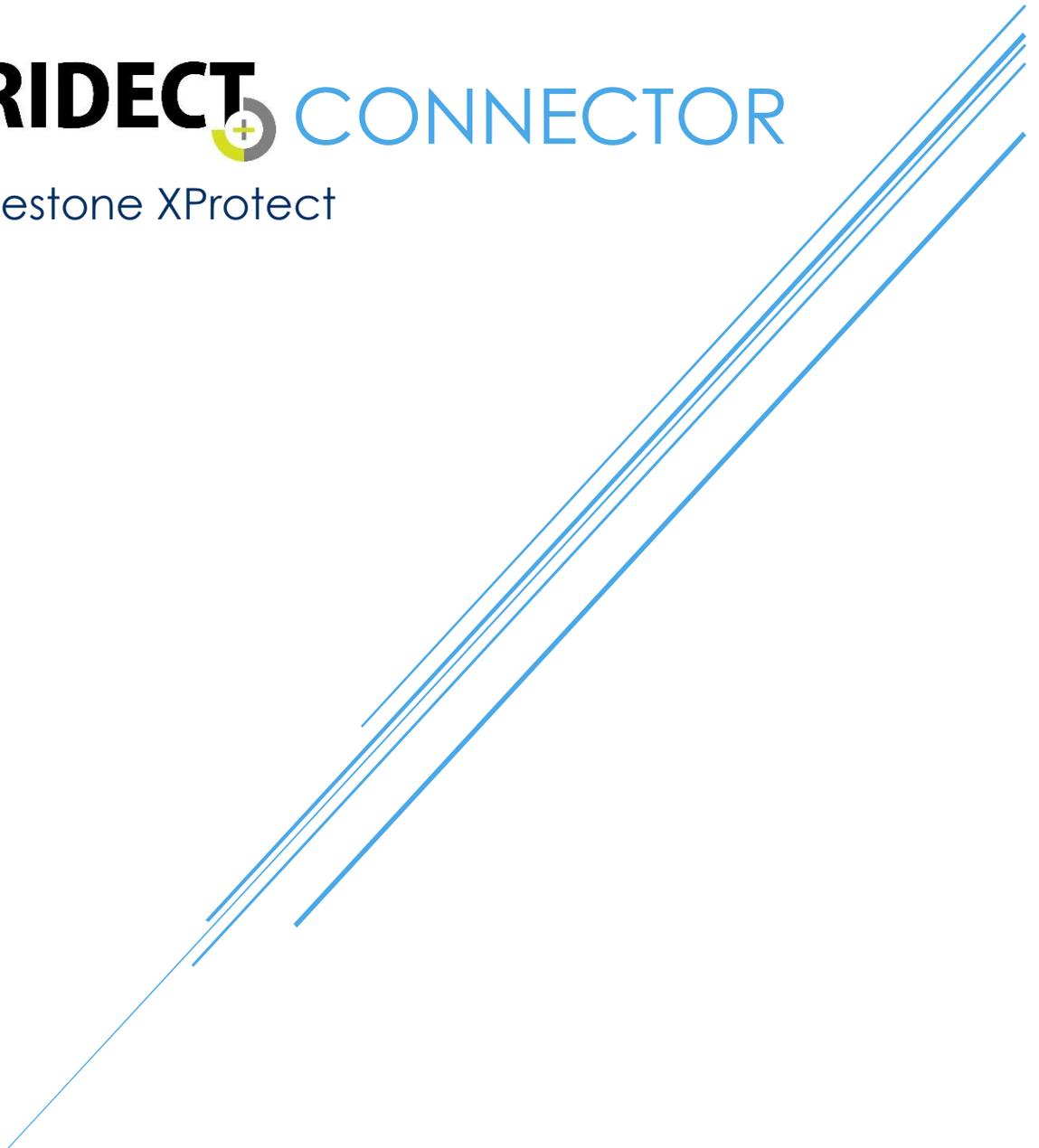




# PERIDECT CONNECTOR

for Milestone XProtect



## TABLE OF CONTENTS

1 Installation .....	2
2 License - overview.....	2
3 Connection configuration .....	3
3.1 New connection creation and editing.....	4
3.2 Connection testing.....	4
3.3 Deleting connection .....	4
4 Sensors and events configuration .....	5
4.1 Opening the DSP and LIP sensors list .....	5
4.2 Deleting sensors .....	5
4.3 Manual sensors events assignment .....	6
4.4 Sensor events change .....	7
4.5 Automatic events creation and assignment .....	7
4.6 Error events .....	8
4.7 Automatic error events creation and assignment .....	9
4.8 Additional options for events .....	9
4.9 Event load testing.....	10
5 Redundancy configuration .....	10
5.1 Redundancy configuration for single CUP .....	11
5.2 Redundancy configuration for chain connection .....	12
6 General configuration .....	13
6.1 Verbose logging .....	13
6.2 Test mode .....	13
7 Principle of the plug-in monitoring .....	14
7.1 Alarm state downloading.....	14
7.2 Status state loop .....	15

## 1 INSTALLATION

Plug-in is delivered as zip archive. To install the product it is needed to stop XProtect Event Server service (using services.msc or XProtect Event Server Manager) and XProtect Management Client. After this, please copy folder *Produs.PeridectPlus* from archive to XProtect install folders, by default it will be:

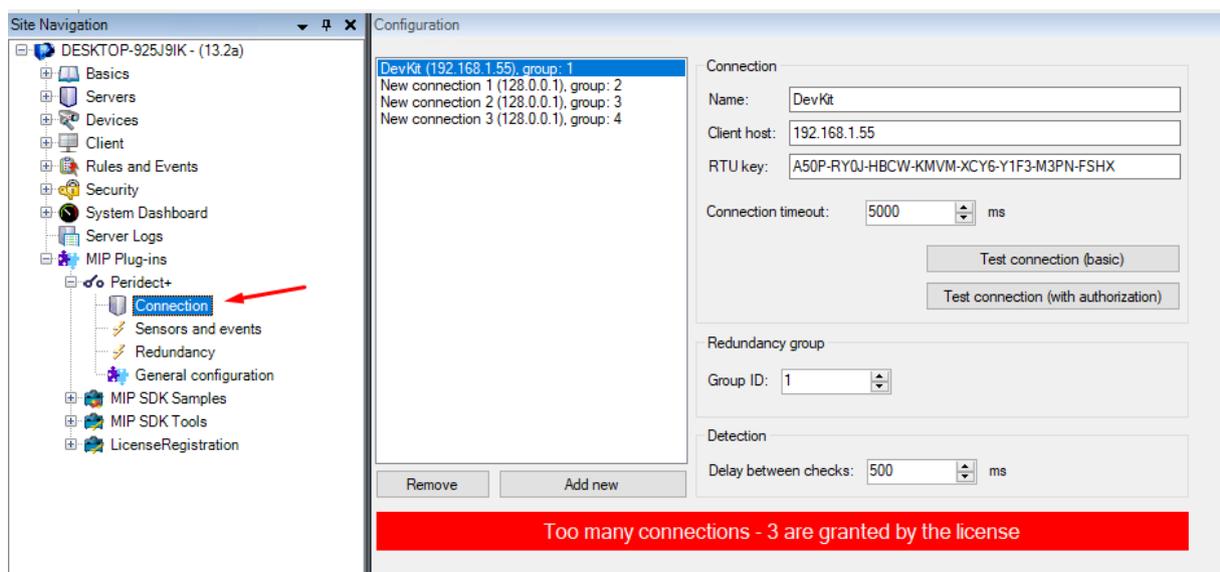
1. C:\Program Files\Milestone\XProtect Management Client\MIPPlugins\
2. C:\Program Files\Milestone\XProtect Event Server\MIPPlugins\

After files are copied, please start previously stopped service. Plug-in need to be installed on all computers where XProtect Management Client is installed.

## 2 LICENSE - OVERVIEW

Digital license for Peridect+ Connector is granted for total number of CUP units which will be communicating with XProtect software. In case number of connections allowed exceeded, plug-in configuration will be possible, but communication with all CUP units and event generation in Event Monitor will be disabled until excess number of connections will be deleted.

In case to many CUPs are added to the system (section [MIP Plug-ins] > [Peridect+] > [Connection]), an appropriate warning will be displayed:

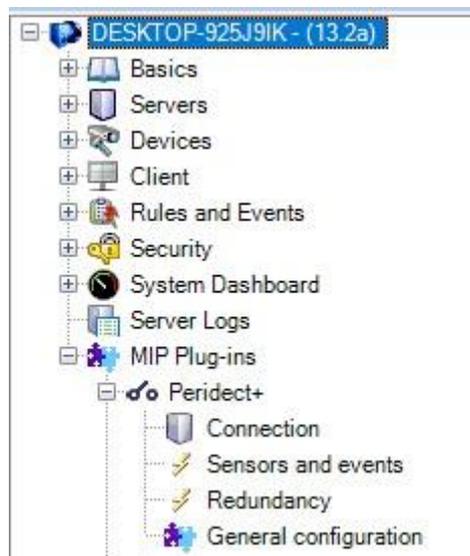


Accordingly, MIP Event Server will log errors as below:

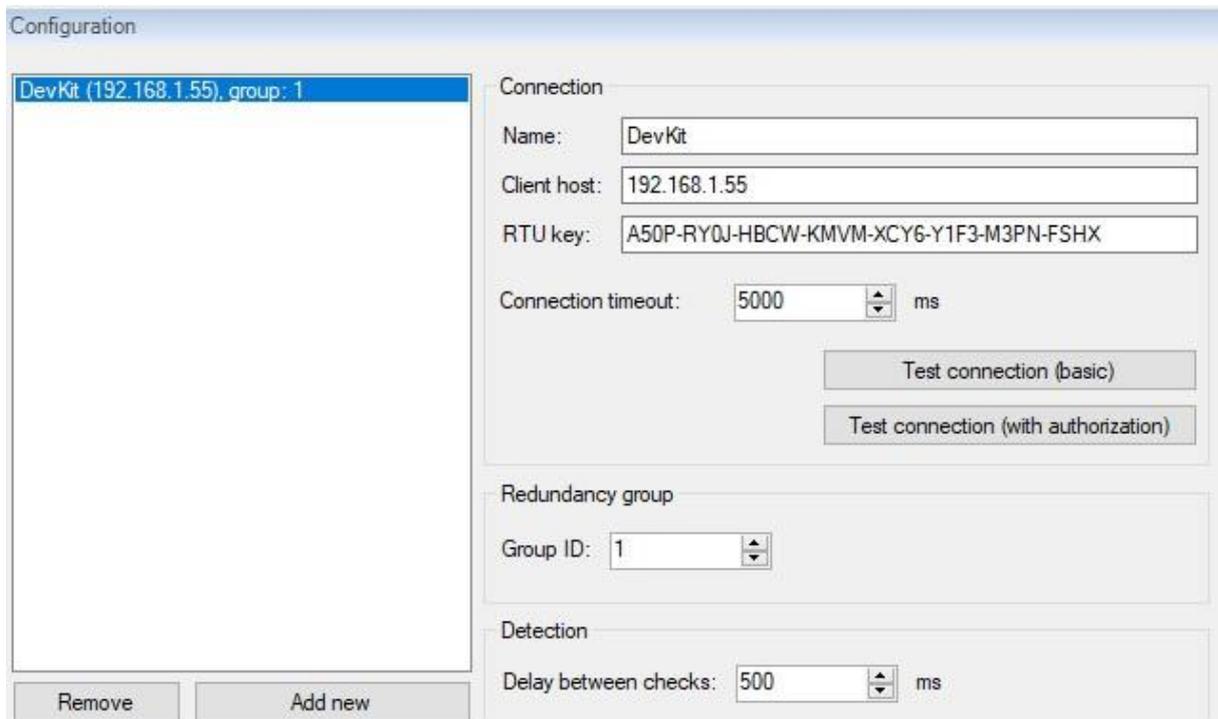
```
2019-07-01 21:32:46.171 UTC+02:00 Error Peridect+ background sensor monitor There are 6 connections out of 3 granted by the license. Aborting monitoring...
2019-07-01 21:32:46.171 UTC+02:00 Info Peridect+ background sensor monitor Cancelling state check task thread
2019-07-01 21:32:46.187 UTC+02:00 Error PostMessage Exception source: PeridectPlus
Exception type: VideoOS.Platform.LicenseMIPException
Exception message: Too many connections
Exception target site: PerformLicenseCheck
```

### 3 CONNECTION CONFIGURATION

Connection configuration of plug-in is done in XProtect Management Client in [MIP Plug-ins] section:



After expanding the [Peridect+] menu and selecting [Connection] the following screen will appear (one connection is already added in this example):



### 3.1 NEW CONNECTION CREATION AND EDITING

To add a new connection, click on the [Add new] button, and then complete the fields on the right side of the panel.

<b>Name</b>	Connection name, i.e. <i>CUP01</i>
<b>Client host</b>	IP address of CUP unit, i.e. <i>192.168.1.55</i>
<b>RTU Key</b>	RTU Key of CUP unit
<b>Connection timeout</b>	Time (in milliseconds) after which the connection will be reset and the "Ethernet Error" event will be sent if the plug-in does not receive a response within the set time.
<b>Group ID</b>	Connection group number - see the redundancy configuration section for more information
<b>Delay between checks</b>	Interval between subsequent central unit inquiries. It is not recommended to set this value less than 200ms.

**Please note that the connection parameters on the list will be updated only after reloading the list (or manually refreshing it).**

### 3.2 CONNECTION TESTING

To test the connection, first press the [Test connection (basic)] button. If any error occurs, please check:

1. If connection parameters are correct (IP address)
2. If there is network connection with CUP unit (i.e. using *ping* command)
3. If the Firewall is properly configured

When the basic connection test is successful, you can perform the authentication test using the [Test connection (with authorization)] button. In case this test fails, please check:

1. If connection parameters are correct (RTU Key)
2. Internal CUP configuration
3. NTP and time synchronisation settings (both on server and CUP unit)

**For communication to be successful, time difference between XProtect server and CUP units must not be greater than 5 seconds.**

### 3.3 DELETING CONNECTION

To remove a connection, select it in the list, and then click [Remove].

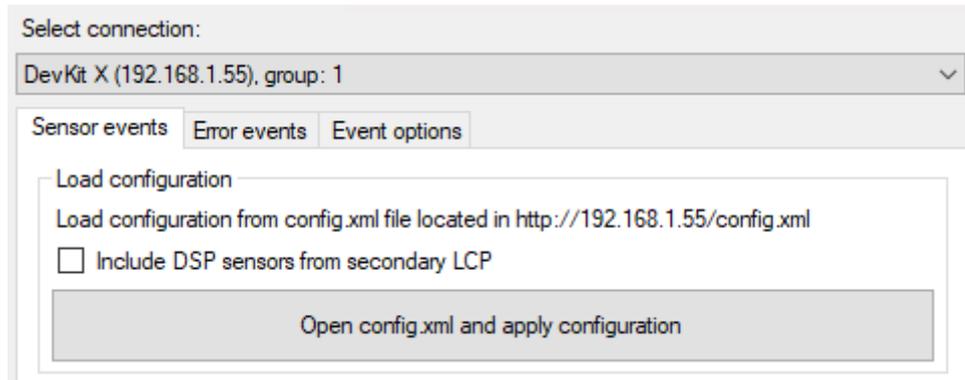
Please have in mind that when redundancy was configured for a given connection, its settings should be verified!

## 4 SENSORS AND EVENTS CONFIGURATION

The configuration of sensors and events is available in the [Sensors and events] menu.

### 4.1 OPENING THE DSP AND LIP SENSORS LIST

To add DSP and LIP sensors, download the config.xml file from the control panel configuration, then select the appropriate connection and press [Open config.xml and apply configuration]:

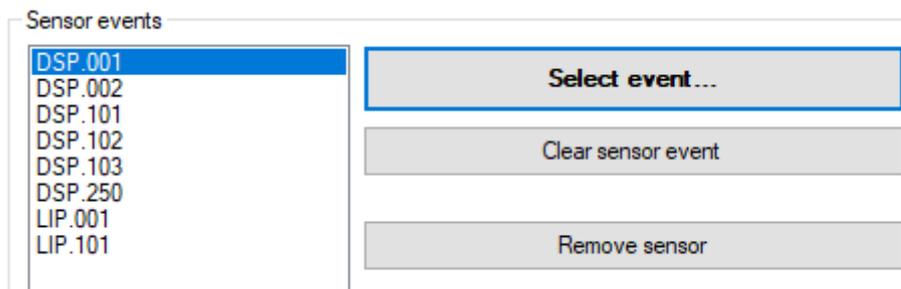


This will cause the available sensors to be assigned to events to appear in the [Sensor events] section.

If a given central unit has two LCP modules with connected DSP sensors that **will not** participate in redundancy, select [Include DSP sensors from secondary LCP] option to include them in the configuration readout.

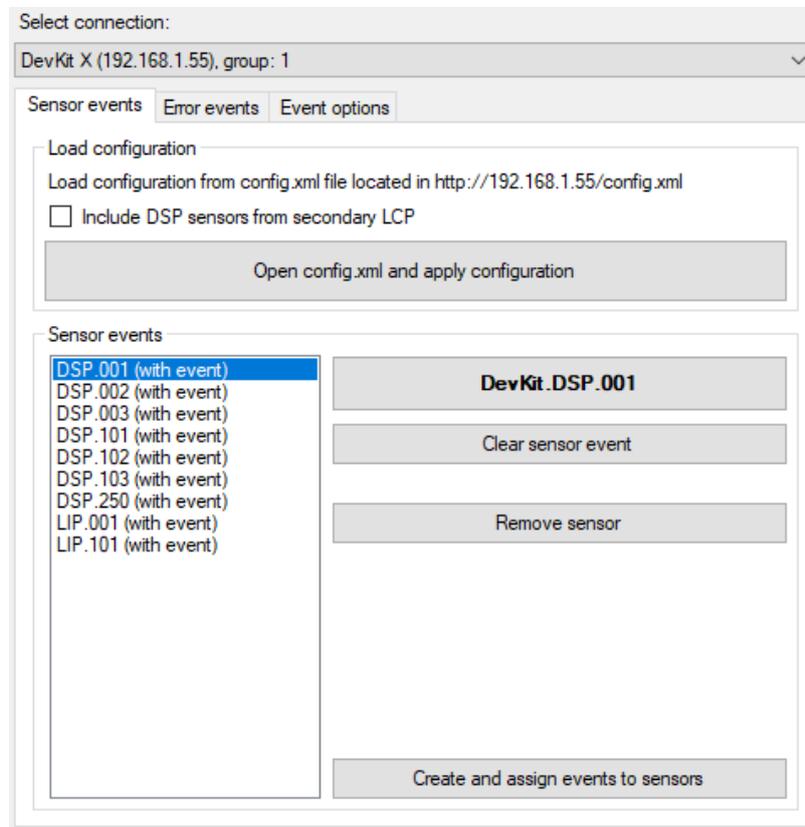
### 4.2 DELETING SENSORS

If the configuration file turns out to be incorrect and redundant sensors are added to the list, select the desired element and then click [Remove sensor].

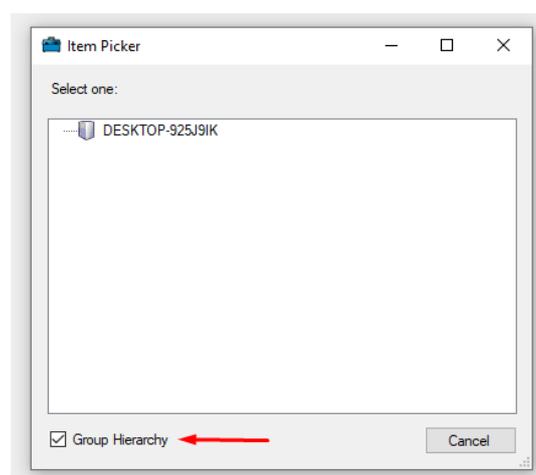


### 4.3 MANUAL SENSORS EVENTS ASSIGNMENT

After selecting the appropriate section in the Management Client application, selecting the connection and loading the config file beforehand, each sensor can be assigned a previously created user defined event in the [Sensor events] tab.



To do this, select the appropriate sensor and then press the [Select event ...] button. When the event selection window appears, uncheck the [Group Hierarchy] option and then select the desired item.



After selecting an event, the button to select it will change its name to the name of the selected event, and the sensor on the list will be marked accordingly.

#### 4.4 SENSOR EVENTS CHANGE

To change the event for a sensor that has already been assigned, select it in the list and click the button with the name of the existing event. The next steps are the same as in section 4.3.

To delete an assigned event, select the sensor in the list, and then click the [Clear sensor event] button. However, this will not delete the event - it must be done manually.

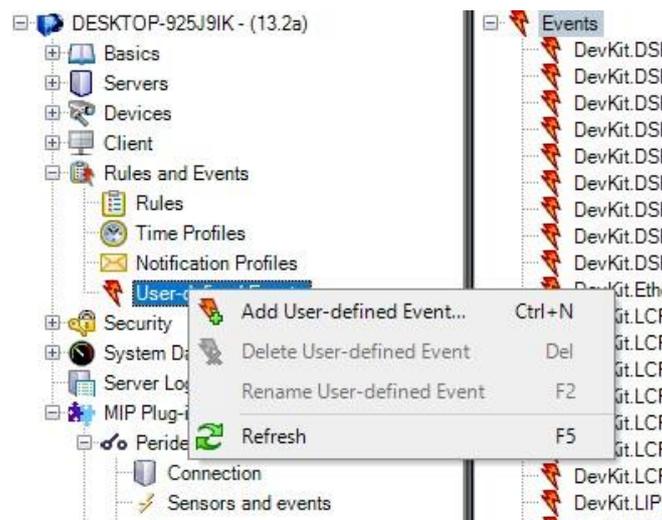
#### 4.5 AUTOMATIC EVENTS CREATION AND ASSIGNMENT

To automatically create the appropriate events and assign them automatically, click on the [Create and assign events to sensors] button. New events will be created according to the scheme:

- Connection\_name.DSP.000 for DSP sensors (where 000 is the sensor number)
- Connection\_name.LIP.000 for LIP sensors (where 000 is the sensor number)

If an event with the given name already exists (e.g. due to an earlier configuration), it will not be overwritten or a duplicate event will be created, but it will be assigned to the sensor.

**If after clicking the button the sensor list updates, but after selecting the sensor, the event selection button still behaves as if it has not been assigned (it is called [Select event ...]), you should manually refresh the list in the Management Client software.**



To do this, find the [User-defined Events] section, right-click and select [Refresh]. New events should appear on the list.

## 4.6 ERROR EVENTS

To configure which events should be triggered when a given error occurs, in the [Sensors and events] menu, select the appropriate connection from the list at the top, and then go to the [Error events] tab.

Select connection:  
DevKit (192.168.1.55), group: 1

Sensor events Error events Event options

Select error type:  
LCP1 Error  Active

DevKit.LCP1\_Error

Clear error event

Trigger event when retrieved flag is in state:  
High

Create and assign events to errors

In the [Select error type] section, select the appropriate type of reported error, and then select event similar to point 4.3.

The [Active] flag means whether the occurrence of a given error is checked by the plug-in, and if it is checked, it will not be triggered even if a given type of error occurs and the event is assigned. By default, all types of errors are set to active.

Depending on the configuration of the system, some errors should only be reported when they have a low flag (default for events is high), such as the configuration for many LIP modules. This option is changed by selecting the appropriate state for [Trigger event when retrieved flag is in state].

The default configurations for errors are listed in the table below:

The type of error	State when error should be triggered
LCP1 Error	High
LCP2 Error	High
ModbusRTU Error	High
ModbusTCP Error	High

Ethernet Error	High
Onvif Error	High
Real Time Clock Error	High
Temperature 1 Error	High
Temperature 2 Error	High
DSP on LCP1 Error	High
DSP on LCP2 Error	Low
LCP1 Active	Low
LCP2 Active	Low
LCP1 Designated Slave	High
LCP2 Designated Slave	Low

#### 4.7 AUTOMATIC ERROR EVENTS CREATION AND ASSIGNMENT

Similarly to point 4.5, pressing the [Create and assign events to errors] button will create and assign events. Event names are created according to the following scheme: Connection\_name.Error\_code.

The rules for creating events are similar to those in section 4.5.

#### 4.8 ADDITIONAL OPTIONS FOR EVENTS

In the [Event options] tab there is an option to suspend the triggering of an event when the previous one was triggered in a shorter time than specified (by default 5000 ms = 5 s).

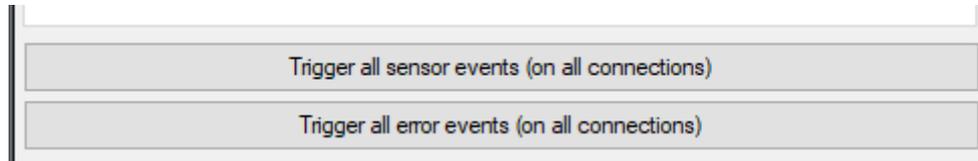
In this case, when the control panel reports an alarm on the sensor (or error), at least 5 s must pass for another event to be triggered.

Setting this option to less than the time between polls set in the connection configuration section is not recommended, because it cause the alarm will be triggered with each query (especially for LIP sensors).

## 4.9 EVENT LOAD TESTING

When many events for the control panels are created, the system stability should be tested in case the alarm is reported for each of them (e.g. when switching to redundancy mode).

The buttons at the bottom of the page [Sensors and events] are used for this:



[Trigger all sensor events (on all connections)] will trigger all configured events for sensors on all CUPs.

[Trigger all error events (on all connections)] will trigger all configured error events on all CUPs.

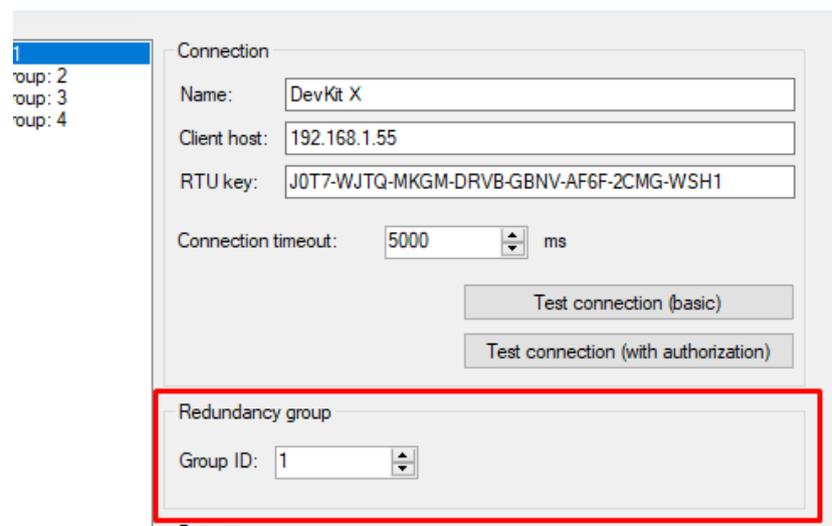
## 5 REDUNDANCY CONFIGURATION

Control panel redundancy can be configured for one control panel and chain, both for DSP and LIP sensors.

Before configuring redundancy, make sure that the connections are configured properly:

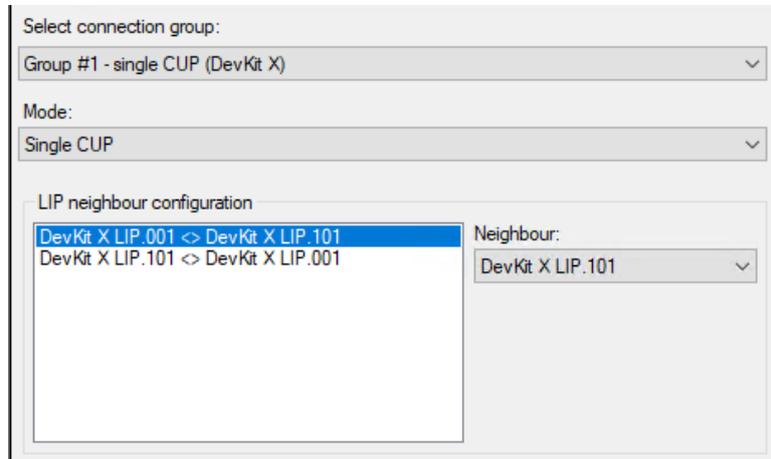
- The appropriate DSP and LIP sensors have been added for each central unit (in the [MIP Plug-ins]> [Peridect +]> [Sensors and Events] section)
- In the case of redundancy for a single CUP, the group number is unique
- For chain redundancy, each switchboard must have the same group number

The group number is set on the [MIP Plug-ins]> [Peridect +]> [Connections] page in the [Redundancy Group] section for each connection separately::

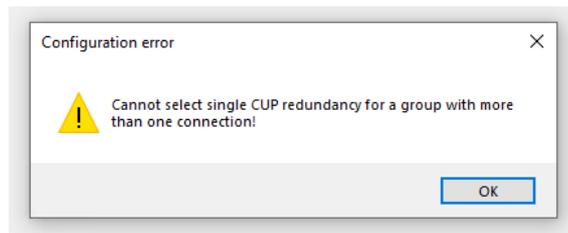
The image is a screenshot of a web-based configuration interface. On the left, there is a list of connections with group numbers 1, 2, 3, and 4. The first connection, "Group: 1", is selected. The main area shows the configuration for this connection. Fields include "Name" (DevKit X), "Client host" (192.168.1.55), and "RTU key" (J0T7-WJTQ-MKGM-DRVB-GBNV-AF6F-2CMG-WSH1). There is a "Connection timeout" field set to 5000 ms. Below these are two buttons: "Test connection (basic)" and "Test connection (with authorization)". At the bottom, there is a "Redundancy group" section with a "Group ID" dropdown menu set to 1. This section is highlighted with a red rectangular border.

## 5.1 REDUNDANCY CONFIGURATION FOR SINGLE CUP

After opening the [MIP Plug-ins]> [Peridect +]> [Redundancy] page, select the connection group from the [Select connection group] list, and then select [Single CUP] in [Mode]:



**Attention! If more than one connection is added to a given group, an error message will be displayed if you choose redundancy for a single CUP:**



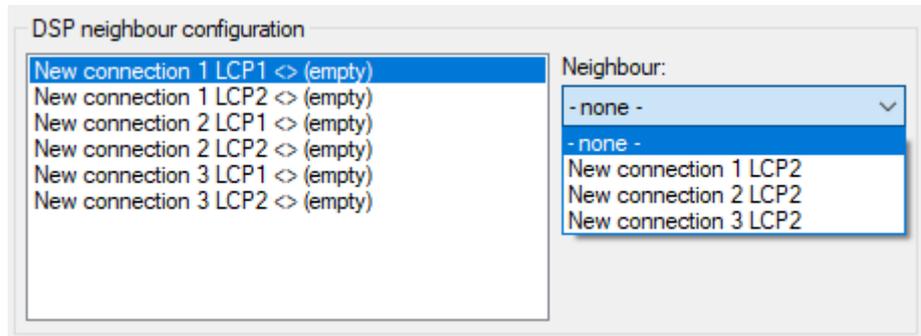
In the redundancy mode for a single CUP, only LIP sensors are configurable - DSP sensors operate in X, X + 500 pairs, i.e.:

- DSP sensor number 1 will have redundancy on sensor number 501
- DSP sensor number 2 will have redundancy on sensor number 502
- DSP sensor number 102 will have redundancy on sensor number 602
- etc.

For LIP sensor configuration, select the desired sensor in the [LIP neighbor configuration] section, and then select the appropriate sensor for redundancy from the [Neighbor] drop-down list. **This sensor will be automatically paired and marked accordingly on the list.**

## 5.2 REDUNDANCY CONFIGURATION FOR CHAIN CONNECTION

If the redundancy is based on connecting the CUP control units in a chain or loop, after selecting the connection group, set [Mode] to "Chain". In this case, the configuration should be started by defining neighbors in the [DSP neighbour configuration] section:



After selecting the connection (divided into LCP1 and LCP2 control panels), indicate the neighbor for the given connection. The list of available neighbors is available in the [Neighbor] list on the right. After selecting a neighbor, it will be automatically paired and updated in the list.

It should be borne in mind that the control panel's neighbor may only be the one with the "opposite" LCP, i.e. the connection with LCP1 may only be the connection with LCP2 and vice versa.

Next, you can configure LIP redundancy (similarly to section 5.1) - **in this case, the list of available LIP sensors for redundancy is possible to be selected only after determining the neighbors in the section for the configuration of DSP pairs!**

This is due to the fact that the available sensors for LIP redundancy can only come from the same unit or CUP directly adjacent to them.

## 6 GENERAL CONFIGURATION

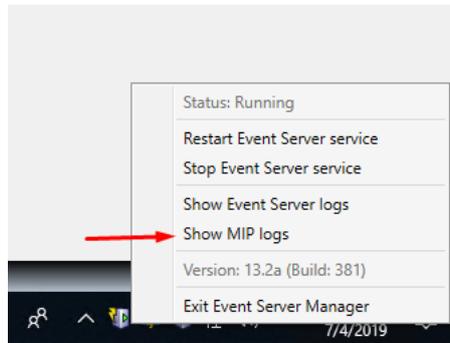
General settings are available on the [MIP Plug-ins]> [Peridect +]> [General configuration] page and contain options that are helpful in troubleshooting configuration problems.



**Attention! Use the above options carefully. Always check that these options are turned OFF when you put the system into production!**

### 6.1 VERBOSE LOGGING

[Verbose logging] - checking this option causes detailed logging in the Event Server (logs are available by right-clicking the Event Server icon in the system tray and selecting [Show MIP logs]):



This option enables logging detailed diagnostic data such as:

- Configurations found in Event Server
- Print out the details of the plug-in and connection initialization
- Alarms received from DSP and LIP sensors
- Errors received from CUPs

**Leaving this option enabled for a longer period of time will result in a large growth of the log file and, as a result, lack of disk space, which may result in system instability.**

### 6.2 TEST MODE

[Test mode] – after activating this mode, random alarms will be triggered at random intervals. This option is used to check the configuration of sensors and events.

When this option is enabled, the plug-in will not physically connect to the CUP control panel, thus it is not used for connection tests. The appropriate options can be found on the connection configuration screen.

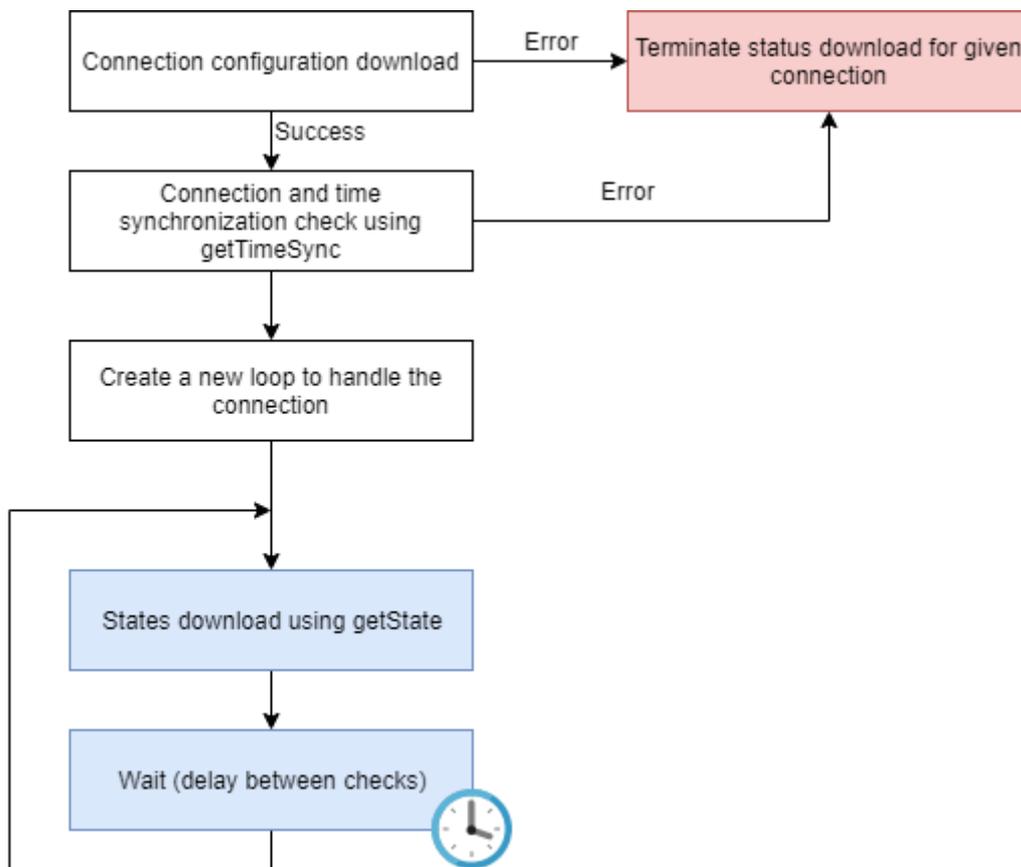
## 7 PRINCIPLE OF THE PLUG-IN MONITORING

The plugin runs its monitoring process on separate threads in Event Server. During each configuration change in the Management Client, a renewal configuration command is sent, which results in the monitoring being reset for all the control panels.

### 7.1 ALARM STATE DOWNLOADING

After running the plug-in, all connection configurations containing the RTU key and host address are downloaded (incorrect configurations are not taken into account), and then a separate thread is created for each connection, in which the states are downloaded.

The general scheme of operation is presented below:



The control panel polling loop is programmed with a configurable delay on the connection screen in the [Delay between checks] field. This is to prevent excessive network traffic and system load.

If an error occurs in the check loop, the system will try to continue working without breaking the loop, but will raise the "Ethernet Error" event. It will also be raised when the connection cannot be started.

## 7.2 STATUS STATE LOOP

The status state loop works independently of downloading them from the control panels – it is dictated by the need for simultaneous access to CUPs depending on the connection configuration.

This loop is performed with a frequency of about 10 times per second (so more often than even the minimum time for downloading states), which eliminates the delay in reporting alarms on sensors and triggering events for errors.

This architecture makes the system immune to connection errors (e.g. long response times), and enables "304 NOT MODIFIED" handling reported when calling the "getState" function.

