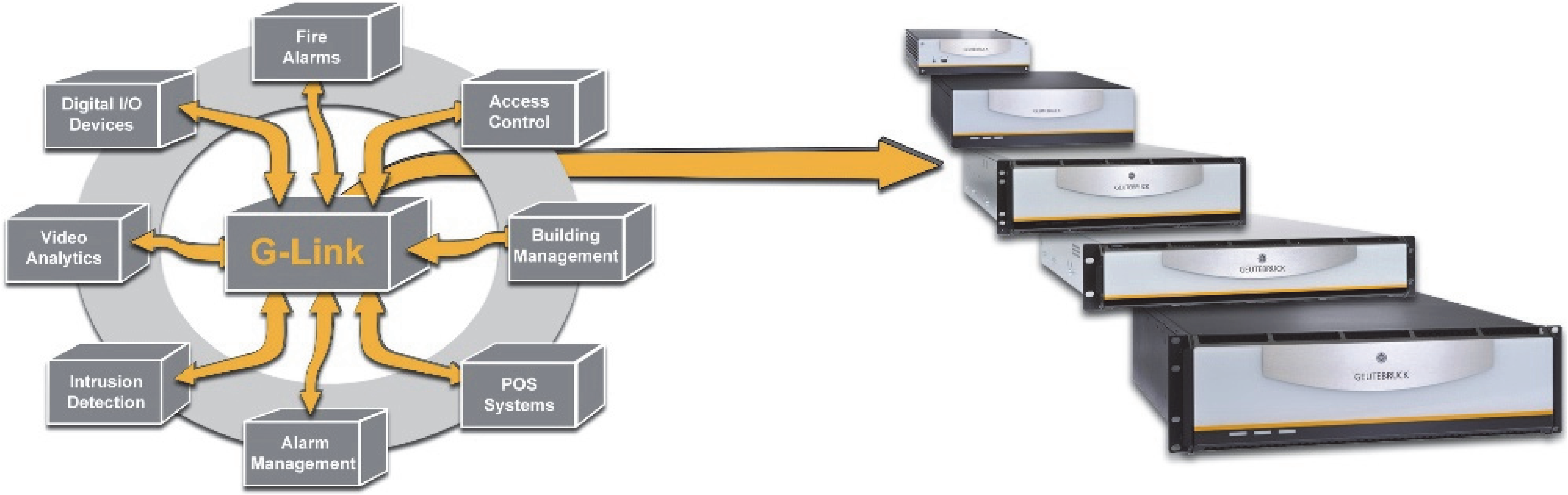
GEUTEBRÜCK

Excellence in Video Security

G-Link

G-Link Integrations-Server



User Manual

Note

This documentation may not be copied, translated or converted to a machine-readable form, whether in whole or in part, without prior permission.

GEUTEBRÜCK GmbH cannot guarantee the correctness of any information provided in this documentation, nor for the software or the information it contains. Any suggested guarantee, assurance of marketable quality or suitability for a specific purpose of the documentation, the software or other information is hereby explicitly rejected.

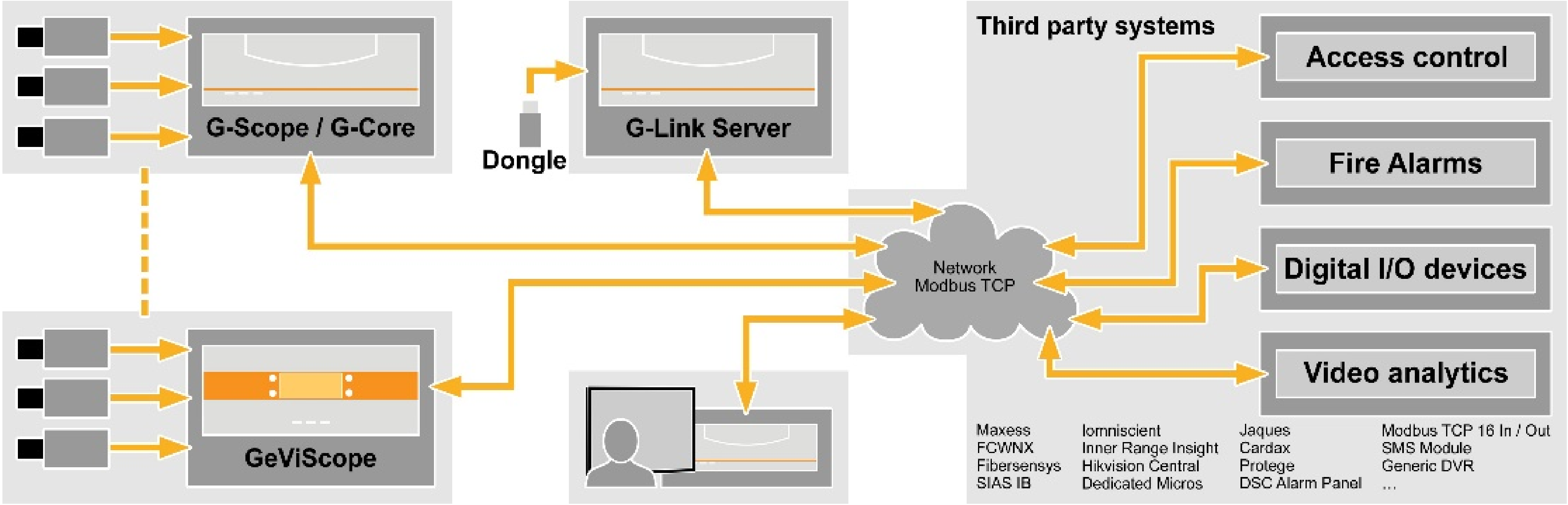
Under no circumstances is GEUTEBRÜCK GmbH liable for direct or indirect subsequent damage or for special subsequent damage resulting from or in association with this documentation, regardless of whether this arises as a result of illegitimate action, of a contract, or for other reasons in association with this documentation, the software or of the information contained or used within it.

GEUTEBRÜCK GmbH retains the right to change this documentation or the information contained within it at any time without warning. The software described in it is subject to the conditions of a special licence contract.

Please note that the illustrations in this documentation will not necessarily match those of your software version.

Contents

System Overview



Simple commissioning, configuration, robust functionality.
Fully automatic control of all system components and third-party systems.

The base G-Link server software is a Windows service that works without an active desktop. The software should be installed on a separate Windows server (PC) on which no other applications are running.

Optionally, a redundancy mode with two synchronized servers (computers) can be set up.

After initial installation, the G-Link server operates under full automation and connects with all integrated systems, for example, after disturbances to the network.

System Requirements

In order to use G-Link properly, your computer must have below software and components already installed. Prerequisites to be able to run properly are:

- Adobe PDF Reader
- .NET Framework 4.5 or later
- Microsoft Visual C++ 2008 SP1 Redistributable Package (x86)
- Microsoft Visual C++ 2010 Redistributable Package (x86)
- Microsoft Visual C++ 2013 Redistributable Package (x64) – 12.0.21005

Supported Operating System:

- Windows XP Professional SP 3 or later
- Windows 7 (32 Bit, 64 Bit)
- Windows Server 2003 SP 2 or later
- Windows Server 2008 (32 Bit, 64 Bit)
- Windows Server 2012 R2

> NOTICE Please note that TCP port range from 1021 to 1025, 5432, 8080 and HTTP port range from 80-81 or for SSL 443-444 (Default SSL is configured) are reserved for server's use. There should not be any other application that uses TCP ports on this range on host computer.

Introduction

Geutebrück G-Link Server enables integrated management of different hardware/software systems including CCTV, Access Control, Fire Alarms, Digital I/O devices, Video Analytics and so on.

> ADVICE It is recommended to have Intel I7 2.8 GHz processor or better and 4 (or more) GB of installed RAM on running computer. This application requires .NET 4.5 framework to be installed on computer.

G-Link is realized as a windows service. As a consequence it does not need a running desktop and starts automatically as soon as operating system initialization is completed. After first time configuration, operators do not need to make any other manual interventions. All of the tasks are automated; network problems and other abnormal situations are handled. Application reestablishes connections to integrated systems as soon as network problems are eliminated.

> NOTICE This windows service can be referred simply as “server” in this document.

Feature Overview

- Third party software integrations: DVR, NVR, Access Control, Intrusion Detection etc.
- Complex Alarm Management
- I/O management
- Control of Cameras: PTZ, remote configurations
- Mapping of event through third party security softwares
- Easily integrate new drivers
- Support unlimited driver types
- Customize driver using parameters
- Refine event transfers (prefix, suffix etc)

Configuration Client

Since server does not have a graphical user interface, a configuration client is needed. GEUTEBRÜCK G-Link Server can be configured with G-Link Setup software. It enables you to configure all settings remotely over TCP/IP.

You can see a shortcut to G-Link Server Setup on desktop after successful installation. As mentioned before it enables you to configure and manage server.

To connect to server please add new connection by right clicking in the Connections pane. Default username is sysadmin and default password is masterkey. Password can be changed from server menu after connecting to server. You can add, edit and remove channels easily. Please click on the Send setup to server button after you complete setup changes.

> NOTICE Note that synchronously (at the same time) only one G-Link Server Setup can be connected to server.

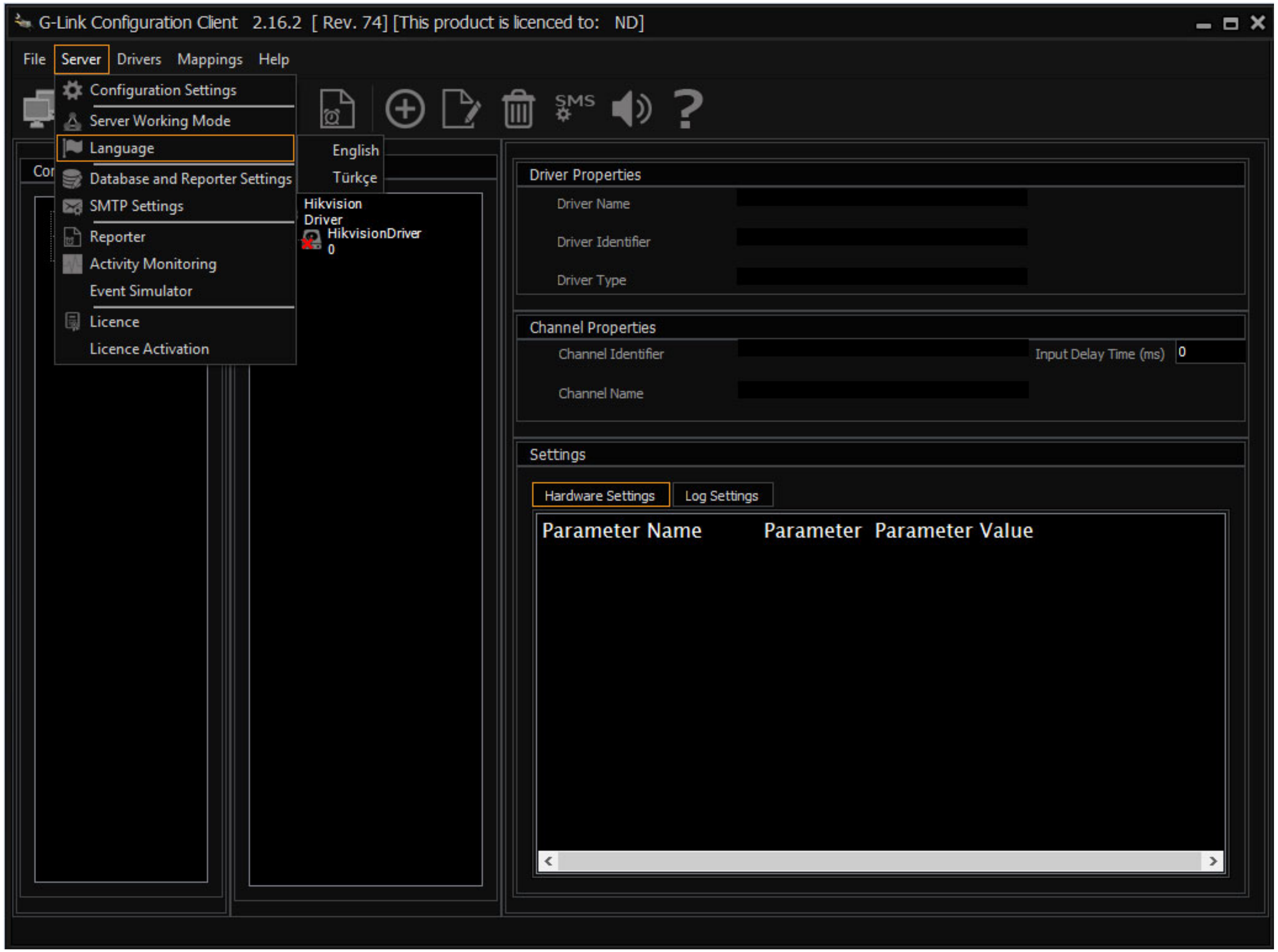
You can see connection statuses of the channels from plugins tree view. By waiting on the channel’s label you can see more information related to connection status of a channel. Even for more detail about connection statuses and error messages please have a look at application event log of Windows.

All connection loses are logged to application event log as a warning and all connection establishments are also logged to application event log as an information. It is recommended to set maximum event log size to 2048 KB on windows XP platform, which is 512 KB by default. To change maximum log size, please go to *Control panel* -> *Administrative Tools* -> *Computer Management* -> *System Tools* -> *Event Viewer* -> *Application*, than please right click on *Application* and select *Properties*, you should see maximum log size parameter there.

Multilanguage Support

G-Link is a multilingual platform. A wide range of languages provided to users such as English, French, Italian, German, etc. G-Link also allows to add new languages to system.

The languages which are defined on G-Link can be switched easily. In order to switch languages in G-Link, go to Language menu item in Server menu. The languages in system can be seen and can be chosen.



G-Link Configuration Client 2.16.2 [Rev. 74] [This product is licenced to: ND]

Driver Properties

Driver Name

Driver Identifier

Driver Type

Channel Properties

Channel Identifier

Input Delay Time (ms) 0

Channel Name

Settings

Hardware Settings | Log Settings

Parameter Name	Parameter	Parameter Value

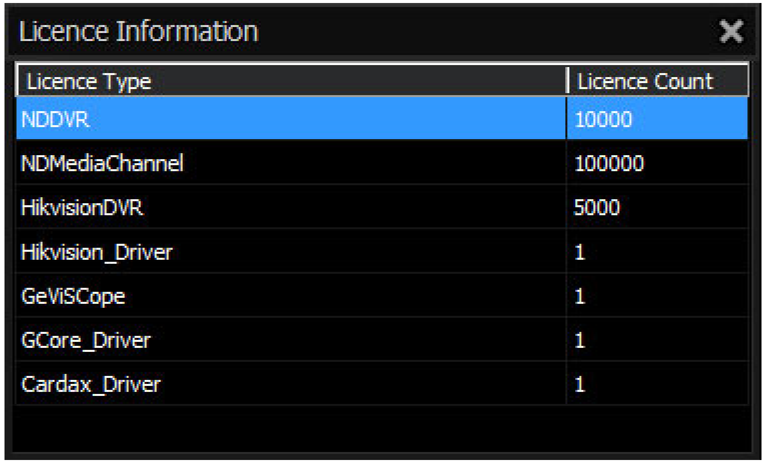
Licenses

Licence menu shows the licence numbers of the system parts such as cameras, alarm systems, alarm panels etc. *Server->Licence* menu item should be clicked for viewing licences.

> NOTICE Please note that licence changes are checked at every 30 seconds. You don‟t need to restart G-Link Server if licences are applied/changed.

To be able to use your licences, licence activation/verification is required. For licence activation your physical machine must have a working internet connection. Licence activation is done only once, so having an internet connection for just a couple of minutes is enough. After licence activation is performed you may use your system forever without any internet connection.

If you change number of licences you use, re-activation is required.

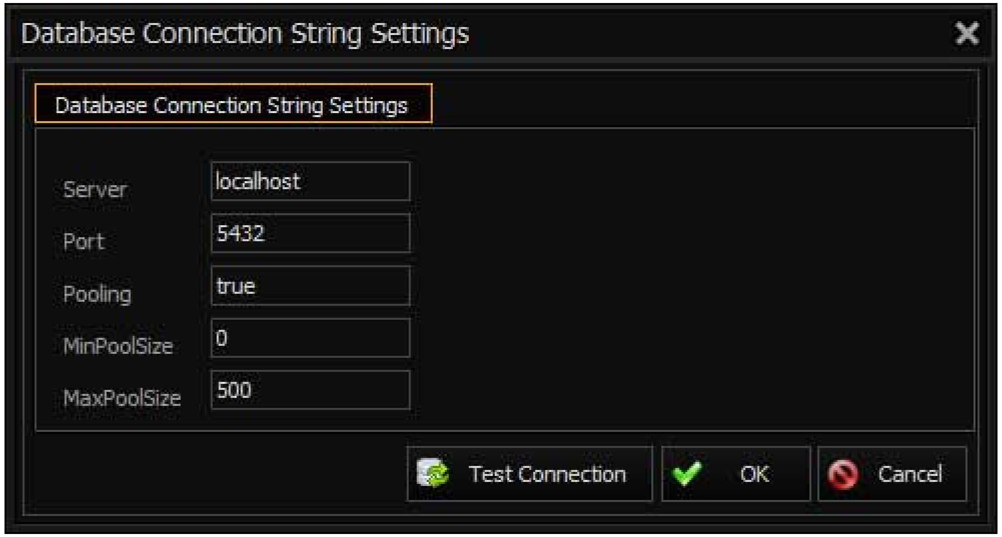


Licence Information

Licence Type	Licence Count
NDDVR	10000
NDMediaChannel	100000
HikvisionDVR	5000
Hikvision_Driver	1
GeViSCope	1
GCore_Driver	1
Cardax_Driver	1

Database Settings

Database Settings allows changing and testing database parameters. You can open that page from *Server->Database Settings*.



Database Connection String Settings
Database Connection String Settings
Test Connection
OK
Cancel

Server localhost

Port 5432

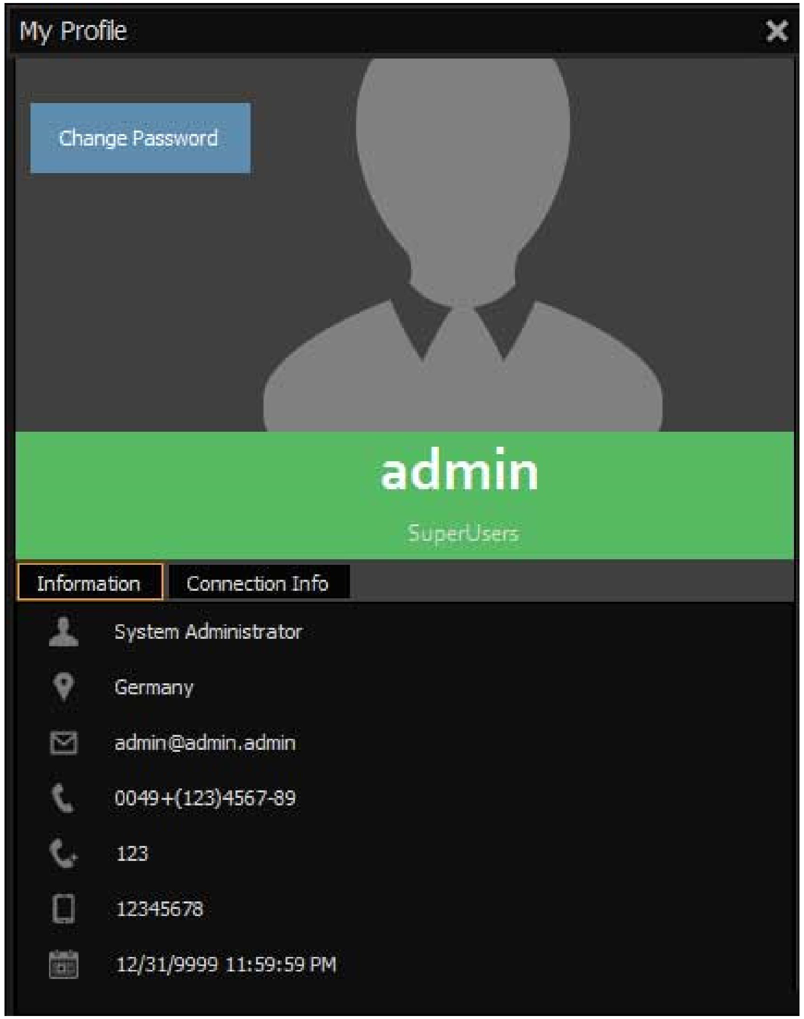
Pooling true

MinPoolSize 0

MaxPoolSize 500

Server, port and other parameters can be set via this page. Also it is possible to test database connection clicking to Test Connection button. If connection is OK, operator will see ✓icon next of button.Otherwise, operator will see ✗icon.

Profile Settings



My Profile

Change Password

admin

SuperUsers

Information | Connection Info

System Administrator

Germany

admin@admin.admin

0049+(123)4567-89

123

12345678

12/31/9999 11:59:59 PM

The operator is able to see his/her personal information from *Server* -> *Configuration Settings* -> *My Profile*. The operator is also able to change password by clicking the *Change Password* button. Connection info tab contains login information such as last logged device, last login time, last logout time, etc.

SMS Settings

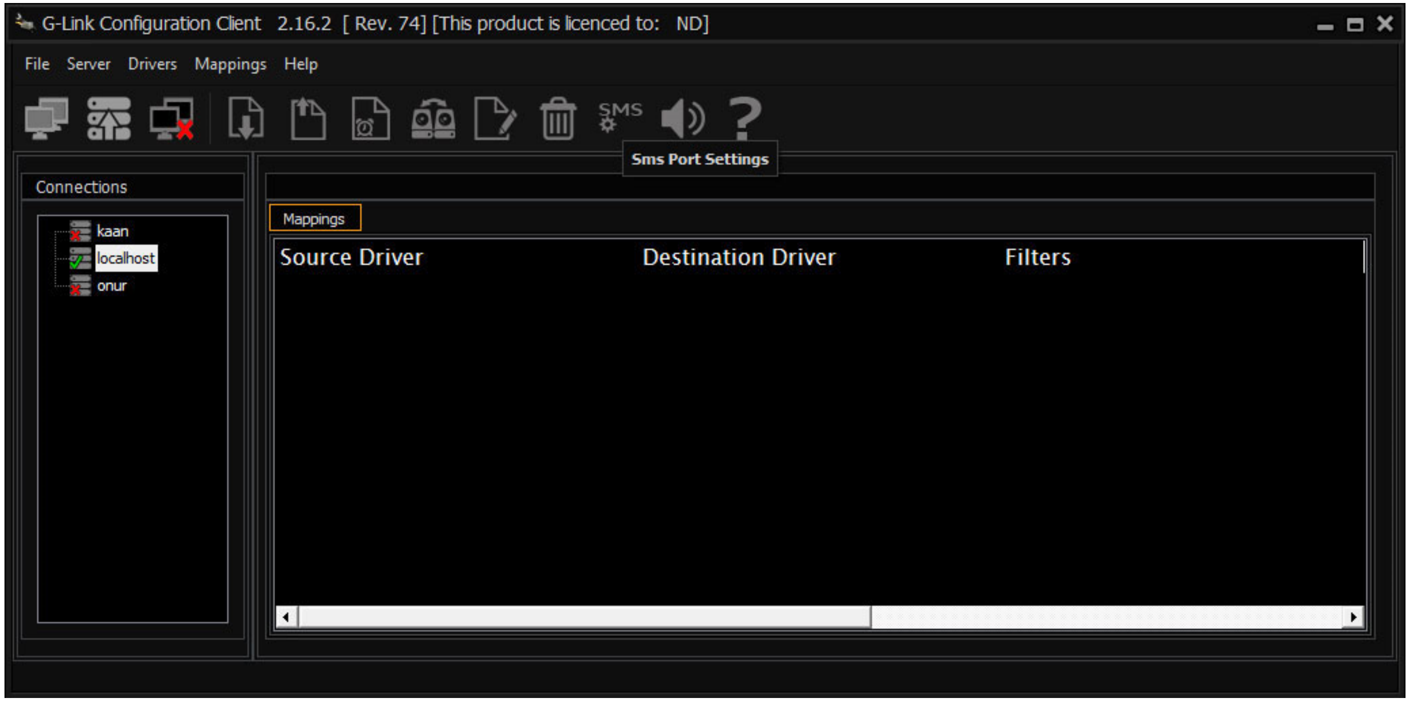
As mentioned before G-Link provides interaction between users and G-Link system. There is more than one way in order to make G-Link as an interactive system. First way is instant messages between users, system and user, system and user groups. Second way is sending email from G-Link to users. The last way is Sending SMS from system to users at specified scenarios. For example these scenarios can be sending SMS when an alarm fired or when a managed event stopped etc.

System needs some external hardware for sending SMS. These external hardware are GSM modem and SIM Card which sends and accepts text messages.

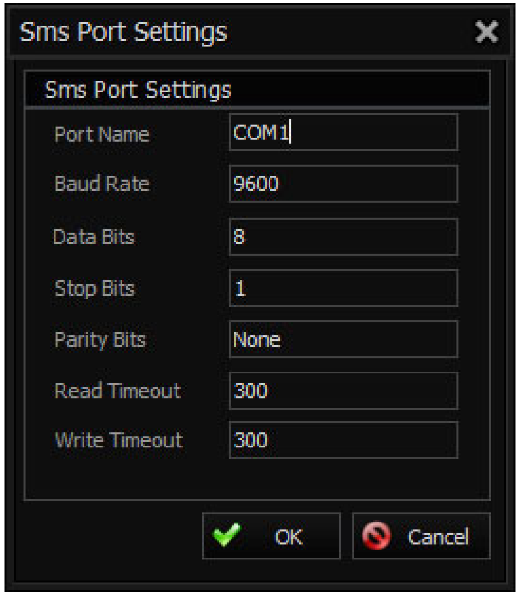
GSM Modem has to support AT commands for sending short text messages. As mentioned above, GSM Modem needs a SIM card and this SIM card has to be inserted into GSM Modem.

Although some of GSM Modems support both Ethernet and serial connection, most of the GSM Modems support only serial (RS232) connection. But serial connection is old technology and computers do not contain serial connection slot. So a serial to USB converter is needed.

Besides external hardware, some internal settings should be done such as port number, baud rate, parity bit etc. for sending messages. *SMS Settings* button in G-Link Setup Main Form is clicked for setting values.



After clicking button SMS Port Settings form is opened.



Sms Port Settings

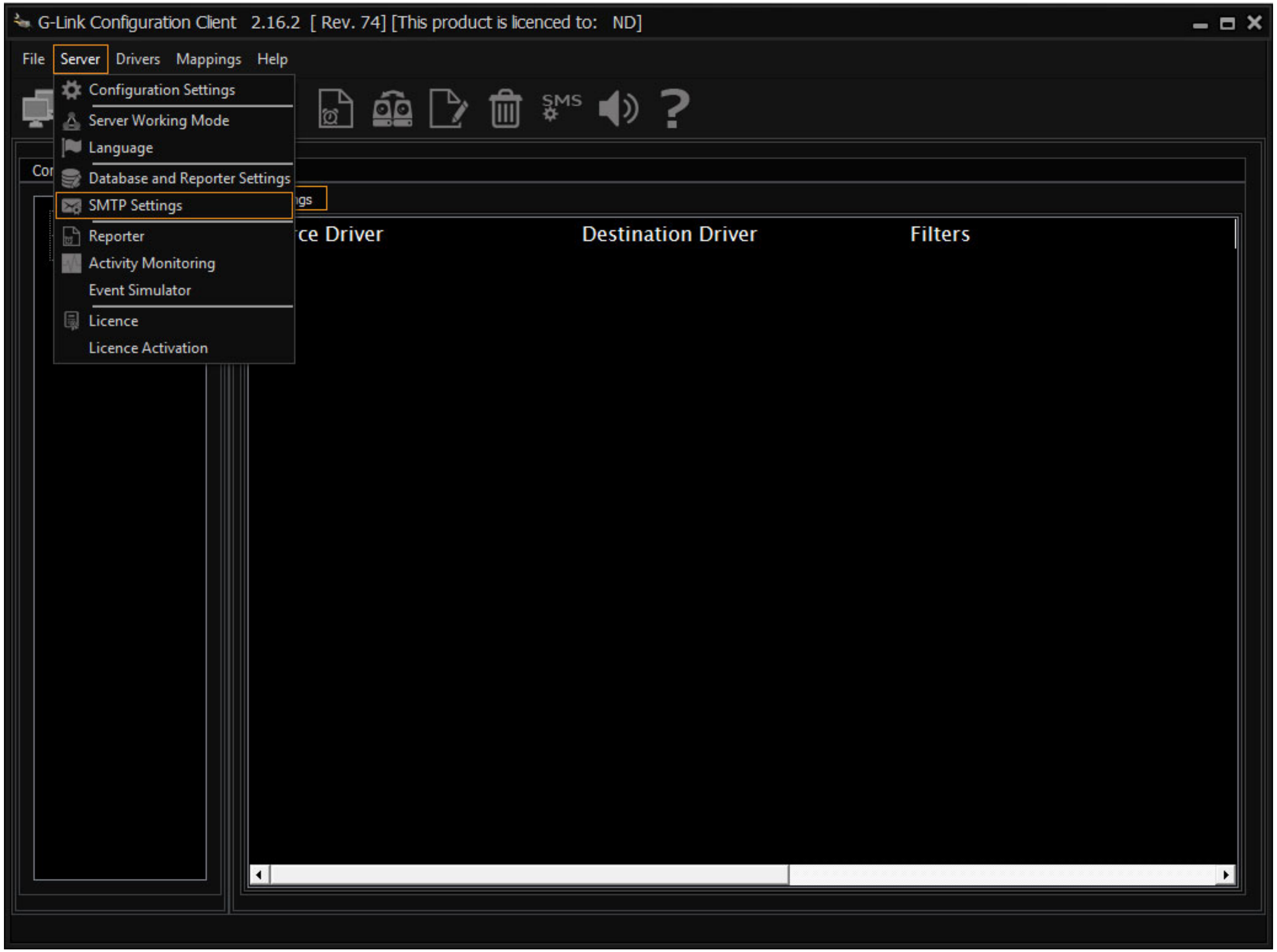
Port Name	COM1
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Read Timeout	300
Write Timeout	300

- Port Name field sets the port which is used for GSM Modem. Serial Ports in PC can be seen at *Control Panel -> Device Manager*
- Baud Rate field set the value for GSM Modem
- Data Bits field sets the value of data bits for GSM Modem.
- Stop Bits field sets the value of stop bits for GSM Modem.
- Parity Bits field sets the value of parity bits for GSM Modem.
- Read Timeout field sets the value of timeout of reading incoming messages from GSM Modem.
- Write Timeout field sets the value of timeout of writing commands to GSM Modem.

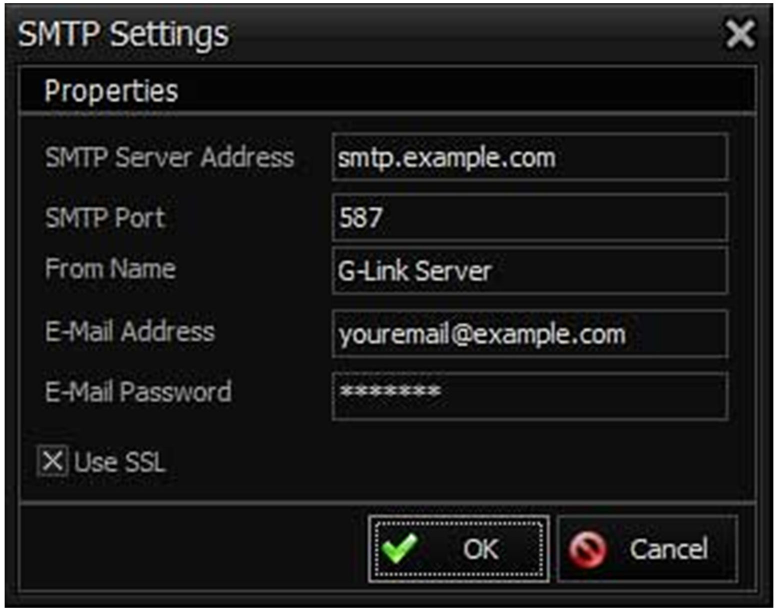
SMTP Settings

As mentioned before G-Link is an interactive system. It enables interaction between user and system, between user and user groups by providing instant messaging, sending short text messages etc. G-Link also support sending mail to system users for enhancing interaction between system and system users, in addition to “Short Text Messages” and “Instant Messaging”.

For sending email to users some basic settings related for SMTP (Simple Mail Transfer Protocol). Go to *Server* -> *SMTP*.



After clicking menu item *SMTP Settings* form is opened.



SMTP Settings

Properties

SMTP Server Address: smtp.example.com

SMTP Port: 587

From Name: G-Link Server

E-Mail Address: youremail@example.com

E-Mail Password: *******

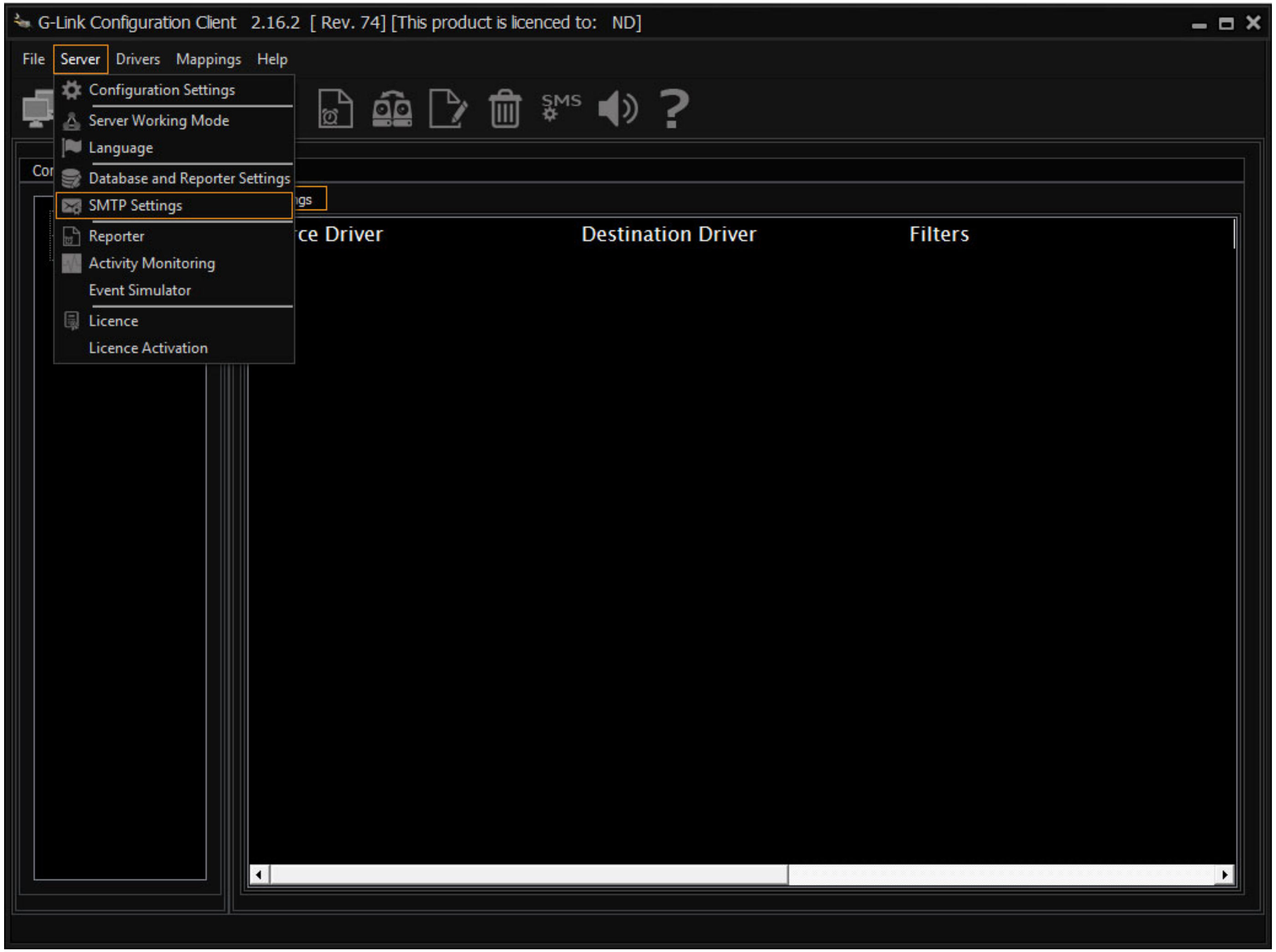
☒ Use SSL

- SMTP Server Address field sets the server address
- SMTP Port field sets the port number for sending mail
- From Name field sets the name for “Sending Name” field for mail
- Email Address field sets the sending mail address
- Email Password field sets the password
- Use SSL check box sets the using of SSL

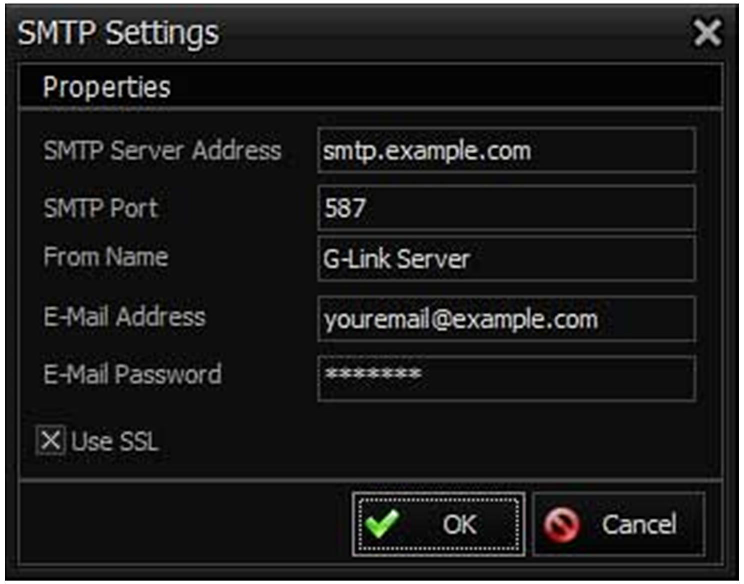
For saving the changes *OK* button has to be clicked, *Cancel* button is clicked for discarding.

SMTP Settings

As mentioned before G-Link is an interactive system. It enables interaction between user and system, between user and user groups by providing instant messaging, sending short text messages etc. G-Link also support sending mail to system users for enhancing interaction between system and system users, in addition to “Short Text Messages” and “Instant Messaging”. For sending email to users some basic settings related for SMTP (Simple Mail Transfer Protocol). Go to *Server -> SMTP*.



After clicking menu item *SMTP Settings* form is opened.



SMTP Settings

Properties

SMTP Server Address: smtp.example.com

SMTP Port: 587

From Name: G-Link Server

E-Mail Address: youremail@example.com

E-Mail Password: *******

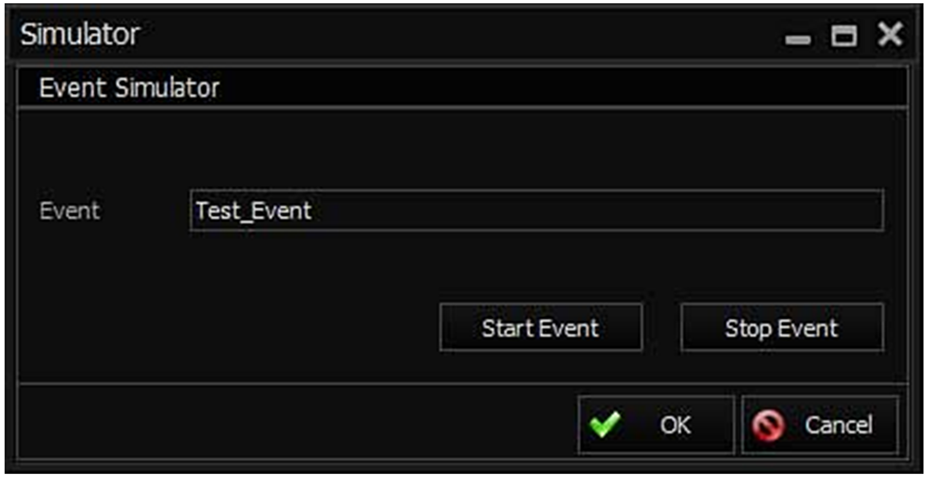
☒ Use SSL

- SMTP Server Address field sets the server address
- SMTP Port field sets the port number for sending mail
- From Name field sets the name for “Sending Name” field for mail
- Email Address field sets the sending mail address
- Email Password field sets the password
- Use SSL check box sets the using of SSL

For saving the changes *OK* button has to be clicked, *Cancel* button is clicked for discarding.

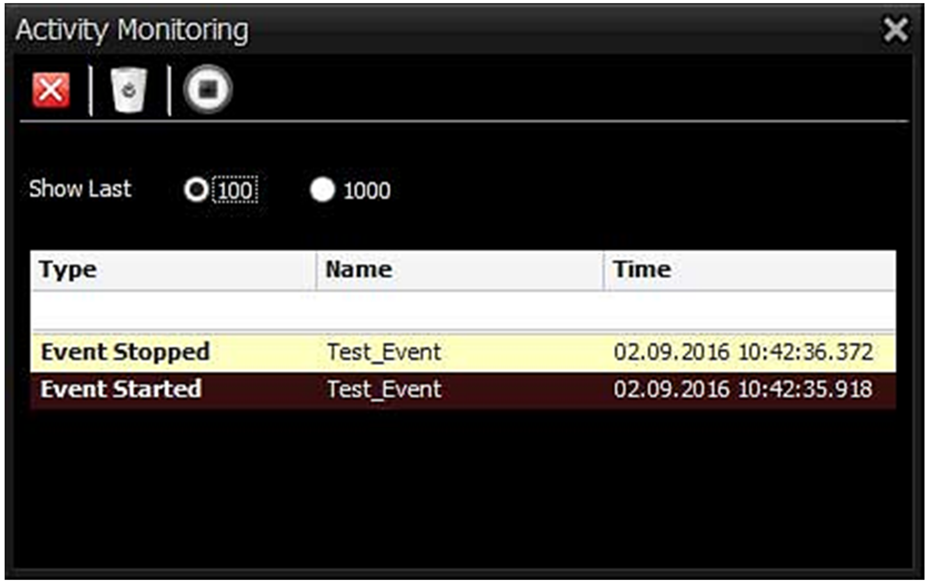
Event Simulator

Event simulator allows to simulate events in G-Link. Operator is able to start a custom event as writing name of event in Event Simulator page.It can be opened from *Server -> Event Simulator*.



Event: Test_Event

Assume that we have an event named *Test_Event*. The operator is able to start and stop that event. And it is possible to see event situation in the Activity Monitoring window. It is opened from *Server -> Activity Monitoring* button.



Show Last ○ 100 ● 1000

Type	Name	Time
Event Stopped	Test_Event	02.09.2016 10:42:36.372
Event Started	Test_Event	02.09.2016 10:42:35.918

Plugins

Each plugin is a module which handles communication with an external hardware or software system. Which means GeViSoft plugin is the module handling communication with GeViSoft system and CIAS plugin is the module which communicates with IBServer hardwares of CIAS.

Besides logging connection loses to application event log, you can also start events on connection loses. After selecting the plugin node, if “Notify Connection Losses” option is selected, in case of a connection loss of a channel, so called "Connection Loss Event" starts and as soon as connection re-establishes, this event stops. This event's name is determined by "Connection Loss Event Suffix" preceded by channel's name. So connection loss event named as “Channel Name + Connection Loss Event Suffix”.

To give an example: If channel name is “IBServer 0” and connection loss event suffix is “_CONN_LOST” than this channel’s connection loss event name is, “IBServer 0_CONN_LOST”.

> ADVICE Please note that you should create this event on GeViSoft because it is not possible to start/stop events which do not exist in GeViSoft setup.

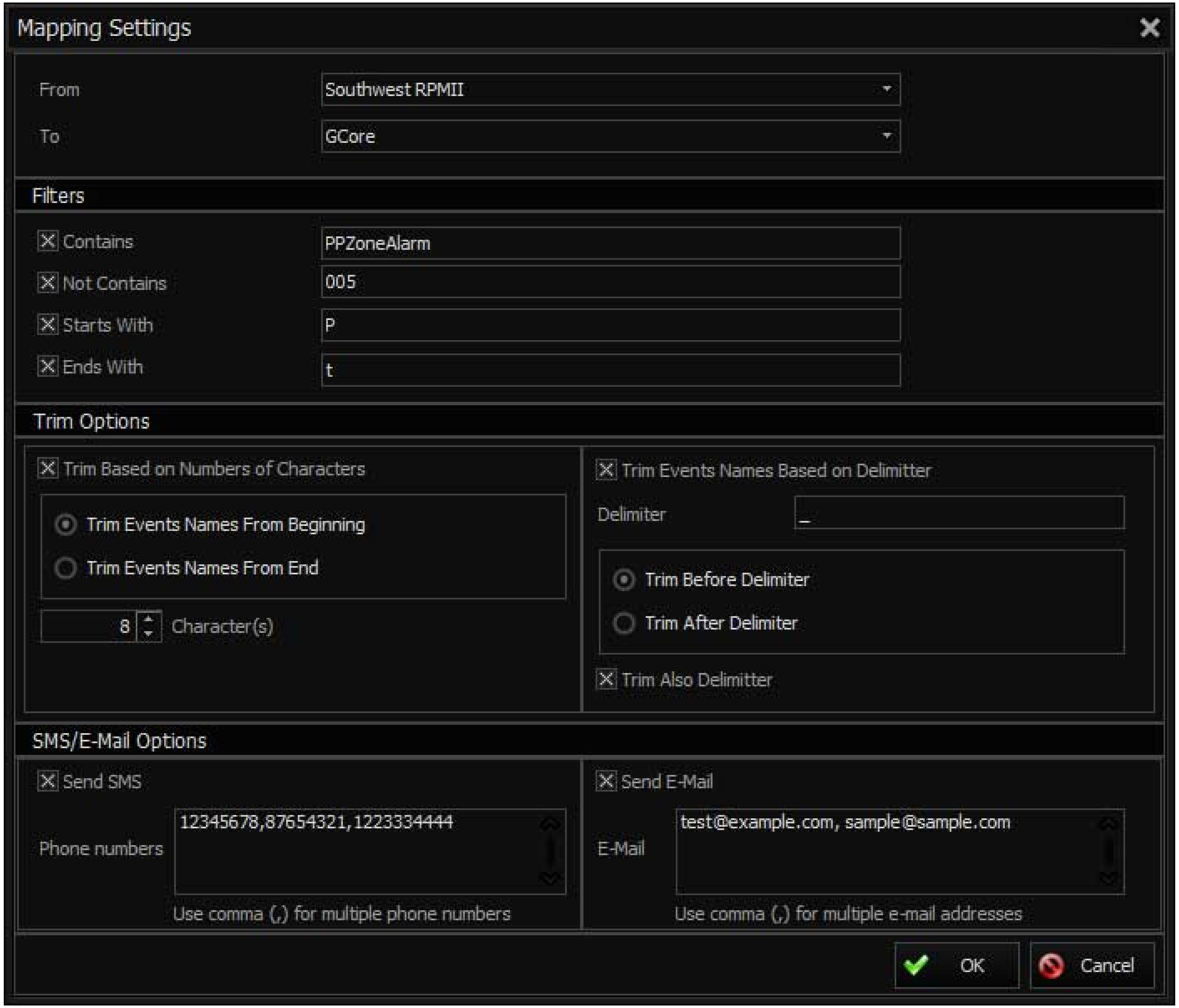
Plugin list

Geutebrück G-Link Server supports many popular third part system. In the listening below all integrated plugins are listed with supported count of devices.

Third Party Plugins	Count		Third Party Plugins	Count	
Maxess plugin	1	Web Page	Dedicated Micros plugin	1	Web Page
FCwnx plugin	1	Web Page	Jacques plugin	1	Web Page
Fibersensys APU plugin	128	Web Page	Cardax plugin	1	Web Page
CIAS IB Server	48	Web Page	Protege plugin	1	Web Page
IOmniscient plugin	4	Web Page	DSC Alarm Panel licence (Alarm Panels)		Web Page
GCore	32		ASV channel licence (Automatic Sea Vision)	64	Web Page
GSC Licence	32		Micros plugin	1	Web Page
GeViSoft Licence	1		IGT Server Licence	1	Web Page
Inner Range Insight plugin	1	Web Page	Southwest RPMII	48	Web Page
Hikvision plugin	1	Web Page	Cyviz Display Controller	32	

G-Link Mapping Configuration

Mapping provides to send events, alarms or actions from 3rd party integrations to another 3rd party integrations.



Mapping Settings

From: Southwest RPMII

To: GCore

Filters

☒ Contains: PPZoneAlarm

☒ Not Contains: 005

☒ Starts With: P

☒ Ends With: t

Trim Options

☒ Trim Based on Numbers of Characters

● Trim Events Names From Beginning

○ Trim Events Names From End

8 Character(s)

☒ Trim Events Names Based on Delimitter

Delimiter: _

● Trim Before Delimiter

○ Trim After Delimiter

☒ Trim Also Delimitter

SMS/E-Mail Options

☒ Send SMS

Phone numbers: 12345678,87654321,1223334444

Use comma (,) for multiple phone numbers

☒ Send E-Mail

E-Mail: test@example.com, sample@sample.com

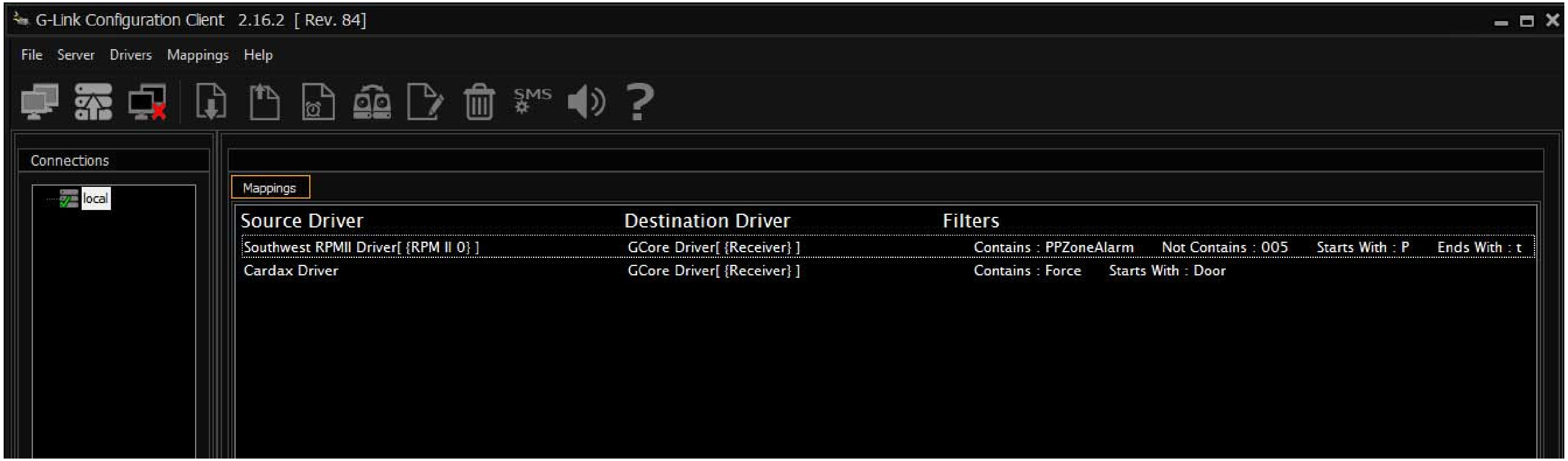
Use comma (,) for multiple e-mail addresses

Mapping allows to operator to limit events or actions with restrictions. Above image is a Southwest – GCore mapping and it has some restrictions. The restrictions and meanings are

Contains	G-Link sends only event which contains the filters. For this sample, it is *PPZoneAlarm*. That means, if event doesn't contain *PPZoneAlarm*, G-Link will not send the event to G-CorePlugin's mapped channel.
Not Contains	G-Link sends only event which doesn't contain word in box. For this sample, it is 005. That means, if event contains *005*, G-Link will not send the event to G-CorePlugin's mapped channel.
Starts With	G-Link sends only event which starts with word in box. For this sample, it is P. That means, if event doesn't start with *P*, G-Link will not send the event to G-CorePlugin's mapped channel.
Ends With	G-Link sends only event which ends with word in box. For this sample, it is t. That means, if event doesn't end with t, G-Link will not send the event to GCorePlugin's mapped channel.

> NOTICE Each G-CorePlugin's channel is a G-Core server.

You can see main mapping view of G-Link here:


G-Link Configuration Client 2.16.2 [Rev. 84]
File Server Drivers Mappings Help
SMS
?
Connections
local
Mappings

Source Driver	Destination Driver	Filters
Southwest RPMII Driver[{RPM II 0}]	GCore Driver[{Receiver}]	Contains : PPZoneAlarm Not Contains : 005 Starts With : P Ends With : t
Cardax Driver	GCore Driver[{Receiver}]	Contains : Force Starts With : Door

Trim Options

You can also limit events with Trim Options. It allows to you to trim event from beginning or end with character number we choose. In Figure 1, it is limited with 8. That means G-Link will send events first 8 characters. If event name is *PPZoneAlarm_South*, it will send as *PPZoneAl*.

And it is also possible to delimit event name while sending. You can provide it using Delimiter. In Figure 1, it is delimited with _ , that means if event name is *PPZone_South*, it will be send as *PPZone*.

Please pay attention that an event must provide all restriction in a mapping for all activated filters. That means restrictions are in **AND** logic.
For sample, it must contain PPZoneAlarm **and** not contain 005 **and** start with P **and** end with t.

Configuration of one source to many destinations is possible. Regarding to the example above:

To send just *PPZoneAlarm* (and other filters) you can configure it like above.

To send just *Tamper alarms* you can send it to another G-Core server. To achieve this add a filter to contain *Tamper*.

Or another example: Source driver is an Access Management System. For example you can transfer all events to a G-Core Server but just important events like *AccessDenied* to a main G-Core alarm server.

It is also possible to send events, actions, alarms as SMS and/or email. It is possible to set more than one phone number or email address.

Please see SMS Settings chapter for more SMS detail or the SMTP Settings chapter for more E-Mail detail.

Automatic Sea Vision (ASV) plugin

ASV plugin enables transfer of detections made by ASV Server. It is also possible to configure masked areas and enable/disable them via ASV plugin.

Supported Hardware/Software

ASV Software development kit 1.6.2 is used for integration.

How To Configure plugin

ASV plugin is capable of getting configuration automatically from ASV Server. So it’s recommended that first finalize ASV configuration than take required actions for integration.

> **IMPORTANT** ASV plugin uses camera names defined on ASV Server. And it automatically links cameras defined on ASV Server with cameras defined on NVR. So camera (i.e. media channel) names on NVR and ASV Server must be exactly same.

For configuration please add random ASV channel (e.g. ASV Channel 1). Click on “ASV plugin” node and enter “ASV Server IP Adress”. If you have more than one ASV Server than please write them by separating with semicolon. If you have two ASV servers than please enter “192.168.1.102 ; 192.168.1.103”

After that right click on *ASV plugin* and click on *Get ASV Configuration* menu item. By clicking this, ASV plugin gets all cameras defined on ASV Server.

Configuring Masked Zones

After getting ASV configuration please right click on channel for which you would like to configure masked zones. After clicking *Configure Masked Zones* menu item, ASV plugin open live video view of related media channel within NVRs. (Please refer to DVR Integrations section for more detail)

> NOTICE Please note that if live video is not available (camera or DVR is not accessible) than it is **not** possible to configure masked zones.

While viewing live video it is possible to add or delete masked zones. If a masked zone is not saved than its id is “NA”. After making changes please do not forget to save your changes to take effect.

As soon as location of masked area is changed, its ID is changed to “NA”. Because there is no edit option for masked areas in ASV Server.

Supported Functionality

As soon as new object detected by ASV server, a new event with name #CameraName#_ObjectDetected starts. And when object detected goes out of scope than same event stops. If camera name is “Camera001” than sample detection event name is “*Camera001_ObjectDetected*”.

It is also possible to enable masked areas as detection or non-detection areas via events. To enable masked area as NON-detection area which has ID #X# start event named #CameraID#_EnableMA_#X# .

To enable same masked area as detection area, stop same event. If you would like to enable masked area 3 as detection or NON-Detection and if your camera name is “Camera001” than event name should be “*Camera001_EnableMA_3*”. Starting this event enables masked area 3 as NON-detection area and stopping this event enables masked area 3 as detection area.

> NOTICE Please note that it is also possible to enable/disable masked areas while configuring masked areas via graphical user interface. Right click on masked zone to enable/disable masked area.

It is also possible to set sensitivity of each detection channel of ASV Server via events. To set sensitivity of a channel to value #X# please start event named as #CameraID#_SetSens_#X# .

X is an integer between 0 and 3;

0 : no processing

1 : low sensitivity (False Alarm rate decreased)

2 : normal tuning

3 : high sensitivity

Let’s say to set channel’s sensitivity to 2 please start event named as “*Camera001_SetSens_2*” where Camera001 is the name of the channel.

ASV plugin also fires events depending on if detection intersects with masked areas which are enabled. And for each intersected masked area an event which is named as #CameraName#_ObjectDetected#_Zone#MaskedAreaID# is started.
Let’s say if masked area 2 and masked area 3 intersects with detection. Than (additional to the “Camera001_ObjectDetected” event) two events are fired “Camera001_ObjectDetected_Zone2” and “Camera001_ObjectDetected_Zone3”.

> NOTICE Please note that zone events do not have correspondent events. So they must be configured as auto-stop event.

Cardax plugin

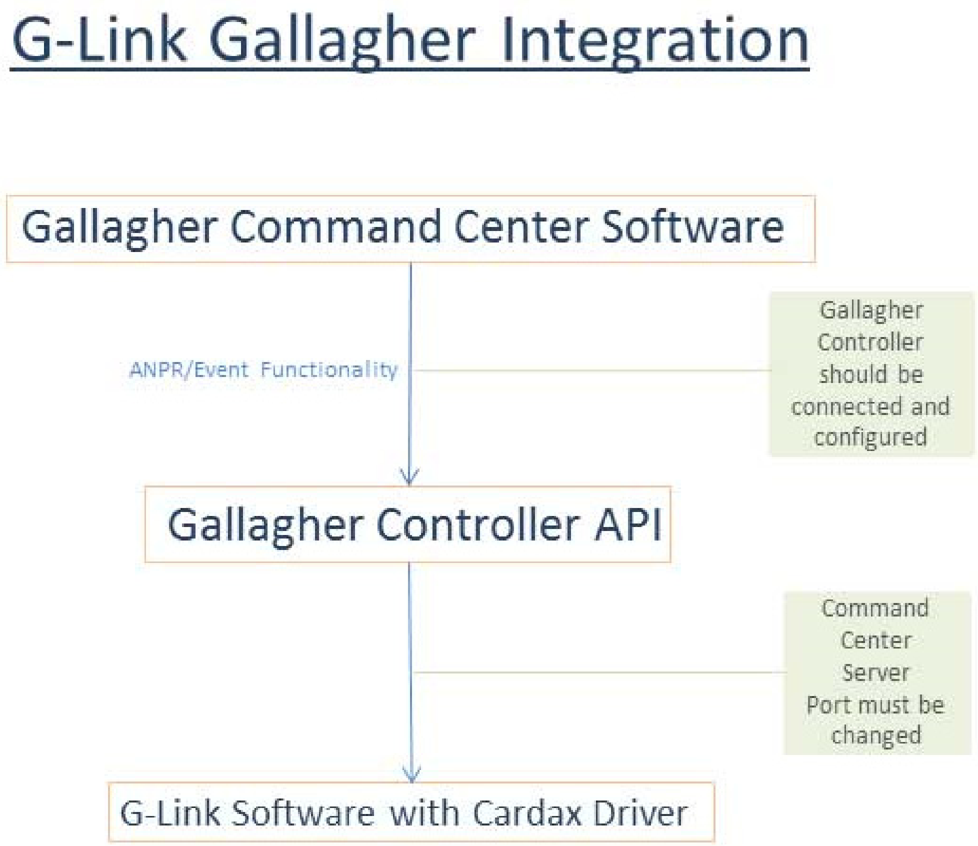
Cardax is an access control and intruder alarm security system - a platform for integration. It is comprised of software and hardware. Cardax systems are sold through a network of Gallagher Certified Channel Partners throughout the world.

Supported Hardware/Software

Supported and test API version is Controller API v7.10.11 and Command Centre version 7.10,7.20,7.30.

After version 1.0.9.610 of G-Link it is possible to transport Automatic Number Plate Recognition (ANPR) from GeViScope to Gallagher Command Centre (v7.10) via Cardax plugin.

For Quick Installations Steps, see figure G-Link Gallagher Integration:


G-Link Gallagher Integration
Gallagher Command Center Software
ANPR/Event Functionality
Gallagher Controller should be connected and configured
Gallagher Controller API
Command Center Server Port must be changed
G-Link Software with Cardax Driver

Supported Functionality

Cardax plugin enables Event/Alarm/ANPR data transfer between G-Link and Gallagher.

How To Configure ANPR

> **IMPORTANT** It is recommended to install G-Link on same server as Gallagher Command Centre.

Gallagher Command Centre provides support for text-based card identifiers. A person's vehicle license plate number can be used to identify a person and control access to car-parks in conjunction with G-Link.

The Command Centre text-based card format requires the integration with G-Link to detect the license plate of a vehicle approaching a barrier arm and via the Controller API can supply the vehicle license plate number to the Gallagher Controller as a Card Event. The Controller makes the access decision based on the current 'card' assignment of this license plate to a person in Command Centre.

Text card number formats are specified as a separate card type and can be validated at the time of entry into Command Centre via a regular expression. The regular expression ensures that the card data entered or imported, such as a vehicle license plate number, is valid for the country of implementation and hence reduces the incidence of data entry errors. Text-based card identifiers can be entered into Command Centre by any of the following methods:

- Operator Card Entry, e.g. ABC12345 (see Add new Card Type)
- Card Import via XML (see Gallagher Command Center User Guide)
- Card Import via Enterprise Data Import Interface (see Gallagher Command Center User Guide)

> **IMPORTANT** At least one DVR and one Channel have to be configured on Gallagher Command Center to receive ANPR data. But it is recommended to enter all DVRs and cameras to Command Centre configuration.

Install Gallagher Controller API

Install FTCAPI

1. Locate Controller API v7.10.11.
2. Click FTCAPIInstall.msi and follow the instructions of setup.

> NOTICE Gallagher Command Center Server and Gallagher Controller API uses same Port (1072). Please change Port of Command Center Server as below.

Change Port of Gallagher Command Center Server

1. Stop the Command Centre services.

2. Open up the registry editor and browse to HKEY_LOCAL_MACHINE\SOFTWARE\Gallagher\Command Centre

> NOTICE If using a 64 bit system, browse to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Gallagher\Command.

3. Create a new DWORD value and rename it to *ListenPort*.

4. Edit the value of *ListenPort* by selecting the decimal radio button and then typing in the desired port number.

> NOTICE The valid range is 1024 to 65535. Do not try to use port numbers outside of that range.

5. Start the Command Centre services and logon to Gallagher Command Centre. All of the Controllers will appear as offline and will not come online by themselves.

6. Select *Push Configuration* on each Controller in turn. They should each come online after they are pushed.

Gallagher Command Center Configuration

Add new Card Type

This procedure details how to set up a new Card Type.

1. Start Command Center Classic Software.

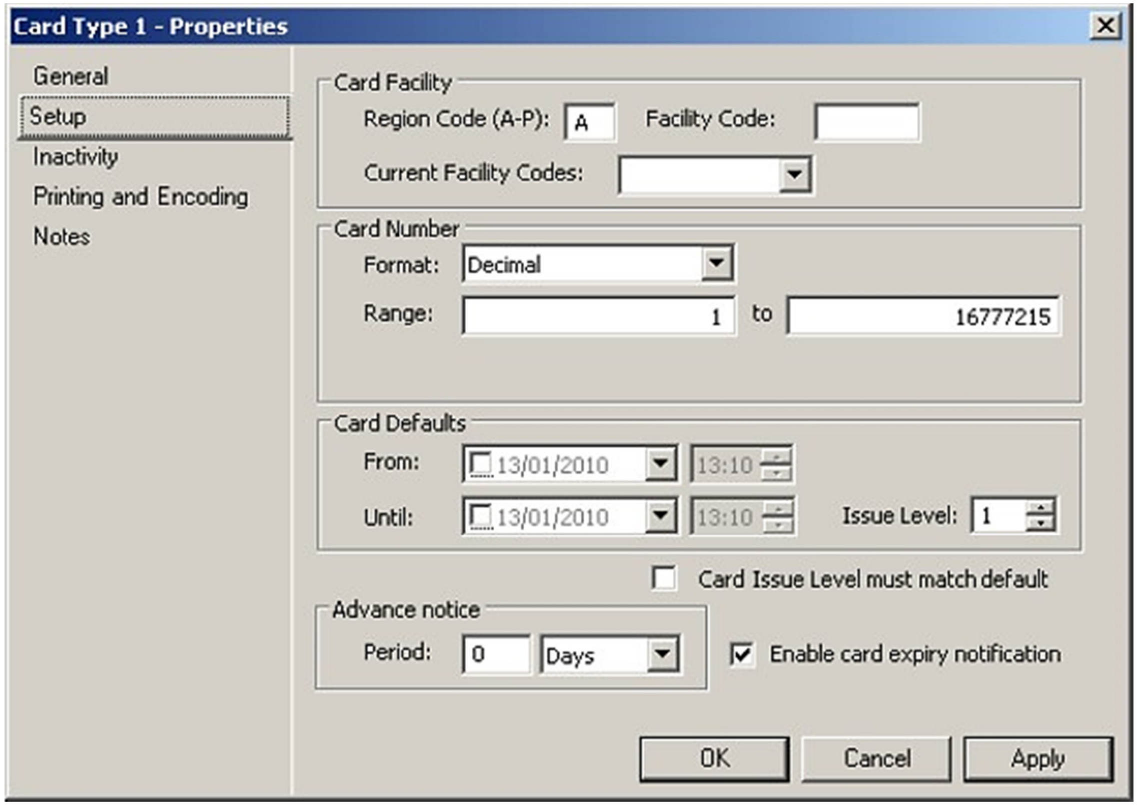
2. *Login* Username: *system* Password: *system*

3. Click *Configure* from the menu bar, then *Card Types*. The Card Type Master List Window opens (in grid view).

4. Right click and select *New…Card Type*.

5. Complete the fields as required.

6. Click the *Setup* tab.



Card Facility

Region Code (A-P): A

Facility Code:

Current Facility Codes:

Card Number

Format: Decimal

Range: 1 to 16777215

Card Defaults

From: □ 13/01/2010 13:10

Until: □ 13/01/2010 13:10

Issue Level: 1

□ Card Issue Level must match default

Advance notice

Period: 0 Days

☑ Enable card expiry notification

Your site Facility Code is entered in the *Card Facility* section on this tab. Command Centre references the Facility Code to identify cards for use on site.

Gallagher Group Limited supply sites with Facility Codes, and ensure different sites have different facility codes. This allows several sites to use identical card numbers.

7. If your site Facility Code has already been entered, then select it from the *Current Facility Codes* drop-down box.

OR

If you wish to enter your *Facility Code*, then enter the letter representing the *Region Code* for your Facility Code, and enter the number in the Facility Code field.

> NOTICE Facility Codes can only be used on one card technology.
> One Facility Code cannot be used by two card types that have different card number formats. This is due to the difficulty in converting the byte array representation of a card number to its displayable string representation.

8. The settings configured in the *Card Number* and *Card Defaults* sections will be used when you allocate a new card to a cardholder. They can then be overwritten if required.

In the Card Number section select the *Text* from the Format. Text based card formats support Unicode characters. This allows entry of a wide range of characters or symbols as part of a card identifier, including:

- Any number or letter
- Hyphens, spaces, commas or full stops
- Foreign language characters such as Chinese, Arabic or Farsi

Enter the range in the *Range* fields (Defaults = 1 to 16,777,215).

If you want to force the card number format to fit a regular expression for the Card Type, enter a syntax string into the Syntax field. This string will be used to validate a card number that is entered by an Operator.

> NOTICE Refer to Sample Regular Expressions on page 7-8 of Command Centre Classic User Guide for a list of example regular expressions.
> The syntax string can be changed after the Card Type is saved. For example: Card Numbers for alphanumeric vehicle number plates may initially support 2 English letters and 4 number digits, (e.g. 'AB1234') and later support 3 English letters and 3 number digits, (e.g. 'ABC123').
> To allow any characters leave Syntax field empty.

Enter a *description* of the syntax in the Description field.

> NOTICE This message will be displayed to an operator if the value entered cannot be saved because it doesn't meet the regular expression validation.

9. For further property setting see Gallagher Command Center Classic User Guide.

Assigning Card Type to Cardholder

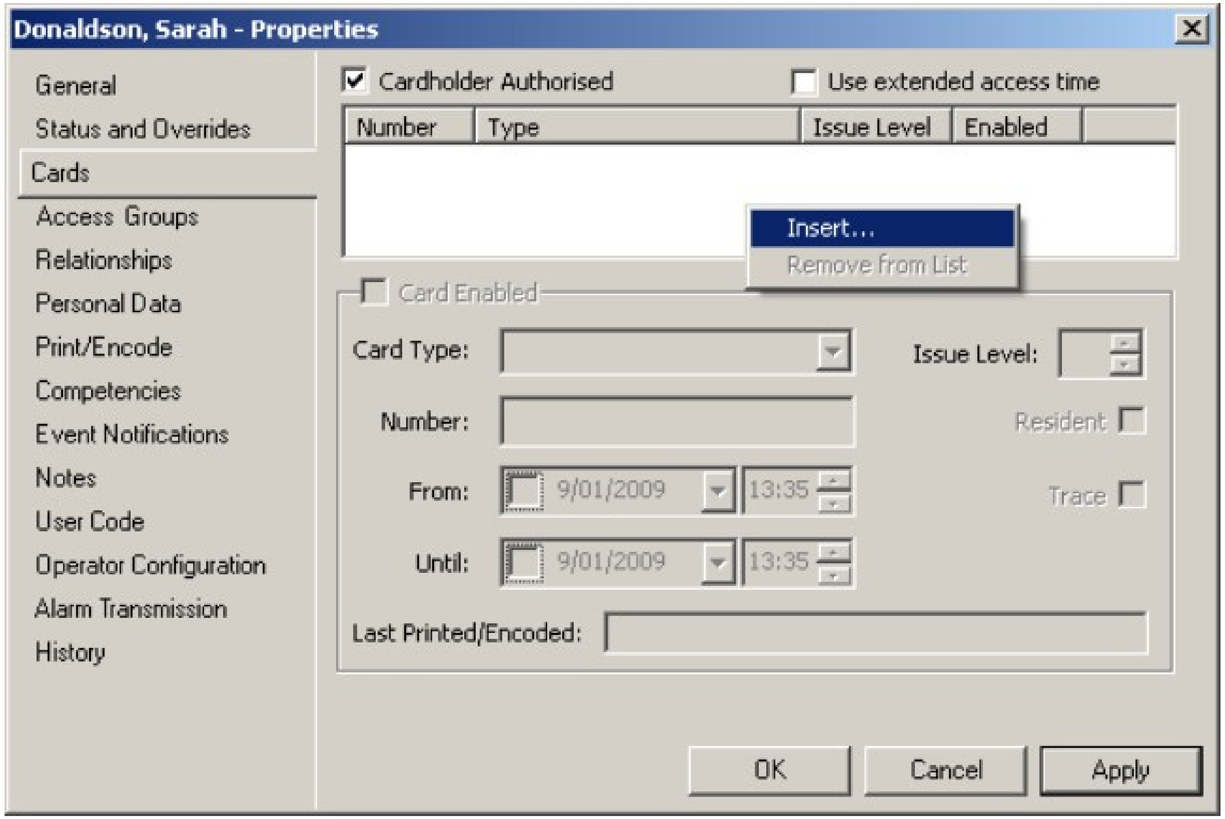
1. Click *Manage* from the menu bar, then *Cardholders*. The Cardholder Master List Window opens (in grid view).

2. Locate, and highlight, the Cardholder to edit.

3. Right click and select *Properties*.

4. Click the *Cards* tab.

5. Right click anywhere within the upper grid and select Insert.



Donaldson, Sarah - Properties

☑ Cardholder Authorised　□ Use extended access time

Number	Type	Issue Level	Enabled

□ Card Enabled

Card Type:

Issue Level:

Number:

Resident □

From: □ 9/01/2009 13:35

Trace □

Until: □ 9/01/2009 13:35

Last Printed/Encoded:

6. Right click anywhere within the upper grid, (i.e. on a column header, on the scroll bar, in the blank area or on a card if there is one), and select Insert. A "new card" is added to the upper grid and highlighted. This new card is enabled and if it has had card defaults already configured fields will be populated with those defaults.

7. Click the *Card Type drop-down* menu box and select the correct Card Type.
8. For further property setting see Gallagher Command Center Classic User Guide.

> NOTICE Where cardholders have more than one vehicle, multiple ‘cards’ can be added to the cardholder so that any registered vehicle will be allowed access.

Cardax G-Link Configuration

Add plugins (example with GSC plugin)

1. Open G-Link Configuration Client.

2. Login

3. Click *Add plugin* from menu bar and select one GSCClient and CardaxChannel from plugins list.

4. Click on *GSCClient* and verify that GSCClient plugin ID is the same as configured in Gallagher Command Center External System.

5. Click CardaxChannel

6. Edit *Facility Code* and *Region Code*, if default settings do not appear to Gallagher Card Type configuration.

> NOTICE Region Code must be a single character (A – P) in upper case (see Command Center settings for Card Types).
> Facility Code must be a numeric value.

7. Send Setup to Server.

After approximated **45 second** a connection to Gallagher Command Center Server over CardaxChannel is etablished.

Add G-Link Mappings (example with GSC plugin)

1. Click *Mappings* on the menu bar.

2. Select GSCplugin in *From* section and check GSCClient.

3. Select Cardaxplugin in *To* section and check CardaxChannel.

4. Click *OK*.

5. Click *Mappings* on the menu bar.

6. Select Cardaxplugin in *From* section and check CardaxChannel.

7. Select GSCplugin in *To* section and check GSCClient.

8. Click *OK*.

9. Send Setup to Server.

After Gallagher Command Center Server restart, please restart G-Link Server as well.

Troubleshooting

- G-Link and Cardax Server must be installed on same server
- Gallagher Controller must be configured and connected to Gallagher Command Center Server
- Gallagher Controller API must be installed on same machine as Gallagher Command Center Server
- Licence should include Gallagher Controller API Licence
- Gallagher Controller API and Gallagher Command Center Server use same Port (1072). Cardax Server Port must be change to 1073
- External System (DVR) Unique ID must be the same as on NDIS plugin Name
- External System Item ID (Channel) must be the same as on GSC Global MediaChannel ID If everything is configured but there is no transfer of NPR or Event please try following steps:

1. Open Command Prompt (cmd.exe)
2. Locate to Controller API Folder cd C:\Program Files (x86)\Gallagher\FTCAPI
3. Type: regsvr32 CardaxFTCAPI.dll

For further information please refer to

- Gallagher Controller API Install Notes_Feb2013.pdf – Version 7.10 February 2013
- FTCAPI Middleware Simulator v7-00.pdf – Version V7.00 October 2011
- 3E1011 Gallagher Command Centre Classic User Guide - v710 Nov2012 (Vol1).pdf
- 3E1011 Gallagher Command Centre Classic User Guide - v710 Nov2012 (Vol2).pdf

CIAS plugin

CIAS plugin supports up to 32 IBServers. Each IBServer supports up to 128 (from 0 to 127) IBDevices. IBDevice refers to any device connected to IBServer. Main duty of CIAS plugin is to transfer all kinds of alarms generated by IBDevices. Alarm types include PREALARM, ALARM, TAMPER, FAULT, NO_ANSWER.

Supported Hardware/Software

All devices connected to an IBServer are supported.

Type	Name
Microwave barriers	Ermo 482X Pro Ermo 482 Coral Manta Ermusa Minermo
Infrared barriers	Darwin Darwin DT Newton2 Newton Plus Newton Pro
Transceiver sensors	Alfa Murena
Fence protection	ISC Cable

Basically IBServer is polling each IBDevice periodically. And this polling information is read, parsed and decrypted by CIAS plugin.

Supported Functionality

CIAS plugin enables you to configure almost everything without making the first time configuration cumbersome. Because default configuration values are provided as soon as you add new IBServer. For customizations please find detailed descriptions of parameters below:

Maximum number of requests without reply	This parameter is a plugin-wide parameter that means it is a global variable for all of the IBServers. To view and edit this parameter please click on the CIAS plugin node. As mentioned previously, each IBServer sends polling requests to IBDevices periodically and in response to that IBDevices are sending polling replies to IBServer. If an IBDevice is not replying to polling requests for some time than NO_ANSWER event of that IBDevice is started. This parameter determines threshold value for starting NO_ANSWER event. By default this parameter is 10. Let's say 10 polling requests are sent to IBDevice but there is no polling reply coming from IBDevice, than at next polling request NO_ANSWER event is started. NO_ANSWER event is stopped as soon as polling reply received from IBDevice. Please note that if there is a connection loss with IBServer this means there is a problem about IBServer's connection to server computer. But, if NO_ANSWER event is started, this means connection to IBServer is alive and IBServer is up and sending polling requests to IBDevice but there is a problem with related IBDevice.
IBServer IP Address	IP Address of IBServer
IBServer Port	Port number on which IBServer communication should be established.
Active IBDevices	Each IBServer can handle up to 128 IBDevices. But for some technical restrictions in real world projects it is not always possible to connect 128 devices to an IBServer. This parameter determines the active IBDevices whose events should be transferred. Please enter IBDevice numbers in comma separated format. By default first 48 IBDevices are active (which means from 0 to 47). You can also enter range with "-"character. If you would like to enter device 0 to 127 as active devices for example you should enter "0-127"
IBServer Prefix	This parameter is used for determining event names with IBDevice Prefix. Please see Event Naming section for details.
IBDevice Prefix	This parameter is used for determining event names in conjunction with IBServer Prefix. Please see *Event Naming* section for details.

Event Naming

All events generated by barriers are integrated. “IBServer Prefix” and “IBDevice Prefix” parameter, gives you the possibility to determine event names. Event names are determined as follows:

“IBServer Prefix” + “IBDevice Prefix” + “IBDevice Number” + “_” + “Event Type”

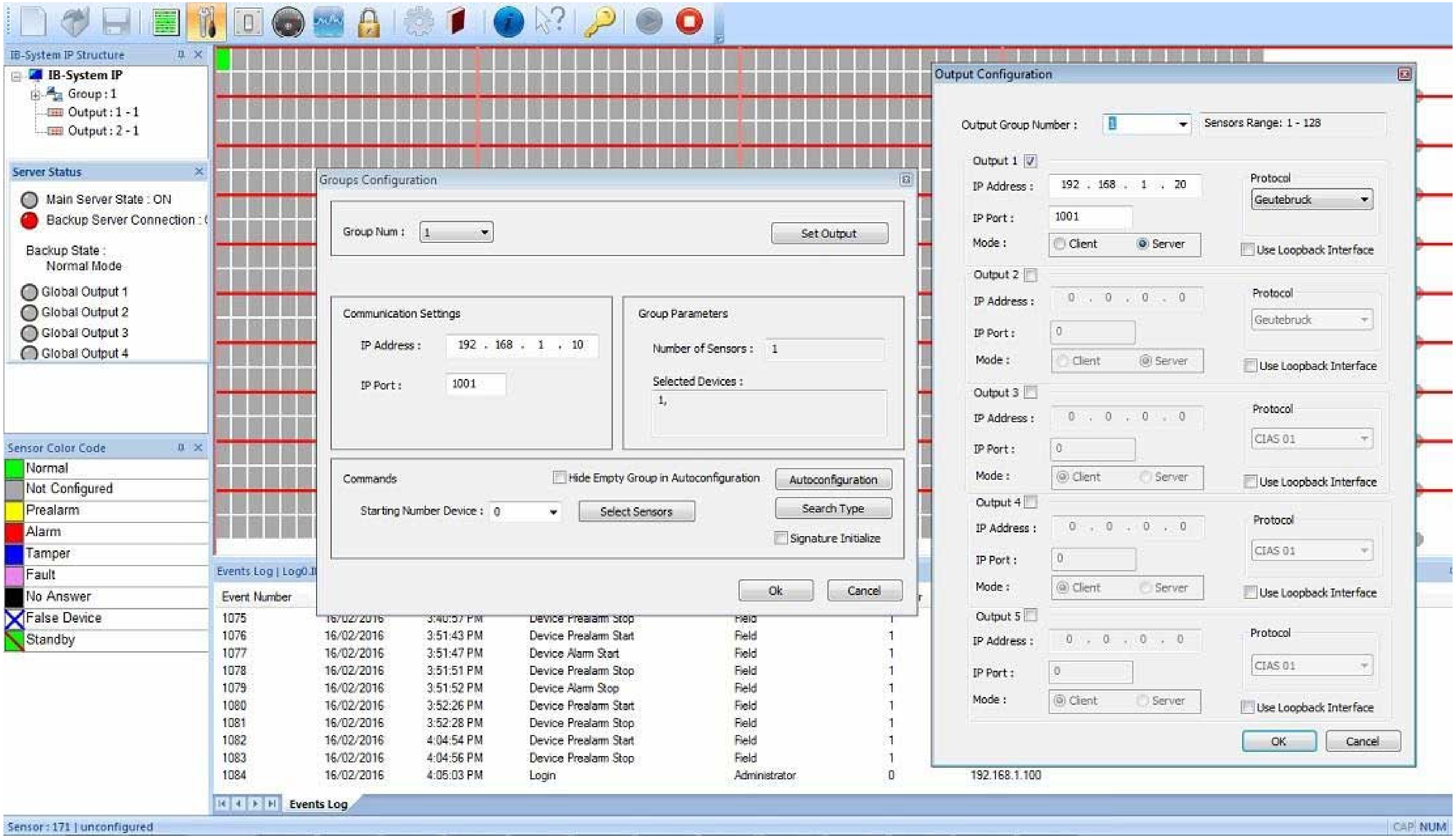
“IBDevice Number” refers to actual device number of the barrier, which changes from 0 to 127. “Event Type” refers to anyone of the PREALARM, ALARM, TAMPER, FAULT, NO_ANSWER. For example, let’s say IBServer Prefix is, IBServer0_ and IBDevice prefix is IBDevice, if FAULT event occurs at IBDevice 5, than this is reflected as IBServer0_IBDevice5_FAULT event. And all events for this device are named as follows:

- IBServer0_IBDevice5_PREALARM
- IBServer0_IBDevice5_ALARM
- IBServer0_IBDevice5_FAULT
- IBServer0_IBDevice5_TAMPER
- IBServer0_IBDevice5_NO_ANSWER

Each IBDevice has five events as shown above.

IB System IP Configuration

IB system IP configuration must be done as shown in below pictures.



IB-System IP Structure

- IB-System IP
  - Group : 1
    - Output : 1 - 1
    - Output : 2 - 1

Server Status

- Main Server State : ON
- Backup Server Connection : (

Backup State :
Normal Mode

- Global Output 1
- Global Output 2
- Global Output 3
- Global Output 4

Sensor Color Code

🟩	Normal
▨	Not Configured
🟨	Prealarm
🟥	Alarm
🟦	Tamper
🟪	Fault
⬛	No Answer
☒	False Device
🟩	Standby

Groups Configuration

Group Num : 1

Set Output

Communication Settings

IP Address : 192 . 168 . 1 . 10

IP Port : 1001

Group Parameters

Number of Sensors : 1

Selected Devices :
1,

Commands

□ Hide Empty Group in Autoconfiguration

Autoconfiguration

Starting Number Device : 0

Select Sensors

Search Type

□ Signature Initialize

Ok Cancel

Output Configuration

Output Group Number : 1

Sensors Range: 1 - 128

Output 1 ☑

IP Address : 192 . 168 . 1 . 20

IP Port : 1001

Mode : ○ Client ● Server

Protocol: Geutebruck

□ Use Loopback Interface

Output 2 □

IP Address : 0 . 0 . 0 . 0

IP Port : 0

Mode : ○ Client ● Server

Protocol: Geutebruck

□ Use Loopback Interface

Output 3 □

IP Address : 0 . 0 . 0 . 0

IP Port : 0

Mode : ● Client ○ Server

Protocol: CIAS 01

□ Use Loopback Interface

Output 4 □

IP Address : 0 . 0 . 0 . 0

IP Port : 0

Mode : ● Client ○ Server

Protocol: CIAS 01

□ Use Loopback Interface

Output 5 □

IP Address : 0 . 0 . 0 . 0

IP Port : 0

Mode : ● Client ○ Server

Protocol: CIAS 01

□ Use Loopback Interface

OK Cancel

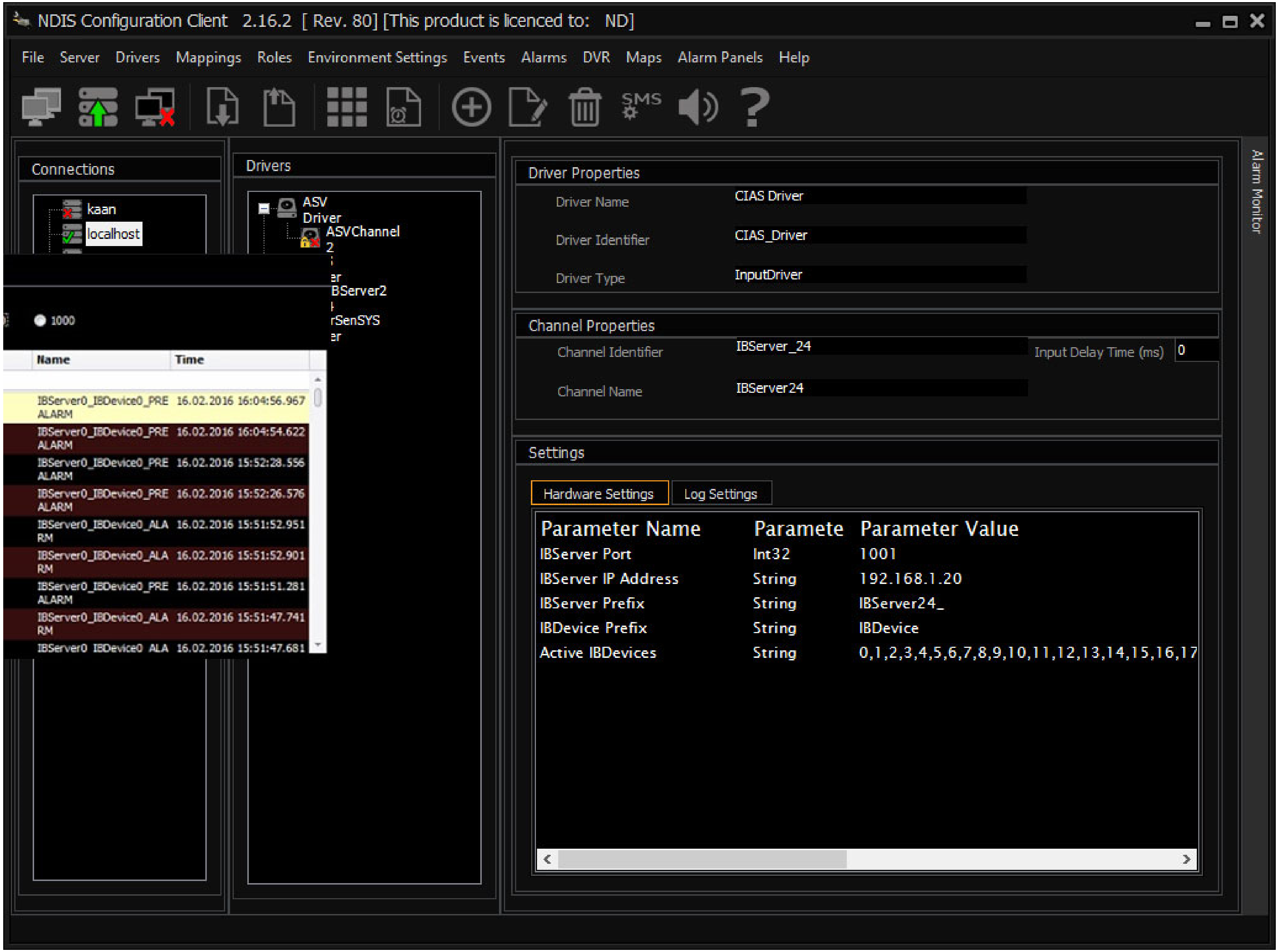
Events Log | Log0.I

```
Event Number
1075         16/02/2016   3:40:57 PM   Device Prealarm Stop    Field           1
1076         16/02/2016   3:51:43 PM   Device Prealarm Start   Field           1
1077         16/02/2016   3:51:47 PM   Device Alarm Start      Field           1
1078         16/02/2016   3:51:51 PM   Device Prealarm Stop    Field           1
1079         16/02/2016   3:51:52 PM   Device Alarm Stop       Field           1
1080         16/02/2016   3:52:26 PM   Device Prealarm Start   Field           1
1081         16/02/2016   3:52:28 PM   Device Prealarm Stop    Field           1
1082         16/02/2016   4:04:54 PM   Device Prealarm Start   Field           1
1083         16/02/2016   4:04:56 PM   Device Prealarm Stop    Field           1
1084         16/02/2016   4:05:03 PM   Login                   Administrator   0    192.168.1.100
```

Events Log

Sensor : 171 | unconfigured

CAP NUM



Name	Time
IBServer0_IBDevice0_PRE ALARM	16.02.2016 16:04:56.967
IBServer0_IBDevice0_PRE ALARM	16.02.2016 16:04:54.622
IBServer0_IBDevice0_PRE ALARM	16.02.2016 15:52:28.556
IBServer0_IBDevice0_PRE ALARM	16.02.2016 15:52:26.576
IBServer0_IBDevice0_ALA RM	16.02.2016 15:51:52.951
IBServer0_IBDevice0_ALA RM	16.02.2016 15:51:52.901
IBServer0_IBDevice0_PRE ALARM	16.02.2016 15:51:51.281
IBServer0_IBDevice0_ALA RM	16.02.2016 15:51:47.741
IBServer0 IBDevice0 ALA	16.02.2016 15:51:47.681

Driver Properties

Driver Name: CIAS Driver

Driver Identifier: CIAS_Driver

Driver Type: InputDriver

Channel Properties

Channel Identifier: IBServer_24

Input Delay Time (ms): 0

Channel Name: IBServer24

Settings

Parameter Name	Paramete	Parameter Value
IBServer Port	Int32	1001
IBServer IP Address	String	192.168.1.20
IBServer Prefix	String	IBServer24_
IBDevice Prefix	String	IBDevice
Active IBDevices	String	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17

Cyviz Display Controller

The driver will receive CustomActions from other supported drşver and translate this to commands for the Cyviz Display Controller send with Telnet.

Supported Hardware / Software

Cyviz Display Controller driver supports all versions and is tested with Cyviz Display Controller - API – V3/V4.

Supported Functionality

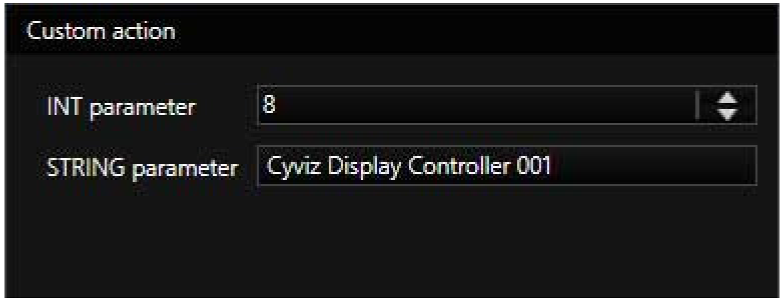
Cyviz Display Controller driver supports

- Connection to multiple display controller
- Sending Custom Action to any TCP server
- Allow change of port, no need to use constant port

Custom Action contains two parameters and they are

- **Integer :** Preset value
- **STRING :** This value should be in format like "Cyviz Display Controller XXX" where XXX indicates the number of the display controller which is using Telnet connection.

For example, if integer value is 8 and STRING value is Cyviz Display Controller 001, then driver sends command to Controller 001 as „load preset 8".



Custom action

INT parameter: 8

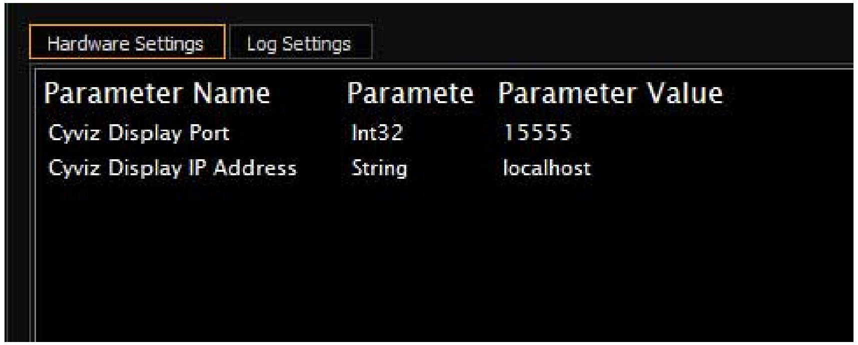
STRING parameter: Cyviz Display Controller 001

How to Configure

Cyviz Display Controller has just two parameters to configure.
Those parameters are:

Cyviz Display Port: Port which is used to listen connection

Cyviz Display IP Address: IP address of where Telnet server is running



Parameter Name	Paramete	Parameter Value
Cyviz Display Port	Int32	15555
Cyviz Display IP Address	String	localhost

Dedicated Micros plugin

Supported Hardware/Software

This plugin enables pushing notifications to Dedicated Micros DV-IP RT systems as alarm inputs. All versions of DV-IP RT is supported.

At each event start notification Alarm Input is set as alarm and in case of event stop Alarm Input is reset to normal state.

FCWnx plugin

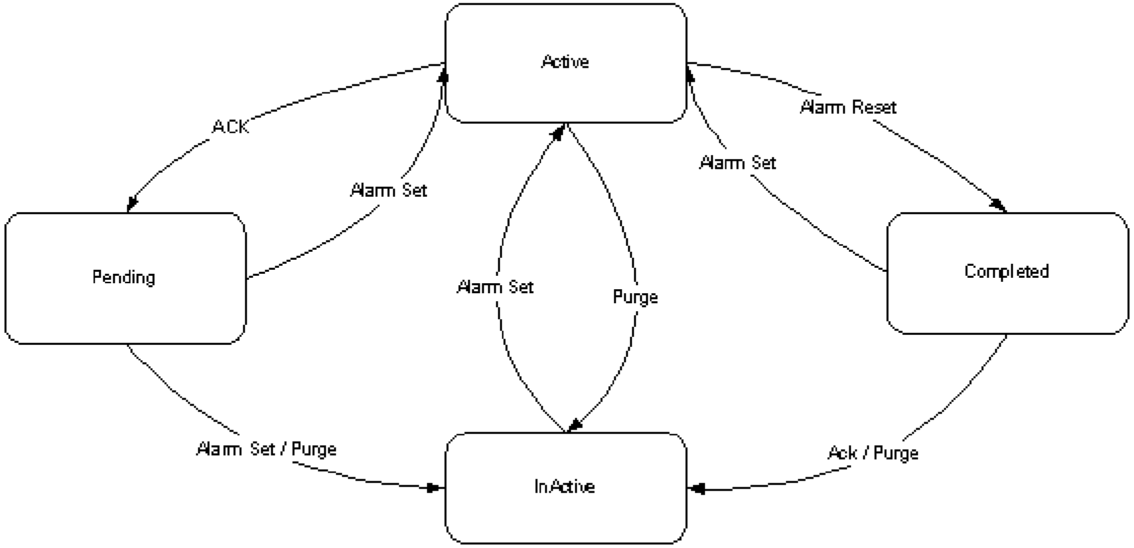
FCWnx plugin enables alarm integration with third party systems. As soon as an event started (on GeViSoft or on another system) FCWnx alarm with same name is set on FCWnx. And as soon as this event is stopped, corresponding FCWnx alarm is reset. Also it is possible to get acknowledgement notification as soon as FCWnx alarm changes state to InActive. For alarm states of FCWnx please refer to below figure.

Supported Hardware/Software

FCWnx has been developed and tested with FCWnx 7.5.1 version.
And it supports all versions after FCWnx 7.5.1 version.

How to configure plugin

To be able to use FcWnx plugin, *FCWnx API Service* needs to be installed on the computer. After adding a valid mapping, FcWnx plugin enables communication between third party systems and FCWnx. Events/Alarms can be sent and received. As soon as an alarm becomes “Active” in FCWnx it is started, and as soon as its state becomes “Inactive” it is stopped on third party systems. Moreover, as soon as an alarm is acknowledged or cleared (i.e. when alarm is in “Inactive” state), alarm cleared notification is transferred automatically.



FCWnx API Username	Username which will be used during API connection. This value should be set to “Application Login” value which is set within the FCWnx.
FCWnx API Password	Password value which will be used during API connection authentication.
FCWnx Alarm Clear Suffix	If an alarm acknowledged or cleared on FCWnx, alarm cleared notification event is started. Started event name is alarm name on FCWnx + Alarm Clear Suffix. For example, if there exists and alarm named “FCWNx_Sample_Alarm” on FCWnx, and if FCWnx Alarm Clear Suffix value is set to “_Cleared”, than as soon as “FCWNx_Sample_Alarm” is acknowledged or cleared, an event named “FCWNx_Sample_Alarm_Cleared” should start. Please note that since this event is acknowledgement notification, it will not be stopped by integration server, which means you should set it as auto-stop on GeViSoft.

Fiber SenSys plugin

Fiber SenSys plugin is an input plugin which is designed to take events/alarm from Fiber SenSys alarm processing units (APU). The plugin works using a TCP connection and this connection provides fast communication with other plugins. The plugin has 128 channels and each of these channels support one APU module. All of the modules works independent from the other and has own parameters to connect to devices.

Supported Hardware/Software

Fibersensys APU has been developed and tested with FD3xx-IP and FD500D-IP. And it supports FD3xx-IP and FD500D-IP versions.

Supported Functionality

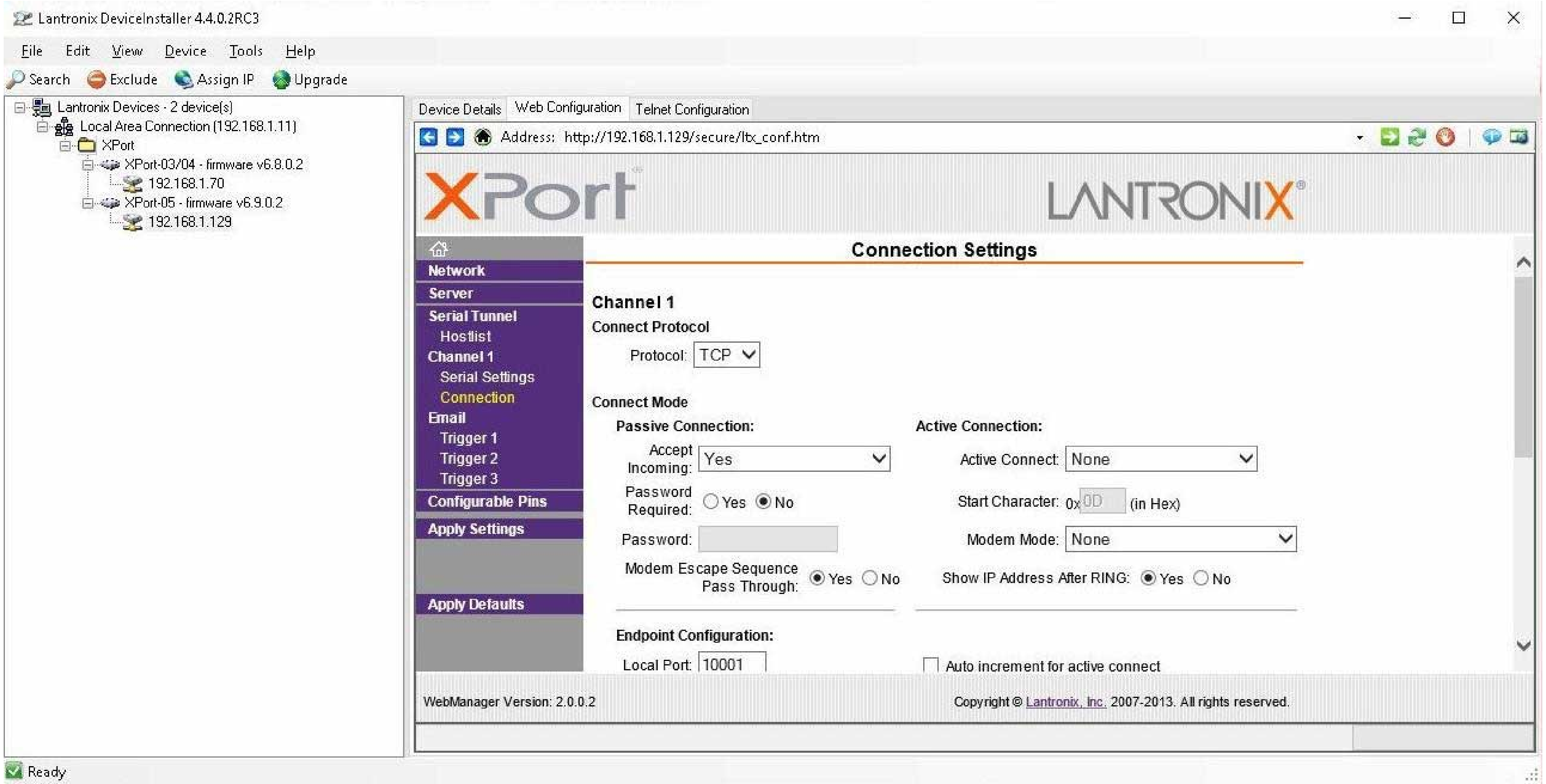
There are 3 types of events:

- Intrusion or alarm
- Fault (broken fiber or hardware malfunction)
- Tamper (a switch which indicates whether the device has been opened).

Events that are coming from Fiber SenSys devices are named like: DEVICENAME_DEVICESTATE, where DEVICENAME is the channel name of plugin.

To give an example:

- APU1.CHb_ALARM
- APU1.CHb_FAULT
- APU1.CHa_TAMPER


Lantronix DeviceInstaller 4.4.0.2RC3
File Edit View Device Tools Help
Search Exclude Assign IP Upgrade
Lantronix Devices - 2 device(s)
Local Area Connection (192.168.1.11)
XPort
XPort-03/04 - firmware v6.8.0.2
192.168.1.70
XPort-05 - firmware v6.9.0.2
192.168.1.129
Device Details Web Configuration Telnet Configuration
XPort
LANTRONIX
Network
Server
Serial Tunnel
Hostlist
Channel 1
Serial Settings
Connection
Email
Trigger 1
Trigger 2
Trigger 3
Configurable Pins
Apply Settings
Apply Defaults
Ready

Address: http://192.168.1.129/secure/ltx_conf.htm

Connection Settings

Channel 1

Connect Protocol

Protocol: TCP

Connect Mode

Passive Connection:

Accept Incoming: Yes

Password Required: ○ Yes ● No

Password:

Modem Escape Sequence Pass Through: ● Yes ○ No

Active Connection:

Active Connect: None

Start Character: 0x 0D (in Hex)

Modem Mode: None

Show IP Address After RING: ● Yes ○ No

Endpoint Configuration:

Local Port: 10001

□ Auto increment for active connect

WebManager Version: 2.0.0.2

Copyright © Lantronix, Inc. 2007-2013. All rights reserved.

Fibersensys APU should be configured as Accept Incoming “Yes”, Active Connect “None”. *FS Module XX Ip Address* is the IP address of Fiber SenSys module on which it is running.

GCore plugin

GCore plugin is a bidirectional plugin and provides event/alarm transfer also serves as a bridge between 3rd party applications and GNG. According to mapping situation of GCore plugin, it could receive or send events/alarms to/from 3rd party systems. And as soon as event/alarm is starts/stops, corresponding insight event/alarm starts/stops.

Supported Hardware/Software

GCore plugin has been tested with all versions of GCore and it supports all GCore versions.

Supported Functionality

GCore plugin receives below actions:

- OnEventStartedEx
- OnEventStopped
- OnCustomAction
- OnDigitalInput
- OnDigitalOutput
- OnCameraOn
- OnCameraOff
- OnSensorVideoAlarm
- OnSensorAlarmFinished

GCore plugin accepts actions below:

- ACSAccessGranted
- ACSRawdata
- GamingMachine
- PPZoneAlarm
- PPDeviceAlarm
- PPDeviceOffline
- PPDeviceOnline
- PPInterfaceOffline
- LiveCheck
- NPRRecognition

Using GeviScope plugin, requested events could be could be transfered to other plugins after setting mapping property of plugins. GeviScope plugin supports transferring events:

Sensor Alarms	This action will be fired when the alarm is finished or video alarm is detected
Custom Actions	This action has no side effects and can be used for customer purposes
Input Events	This action will be fired when the state of the digital input has changed
Generic Events	This action will be fired or finished when the state of the geviscope events has started /stopped

GCore plugin Parameters	
GCore API Username	Username which will be used during GCore Server connection. GCore default username value is “sysadmin”
GeviScope API Password	Password value which will be used during GCore Server connection. GCore default password value is “masterkey”
GCore API Server Name	The IP address of the GCore application was loaded. GCore plugin supports both local and remote GCore server connections. Default server name is “localhost”
Transfer Events	This boolean parameter allows to system receiving events from GeviScope
Transfer Sensor Alarms	This boolean parameter allows to system receiving Sensor Alarms from GeviScope
Transfer Custom Actions	This boolean parameter allows to system receiving customer purposes actions from GCore
Transfer Input Events	This boolean parameter allows to system receiving digital input states when their states has changed from GCore
Send Everything As Custom Actions	Normally all events coming to GCore plugin are sent to related GCore server with start/stop event commands. But if you set this boolean parameter to “true” than everything coming to this plugin is sent as CustomActions. For example let‟s say there is an event coming to this plugin named “DoorAlarm”. Normally it is started and stopped as event on GCore. However if you set this parameter to true, than when “DoorAlarm” starts, CustomAction with name “DoorAlarm” started instead of an event. And when “DoorAlarm” finishes another CustomAction with name “DoorAlarm_STOP” started. So instead of event stop command, CustomAction with trailing “_STOP” is started

Event Naming

All events generated by 3rd party systems that integrated into GCore start/stop using their source name. Source name could be input/output name or custom event names. Event names are determined as follows:

- GCore_Example1_Input Started
- GCore_Example2_Input Stopped

Started means that this input/output is in high state, and stopped means input/output in low state.

- CustomEvent1 Started
- CustomEvent2 Stopped

GeViScope plugin

GeViScope plugin is a bidirectional plugin and provides event/alarm transfer also serves as a bridge between 3rd party applications and Geviscope. According to mapping situation of Geviscope plugin, it could receive or send events/alarms to/from 3rd party systems. And as soon as event/alarm is starts/stops, corresponding Insight event/alarm starts/stops.

There is some kind of „heartbeat" CustomAction is generated and send to GeViScope every 30 seconds. By checking this custom action from the GeViScope side one can detect whether the NDIS server fails or not. GeViScope side could use that action to keep retriggering an event in Geviscope. If it stops receiving the custom action (because NDIS failed) then generates an alarm in the system to inform user.

Supported Hardware/Software

GeViScope plugin has been tested with all versions of GeViScope and it supports all GeViScope versions.

Supported Functionality

GeViScope plugin receives below actions;

- OnEventStartedEx
- OnEventStopped
- OnCustomAction
- OnDigitalInput
- OnDigitalOutput
- OnCameraOn
- OnCameraOff
- OnSensorVideoAlarm
- OnSensorAlarmFinished
- OnViewerConnected
- OnViewerCleared

GeViScope plugin accepts actions below:

- ACSAccessGranted
- ACSRawdata
- ACSAccessDenied
- GamingMachine
- DrawBoundingBox
- ClearBoundingBox
- PPZoneAlarm
- PPDeviceAlarm
- PPDeviceOffline
- PPDeviceOnline
- PPInterfaceOffline
- LiveCheck
- NPRRecognition
- CustomActionEx

Using GeviScope plugin, requested events could be could be transfered to other plugins after setting mapping property of plugins. GeviScope plugin supports transferring events :

Sensor Alarms This action will be fired when the alarm is finished or video alarm is detected.

Custom Actions This action has no side effects and can be used for customer purposes.

Input Events This action will be fired when the state of the digital input has changed.

Generic Events This action will be fired or finished when the state of the geviscope events has started /stopped.

GeViScope plugin Parameters	
GeViScope API Username	Username which will be used during GeViScope Server connection. GeViScope default username value is “sysadmin”.
GeViScope API Password	Password value which will be used during GeViScope Server connection. GeViScope default password value is “masterkey”.
GeViScope API Server Name	The IP address of the GeViScope application was loaded. GeViScope plugin supports both local and remote GeViScope server connections. Default server name is “localhost”.
Transfer Events	This boolean parameter allows to system receiving events from GeviScope.
Transfer Sensor Alarms	This boolean parameter allows to system receiving Sensor Alarms from GeviScope.
Transfer Custom Actions	This boolean parameter allows to system receiving customer purposes actions from GeviScope.
Transfer Input Events	This boolean parameter allows to system receiving digital input states when their states has changed from GeviScope.
Send Everything As Custom Actions	Normally all events coming to GeViScope plugin are sent to related GeViScope server with start/stop event commands. But if you set this boolean parameter to “true” than everything coming to this plugin is sent as CustomActions. For example let’s say there is an event coming to this plugin named “DoorAlarm”. Normally it is started and stopped as event on GeViScope. However if you set this parameter to true, than when “DoorAlarm” starts, CustomAction with name “DoorAlarm” started instead of an event. And when “DoorAlarm” finishes, another CustomAction with name “DoorAlarm_STOP” started. So instead of event stop command, CustomAction with trailing “_STOP” is started.

Event Naming

All events generated by 3rd party systems that integrated into GeViScope start/stop using their source name. Source name could be input/output name or custom event names. Event names are determined as follows:

- Gevisoft_Example1_Input Started
- Gevisoft_Example2_Input Stopped

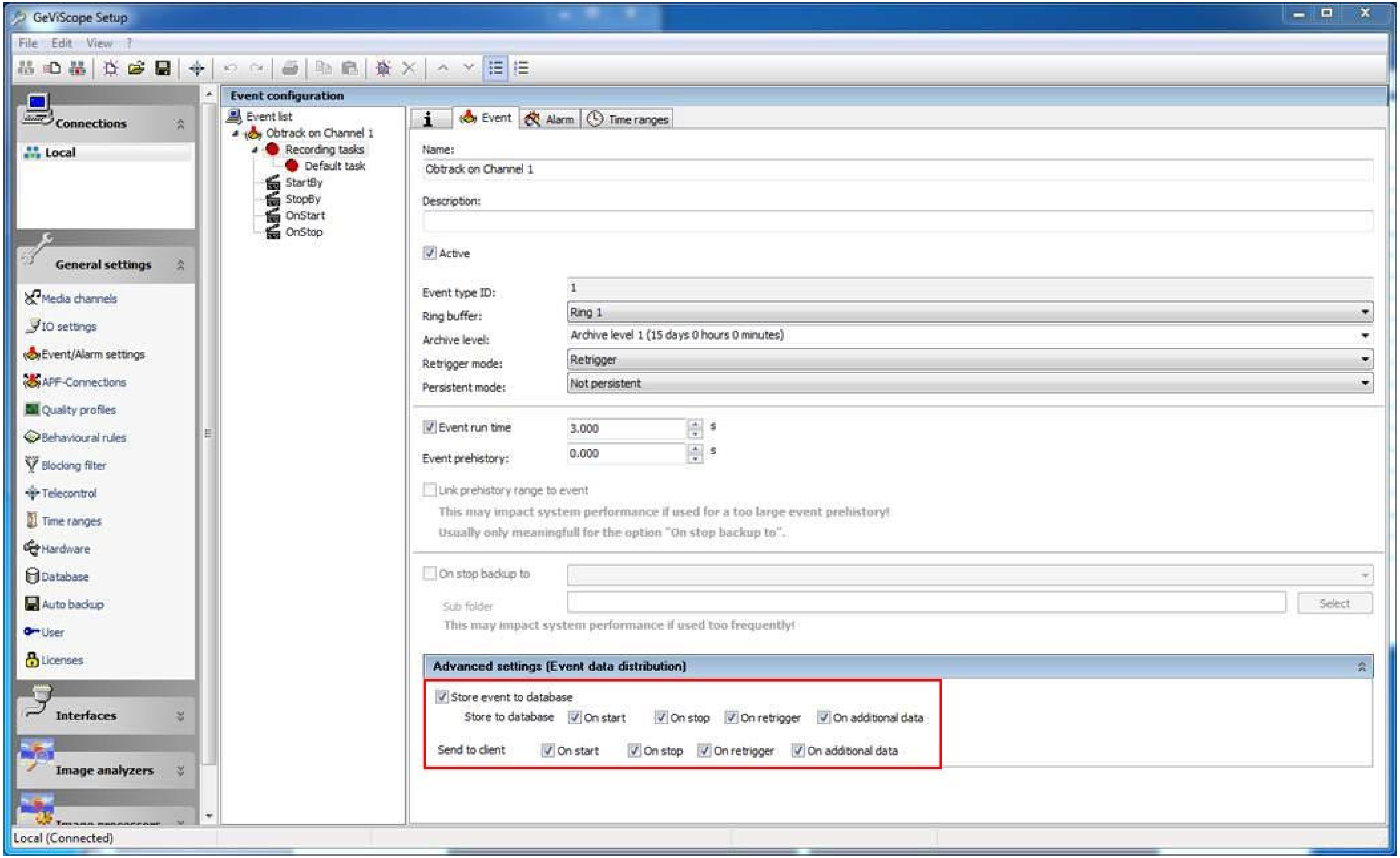
Started means that this input/output is in high state, and stopped means input/output in low state.

- CustomEvent1 Started
- CustomEvent2 Stopped

How to configure GeViScope

1. Open GSCSetup and connect to the local server

2. Add an Event
Please do not forget to check advanced settings:



Name: Obtrack on Channel 1

Description:

☑ Active

Event type ID: 1

Ring buffer: Ring 1

Archive level: Archive level 1 (15 days 0 hours 0 minutes)

Retrigger mode: Retrigger

Persistent mode: Not persistent

☑ Event run time 3.000 s

Event prehistory: 0.000 s

□ Link prehistory range to event

This may impact system performance if used for a too large event prehistory!
Usually only meaningfull for the option "On stop backup to".

□ On stop backup to

Sub folder

This may impact system performance if used too frequently!

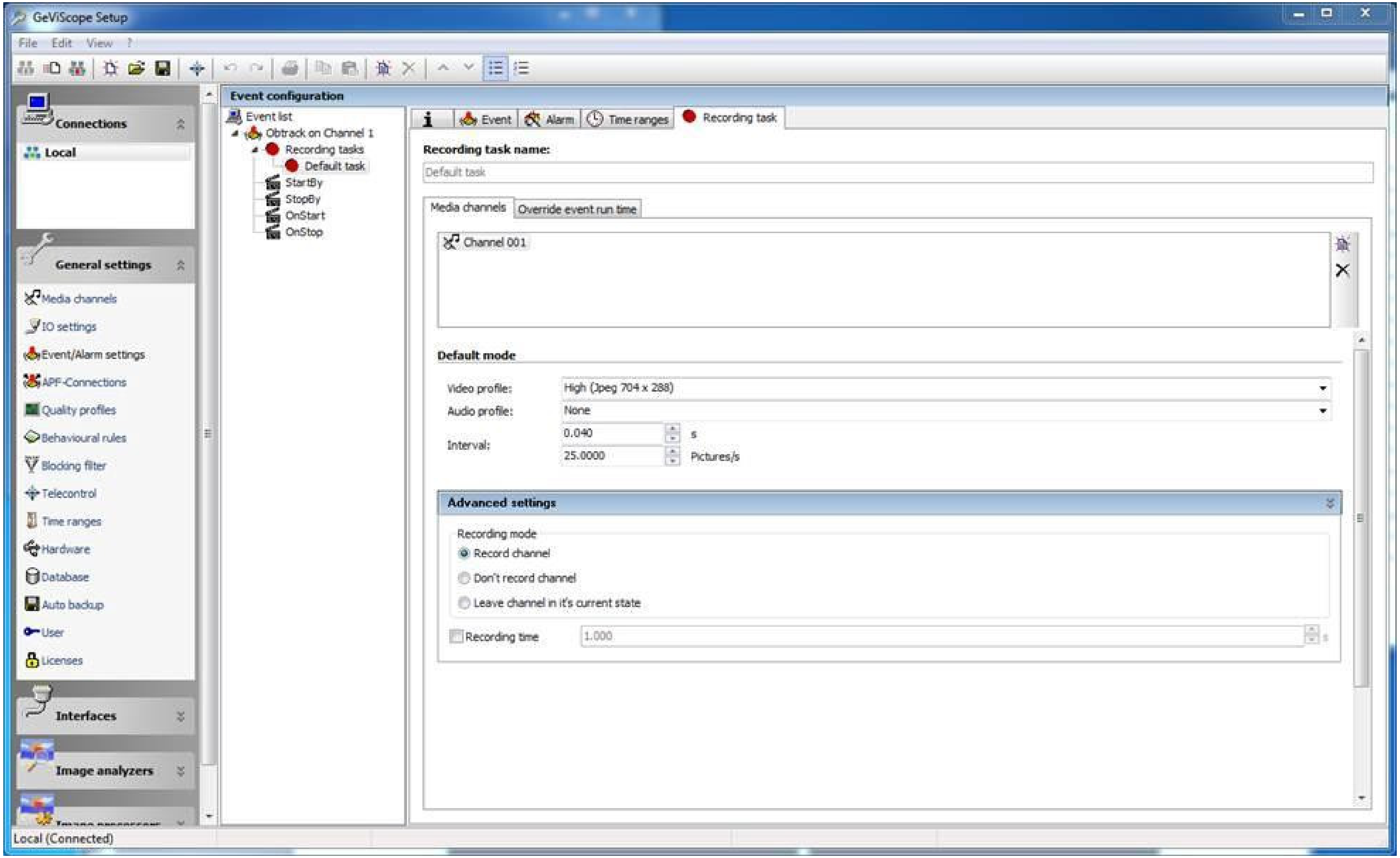
Advanced settings [Event data distribution]

☑ Store event to database

Store to database ☑ On start ☑ On stop ☑ On retrigger ☑ On additional data

Send to client ☑ On start ☑ On stop ☑ On retrigger ☑ On additional data

3. Add related Media Channel to the Recording Task



Recording task name: Default task

Video profile: High (Jpeg 704 x 288)

Audio profile: None

Interval: 0.040 s

25.0000 Pictures/s

Recording mode

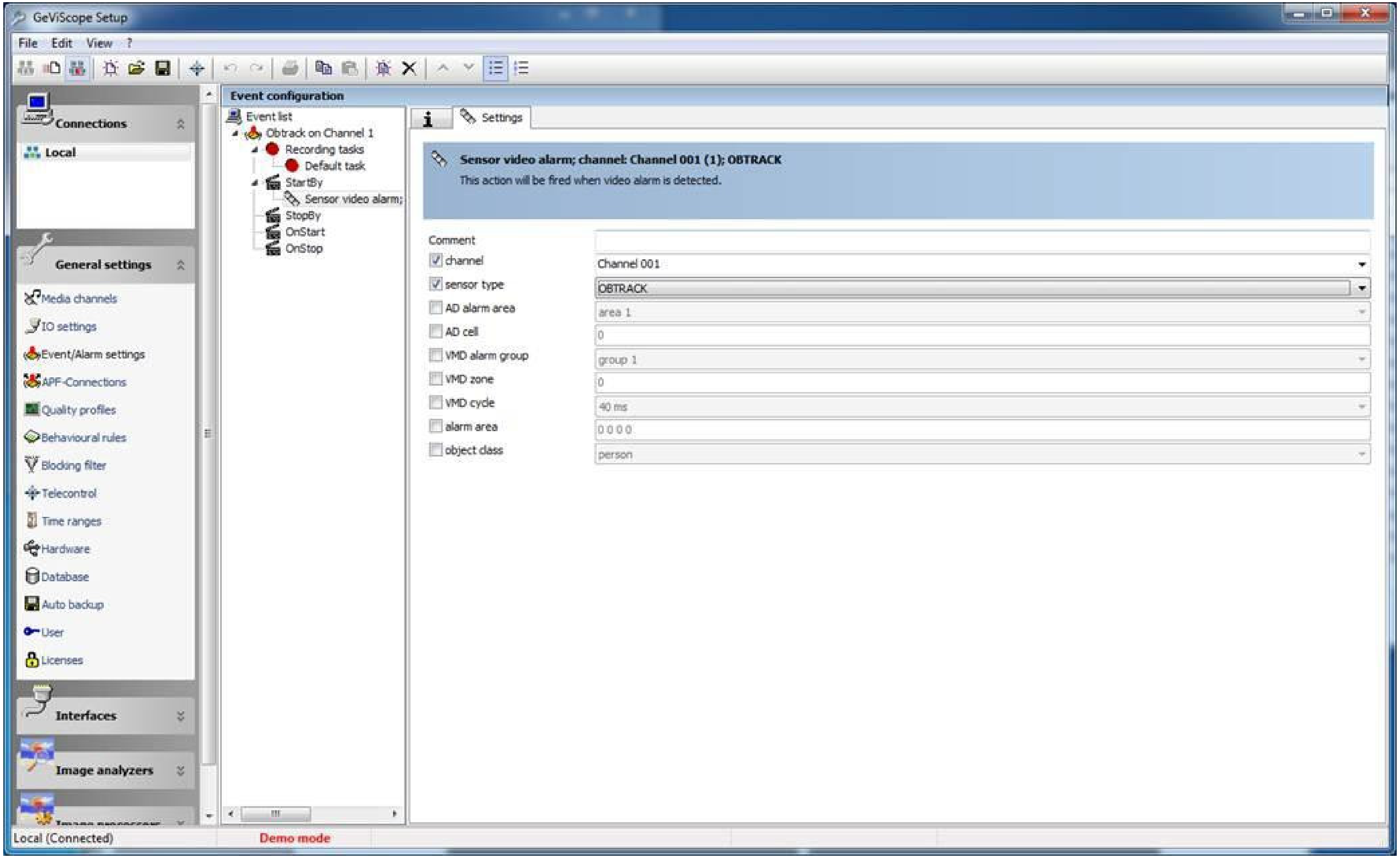
● Record channel

○ Don't record channel

○ Leave channel in it's current state

□ Recording time 1.000 s

4. Set the StartBy action to SensorVideoAlarm with your channel number and sensor type OBTRACK



Sensor video alarm; channel: Channel 001 (1); OBTRACK

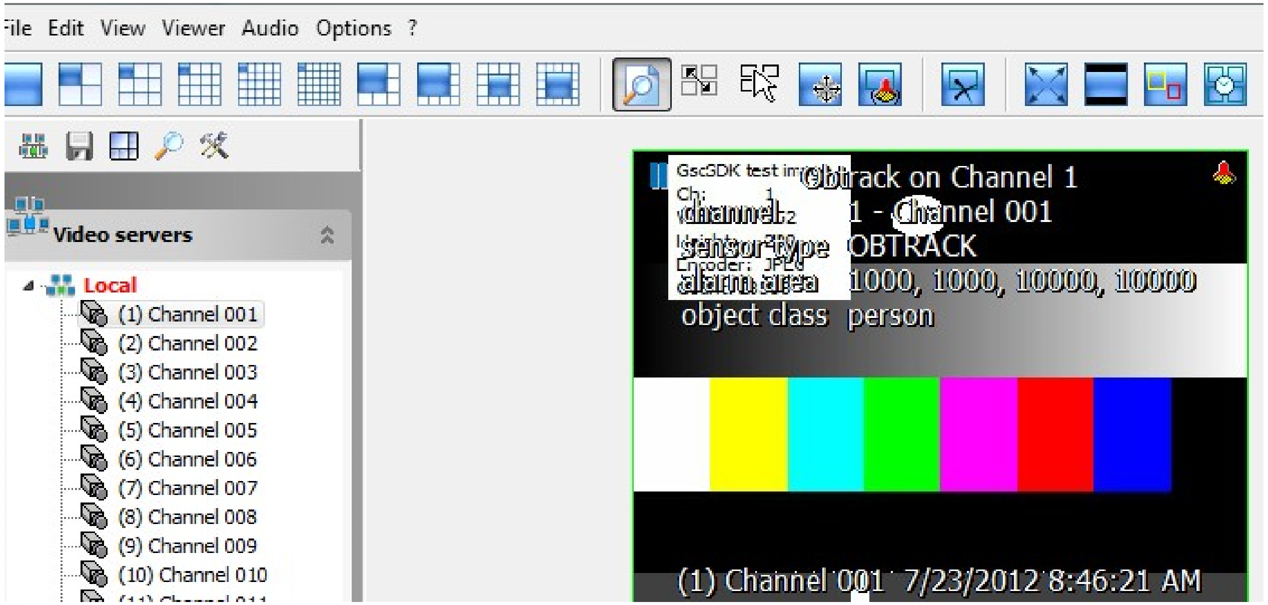
This action will be fired when video alarm is detected.

Comment	
☑ channel	Channel 001
☑ sensor type	OBTRACK
□ AD alarm area	area 1
□ AD cell	0
□ VMD alarm group	group 1
□ VMD zone	0
□ VMD cycle	40 ms
□ alarm area	0 0 0 0
□ object class	person

5. Send the setup to the server

6. Start GscView and display your media channel

7. You should see the Event Text displayed in your media channel when there is detection.



Obtrack on Channel 1
channel 1 - Channel 001
sensor type OBTRACK
alarm area 1000, 1000, 10000, 10000
object class person

(1) Channel 001 7/23/2012 8:46:21 AM

NOTICE If you press the *Draw Marker at position with largest activity* button, the rectangle should also be displayed.

Troubleshooting

ADVICE Please be sure that below prerequisites are installed on the computer:

Microsoft Visual C++ 2008 SP1 Redistributable Package (x86)

Microsoft Visual C++ 2010 Redistributable Package (x86)

Microsoft Visual C++ 2013 Redistributable Package (x86)

And below files resides under application directory of G-Link:

GscViewer.ocx, GscActions.dll GscDBI.dll , GscHelper.dll , GscMediaPlayer.dll, MscDBI.dll , msvcr90.dll

If you are receiving “CLASS_NOT_REGISTERED” error, this means GSCViewer component is not registered correctly. To register GscViewer.ocx file to system:

- Install Microsoft Visual C++ 2008 SP1 Redistributable Package (x86) to system
- Install Microsoft Visual C++ 2010 Redistributable Package (x86) to system
- After creating new folder, put GscViewer.ocx, GscActions.dll GscDBI.dll , GscHelper.dll , GscMediaPlayer.dll, MscDBI.dll , MscDBI.dll to folder.
- Run cmd.exe on Administration privilege, then change the directory to created folder. Run command “regsvr32 GscViewer.ocx”.

GeViSoft plugin

GeViSoft plugin is a bidirectional plugin and provides event/alarm transfer also serves as a bridge between 3rd party applications and GeViSoft. According to mapping situation of Geviscope plugin, it could receive or send events/alarms to/from 3rd party systems. And as soon as event/alarm is starts/stops, corresponding Insight event/alarm starts/stops.

Supported Hardware/Software

GeViSoft plugin enables transferring events generated by CIAS microwave barriers to GeViSoft platform. GeViSoft 1.3.1.71 or later is required for this plugin to run.

Supported Functionality

GeViSoft plugin receives and accepts below actions:

- Event Started and
- Event Stopped

To receive alarms from CIAS IB-Servers you must create corresponding events in your GeviServer according to events generated by CIAS plugin. Please see event naming section for details.

Here is an example:

Assume you have one IBServer which has “IBServer Prefix” IBServer0 and “IBDevice Prefix” IBDevice respectively. And let’s say IBServer has 3 devices connected to it which has device IDs 0, 1 and 2

Than you must create these events on GeViServer:

- IBServer0_IBDevice0_PREALARM
- IBServer0_IBDevice0_ALARM
- IBServer0_IBDevice0_TAMPER
- IBServer0_IBDevice0_FAULT
- IBServer0_IBDevice0_NO_ANSWER
- IBServer0_IBDevice1_PREALARM
- IBServer0_IBDevice1_ALARM
- IBServer0_IBDevice1_TAMPER

- IBServer0_IBDevice1_FAULT
- IBServer0_IBDevice1_NO_ANSWER
- IBServer0_IBDevice2_PREALARM
- IBServer0_IBDevice2_ALARM
- IBServer0_IBDevice2_TAMPER
- IBServer0_IBDevice2_FAULT
- IBServer0_IBDevice2_NO_ANSWER

> ADVICE If you enabled “Notify Connection Losses” feature, than you should also create connection lost event on GeViSoft. If channel name is IBServer 0 and “Connection Loss Event Suffix” is _CONN_LOST than connection loss event name will be IBServer 0_CONN_LOST as mentioned before.

Please make sure that all CIAS events created on GeViSoft are not configured as Auto-Stop. Because server is responsible for both starting and stopping events.

Hikvision Central

Hikvision Central plugin enables users to receive real time notifications from Hikvision DVR/NVR and other devices.

Supported Hardware/Software

It works with all versions of Hikvision products.

Supported Functionality

It can receive:

- Hard disk full
- Sensor Alarm
- Video Lost
- Video Motion Alarm
- Hard disk unformatted
- Hard disk error
- Tampering detection
- Unmatched video output standard
- Illegal operation
- Video signal abnormal
- Record abnormal

IGT plugin

IGT plugin enables integration of DACOM Paging interface. IGT plugin is listening as a TCP Server.

Supported Hardware/Software

IGT plugin has been developed and tested with DACOM Paging Interface. And it supports all versions.

Supported Functionality

Dacom paging interface is not able to send data for some cases. For reliability plugin checks periodically if there are any incoming data. If there is not any incoming data, it starts an event. Name of the event and check period can be configured from plugin channel parameters.

Parameters:

- ***Server Listen Port*****:** TCP Port on which plugin should be listening
- ***Filter Events*** (Semicolon Seperated): List of events which should be transferred

Insight plugin

Insight plugin enables event/alarm transfer and video integration alongside with Insight Geutebrück plugin. As soon as an event started on 3rd party systems, Insight plugin sends the events/alarms to Insight Review and can be viewed from Insight Review Window. And as soon as this event is stopped, corresponding Insight event/alarm is stopped.

Supported Hardware/Software

Plugin is tested with Insight Professional version 5.1 (12437). And it supports all versions after Insight Professional version 5.1.

Supported Functionality

There are two integrations available for Insight plugin. First one is video integration, which enables viewing of videos within Insight Review of Schematics. If you would like to view only videos than it is enough to have DVR integration licence at Insight side.

Second one is bidirectional events/alarms/Digital IO integration. For this to be operational, you have to have COM licence at Insight side. Please note that if you do not have COM licence, status of Insight plugin will be shown as disconnected, but this does not mean any problem. You can still have video integration. You just can not receive events/alarms/Digital IO from external systems.

Bidirectional event/alarm transfer is handled by Insight plugin of GINT. And Insight Geutebruck plugin is responsible for video integration. It is a DLL named “IRGeutebruckPlugin.dll” which is running within the Insight Server process context.

Plugin Parameters

Insight Username	Username which will be used during Insight Server connection. Insight has two default username values “installer” and “admin”. Additional username settings could be set from Edit/User Administration in Insight Launch Pad.
Insight Password	Password value which will be used during Insight Server connection. Insight has two default password values “installer” for installer username and “admin” for admin username. Additional password settings could be set from Edit/User Administration in Insight Launch Pad.
Insight server IP address	IP Address is the machine Ip address of Insight Machine which was loaded. Insight plugin supports both local and remote Insight connections.
Insight server port address	The Insight port number value of the machine on which Insight is installed. This can be changed from Insight Launch Pad section. Default value is “751”.

How To Configure plugin

Insight shows the events from Review window and Insight plugin provides to be viewed the incoming events in this format:

Event Source	Date/Time	Event Number	Event Details
Insight COM sample	5/18/2010 11:53:47 AM	25851	COM Interface: Successfully : Loggged In by INSTALLER

Event Source
Insight plugin sends the source in this format: “3rd party system plugin name_3rd party system channel name”. For instance `GeviScopeAPIplugin_GSCClient 0`

Date/Time
The date and time when an event occurs in 3rd party systems.

Event Number
An integer value that assigned by the Insight system.

Event Details
Event details contains:

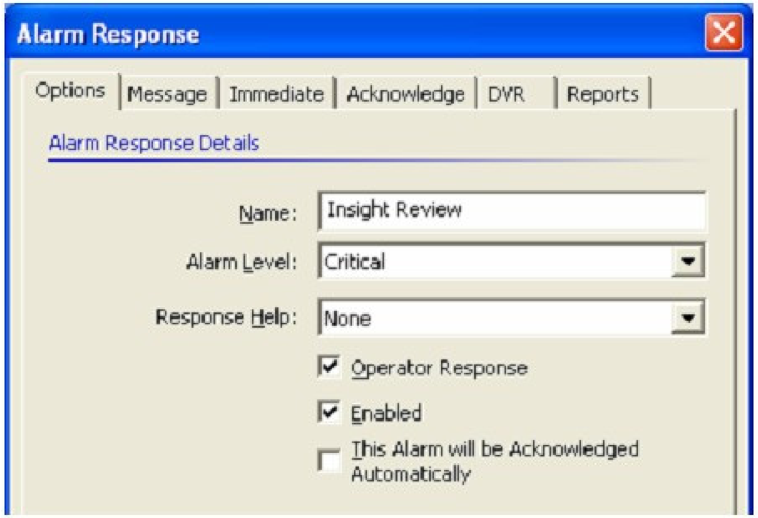
Name value that is the name of the source generating the event. Insight plugin sends the names in “3rd party system plugin name_3rd party system channel name” format. For example `GeviScopeAPIplugin_GSCClient 0`.

Event Name: The name value of Input/output names or the names of events that created from 3rd party systems. Also Event Details part contains the logged user name.

Insight Alarms

Insight alarms are defined by Operators. Operator can choose exactly what conditions must be satisfied for the alarm to be raised. The way Insight reacts to an alarm is controlled by an alarm response. When Insight is first installed, it has a single alarm response set up that handles all panel alarms. You can modify or remove this alarm response, and you can add any number of additional alarm responses. Alarms are displayed in the alarms window, and must be acknowledged. In any module, the number of outstanding alarms is displayed in the lower right hand corner of the screen.

An alarm response defines what rules constitute an alarm and also specifies how Insight reacts when it occurs. Alarms are defined using a filter stack. When incoming review matches the filter stack, the alarm is triggered. A triggered alarm can be configured to attract the Operator’s attention in a variety of ways. Triggered alarms are added to the alarms window and must be acknowledged.



Name: Insight Review

Alarm Level: Critical

Response Help: None

☑ Operator Response

☑ Enabled

☐ This Alarm will be Acknowledged Automatically

To create a new alarm response:

1. In any module, click the alarm counter (bottom right corner). The Alarm Handler window opens.

2. On the Edit Alarms menu, choose “New Alarm Response” and navigate to the type of review event you want to base the alarm response on. A new filter stack is created matching your criteria, and the Alarm Response window is displayed.

3. Enter the settings for this alarm response.

4. Click OK.

Filtering Events and Triggering Alarms

Insight saves every single review event ever received, the number of events can grow to a large number. Usually, you will only be interested in examining review from a particular time period or from a specific panel. You can quickly isolate review of interest by applying filters.

To customize which events trigger an existing alarm response:

1. Open the Alarm Handler window by clicking the alarm count.

2. Click the Alarm Responses button in the toolbar.

3. Select the alarm response you wish to modify, then click Edit. The alarm response filter stack is displayed, then the alarm response window is opened.

4. Click Cancel to close the alarm response window. You will be left with the alarm response filter stack.

5. Modify the filter stack to suit your requirements. Remember, any review messages that satisfy your filter stack will generate an alarm.

6. Close the filter stack. Changes take effect immediately.

To modify how Insight reacts to an existing alarm response:

1. Open the Alarm Handler window by clicking the alarm count.

2. Click the Alarm Responses button in the toolbar.

3. Select the alarm response you wish to modify, then click Edit. The alarm response filter stack is displayed, then the alarm response window is opened.

4. Make any changes to the alarm response.

5. Click OK.

To add a filter to the filter stack:

1. After adding an Event/Alarm Responses, open created response.

2. Modify the filter according to you requirements.

3. If this isn't the only filter in the stack, click the and/or button to determine how this filter interacts with the other filters in the stack.

4. Click the save button to activate your filter.

Troubleshooting

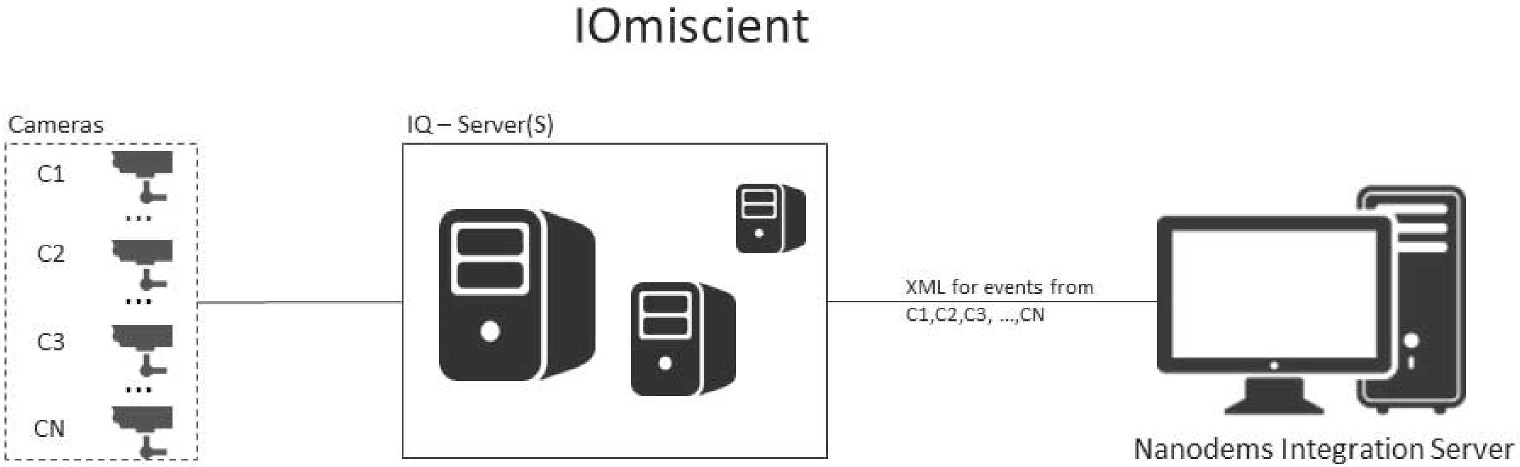
If a license is not present or not valid then the following exception will be thrown when using G-Int Setup. “Failed to successfully login. Insight installation is not licensed for this operation.”

If you install GINT on the computer where Insight Server is running, than nothing else required for installing IRGeutebruck plugin. Because GINT installer handles the process of placing required DLLs under Insight application folder.

If GINT is installed on a computer which is not running the Insight Server than you should run Insight Geutebruck Plugin patch file (which is named as GeutebrückInsightPluginPatchV1.0.8906.exe) on Insight Server computer. Please note that to be able to see GeViScope on DVR list of Insight software you should restart the Insight Server.

IOmniscient plugin

IOmniscient is a video analytic software, which provides detection and identification on cameras.


IOmiscient
Cameras
C1
C2
C3
CN
IQ – Server(S)
XML for events from C1,C2,C3, ...,CN
Nanodems Integration Server

G-Link Server supports a one way integration with IOmniscient IQSeries (Input plugin). The ıntegration contains receiving video analysis event from IOmniscient and depending on mapping configuration sending it to third party integrated software.

Supported Hardware/Software

IQSeries application or above needed to be installed in the network same as the receiver. The server needs to be running and set up for XML Notification.

IOmniscient plugin was developed and tested wirh IQSeries 4.0

Supported Functionality

Supported Alarm Types are

Event Name	Alarm Type	Category
Object Detection	Abandonend Object	Non Motion Alarms
Crowd Management Alarm	Over Crowed	

Configurable properties for IOmniscient plugin are:

- Port
- Event Suffx

Jacques plugin

Jacques is a communication system featuring video and audio intercom.

Supported Hardware/Software

Jacques plugin has been developed and test with:

- Controller: TCH-2MXH | 51660
- Master : IPM-350 | 51516
- Intercom : VSL-361W+ | 51676

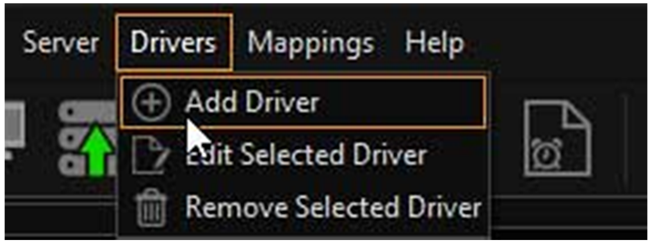
Supported Functionality

- If Video Open event is received, Start Call event occurs in Jacques.
- If Video Close event is received, End Call event occurs in Jacques.

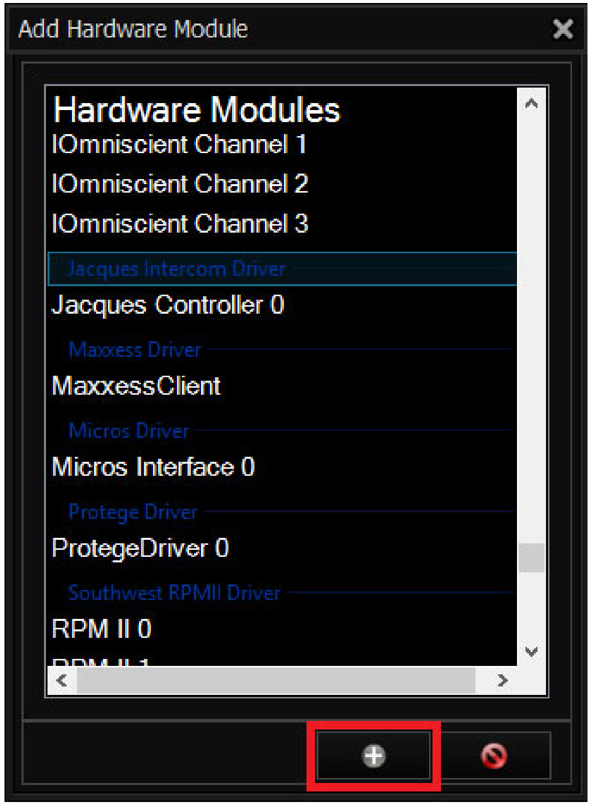
How to configure plugin

Jacques plugin provides event transfer from 3rd party systems to Jacques Device. Via those events, operation of Jacques will be set as automatically. Please follow the steps to add Jacques plugins to G-Link:

1. Click plugins on the bar above and press *Add plugin* button.



2. Select Jacques Controller 0 under Jacques Intercom plugin.



Add Hardware Module

Hardware Modules

IOmniscient Channel 1

IOmniscient Channel 2

IOmniscient Channel 3

Jacques Intercom Driver

Jacques Controller 0

Maxxess Driver

MaxxessClient

Micros Driver

Micros Interface 0

Protege Driver

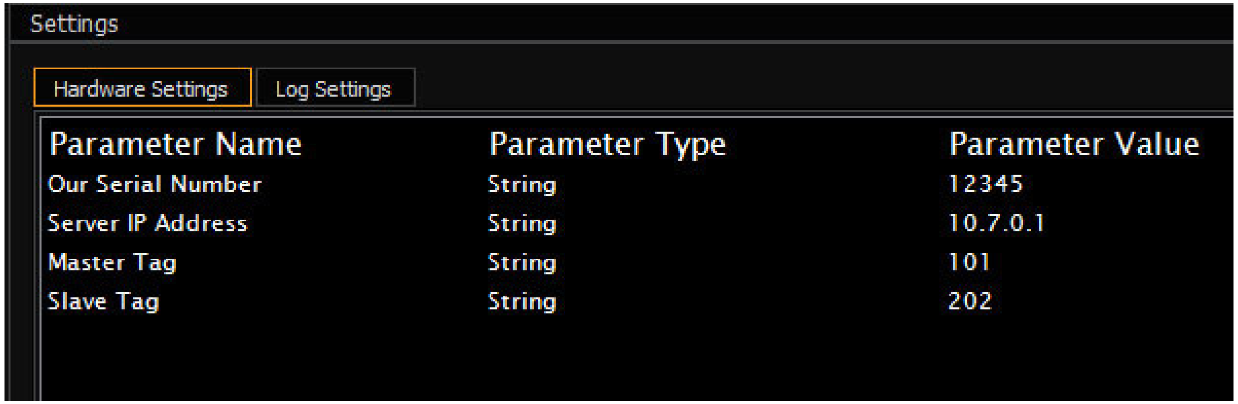
ProtegeDriver 0

Southwest RPMII Driver

RPM II 0

Click on + to add Jacques plugin.

3. Set Jacques Parameters from G-Link.

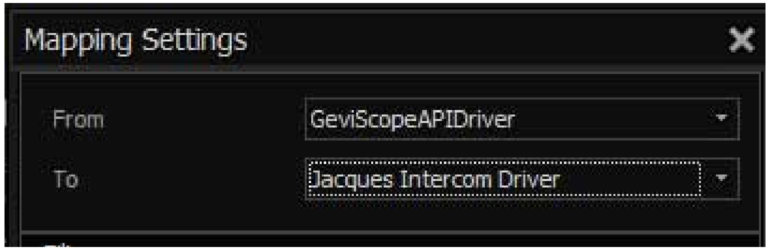


Settings

Parameter Name	Parameter Type	Parameter Value
Our Serial Number	String	12345
Server IP Address	String	10.7.0.1
Master Tag	String	101
Slave Tag	String	202

Jacques plugin Parameters	
Our Serial Number	Serial Number of computer which connects to Jacques. Default is „12345"
Server IP Adress	IP Adress of Jacques Server. Default is „10.7.0.1". Connection to Jacques depens on IP Address
Master Tag	ID of Master. It is similar to phone number of Master
Slave Tag	Slaves are „called" components. According to image of 3.steps, 101 calls 202. Slave Tag can have relationship with other device via 3rd party softwares. For example, via GSCView, if a camera, which has relationship with 202 slave, is dropped to view scene, master will call 202 slave

4. Add Mapping for getting event from other plugins. Below images are sample of adding mapping from GeviScope to Jacques.



From: GeviScopeAPIDriver

To: Jacques Intercom Driver

Set mappings in mappings section. After select *From* and *To* plugins, press *OK* and press *Send Setup to Server to save* changes.

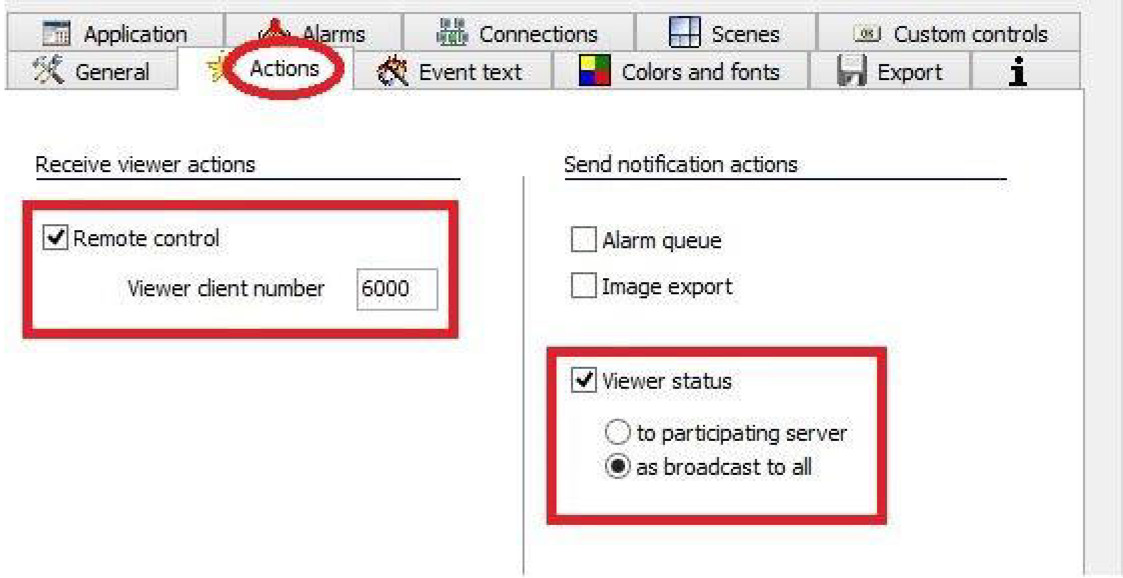
A Sample Relation between GeviScope and Jacques

Events are produced by GSCView program, but that program needs some settings to send events to our system. These settings steps are :

1. Open GSCView and connect to server. (Server must be running)

2. Options -> Profile Manager

3. Select *Options Profile* from left,Click *Actions*.



Receive viewer actions

☑ Remote control

Viewer client number 6000

Send notification actions

□ Alarm queue

□ Image export

☑ Viewer status

○ to participating server

● as broadcast to all

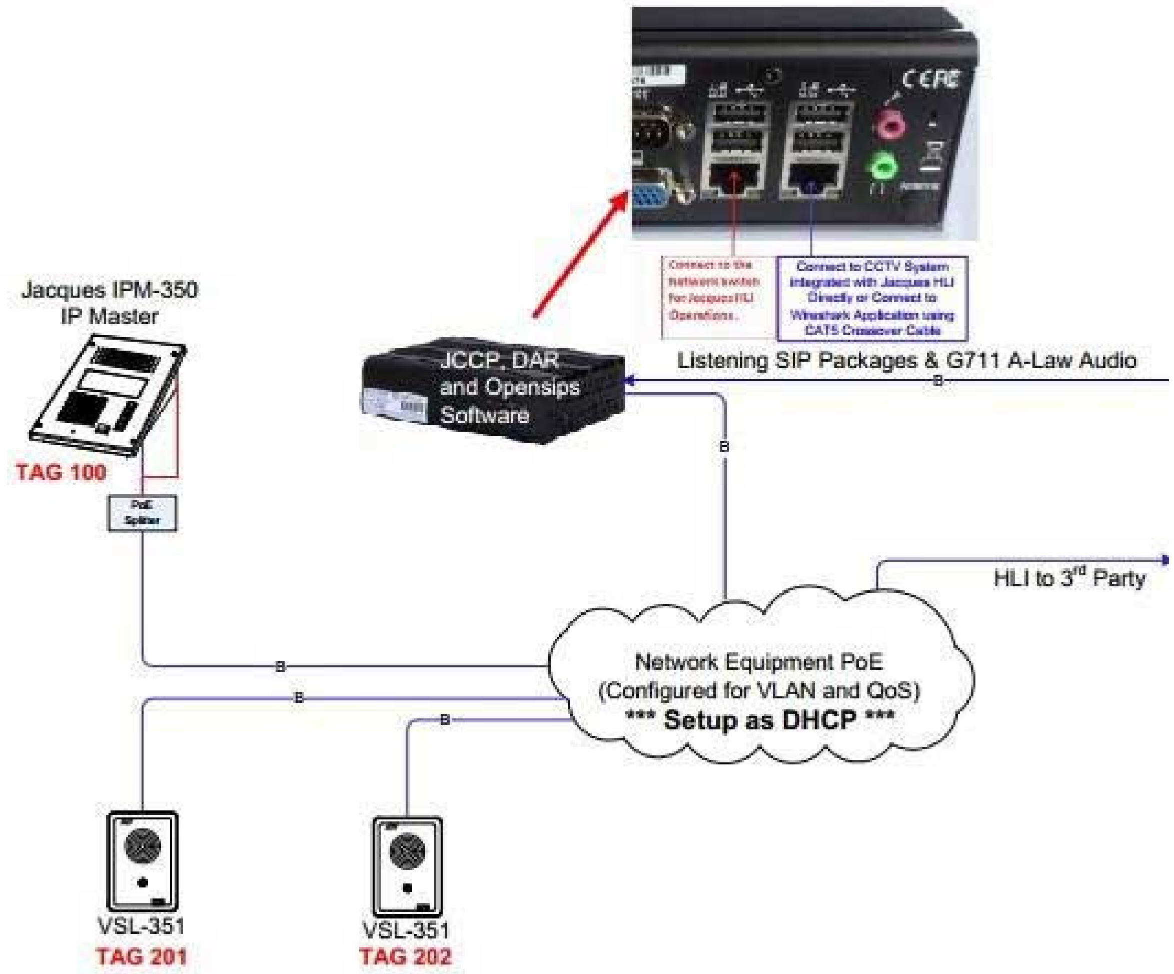
4. Check Viewer status and select as broadcast to all.

5. Check *Remote Control* and enter in Viewer client number.

In fifth property, Viewer client number is the ID of camera which has relation with a slave. For instance, if *6000* ID camera is connected to *202* slave, when *6000* camera is opened, *202* slave will be called.

How to configure Jacques

Slave, master, intercom and HLI must be connected to same switch and that switch will be connected to Ethernet port which is marked with red in the below picture.


Connect to the Network switch for Jacques HLI Operations.
Connect to CCTV System integrated with Jacques HLI Directly or Connect to Wireshark Application using CAT5 Crossover Cable
Listening SIP Packages & G711 A-Law Audio
Jacques IPM-350
IP Master
JCCP, DAR and Opensips Software
TAG 100
PoE Splitter
HLI to 3rd Party
Network Equipment PoE
(Configured for VLAN and QoS)
*** Setup as DHCP ***
B
VSL-351
TAG 201
VSL-351
TAG 202

First, Jacques plugin must be added in G-Link then PC must be added to the SQL Database for interaction with Jacques. The following procedure will outline the smoothest procedure for adding a new device to your system. The first component you need to install is Heidi SQL which will enable you to edit the SQL database of the server.

To enter the Database, please use the following parameters:

- Username : **root**
- Password : **jacques**

And please follow the below steps to set database properties:

1. Find the new intercoms that have been added to the network, but not configured.

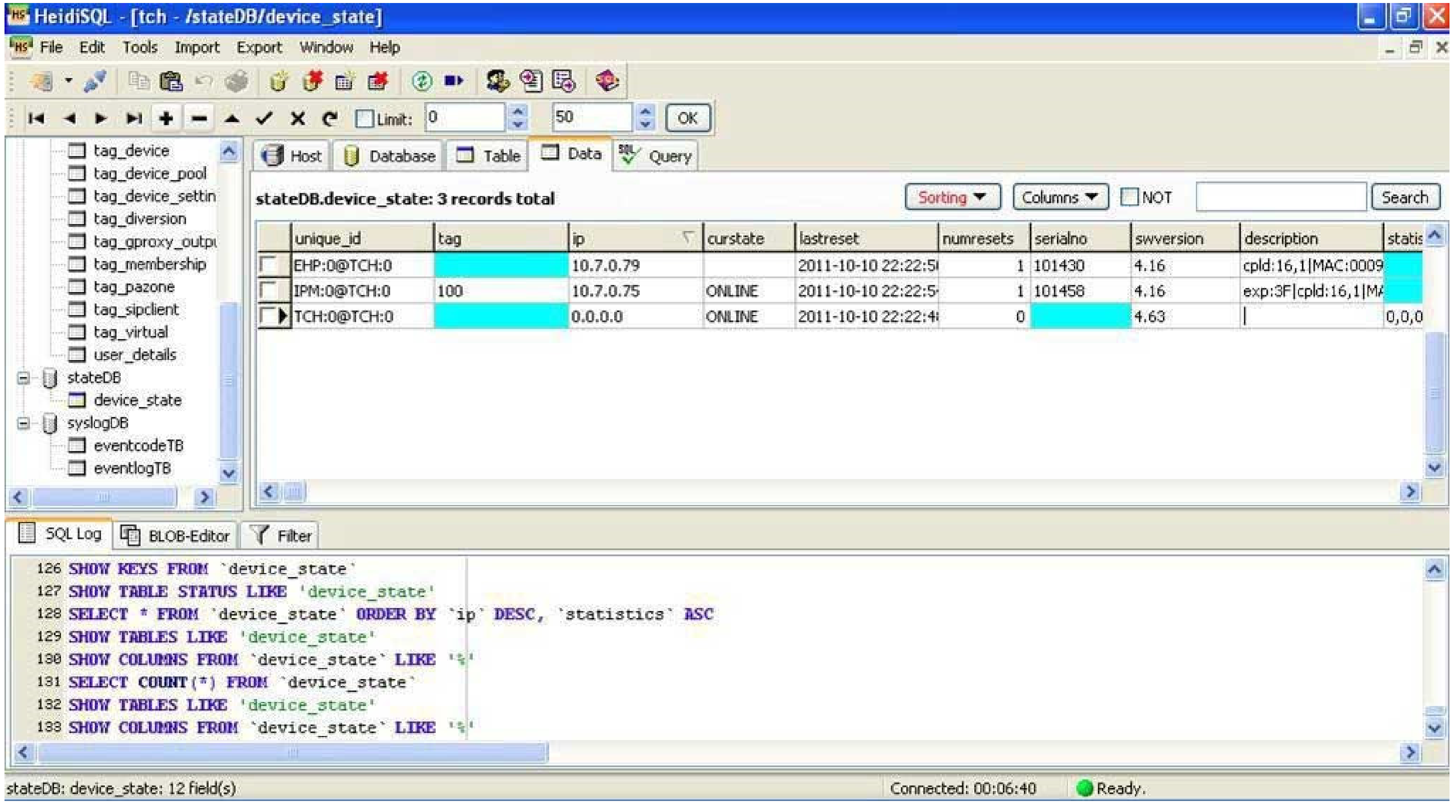
a) Expand the *stateDB* section on the left

b) Select device_state.

c) Choose the *Data* tab in main window list of all the devices on the network will be seen

Unknown Device (EHP@TCH) which has an IP, but is neither online, nor offline.

Any intercoms that you have added to the network without identifying on the server will look like the EHP@TCH device in your listing.



stateDB.device_state: 3 records total

unique_id	tag	ip	curstate	lastreset	numresets	serialno	swversion	description	statis
EHP:0@TCH:0		10.7.0.79		2011-10-10 22:22:5	1	101430	4.16	cpld:16,1|MAC:0009	
IPM:0@TCH:0	100	10.7.0.75	ONLINE	2011-10-10 22:22:5	1	101458	4.16	exp:3F|cpld:16,1|MA	
TCH:0@TCH:0		0.0.0.0	ONLINE	2011-10-10 22:22:4	0		4.63	|	0,0,0

```
SHOW KEYS FROM `device_state`
SHOW TABLE STATUS LIKE 'device_state'
SELECT * FROM `device_state` ORDER BY `ip` DESC, `statistics` ASC
SHOW TABLES LIKE 'device_state'
SHOW COLUMNS FROM `device_state` LIKE '%'
SELECT COUNT(*) FROM `device_state`
SHOW TABLES LIKE 'device_state'
SHOW COLUMNS FROM `device_state` LIKE '%'
```

stateDB: device_state: 12 field(s)

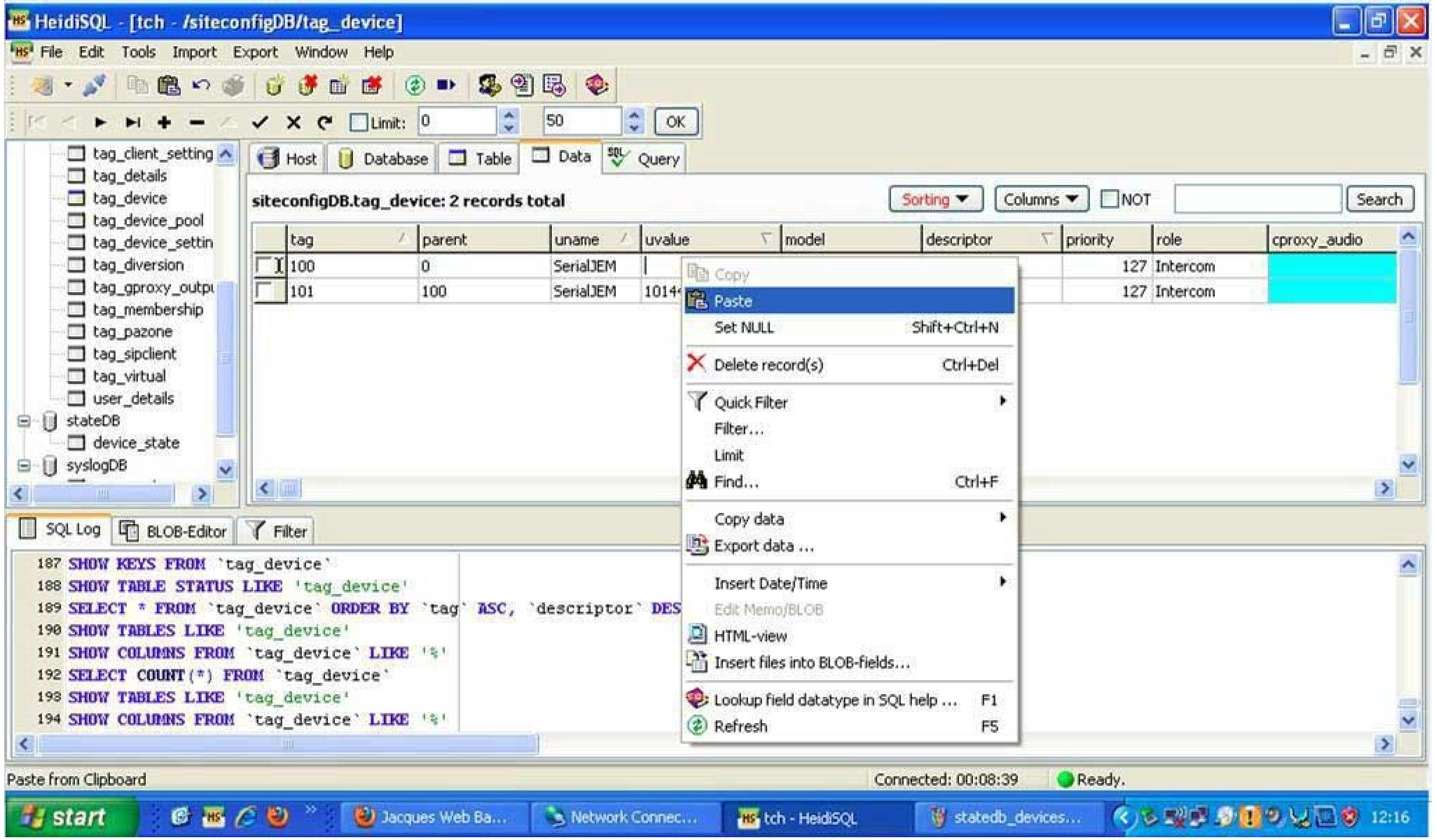
2. The default method which is used to identify intercoms on the network is by using their JEM serial number, which appears in the *serialno* column. The serial number is also labelled on the circuit board of the intercom if you need to check it directly. Choose one of the intercoms (EHPs) that you want to identify first, and copy the serial number from the device state table.

3. Using the menu on the left, navigate to *siteconfigDB*, then *tag_device*. Select the *Data* tab from the main window. Each line represents a different device on the intercom system.

4. Next, you need to create a new line to add the new device. Pressing the plus sign button on one of the menu bars at the top will add a line

5. HLI's tag number must be between 290-299.

6. Slave's tag number must be between 200-289.



siteconfigDB.tag_device: 2 records total

tag	parent	uname	uvalue	model	descriptor	priority	role	cproxy_audio
100	0	SerialJEM	|			127	Intercom	
101	100	SerialJEM	1014			127	Intercom	

```
187 SHOW KEYS FROM `tag_device`
188 SHOW TABLE STATUS LIKE 'tag_device'
189 SELECT * FROM `tag_device` ORDER BY `tag` ASC, `descriptor` DES
190 SHOW TABLES LIKE 'tag_device'
191 SHOW COLUMNS FROM `tag_device` LIKE '%'
192 SELECT COUNT(*) FROM `tag_device`
193 SHOW TABLES LIKE 'tag_device'
194 SHOW COLUMNS FROM `tag_device` LIKE '%'
```

Paste from Clipboard   Connected: 00:08:39   Ready.

7. REPEAT the above process for every device you want to add to the system.

8. So you must have added all the devices you would like to add. Server must be restarted to use change(s). Open ANY internet browser apart from internet explorer which can cause fatal errors – we recommend Mozilla Firefox.

- Type the address 10.7.0.1 into the address bar.
- You will see a login window. Enter the username *root* and the password *jacques*. (All lower case). Left Click *OK*. If this password does not work it may have been reset by the system admin or they may have requested a specific password from Jacques. Please contact your system admin if you think this is the case.
- Navigate to the *Services* tab from the left side menu bar
- Press the restart button for jccpserver. Everything should drop offline for a second or two, then come back with all the changes applied.

Maxxess plugin

When Maxxes API plugin starts, API plugin tries to connect MultiPort until connection is established between API plugin and MultiPort. Moreover, API plugin sends a message for authentication to AXxess API System. If the authentication is successful, the name of the MultiPort sending the status is shown to the screen. Then database communication establishes to take current states of all sensors and doors since states of them are unknown until the first event comes from sensor or door.

According to incoming messages from MultiPort, API plugin transfers the events.

Supported Hardware/Software

Maxxess plugin has been developed and test with Maxxess v4.2 device. And it supports all version after Maxxess v4.2, includes Maxxess v4.2.

Maxxess API Username	is the username that is created while setting up a new a system master / a new administrator / a new operator. The default system master name is "Master".
Maxxess API Password	is the corresponding password system master / a new administrator / a new operator. Enter a password for the system in the password box (3 to 12 alphanumeric characters).
Maxxess DB Username	is the SQL Username and is used for making connection with database. Default SQL Server User is "sa".
Maxxess DB Password	is the SQL User Password and is used for making connection with database. Default SQL Server User is "AXxess".
Maxxess API Ip Address	is the machine Ip address of Maxxess Machine which was loaded.
Maxxess API Port Number	is the machine port address of Maxxess Machine which was loaded.
Event Prefix	parameter is used for determining starting names of Maxxes Events. Please see Event Naming for Maxxess section for details.
Door Forced Event Prefix	parameter is used for indicating the name of Door Forced Maxxess events. Please see Event Naming for Maxxess section for details. Door Forced Events start with states/messages which contain: D2 Door forced C2 Alarm

	Door Forced Events stop with states/messages which contain: C1 Secure
Door Open Event Prefix	parameter is used for indicating the name of Door Opened Maxxess events. Please see Event Naming for Maxxess section for details. Door Open Events start with states/messages which contain: D4 Door Held open Door Open Events stop with states/messages which contain: D9 Door Closed (Held open) D8 Door Closed (Forced)
Controller Lost Event Prefix	parameter is used for indicating the name of the events deal with Communication, Power, Hardware, Panel, Encryption Errors etc. Please see Event Naming for Maxxess section for details. Controller Lost Events start with states/messages which contain: R1 Panel has totally reset R2 Panel has lost power R3 Panel on battery power X2 Communication lost X3 Panel not responding X4 No response+ X5 Hardware error+ X6 Encryption error+ Controller Lost Events stop with states/messages which contain: X1 Communication back R4 Panel on main power
Door Unlock Event Prefix	parameter is used for indicating the name of the events deal with Lock, Unlock. Please see Event Naming for Maxxess section for details. Door Unlock Events start with states/messages which contain: O2 Unlocked O3 Allow access Door Unlock Events stop with states/messages which contain: D1 Door closed O1 Locked O5 Sensor closed

Maxxess Event Naming

All events generated manually by the operator or the barriers are integrated . “Event Prefix”, “Door Forced Event Prefix”, “Door Open Event Prefix”, “Controller Lost Event Prefix”, and “Door Unlock Event Prefix” parameters, gives you the possibility to determine event names. Event names are determined as follows:

“Event Prefix”	The name of the point creating the event	“Door Forced Event Prefix” “Door Open Event Prefix” “Controller Lost Event Prefix” “Door Unlock Event Prefix”	Event Type

MaxxessEvent_SECURITY-PC.R1.10.1_DOOR_FORCED Stopped

MaxxessEvent_SECURITY-PC.R1.10.1_UNLOCKED Started

MaxxessEvent_SECURITY-PC.R1.10.1_DOOR_OPEN Stopped

MaxxessEvent_SECURITY-PC.R1.10.1_OFFLINE Started

Micros plugin

Micros has an Emon (event monitoring) application which is sending information over a TCP Client.

Supported Software/Hardware

Micros plugin enables Micros 8700 and 9700 systems integration. It supports all versions after Micros 8700.

Supported Functionality

G-Link Micros plugin is listening as a TCP server and Micros is connecting as a client.

Since Micros system does not send check number for each transaction, plugin keeps track of each check session on a till. As soon as any of the start check actions notification received from a till, incoming actions are cached until any of the end check actions are received. All actions between these start and end check notifications are assigned same check number.

Start Check Events	End Check Events
Begin Check	Close Check
Adjust Check	Transaction CXL
ReOpen Check	Service Total
PIckUp Check	

To be able to get change due there is a special script running at micros side on CLOSE_CHECK action.

Parameters

PMS Name :

UWS Number :

Server Listen Port: TCP Port on which plugin should be listening

Monitored Events(comma seperated) : This parameter determines which events from Micros is being transferred. By default below events are monitored.

Micros Event
ADJUST_CHECK
BEGIN_CHECK
CLOSE_CHECK

Micros Event
DSC
DSC_VOID
MI
MI_VOID
NO_SALE PICKUP_CHECK
REOPEN_CHECK
SIGN_IN
SIGN_OUT
SRVC_TOTAL
SVC
SVC_VOID
TNDR
TNDR_VOID
TRANS_CNCL

You can see all event names below:

Event	Descripton
ADJUST_CHECK	Check has been dejusted
ALL	Send all events
BEGIN_CHECK	Check has been started
CLOCK_IN	Employee clock in
CLOCK_OUT	Employee clock out
CLOSE_CHECK	Check has been closed
DSC	Discount has been entered

Event	Descripton
DSC_VOID	Discount has been voided
ERR_MSG	An error message
EXT_AUTH	An external authorization has occurred
HRD_ERR	Error condition
MGR_PROC	A manager procedure has been run
MI	Menu item has been entered
MI_RET	Menu item has been returned
MI_VOID	Menu item has been voided
NO_SALE	No sale
PICKUP_CHECK	Check has been picked up
PICKUP_LOAN	Pickup loan
REOPEN_CHECK	Check has been reopened
RPT_GEN	A report has been generated
SFT_ERR	Error condition
SIGN_IN	Employee sign in
SIGN_OUT	Employee sign out
SRVC_TOTAL	Check has been service totalled
SVC	Service charge has been entered
SVC_VOID	Service charge has been voided
SYS_AUTH	A system authorization has occurred
TNDR	Tender has been entered
TNDR_VOID	Tender has been voided
TRANS_CNCL	Transaction cancel
WS_DOWN	Workstation down
WS_UP	Workstation up

Protege plugin

Protege plugin is an input plugin which is designed to take events from Protege GX Access Control. The plugin works by using a Protege‟s Soap Service. Protegeplugin requests SOAP service periodically if there any new events. If there are new events, it starts a new alarm.

Supported Software/Hardware

Protegé plugin has been developed and tested using Protege GX DIN Rail System Controller (SDK 1.0.0.7).

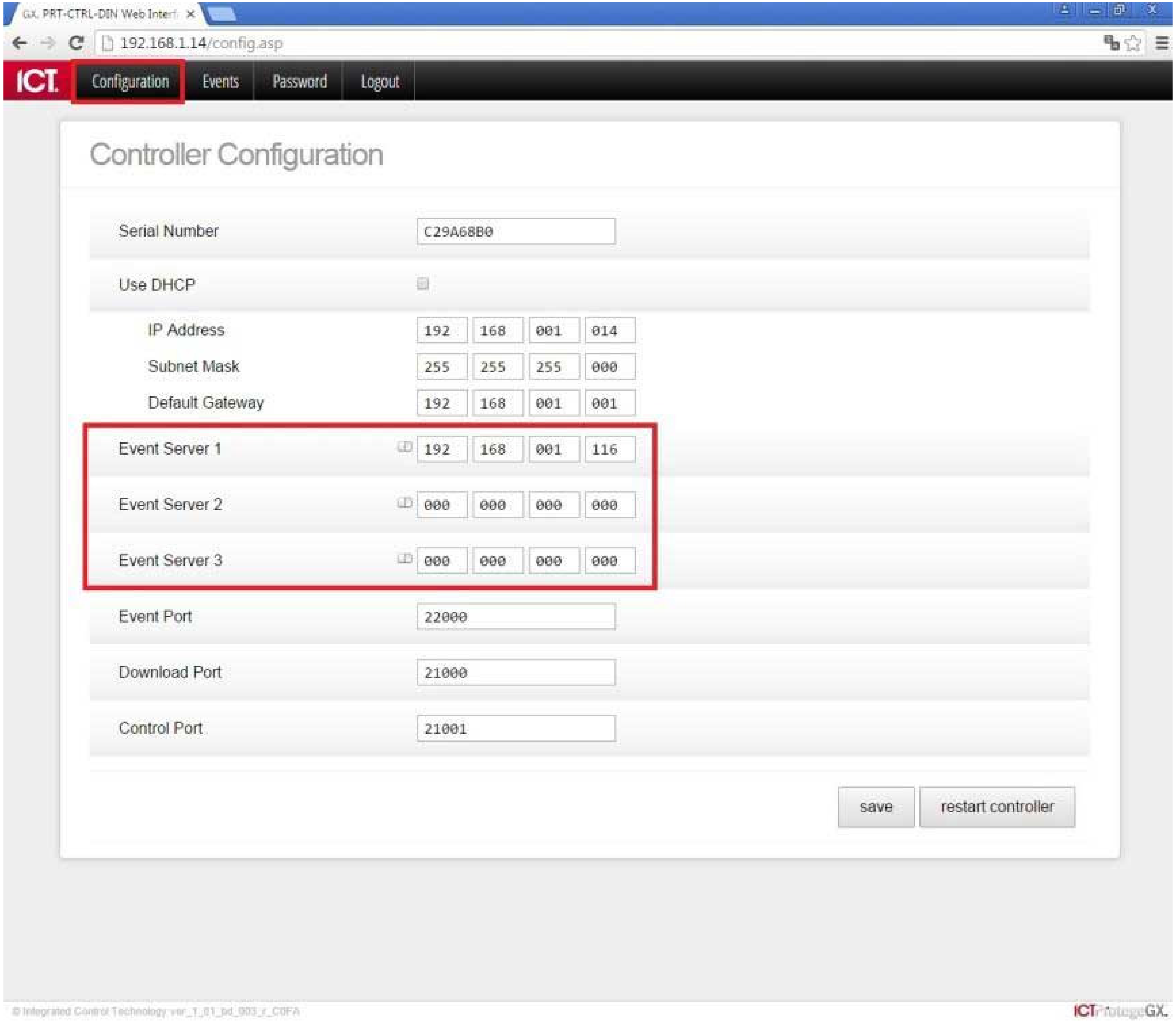
How To Configure Protege

The event server of *Protege GX Access Control Device* must be the same IP address of the machine, which has *Protege GX Soap Service* running. First open *Protege GX Web Interface of Protege GX Access Control Device*, by entering the IP address to a web browser. The *Protege GX Access Control Device* main page will be loaded. Please login by using following credentials:

- Default Username : **admin**
- Default Password : **admin**

On top of the Protege webpage are located some settings parameters.

Please click *Configuration*, change the IP address of the *Event Server* to one on which *Protege Soap Service* is running. Click *Save* and restart controller to apply your changes.

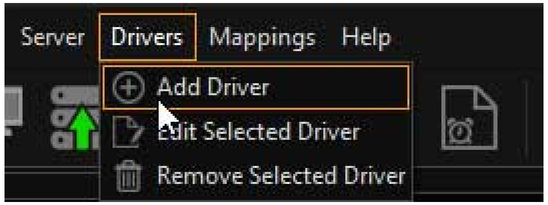


Controller Configuration

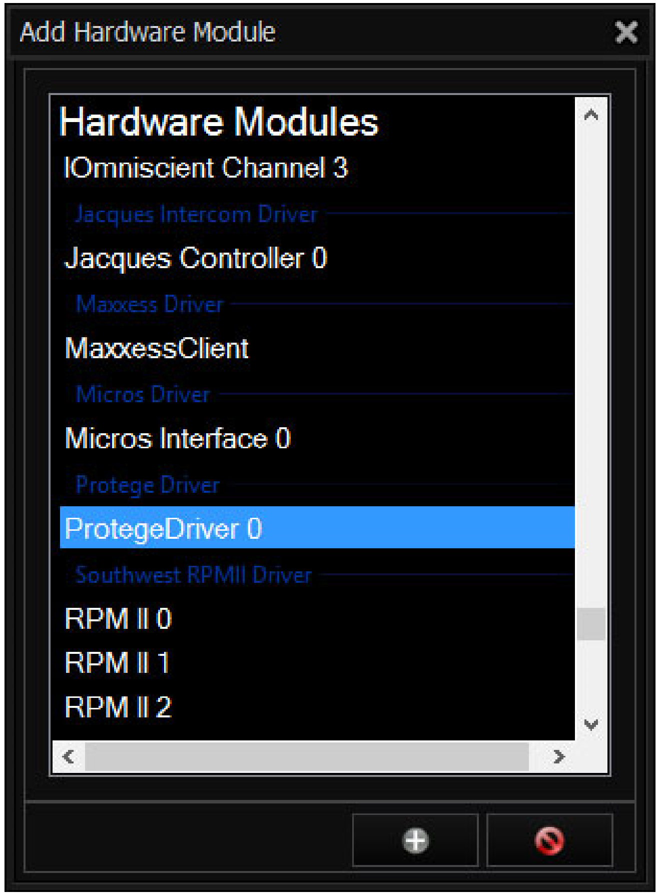
Serial Number	C29A68B0
Use DHCP	□
IP Address	192 . 168 . 001 . 014
Subnet Mask	255 . 255 . 255 . 000
Default Gateway	192 . 168 . 001 . 001
Event Server 1	192 . 168 . 001 . 116
Event Server 2	000 . 000 . 000 . 000
Event Server 3	000 . 000 . 000 . 000
Event Port	22000
Download Port	21000
Control Port	21001

How to configure plugin

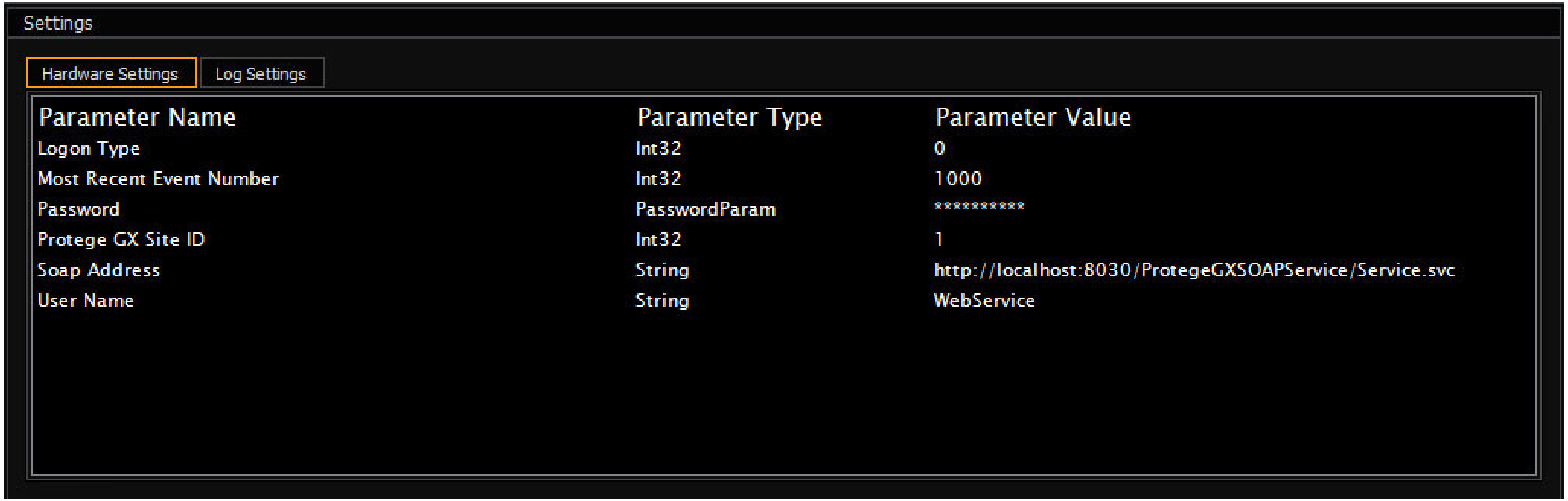
To configure Protege plugin into G-Link, please follow steps below.



Click Add plugin.



Click on + to add Protege plugin.



Parameter Name	Parameter Type	Parameter Value
Logon Type	Int32	0
Most Recent Event Number	Int32	1000
Password	PasswordParam	**********
Protege GX Site ID	Int32	1
Soap Address	String	http://localhost:8030/ProtegeGXSOAPService/Service.svc
User Name	String	WebService

Set Parameters:

Logon Type	1- if the password is plain text 2- if the password is hashed (password need to be MD5 hash with base64 string)
Protege GX Site ID	The site ID from Protege GX
Most Recent Event Number	Getting number of events on SOAP request. Interval of 100 to 1000 is ideal for this parameter
Soap Address	Address of the Protege GX SOAP Service which is running on a machine, where Protege GX Software is running. Please note: this is not the IP address of the Protege GX Access Control device unit.
User Name	Valid operator name in Protege GX (Default: WebService)
Password	Valid operator password in Protege GX (Default: WebService)

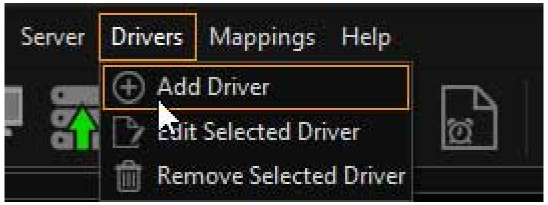
Set the valid parameters and then click button *Send Setup To Server*.

Southwest plugin

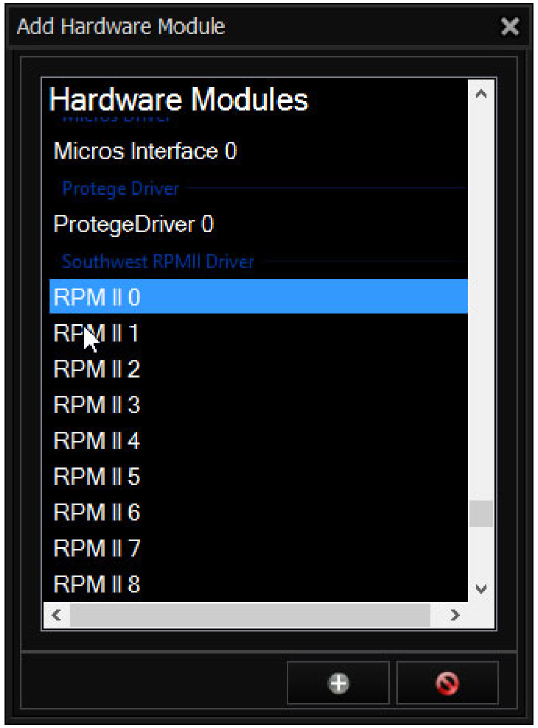
Southwest is a perimeter security system provided by Universal INTREPID System Controllers. Southwest is conceived to protect the external perimeter of a facility.

Southwest plugin Configuration for G-Link

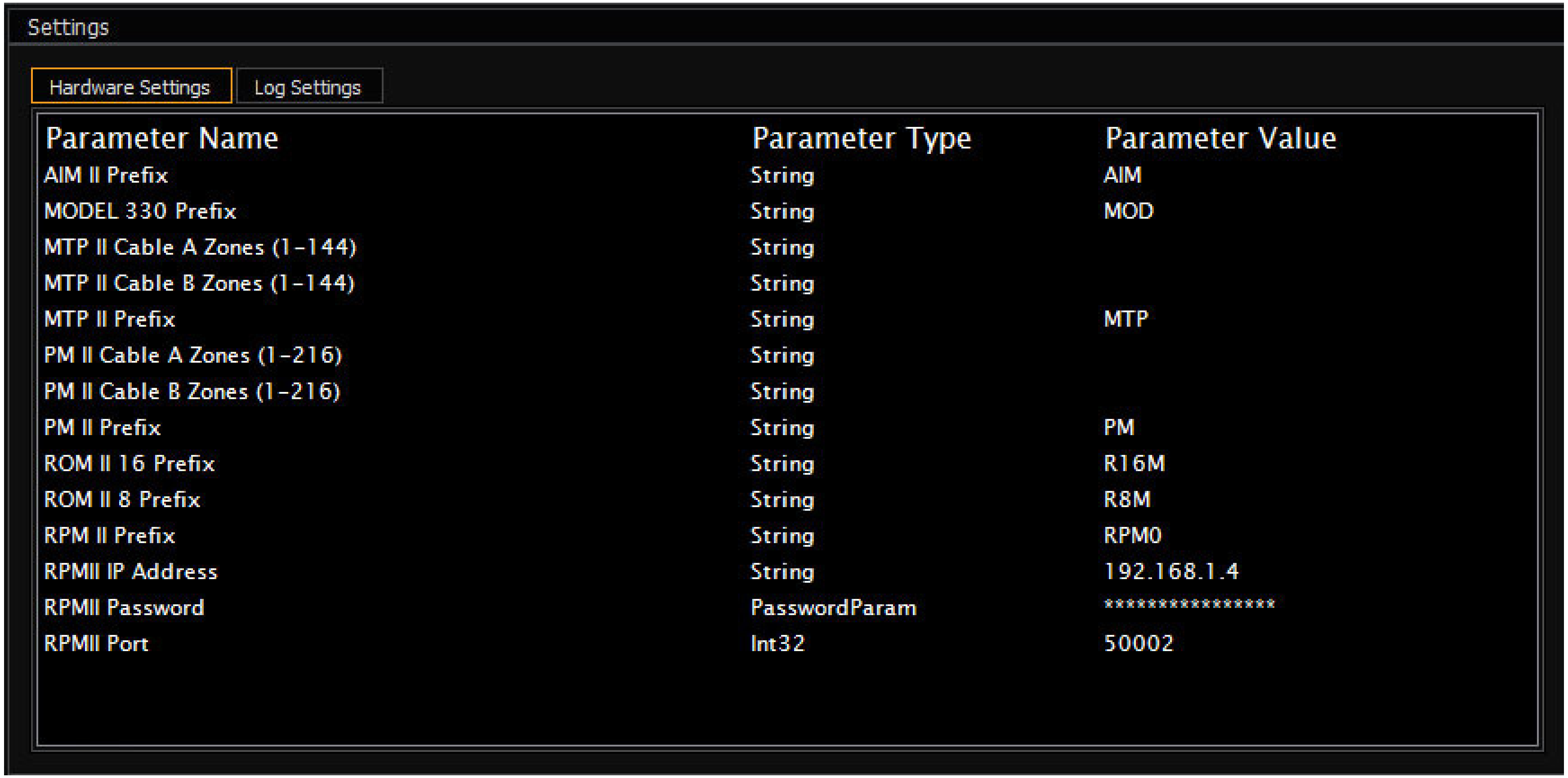
To configure Southwest plugin into NDIS, please follow steps below.



Click Add plugin.



Click on + to add Southwest plugin.



Parameter Name	Parameter Type	Parameter Value
AIM II Prefix	String	AIM
MODEL 330 Prefix	String	MOD
MTP II Cable A Zones (1-144)	String	
MTP II Cable B Zones (1-144)	String	
MTP II Prefix	String	MTP
PM II Cable A Zones (1-216)	String	
PM II Cable B Zones (1-216)	String	
PM II Prefix	String	PM
ROM II 16 Prefix	String	R16M
ROM II 8 Prefix	String	R8M
RPM II Prefix	String	RPM0
RPMII IP Address	String	192.168.1.4
RPMII Password	PasswordParam	****************
RPMII Port	Int32	50002

Channel Parameters	
RPMII Port	TCP port which is used to connect to Southwest RPM II. Default value = 50002
RPMII IP Address	IP address which is used to connect to Southwest RPM II, it MUST be set. Default value = "192.168.1.4"
RPMII Password	Password which is used to login to Southwest RPM II. Default value = "0000000000000000"
RPM II Prefix	Explanatory name for RPM II, for InterfaceID this given name is used. Default value = "RPM" + ChannelNo Helpful name for PM II type of devices. In addition to "Device No" [1-239], we can be notified with this configurable device name for PMII.

Channel Parameters	
	In the notification, "Device Prefix" and "Device No" is used together, by this way alarm place can be easily differentiate. Default value = "PM"
AIM II Prefix	Helpful name for AIM II type of devices. In addition to "Device No" [1-239], we can be notified with this configurable device name for AIMII. In the notification, "Device Prefix" and "Device No" is used together, by this way alarm place can be easily differentiate. Default value = "AIM"
MODEL 330 Prefix	Helpful name for MODEL 330 type of devices. In addition to "Device No" [1-239], we can be notified with this configurable device name for MODEL 330. In the notification, "Device Prefix" and "Device No" is used together, by this way alarm place can be easily differentiate. Default value = "MOD"
MTP II Prefix	Helpful name for MTP II type of devices. In addition to "Device No" [1-239], we can be notified with this configurable device name for MTPII. In the notification, "Device Prefix" and "Device No" is used together, by this way alarm place can be easily differentiate. Default value = "MTP"
ROM II 16 Prefix	Helpful name for ROM II 16 type of devices. In addition to "Device No" [1-239], we can be notified with this configurable device name for ROMII16. In the notification, "Device Prefix" and "Device No" is used together, by this way alarm place can be easily differentiate. Default value = "R16M"
ROM II 8 Prefix	Helpful name for ROM II 8 type of devices. In addition to "Device No" [1-239], we can be notified with this configurable device name for ROMII8. In the notification, "Device Prefix" and "Device No" is used together, by this way alarm place can be easily differentiate. Default value = "R8M"
MTP II Cable A Zones (1-144)	Zone configuration for MTP II device‟s Cable A subcells. Beginning of subcells starts with 1 and ends with 144. Others are omitted. In the notification, "Zone1" – "Zone2" .. is used in PPZoneAlarm action. Default value = "" (empty) Example Setting: "1-25, 26-30, 30-31, 144". 4 zones are created. Zone1 contains subcells in range 1-25 (both are included), Zone2 contains subcells in range 26-30 (both are included), Zone3 contains subcells in range 30-31 (both are included) and Zone4 only contains 144. When other alarm occurs in other subcells not specified in this setting (i.e. 32, 33, 34 …) can be only taken as CustomActionEx. *All zones are comma seperated and each zone can be single number (144) or range of numbers (begin-end (1-25)).*
MTP II Cable B Zones (1-144)	Zone configuration for MTP II device‟s Cable B subcells. Beginning of subcells starts with 1 and ends with 144. Others are omitted.

Channel Parameters	
	In the notification, "Zone1" – "Zone2" .. is used in PPZoneAlarm action. Default value = "" (empty). Value settings are similar to MTP II Cable A Zones
PM II Cable A Zones (1-216)	Zone configuration for PM II device‟s Cable A subcells. Beginning of subcells starts with 1 and ends with 216. Others are omitted. In the notification, "Zone1" – "Zone2" .. is used in PPZoneAlarm action. Default value = "" (empty) Value settings are similar to MTP II Cable A Zones
PM II Cable B Zones (1-216)	Zone configuration for PM II device‟s Cable B subcells. Beginning of subcells starts with 1 and ends with 216. Others are omitted. In the notification, "Zone1" – "Zone2" .. is used in PPZoneAlarm action. Default value = "" (empty). Value settings are similar to MTP II Cable A Zones

Set the valid parameters and then click button *Send Setup To Server*.

Plugin's actions for GCore

Plugin's actions for GCore	
PPInterfaceOnline Action	If this action is taken, then it means that for the given InterfaceID, Southwest RPM II is connected and online. InterfaceID = Channel Parameter Value of "RPM II Prefix"
PPInterfaceOffline Action	If this action is taken, then it means that for the given InterfaceID, Southwest RPM II is disconnected and offline/not reachable. InterfaceID = Channel Parameter Value of "RPM II Prefix"

PPDeviceOnline Action	If this action is taken, then it means that for the given InterfaceID & DeviceID, device with the given deviceID is online now.
	InterfaceID = Channel Parameter Value of "RPM II Prefix"
	DeviceAddress = Device Address No [1-239]

PPDeviceOffline Action	If this action is taken, then it means that for the given InterfaceID & DeviceID, device with the given deviceID is offline/not reachable now.
	InterfaceID = Channel Parameter Value of "RPM II Prefix"
	DeviceAddress = Device Address No [1-239]

CustomActionEx Action	This action is taken if ONLY CHANGE in the device alarm states. (NORMAL or ALARM) If the device was in NORMAL state and alarm is on, then Action with ALARM state is taken.

Plugin's actions for GCore	

	If the device was in ALARM state and alarm is off, then Action with NORMAL state is taken.
	StringFieldA = Channel Parameter Value of "RPM II Prefix"
	StringFieldB = Device type prefix (helpful name of the device)
	Int32FieldA = Device Address No [1-239] (for RPMII 0 is send)
	StringFieldC = Sensor kind (listed below)
	Int32FieldB = Corresponds to the input/sub unit no of the the device and sensor kind, in which alarm is occured. (for sensors which do not have sub unit no, 0 is send)
	StringFieldD = "NORMAL" or "ALARM"

PPZoneAlarm Action	Subcells are combined and grouped together as zones. If PPZoneAlarm Action is taken, then it means that for the given range, some of the subcell states are changed. If one of the subcell alarm is raised then corresponding zone alarm action is also raised. If all of the subcell alarms are off, then zone alarm is turned off as well. InterfaceID = Channel Parameter Value of "RPM II Prefix" DeviceAddress(numeric) = Device Address No [1-239] ZoneID(alpha-numeric) = Depends on the parameter setting Zone+Number(starts from 1 and increases one by one). (i.e. Zone1, Zone2 …) Cable(numeric) = 0 for CableA, 1 for CableB (always set) Subcell(numeric) = optional parameter not used State(numeric) = 1 for ALARM, 0 for NORMAL

Plugin's actions for GeviScope

Plugin's actions for GeviScope	
PPInterfaceOnline Action - The same as in GCore	If this action is taken, then it means that for the given InterfaceID, Southwest RPM II is connected and online. InterfaceID = Channel Parameter Value of "RPM II Prefix"
PPInterfaceOffline Action - The same as in GCore	If this action is taken, then it means that for the given InterfaceID, Southwest RPM II is disconnected and offline/not reachable. InterfaceID = Channel Parameter Value of "RPM II Prefix"
PPDeviceOnline Action - The same as in GCore	Description = If this action is taken, then it means that for the given InterfaceID & DeviceID, device with the given deviceID is online now.

Plugin's actions for GeviScope	

	InterfaceID = Channel Parameter Value of "RPM II Prefix"
	DeviceAddress = Device Address No [1-239]

PPDeviceOffline Action - The same as in Gcore	If this action is taken, then it means that for the given InterfaceID & DeviceID, device with the given deviceID is offline/not reachable now.
	InterfaceID = Channel Parameter Value of "RPM II Prefix"
	DeviceAddress = Device Address No [1-239]

CustomAction Action	This action is taken if ONLY CHANGE in the device alarm states. (NORMAL or ALARM) If the device was in NORMAL state and alarm is on, then Action with ALARM state is taken. If the device was in ALARM state and alarm is off, then Action with NORMAL state is taken. StringField = [Channel Parameter Value of "RPM II Prefix"] + "_" + [Device type prefix (helpful name of the device) and (if >= 0) Device Address No [1-239]] + "_" + [Sensor kind (listed below) + (if >= 0) Corresponds to the input/sub unit no of the the device and sensor kind, in which alarm is occured. (for sensors which do not have sub unit no, 0 is send)] + "_" + ["NORMAL" or "ALARM"]
PPZoneAlarm Action	Subcells are combined and grouped together as zones. If PPZoneAlarm Action is taken, then it means that for the given range, some of the subcell states are changed. If one of the subcell alarm is raised then corresponding zone alarm action is also raised. If all of the subcell alarms are off, then zone alarm is turned off as well. InterfaceID = Channel Parameter Value of "RPM II Prefix" DeviceAddress(numeric) = Device Address No [1-239] ZoneID(alpha-numeric) = Depends on the parameter setting Zone+Number(starts from 1 and increases one by one). (i.e. Zone1, Zone2 …) Cable(numeric) = 0 for CableA, 1 for CableB (always set) Subcell(numeric) = optional parameter not used State(numeric) = 1 for ALARM, 0 for NORMAL

Sensor Kinds

- Tamper
- LowInVolt (LowInputVoltage)
- LineBreak
- DeviceCompromised
- CommFailure (CommunicationFailure)
- CableA
- CableB
- AuxInput (AuxiliaryInput)
- CableAFault
- CableBFault
- EncTamper (EnclosureTamper)
- Service
- AlarmInput
- LineStatus
- Microwave
- AlignPath
- RelayStatus

Cable Kinds

- Cable A
- Cable B

Redundancy

You can have application level redundancy with G-Link.

> NOTICE Please note that redundant software needs same licenses as main software to be fully operational.

Main and redundant computers must be reachable to each other over network.

After finishing configuration of main server please connect to redundant server and from *Server* menu select *Server Working Mode* as *Redundant Mode*. After selecting *Redundant Mode* please enter main server's IP address and send this setup to server. Main and redundant servers are synchronized automatically. In other words, configuration of main server is taken automatically by redundant server. And as soon as any of the configurations changed on main server, redundant server is taking these changes automatically. So you do not need to worry about synchronization of two servers.

Known Issues

- For version 1.0.9.530 and earlier:
  Open Configuration Client and navigate under menu *Server – Database Settings* :
  Add new parameter `SyncNotification=true;` and send changes to server.

- For version 1.0.9.530 or later:
  Quick Viewer at Configuration Client should be used after all changes are sent to server. So prior to opening it please click on *Send to Server* button to commit your configuration changes to server.

- In case of WCF Timeout (database command took longer than expected), please log off from Client and login again to continue working without any problems.

How to change port of G-Link Web Server?

G-Link Web Server requires HTTP SSL Port 443. In case of problem of log in to any G-Link client, please verify that port 443 is free. Regarding to port usage of 443, it has to be changed for G-Link.

To change port of G-Link Web Server on a full installed G-Link version, please follow these steps:

1. Please stop services of G-Link:

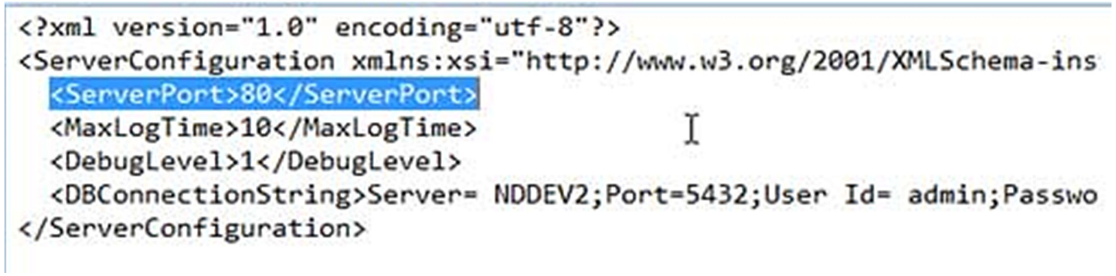
Geutebrück G-Link Server

G-Link Web Server

2. Change port of G-Link Web Server.

G-Link Web Server Configuration file is located under

`C:\ProgramData\Nanodems\NDIS\G-LinkWebServerConf.xml`



```
<?xml version="1.0" encoding="utf-8"?>
<ServerConfiguration xmlns:xsi="http://www.w3.org/2001/XMLSchema-ins
  <ServerPort>80</ServerPort>
  <MaxLogTime>10</MaxLogTime>
  <DebugLevel>1</DebugLevel>
  <DBConnectionString>Server= NDDEV2;Port=5432;User Id= admin;Passwo
</ServerConfiguration>
```

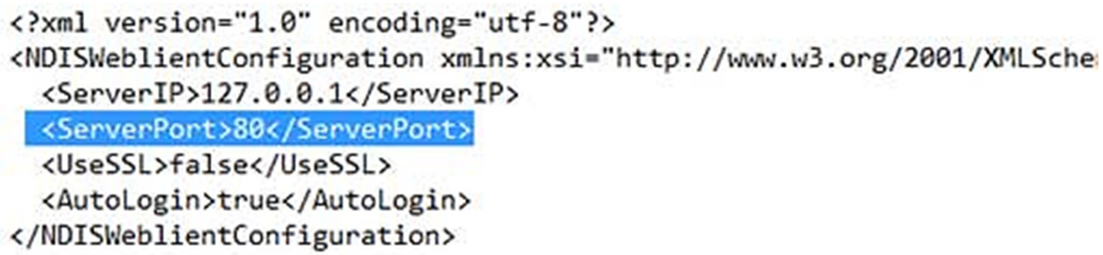
3. Change *ServerPort* to a free port number and save file.

> NOTICE Please verify that the new port is not used by another process.

4. Start services again.

5. Now you have to change client's configuration. Please open configuration file of G-Link Configuration Client/Operator Console:

`C:\Program Files\Geutebrueck\Geutebrueck G-Link Server\NDISWebClientConf.xml`



```
<?xml version="1.0" encoding="utf-8"?>
<NDISWeblientConfiguration xmlns:xsi="http://www.w3.org/2001/XMLSche
  <ServerIP>127.0.0.1</ServerIP>
  <ServerPort>80</ServerPort>
  <UseSSL>false</UseSSL>
  <AutoLogin>true</AutoLogin>
</NDISWeblientConfiguration>
```

6. Please set exactly same port number for *ServerPort*, which you have changed for G-Link Web Server configuration. Save configuration file, start your client and log in.

> NOTICE Machines, where just one of the G-Link Clients is installed, follow step 5 and step 6.

Plugin Overview

Plugin Name	Products	Supported Software/Hardware	Description	Functionality	Plugin Type*
Maxess	Maxess	Maxxess Access Platform v 4.2 or later	Event transfer of access management system.	Door Forced Door Open Controller Lost Door Unlock Locked Sensor Closed	Input plugin
FCWnx	FCWnx	Fcwnx Access Commander 7.5.1 or later	Event and alarm transfer of facility commander access control and management system.	Camera Video Loss Video Device Disk Full	Bidirectional plugin
Fibersensys APU	FD3xx-IP FD500D-IP	FD3xx-IP FD500D-IP	Transfer of fiberoptic alarms which is created by FiberSensys system.	Intrusion or alarm Fault (broken fiber or hardware malfunction) Tamper (a switch which indicates whether the device has been opened).	Bidirectional plugin
CIAS IB Server	Ermo 482X Pro Ermo 482 Coral Manta Ermusa Minermo Darwin Darwin DT Newton2 Newton Plus Alfa	Up to 32 IBServers. Each IBServer supports up to 128 (from 0 to 127) IBDevices.	Transfer perimeter alarm and events which are generated by IBServers.	PREALARM ALARM TAMPER FAULT NO_ANSWER.	Input plugin

Plugin Name	Products	Supported Software/Hardware	Description	Functionality	Plugin Type*
	Murena ISC Cable				
IOmniscient	IQSeries 4.0	IQSeries 4.0 or later	Transfer alarms when object detected or invalid object is identificated on camera	Object Detection Crowd Management Alarm Abandonend Object Over Crowed	Input plugin
Gcore	All versions	All versions	Bidirectional event transfer with Gcore Server and 3rd party systems.	Receives: OnEventStartedEx, OnEventStopped, OnCustomAction, OnDigitalInput, OnDigitalOutput, OnCameraOn, OnCameraOff, OnSensorVideoAlarm, OnSensorAlarmFinished Accepts: ACSAccessGranted, ACSRawdata, GamingMachine, PPZoneAlarm, PPDeviceAlarm, PPDeviceOffline, PPDeviceOnline, PPInterfaceOffline, LiveCheck, NPRRecognition, CustomActionEx	Bidirectional plugin
GSC	All versions	All versions	Bidirectional event transfer with GSC Server and 3rd party systems.	Receives: OnEventStartedEx, OnEventStopped, OnCustomAction, OnDigitalInput, OnDigitalOutput, OnCameraOn, OnCameraOff, OnSensorVideoAlarm, OnSensorAlarmFinished, OnViewerConnected, OnViewerCleared Accepts: ACSAccessGranted, ACSRawdata, ACSAccessDenied, GamingMachine, DrawBoundingBox, ClearBoundingBox,	Bidirectional plugin

Plugin Name	Products	Supported Software/Hardware	Description	Functionality	Plugin Type*
				PPZoneAlarm, PPDeviceAlarm, PPDeviceOffline, PPDeviceOnline, PPInterfaceOffline, LiveCheck, NPRRecognition, CustomActionEx	
GeViSoft	GeViSoft 1.3.1.71 and later	All versions	Bidirectional event transfer with GevİSoft Server and 3rd party systems.	All events	Bidirectional plugin
Inner Range Insight	Insight Professional	Insight Professional version 5.1 (12437) or later	Event/alarm transfer and video integration.	Alarm management Access management	Output plugin
Hikvision Central	DVR/NVR	All versions	Hikvision Central plugin enables users to receive real time notifications from Hikvision DVR/NVR and other devices.	Hard disk full Sensor Alarm Video Lost Video Motion Alarm Hard disk unformatted Hard disk error Tampering detection Unmatched video output standard Illegal operation Video signal abnormal Record abnormal	Input plugin
Dedicated Micros	Dedicated Micros DV-IP RT	All versions of DV-IP RT	Pushing notifications to Dedicated Micros DV-IP RT systems as alarm inputs.is supported.	Video Motion Detection	Output plugin
Jacques	Controller: TCH-2MXH | 51660 Master : IPM-350 | 51516 Intercom :	IPM-360 | 51516, IPM-360H | 51533, IPM-360G | 51534, IPM-360GH | 51535	Jacques is a communication system featuring video and audio intercom.	Start Call End Call	Input plugin

Plugin Name	Products	Supported Software/Hardware	Description	Functionality	Plugin Type*
	VSL-361W+ | 51676				
Cardax	Gallagher Access Control	Version from 7.10 to 7.40.	Event transfer of access control and ANPR system.	ANPR Events	Bidirectional plugin
Protege	Protege GX DIN Rail System Controller	ProtegeGX DIN RAIL Single Door Controller	Event and alarm transfer of access management system.	All access management events	Input plugin
Micros Server	Micros 8700 and 9700	Micros 8700 or later	Transfer POS events which are generated by Micros POS device.	ADJUST_CHECK ALL BEGIN_CHECK LOCK_IN CLOCK_OUT CLOSE_CHECK DSC DSC_VOID ERR_MSG EXT_AUTH HRD_ERR MGR_PROC MI MI_RET MI_VOID NO_SALE PICKUP_CHECK PICKUP_LOAN REOPEN_CHECK RPT_GEN SFT_ERR SIGN_IN SIGN_OUT SRVC_TOTAL SVC SVC_VOID SYS_AUTH TNDR TNDR_VOID	Input plugin

Plugin Name	Products	Supported Software/Hardware	Description	Functionality	Plugin Type*
				TRANS_CNCL WS_DOWN WS_UP	
IGT Server	DACOM Paging Interface	All versions	Event transfer of Gaming Machine.	No Data Received For Long Time Event Period (seconds) To Raise No Data Event	Input plugin
Southwest	INTREPID™ MicroPoint™ I or later	RPMII	Southwest is a perimeter security system provided by Universal INTREPID System Controllers. Southwest is conceived to protect the external perimeter of a facility.	Tamper LowInVolt (LowInputVoltage) LineBreak DeviceCompromised CommFailure (CommunicationFailure) CableA CableB AuxInput (AuxiliaryInput) CableAFault CableBFault EncTamper (EnclosureTamper) Service AlarmInput LineStatus Microwave AlignPath RelayStatus	Input plugin
Cyviz Display Controller	All Versions	All Versions	The plugin will receive CustomActions and translate this to commands for the Cyviz Display Controller send with Telnet.	Load Preset	Output plugin

* Input plugin: Only sends events. Output plugin: Only receives events.

** Not a plugin

Other names and brands may be claimed as the property of others.

G-Link_BA_EN 21.12.2016

GEUTEBRÜCK
Excellence in Video Security

GEUTEBRÜCK GmbH
Im Nassen 7-9 | D-53578 Windhagen
Tel. +49 (0)2645 137-0 | Fax-999
info@geutebrueck.com

www.geutebrueck.com

Technische Änderungen vorbehalten.

Technical alterations reserved.

Sous réserve des modifications.

Suministro sujeto a modificaciones técnicas o disponibilidad.