProtect Administrator's Manual* for more information.

### System validation testing

To complete validation of your integration, you will want to test the entire system. This section recommends an approach for testing the Fiber SenSys aspects of your system.

Full validation should consist of testing each type of condition for each element of the system. To obtain a complete list of conditions

for the Fiber SenSys APUs and zones, you can refer to the list of events generated by Integrator. This can be helpful in making a checklist of tests to perform.

The following table explains the actions you can take to test for each type of condition.

| Condition Type | Recommended test |
|---|---|
| Tamper condition on an APU | This test is only neccessary for APUs that have been configured to report the tamper condition. To test this condition, open the enclosure protected by the tamper switch. This will cause Integrator to send a TAMPERON message for that APU. Then close the enclosure protected by the tamper switch. This will cause Integrator to send a TAMPEROFF message for that APU. |
| Communications failure on an APU | Unplug the Ethernet cable from the APU. After a few moments, this will cause Integrator to send a COMMFAILON message for that APU. Then re-insert the Ethernet cable to the APU. After a period of waiting for the handshake with the APU, Integrator should report Connected. This will cause Integrator to send a COMMFAILOFF message for that APU. In addition, existing trouble conditions will also be sent. If the APU is in tamper, a TAMPERON will be sent. If a zone is in cable fault, then a FAULTON will be sent. (Note: For historical reasons, two FAULTOFF messages may be sent after the COMMFAILOFF is sent. These messages are not meaningful.) |
| Intrusion on a zone | Shake the fence or otherwise simulate a real intrusion for the zone under test. This will cause Integrator to send an ALARM message for that zone. |
| Cable fault for a zone | Disconnect the optical cable for the zone to be tested. This will cause Integrator to send a FAULTON message for that zone. (Some APUs will have a single optical cable for multiple zones. In this case, you will be testing those zones together.) Clean the optical connector before re-inserting. After re-inserting, a FAULTOFF message will be sent for that zone. |

**Table 2. How to test for each type of condition.**

The checklist of completed validation tests can be used to provide documentation of a successful system test, at least for the Fiber SenSys portion of the system.

## Removing APUs

This section explains how to remove the configuration for an APU.

Open the Fiber SenSys XProtect Integrator software. Select the APU to remove and click the **Remove** button.

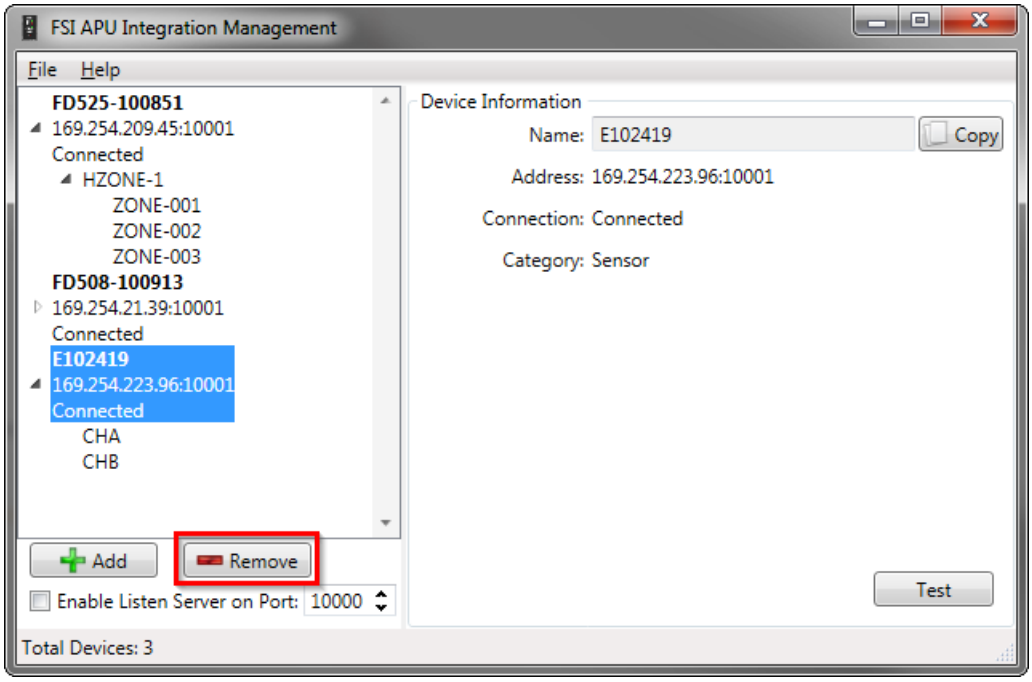



**Figure 14. Click Remove to remove the selected device from XProtect Integrator.**

Because Integrator will no longer be reporting Generic Events for the APU, it is not neccessary to remove anything from XProtect. However, if you prefer to remove the entries, you can revisit the Generic Events and Alarm Definitions that had been added for that APU.

## Appendix A: Installing Integrator on a separate computer

This section describes the additional steps required when Integrator is installed on a different computer than XProtect Event Server.

You'll need to know the IP addresses for both computers.

**NOTE:** This configuration complicates installation and is not recommended unless you have experience with troubleshooting TCP/IP and networking problems.

### Configuring Integtrator

The Integrator will need to be modified to make connections to the other computer.

In Integrator, select the **File** menu and then the **Configuration...** item. Then change the **Server name** to the IP address for the computer running XProtect.

Then click **OK** to complete the change.

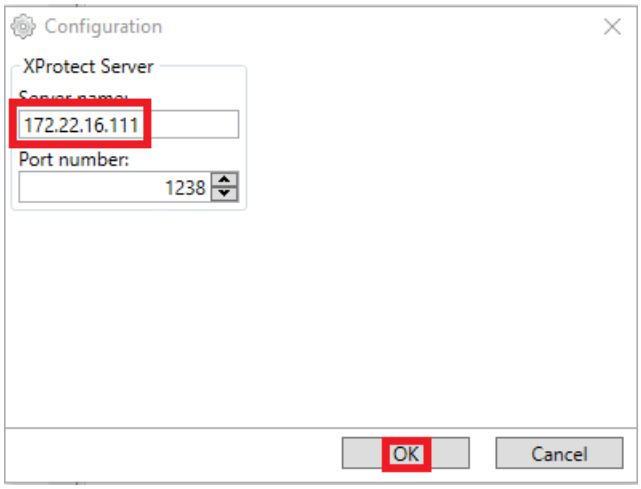



Figure 15. Adding the IP address of the computer running XProtect.

### Configuring XProtect

The Fiber SenSys Generic Event configuration in XProtect will need to be modified to allow connections from the other computer.

In Management Client, select the **Tools** menu and then the **Options...** item. Then select the **Generic Events** tab, select the **Fiber SenSys** item, and add the IP address for the computer running Integrator.

Then click **OK** to complete the change.

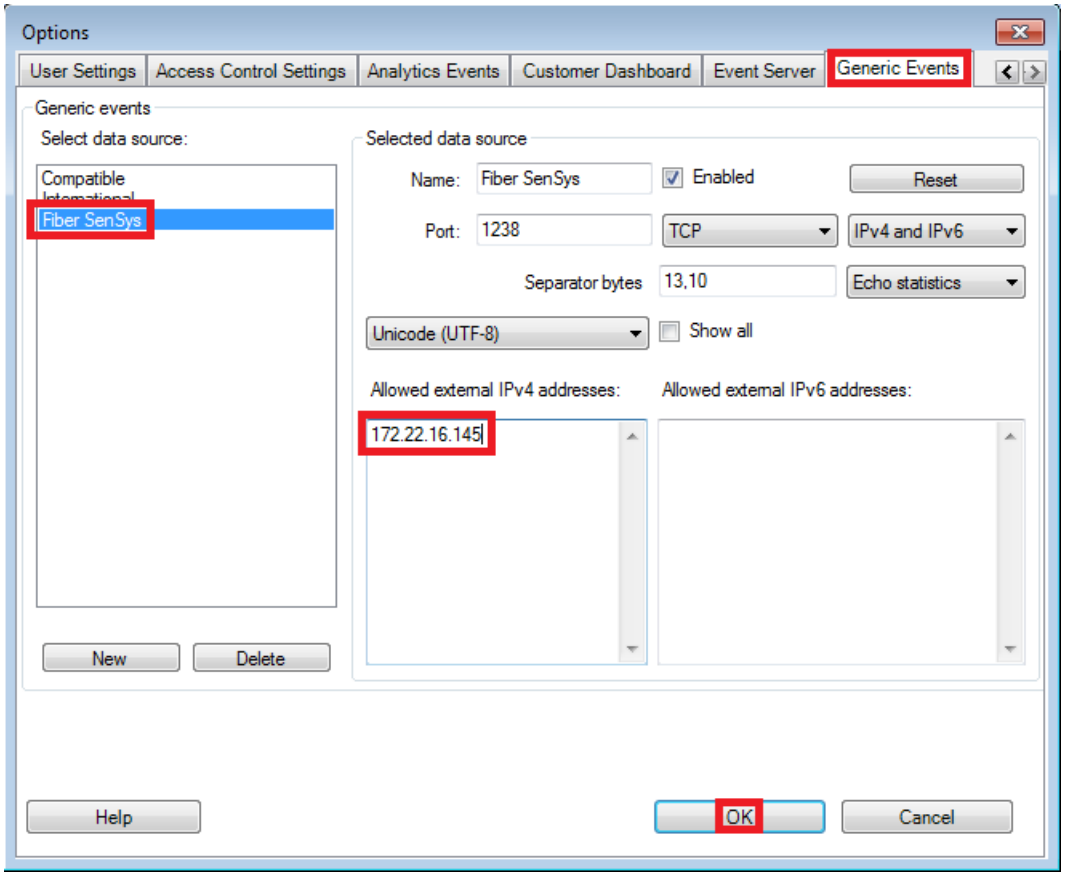



Figure 16. Adding the IP address of the computer running Integrator.

## Configuring Windows Firewall for XProtect

The Windows Firewall on the XProtect Event server must be configured to allow incoming connections. Start the Windows Firewall with Advanced Security application and create a new inbound rule.

**NOTE:** These instructions were written based on Windows 7 and Windows 10. Your version of Windows may have a different user interface for setting the firewall rules.

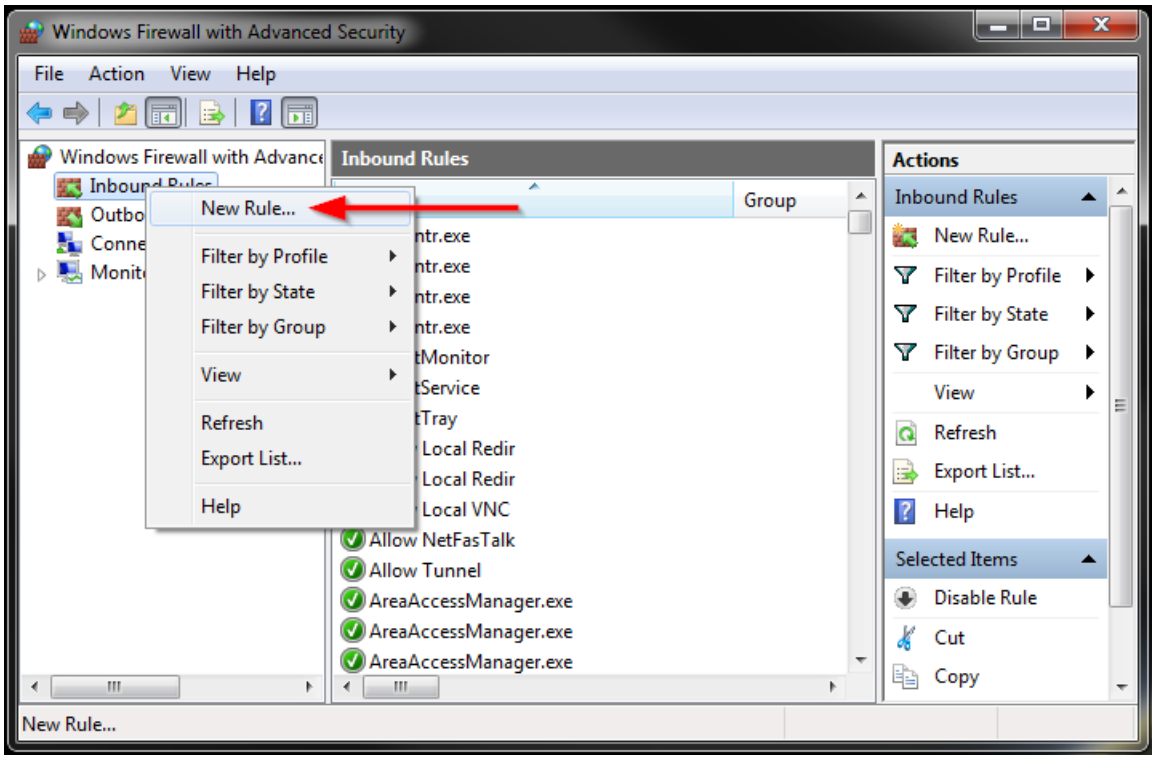


Figure 17. Windows Firewall new rule menu.

In the **New Inbound Rule Wizard** click **Port** then click **Next**.

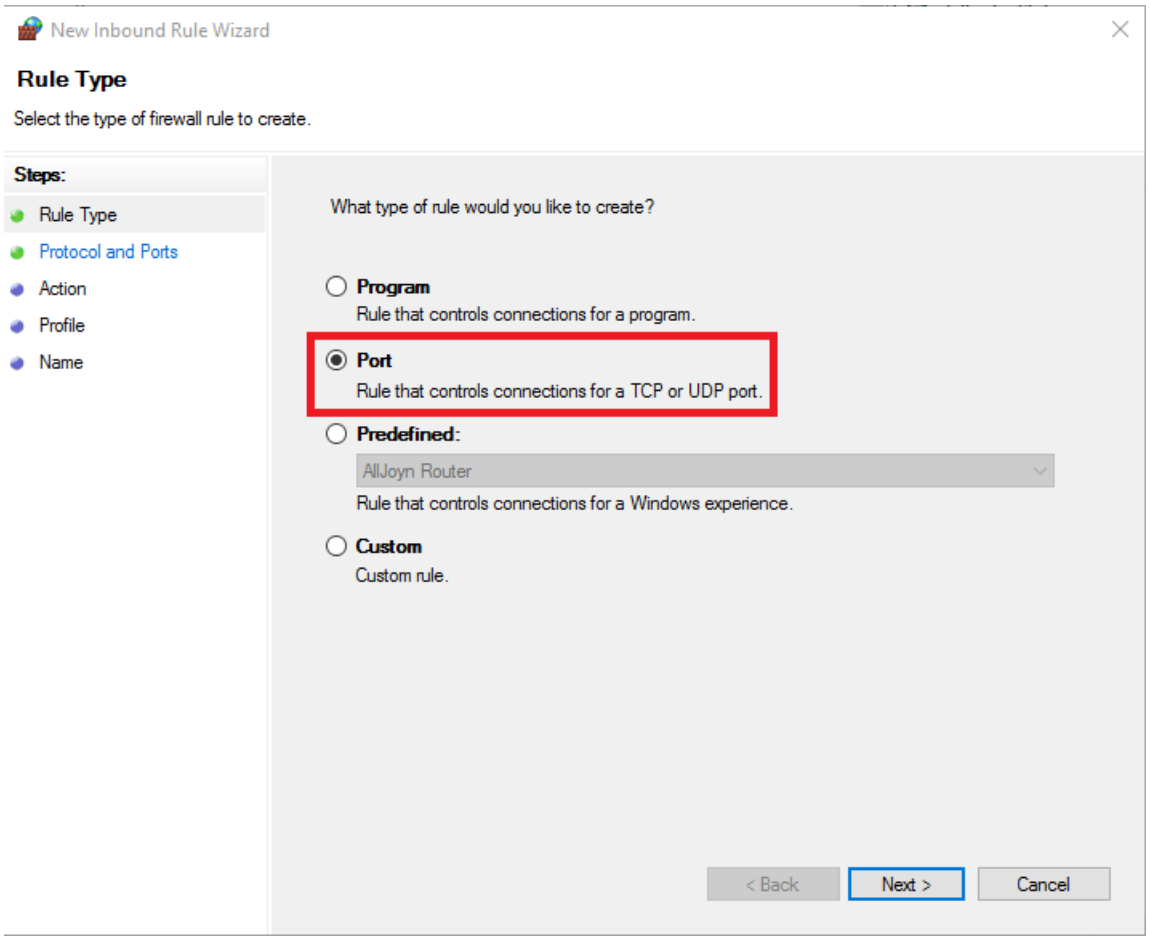



Figure 18. Windows Firewall rule options.

Select the **TCP** option and enter the port number for the Fiber SenSys Generic Event server. Then click **Next**.

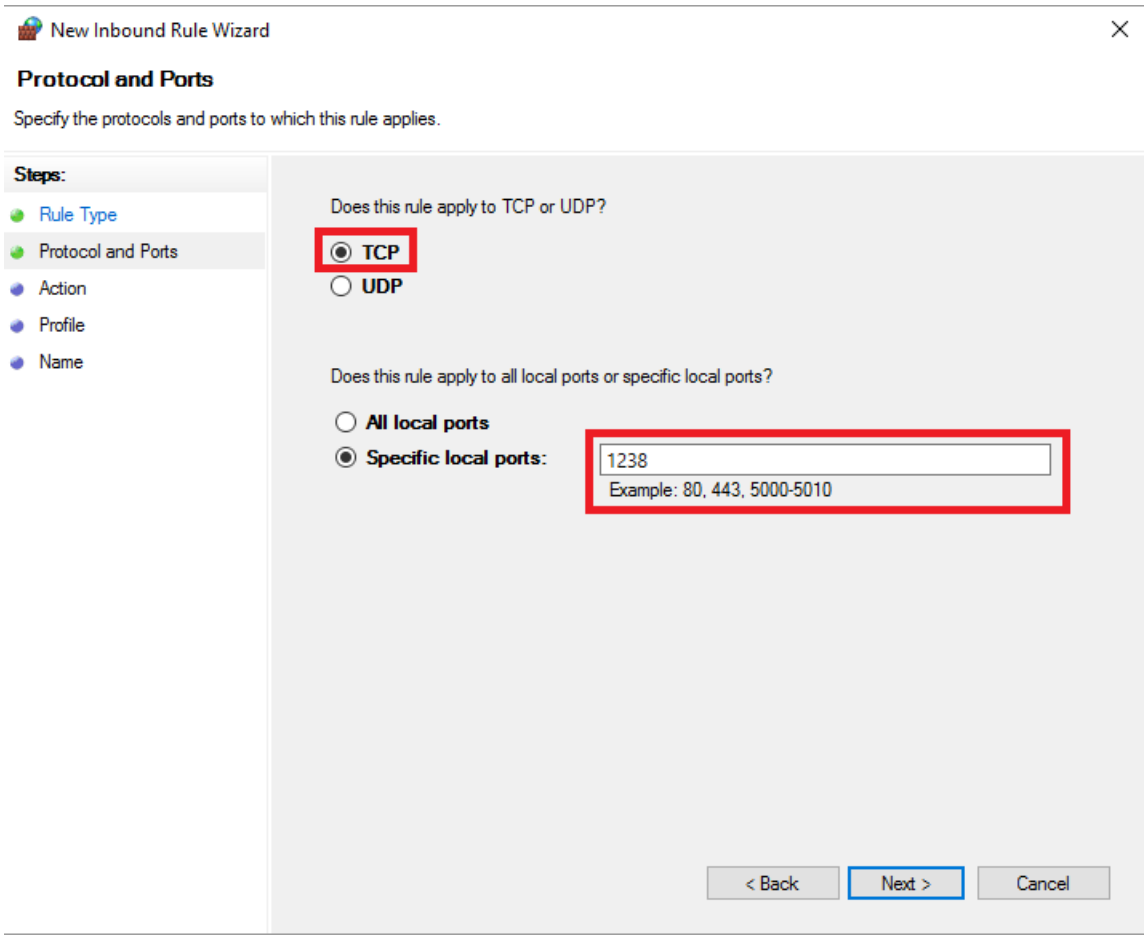



Figure 19. Windows Firewall port rule specification.

Click the **Allow the Connection** option, then click **Next**.

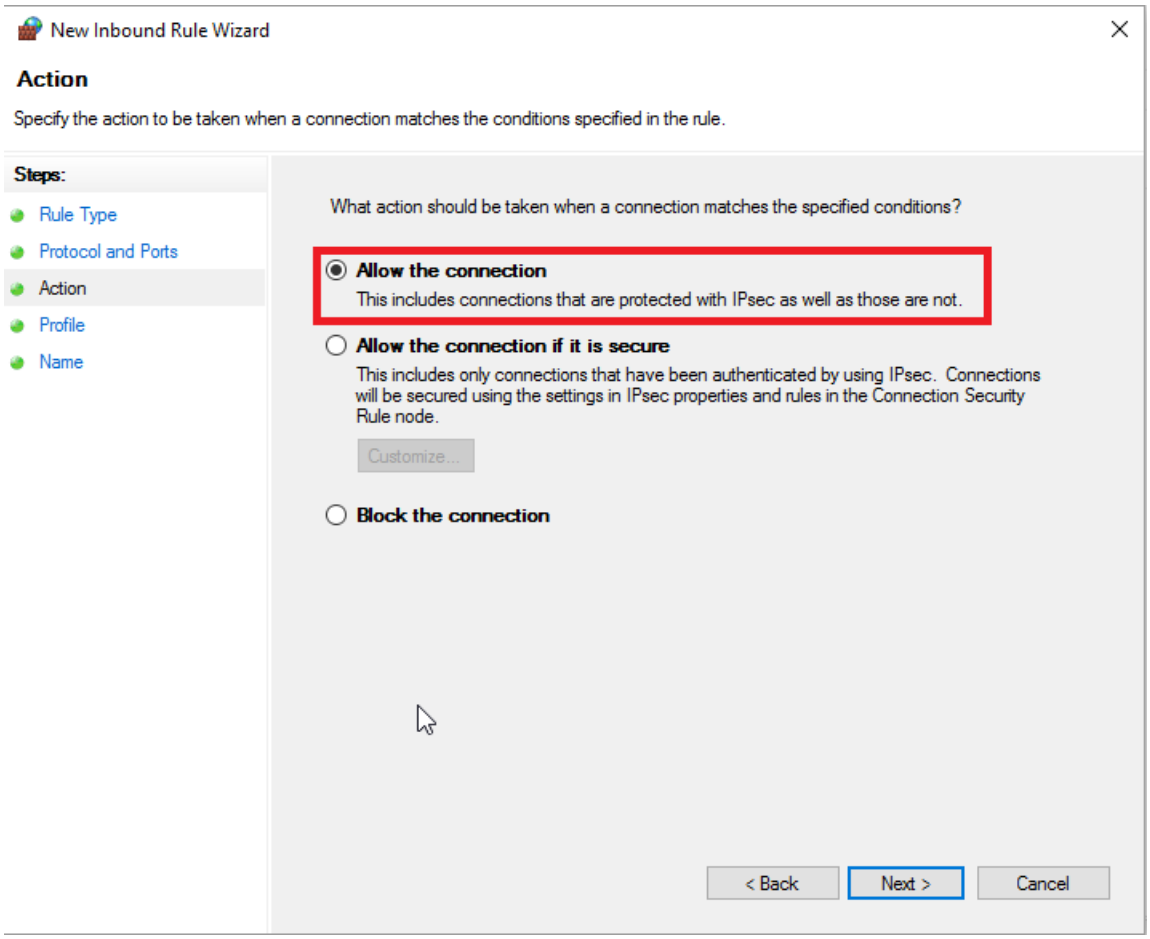



Figure 20. Allow incoming connections.

On the rule Profile panel, keep the default options and click **Finish**.

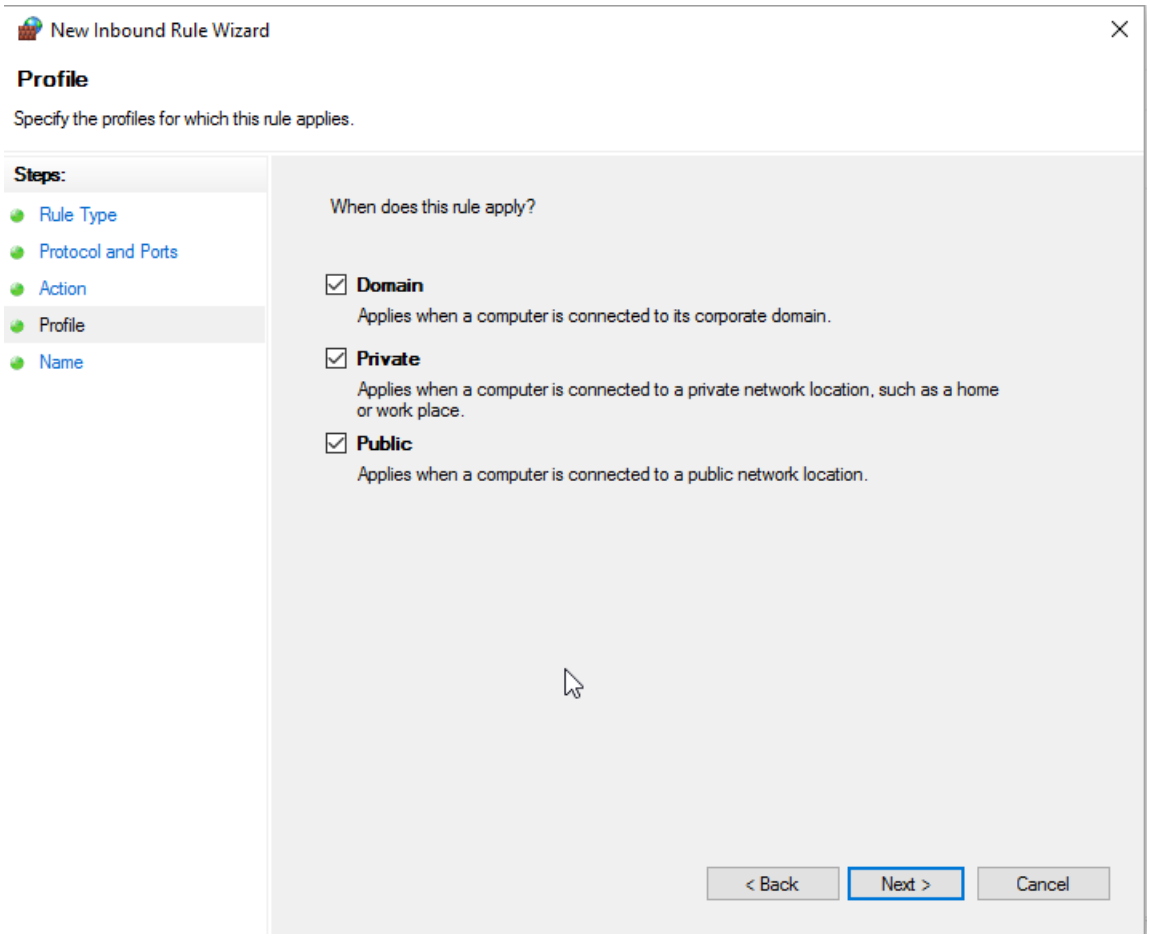



**Figure 21. Allow incoming connections under all conditions.**

## Appendix B: Supporting unusual APU networking configurations

Integrator should be able to connect properly to APUs configured for incoming connections according to the instructions in the *APU Networking Application Note*.

If, for some reason, your site has special networking requirements such that you cannot follow the instructions for incoming connections, you will have to determine which aspects of the section on adding APUs to Integrator must be adjusted for your site.

The rest of this appendix discussions certain specific adjustments that may or may not apply to your situation.

### Altered incoming connection port number

If an APU's port number for incoming connections has been changed from the default of 10001, then you will need to match the port number in Integrator.

To do this, set the port number along with the IP address when adding the APU. If you have already added the APU with the wrong port number, you will need to first remove the APU and then add it back with the proper port number.

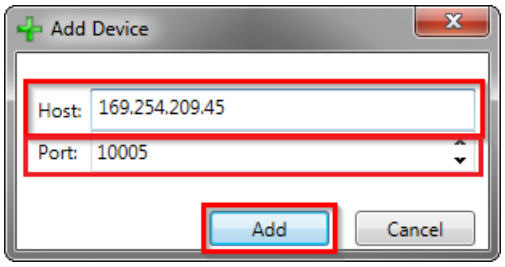



Figure 22. The Add Device dialog window with an adjusted port number.

### Outgoing connections

Integrator can be configured to accept connections initiated from APUs. This is useful when the APUs have been configured to make Outgoing Connections as described in the *APU Networking Application Note*.

To enable the listen server first enter the port to listen on in the **Port** box. The default port is 10000. Next select **Enable Listen Server**. The port cannot be changed while the server is running.

**NOTE:** Make sure the listen server port number is not in use by any other application.

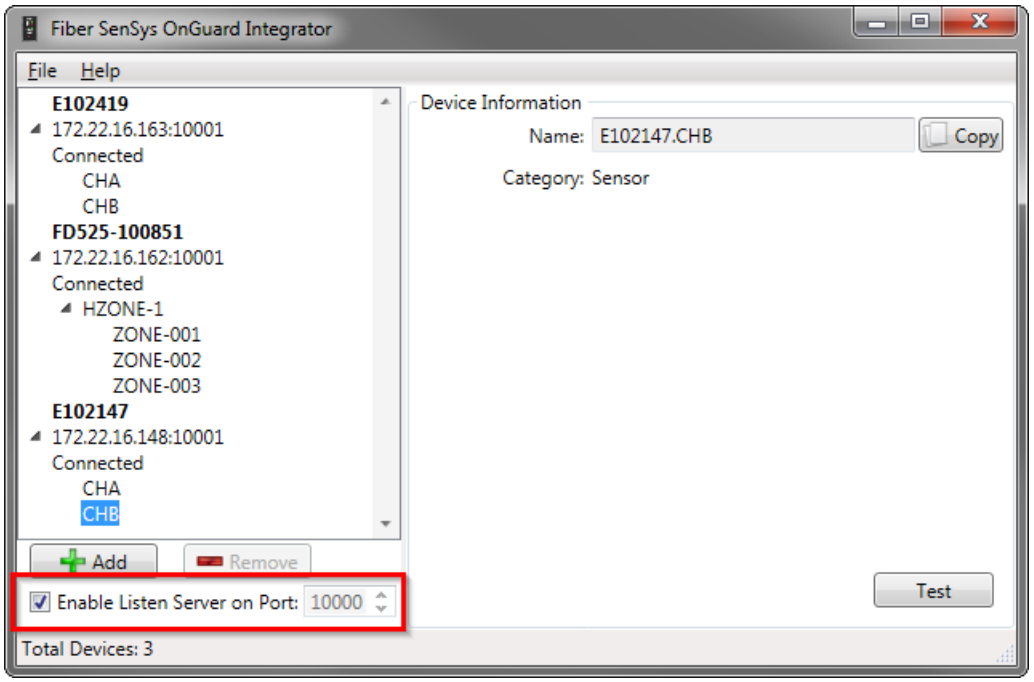



Figure 23. The listen server allows APUs to actively connect to Integrator.

When an APU connects to Integrator, the APU will automatically be added to the device list.

## Appendix C: Troubleshooting

If Integrator detects a problem while reporting test events to XProtect, a message will be shown. These messages indicate a problem with the connection to the Generic Event server.

If this occurs, verify that the IP address specified in Integrator matches the IP address for the computer running the XProtect Event server. Also verify that support for “Compatible” Generic Events has been enabled in Management Client and that the port number in Integrator matches the port number specified in Management Client.

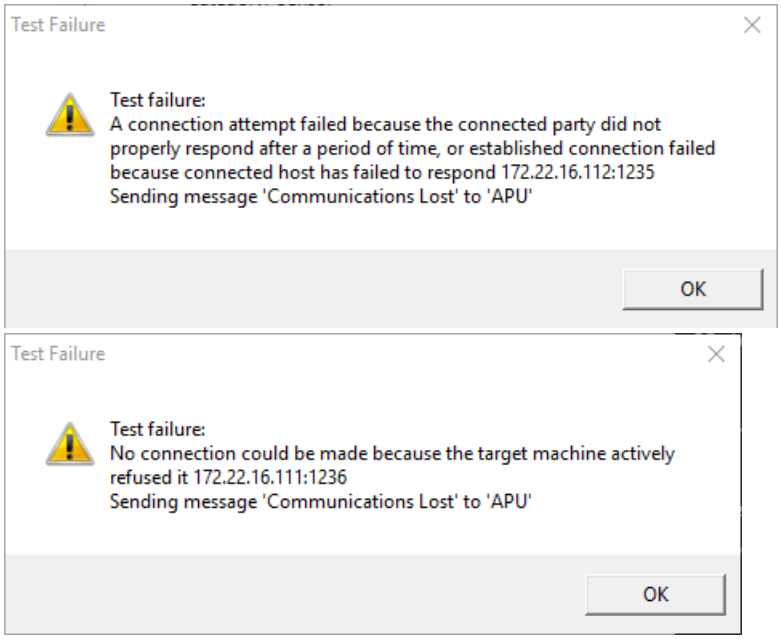



Figure 24. Example errors reported by Integrator.

### Troubleshooting problems with your XProtect configuration

This section is a supplement to the Generic Events section of the XProtect Administrator's Manual.

Once the messages are received by XProtect, Integrator won't be aware of any problems and cannot report them.

This document cannot describe how to configure XProtect to meet the requirements for your site. However, when difficulties are encountered, it can be helpful to create a simplified configuration to assist with troubleshooting.

This section will use the following fictional installation site as an example. In this site, there are two APUs. APU1 is a 500 series APU with 3 zones and APU2 is a 300 series APU with 2 zones.

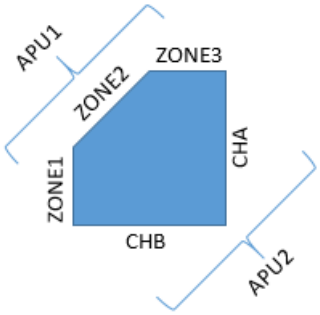



Figure 25. A rough site diagram for our example.

**NOTE:** For historical reasons, the ZONENAME is hierarchically constructed. For 300 series APUs the ZONENAME will look something like APU2.CHA. For 500 series APUs the ZONENAME will look something like APU1.HZONE1.ZONE1.

The exported file for this site would look like this:

```
The following is the list of intrusions to monitor:
```

```
"APU1:APU1.HZONE1.ZONE1:ALARM"
"APU1:APU1.HZONE1.ZONE2:ALARM"
"APU1:APU1.HZONE1.ZONE3:ALARM"
"APU2:APU2.CHA:ALARM"
"APU2:APU2.CHB:ALARM"

The following is the list of each trouble condition:
"APU1:APU1.HZONE1.ZONE1:FAULTON"
"APU1:APU1.HZONE1.ZONE2:FAULTON"
"APU1:APU1.HZONE1.ZONE3:FAULTON"
"APU2:APU2.CHA:FAULTON"
"APU2:APU2.CHB:FAULTON"
"APU1::COMMFAILON"
"APU1::TAMPERON"
"APU2::COMMFAILON"
"APU2::TAMPERON"

The following is the list of the END of each trouble condition:
"APU1:APU1.HZONE1.ZONE1:FAULTOFF"
"APU1:APU1.HZONE1.ZONE2:FAULTOFF"
"APU1:APU1.HZONE1.ZONE3:FAULTOFF"
"APU2:APU2.CHA:FAULTOFF"
"APU2:APU2.CHB:FAULTOFF"
"APU1::COMMFAILOFF"
"APU1::TAMPEROFF"
"APU2::COMMFAILOFF"
"APU2::TAMPEROFF"
```

Figure 26. The event list for our example site.

## Adding an example Generic Event

For this example, we will be adding a Generic Event for an intrusion on zone 2 of our example site.

In the **Rules and Events** section of Management Client, select **Generic Events**. Then, right click on the top **Generic Events** item and select **Add New...**.

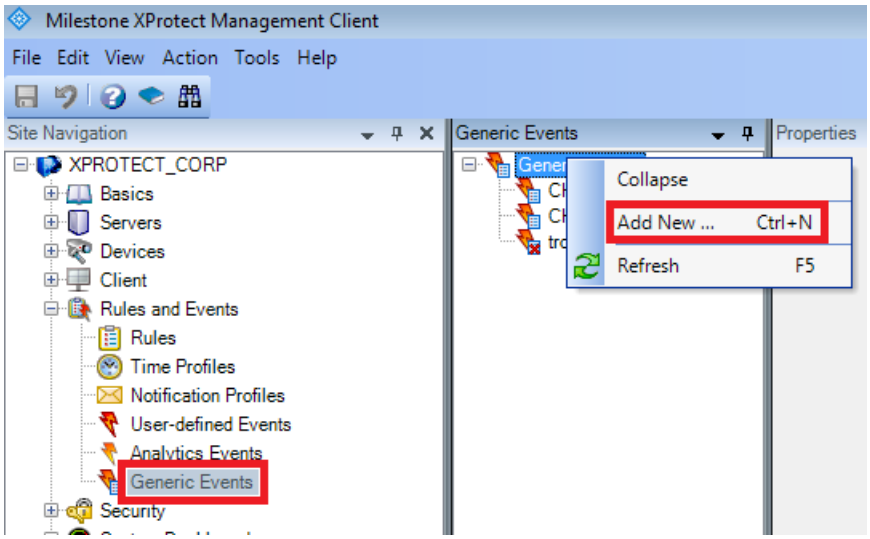



Figure 27. The Generic Events section.

A dialog window will appear. Enter the name of the event. This name will appear in the client interface, so you will want to make it descriptive. Click **OK**.

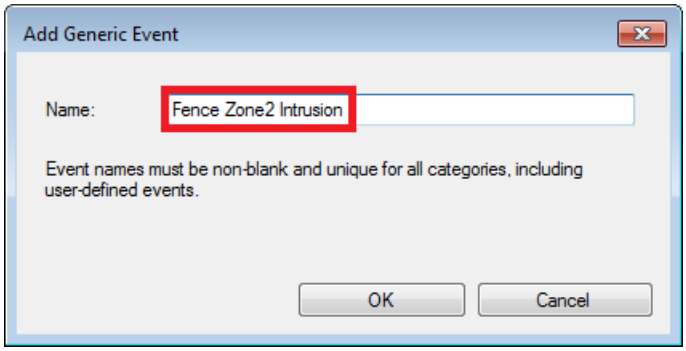



Figure 28. The Generic Event name dialog.

In the **Data source** dropdown, select the **Fiber SenSys** entry.

Now we must tell the Generic Event what messages to match. Copy the line of text from the *EventList.txt* file and paste it into the **Expression** field in the **Properties** pane for the Generic Event.

```
"APU1:APU1.HZONE1.ZONE2:ALARM"
```

Figure 29. A message description from the list of events.

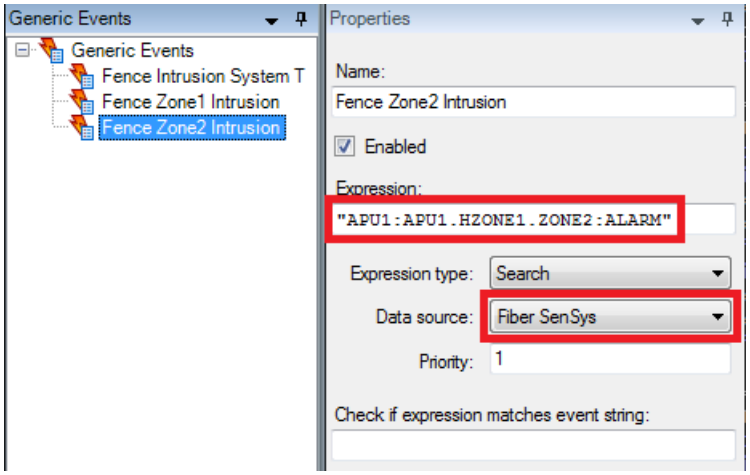



Figure 30. Generic Event properties.

Repeat these steps for each event you want to add.

For our example site, there would be 6 events: intrusions for zone 1, zone 2, zone 3, CHA, and CHB, and a trouble event for the entire system.

## Adding an example alarm

For this example, we will be adding an alarm to report to the guard an intrusion on zone 2 of our example site. This alarm will be based on the Generic Event added in the previous section.

In the **Alarms** section of Management Client, select **Alarm Definitions**. Then, right click on the top **Alarm Definitions** item and select **Add New...**. A new alarm will be created.

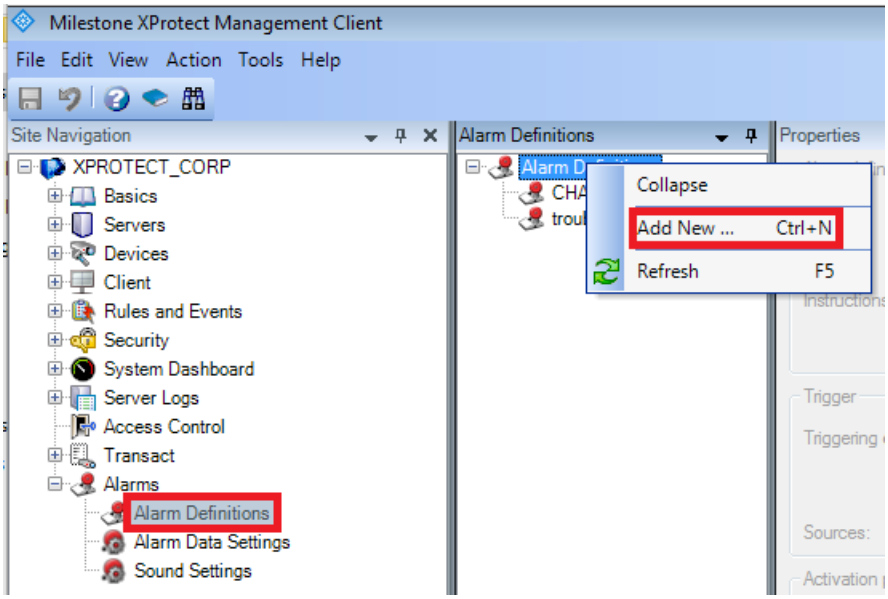



Figure 31. The Alarms section.

In the properties pane, edit the name of the alarm, select **External Events** as the triggering event, and click the **Select...** button.

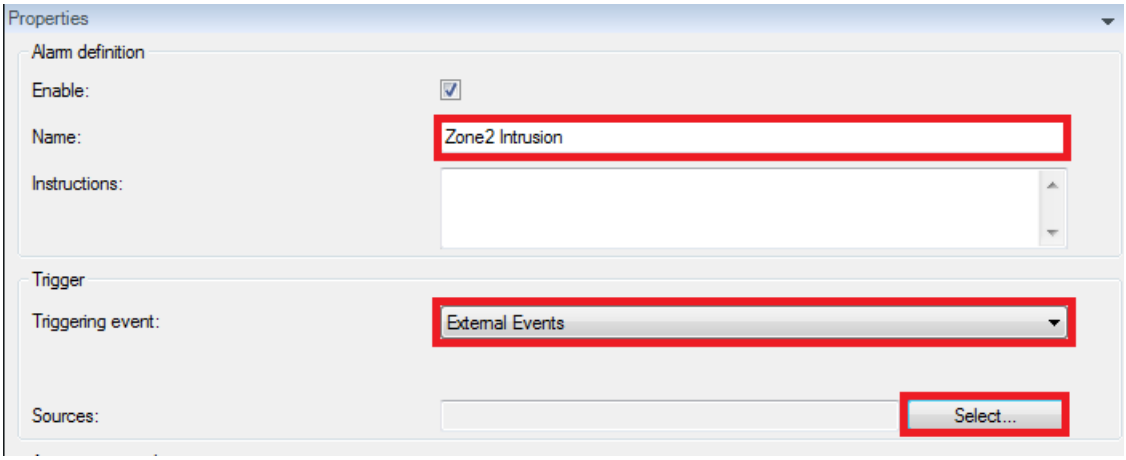



Figure 32. The alarm properties pane.

A dialog window will appear. Under the **Servers** tab, select the user-defined event for the zone 2 intrusion. Click **Add**, then click **OK**.

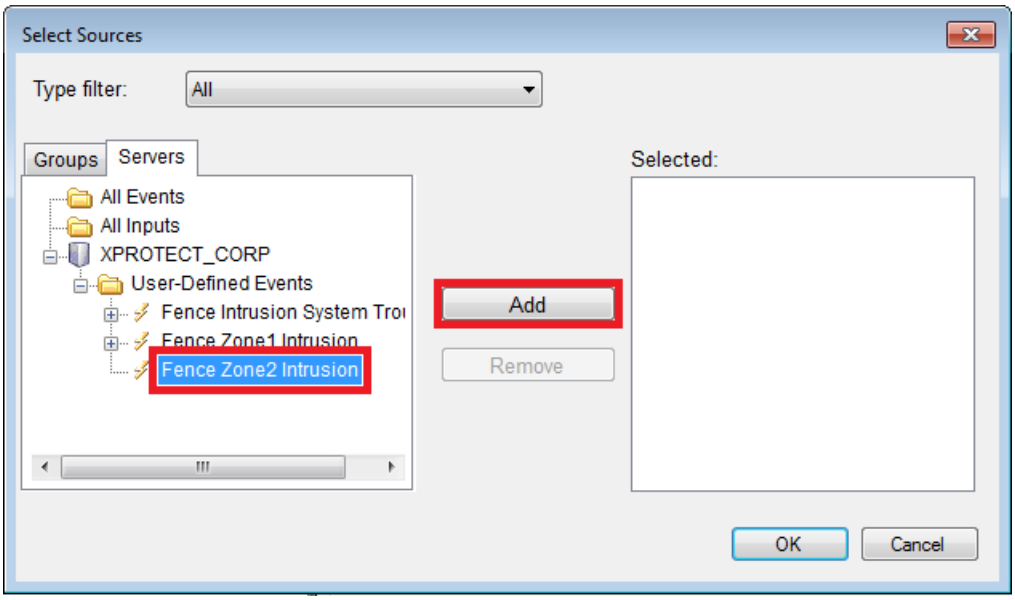



Figure 33. The alarm Select Sources dialog window.

To finish adding the alarm, click on some other alarm definition or other item. A dialog box will confirm that you want to save. Click **Yes**.

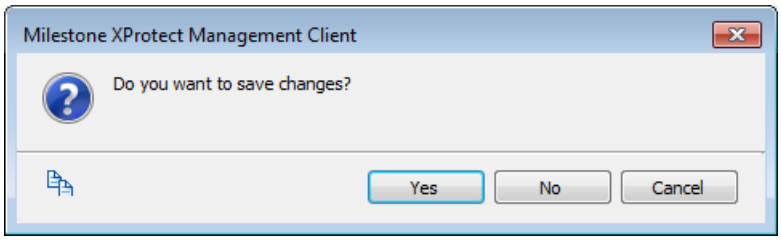



Figure 34. A save changes dialog window.

Repeat these steps for each alarm you want to add.

For our example, there would be 6 alarms: intrusions for zone 1, zone 2, zone 3, CHA, and CHB, and a trouble alarm for the entire system.

## Testing the example

Please read the main *Testing the integration* section for intructions on testing each APU and zone.

For our example site, the test button should cause two trouble alarms for APUs and an intrusion alarm plus a trouble alarm for zones.

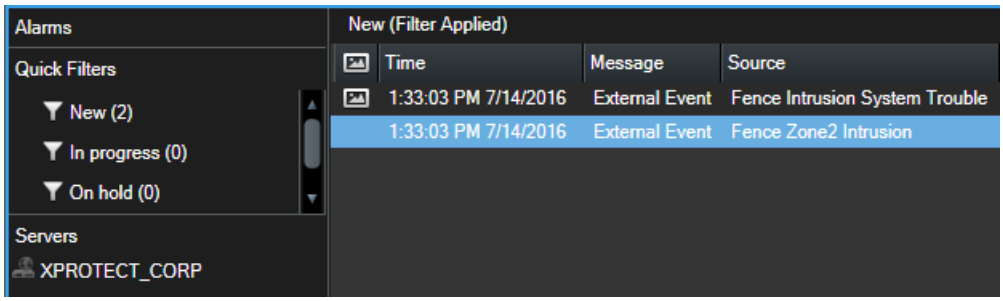



Figure 35. Example alarms in Smart Client.

## About Fiber SenSys

Fiber SenSys is the market leading manufacturer of fiber-optic intrusion detection solutions for government and military installations, airports, oil refineries, electrical substations, nuclear power plants, water purification and storage, corporate headquarters, and manufacturing facilities. As the only fiber optic solution that is PL-1 Nuclear Certified, Fiber SenSys products offer superior operations in the harshest environments. Simple installation with hand tools and designed for a 20 year lifespan, Fiber SenSys offers the lowest Total Cost of Ownership in the industry. In addition to keeping intruders out, Fiber SenSys intrusion detection systems can be used to protect the most important resources. Please visit the company's website where additional software and product information can be found: www.fibersensys.com.

**Corporate Office:**
2925 NW Aloclek Drive, #120
Hillsboro, Oregon 97124, USA
Tel: +1(503)692-4430
Toll free (US) +1(888)736-7971

Fiber SenSys®

HIGH PERFORMANCE ▪ HIGH RELIABILITY ▪ HIGH SECURITY