



SGSE

Soluciones Globales de Seguridad Electrónica

MONITOR GALAXY

Installation and user manual

Contenido

2.	Introduction.....	3
3.	Requirements	4
4.	Arquitecture	5
5.	Installation.....	7
	Installation of SGSE Avigilon Integration Service.....	7
	Installation of Floor Plan Service	11
6.	Configuration.....	18
	6.1 Galaxy configuration	18
	6.1.1 Ethernet module.....	18
	6.1.2 Serial to Ethernet converter	19
	6.2 Configuration of SGSE Avigilon Integration Service.....	21
	6.3 Configuration of the "Floor Plan" web service	26
7.	Operation	27
	Operation on the Avigilon platform	27
	Operation with the Floor Plan Manager	28
	User Profile.....	29
	Navigation Buttons	30
	Sidebar.....	31
	Within the Floor Plan.....	31
	Administrator profile.....	33
	Sidebar.....	33
	Editing Mode	34
8.	Troubleshooting	37
	Additional Information	37

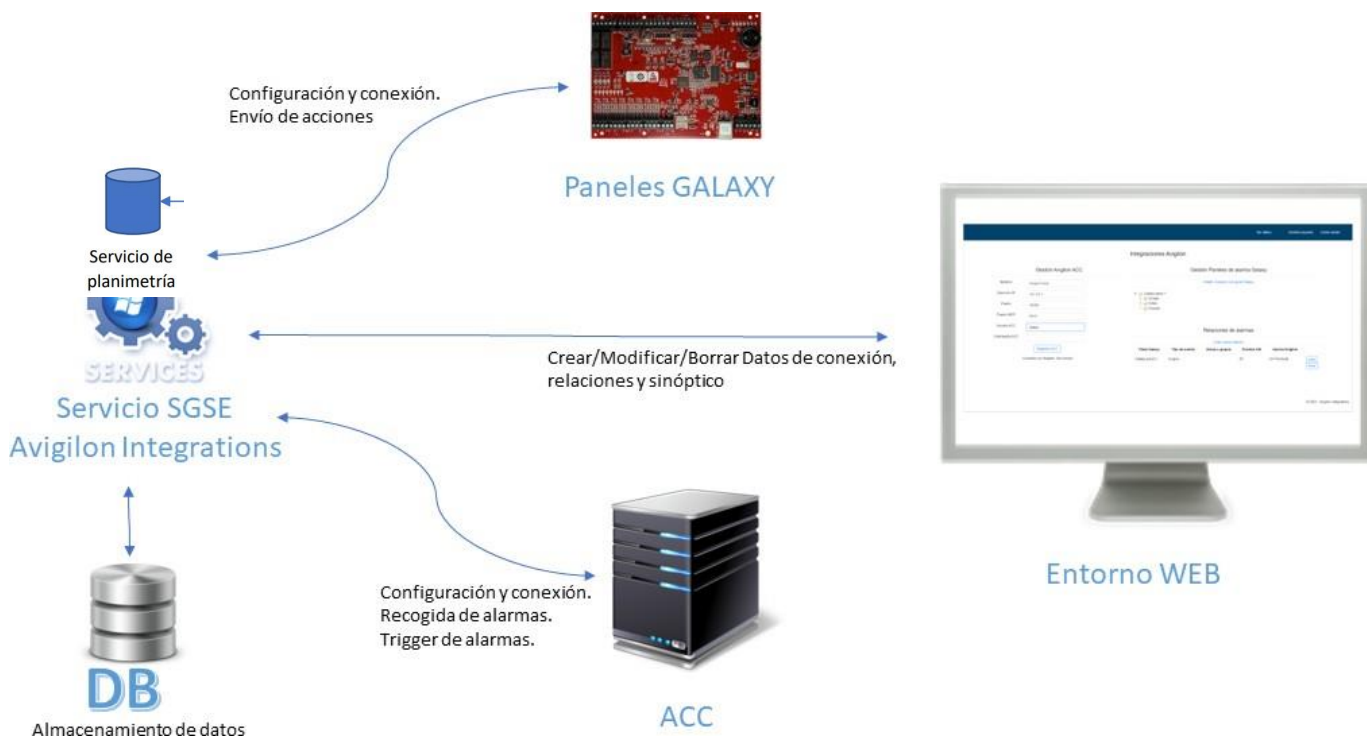
1. Document versions

Version	Date	Author	Version description
1.0	09/2023	JAFUNES	First document version

2. Introduction

Galaxy Monitor is an application that enables seamless integration of Galaxy intrusion panels, in any of their models, as part of the Avigilon Unity platform. This integration allows the establishment of connections between alarms generated in Avigilon and events triggered by Galaxy intrusion panels.

Moreover, the Galaxy Monitor is interactive, facilitating the execution of actions on partitions, zones, and outputs configured in different Galaxy panels through a synoptic panel. This panel also aids in real-time monitoring of the panel status. The solution is complemented by a web service that allows graphical representation of various integrated devices on one or multiple floor plans, along with their statuses, enabling user interaction with them.



3. Requirements

The following outlines the resources required for the application.

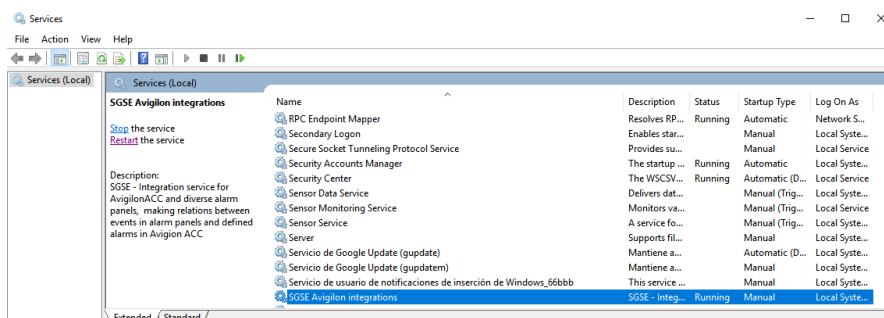
Resources	Description
License	License per Panel and Number of Elements
CPU	Minimum i3 1 Core or similiar
Operation system	Minimum Windows 10
Storage	Minimum 300MB
RAM	Minimum 8Gb
ACC Version	ACC7 or higher
SQL	SQL 2019 or higher

4. Architecture

The application is presented in two distinct environments:

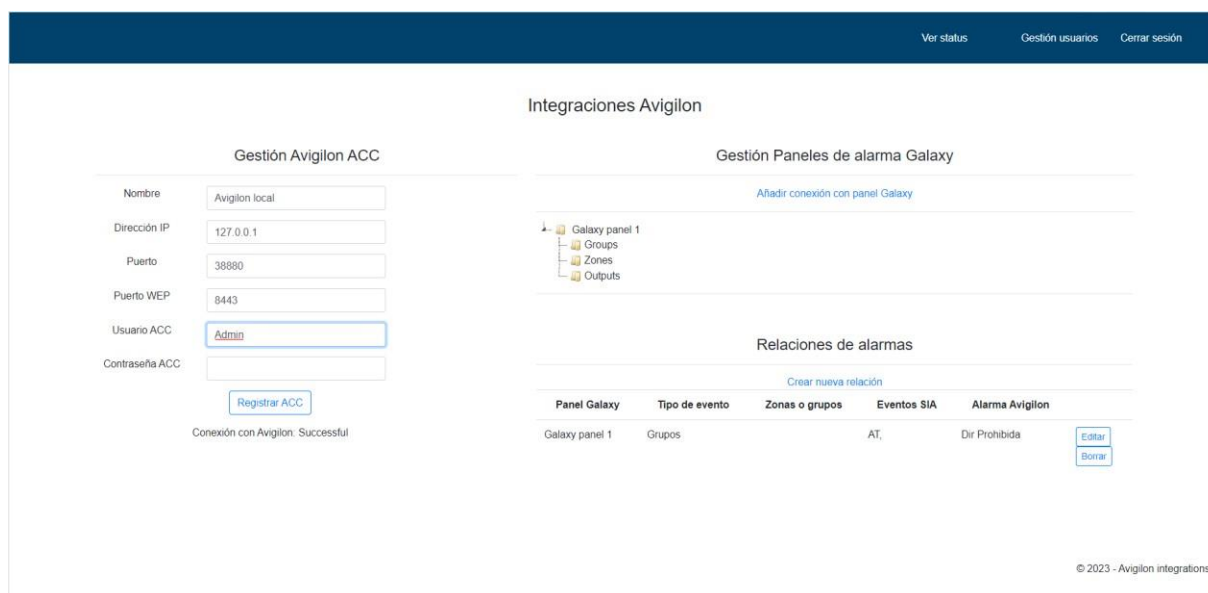
- Avigilon integrations service.

This is the primary integration application that stores all registered data, initializes communications with alarm panels, connects with ACC, and manages the relationships between ACC alarms and panel events. It triggers these alarms, allowing them to be managed from the ACC client.



- Web-based Management Application:

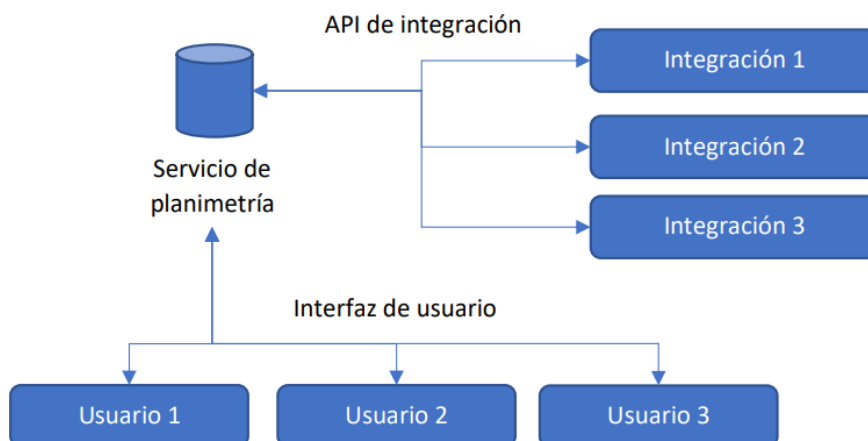
This web application serves as a management interface between intrusion panels and the ACC platform. It facilitates the creation, modification, updating, and deletion of relationships between panel events and ACC alarms.



The web management application will not function if the Avigilon Integrations service is not active. It is essential to always check that the service is running and operational to ensure that the web management application can display all the information.

- Floor Plan Service

The solution's architecture is depicted in the following diagram.



On one hand, the web service exposes an integration API used to transmit data about devices intended for integration to the floor plan service. On the other hand, it provides a user interface through which floor plans can be created, and devices registered via the integration API can be represented.

5. Installation

Installation of SGSE Avigilon Integration Service

Before initiating the installation, it is imperative to have the following software installed on your system:

- Internet Information Services (IIS)

[Plan an ASP.NET Website on IIS | Microsoft Learn](#)

- SQL Server 2018 (or later)

[SQL Server Downloads | Microsoft](#)

- SQL Server Management Studio (2018 or later)

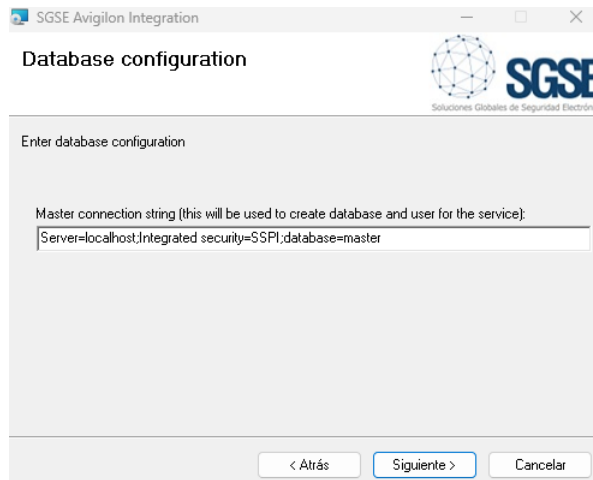
[Download SQL Server Management Studio \(SSMS\) - SQL Server Management Studio \(SSMS\) | Microsoft Learn](#)

Once both software packages are installed, we can proceed with the service installation. Follow these steps:

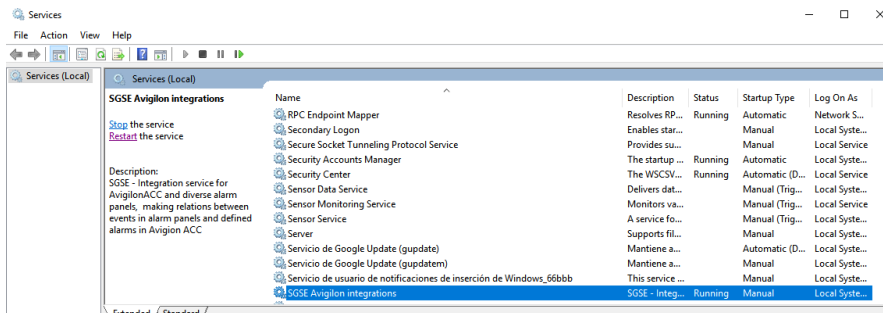
Run the installation MSI file.



Choose the installation path for the database tables by entering the database connection string where everything will be installed:



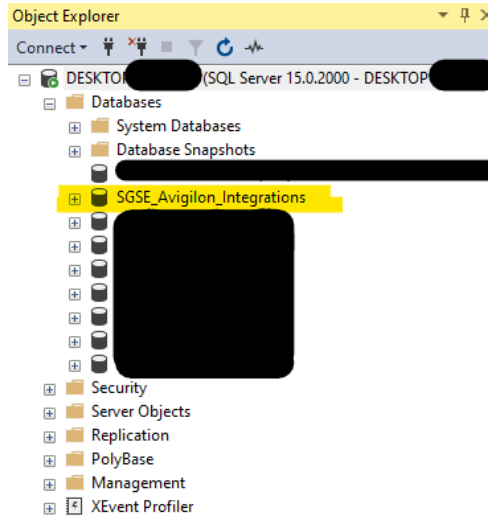
We conclude by confirming the installation. Once completed, the service will appear in the Windows services. You can access them by pressing "Windows + R" keys and running the command "services.msc", or by searching for the "Services" application in the "Start" menu.



In addition to creating the service, the installer generates a new database and an application in Internet Information Services (IIS), both of which are essential for the proper functioning of the integration. You can verify the creation of both in the following programs:

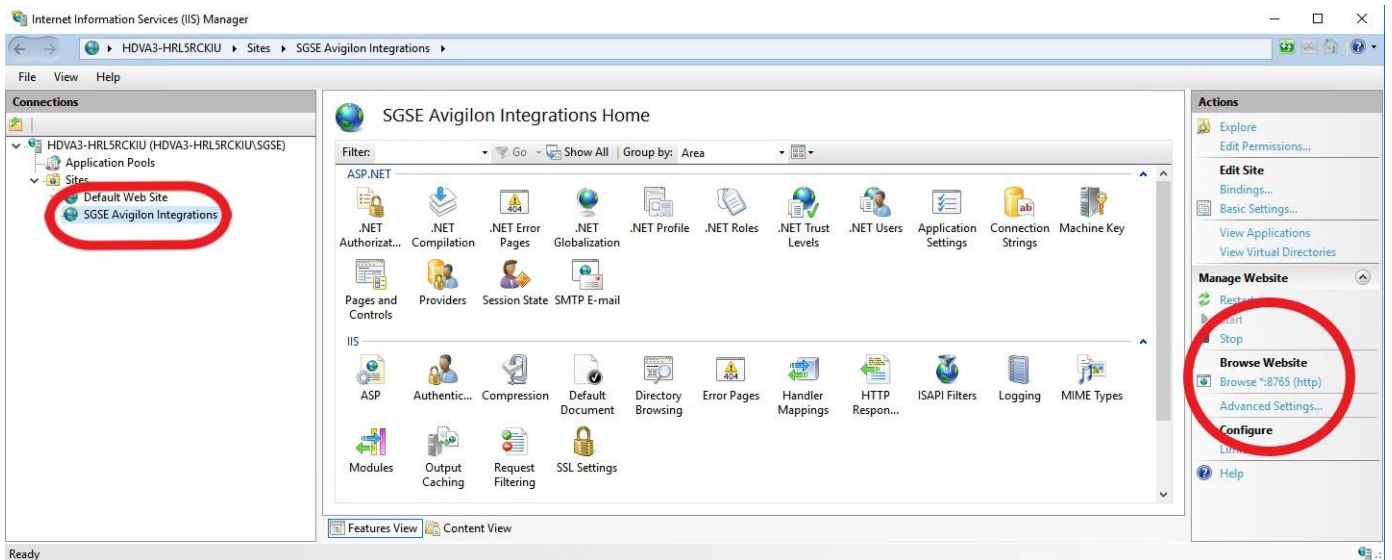
SQL Server Management Studio (Sql Database Management Tool):

Access the configured server using SQL Server Management Studio as set up during the installation. After logging in, you will observe that the SGSE_Avigilon_Integrations database has been successfully created in the "Databases" section.



Internet Information Services:

Open Internet Information Services (IIS) and verify that the web application has been created. Under the "Sites" section, you should locate the application named "SGSE Avigilon Integrations." In the left section (Browse Website), you can confirm that the service is running on port 8765.



To test the newly created site, browse the website from IIS. If everything is functioning correctly, you should see the login page of the application in your default web browser.

Iniciar sesión

Nombre de usuario

Contraseña

¿Recordar cuenta?

La licencia no es válida para este equipo.

Proporcione el siguiente UID a SGSE para que se genere su licencia

1SLYO71-166Q8VB-1ICOZD5-1WGMK53



AVIGILON™

The application will only operate with a valid license generated by SGSE. Users must provide SGSE with the code displayed on the screen, referred to as "UID." SGSE will then provide the necessary license for activation.

← → ↻ ⓘ localhost:8765/Account/Login?ReturnUrl=%2F

Iniciar sesión

Nombre de usuario

Contraseña

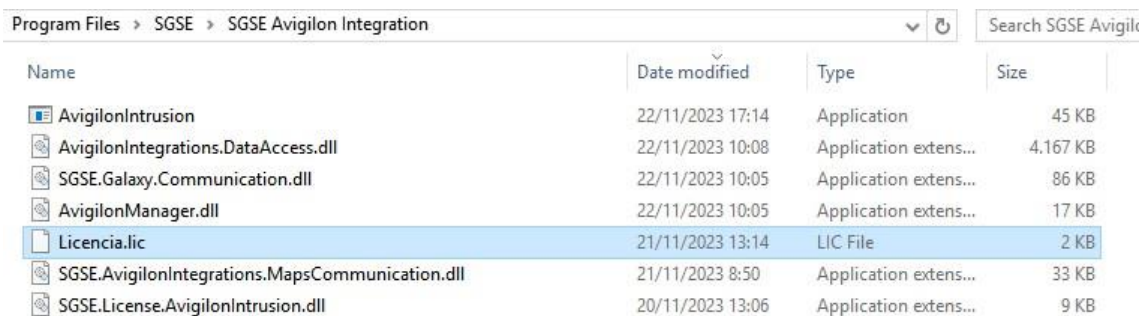
¿Recordar cuenta?

Iniciar sesión



AVIGILON™

Upon receiving the license, it is necessary to include it in the folder "C:\Program Files \SGSE\SGSE Avigilon Integration" or in the chosen directory if its default location has been changed.



Name	Date modified	Type	Size
AvigilonIntrusion	22/11/2023 17:14	Application	45 KB
AvigilonIntegrations.DataAccess.dll	22/11/2023 10:08	Application extens...	4,167 KB
SGSE.Galaxy.Communication.dll	22/11/2023 10:05	Application extens...	86 KB
AvigilonManager.dll	22/11/2023 10:05	Application extens...	17 KB
Licencia.lic	21/11/2023 13:14	LIC File	2 KB
SGSE.AvigilonIntegrations.MapsCommunication.dll	21/11/2023 8:50	Application extens...	33 KB
SGSE.License.AvigilonIntrusion.dll	20/11/2023 13:06	Application extens...	9 KB

After completing the aforementioned steps, it is necessary to restart the service to ensure that the license reading takes effect and the service operates with the updated licensing information.

Installation of Floor Plan Service

To install the service, simply run the installer "SGSE Maps Service Installer.msi" with administrator permissions, as provided by SGSE. The process is automatic. Through the various screens of the installer, you will need to accept the End User License Agreement, which is a mandatory condition for using the plugin. Additionally, specify the connection string to a SQL Server database server, which will be used for creating a database and a user. Let's review the different screens that will appear during the installation process of the mentioned applications.



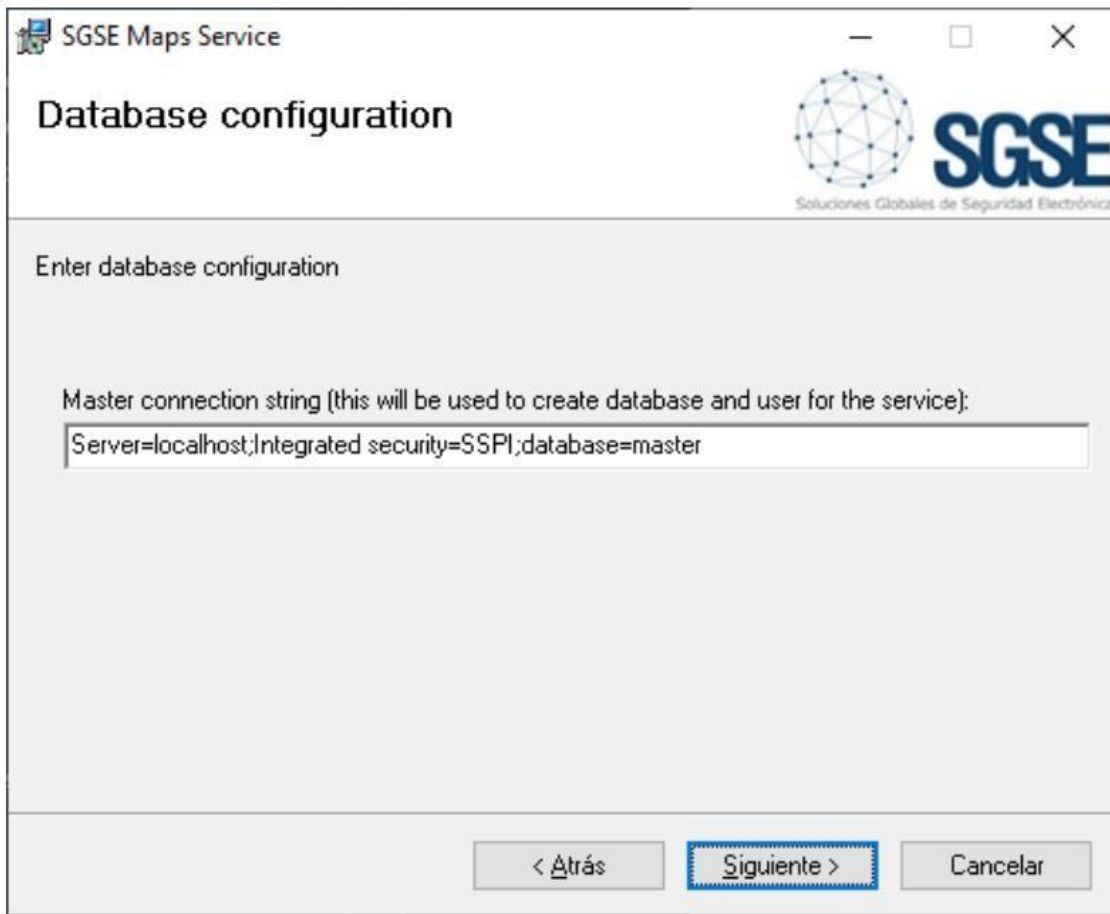
Click "Next >" to start the installation.



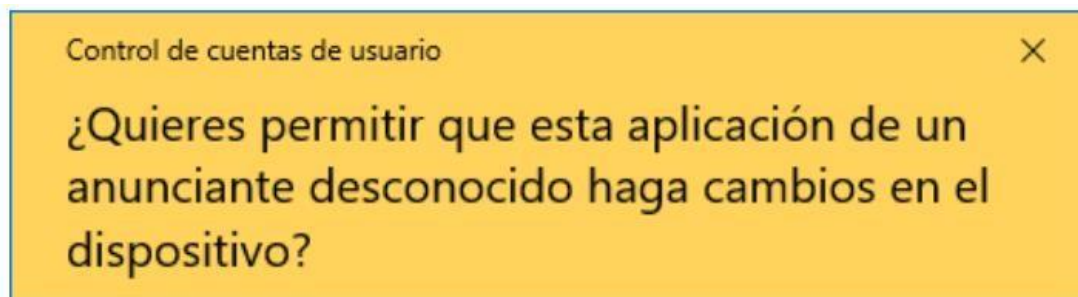
It will be necessary to read and accept the End User License Agreement to proceed with the installation.



Click "Next >" to proceed.



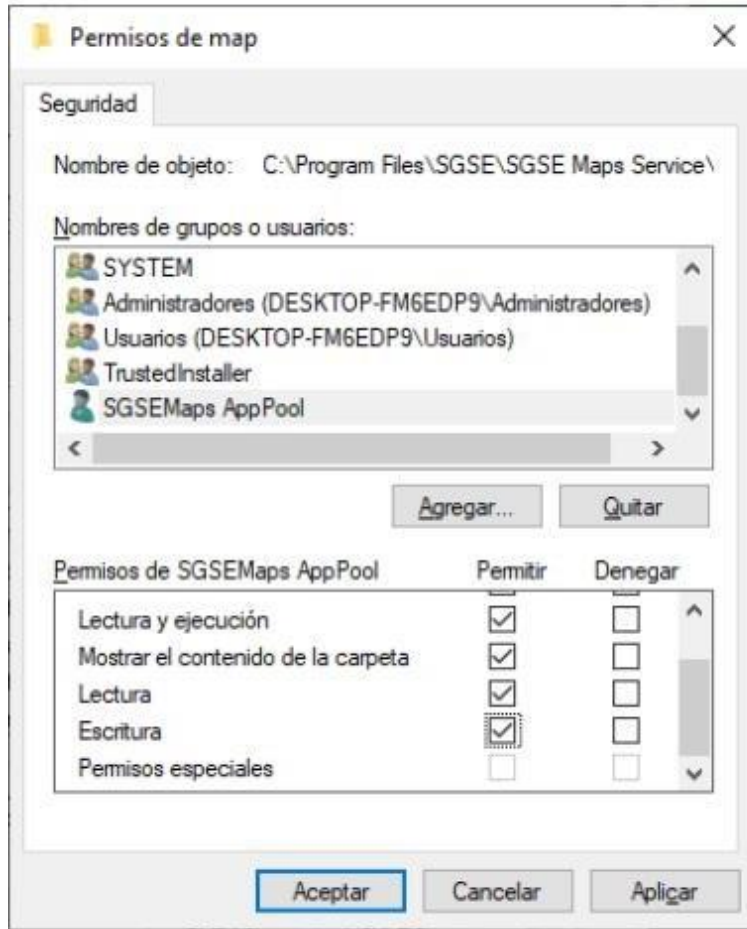
On this screen, enter the connection string or leave the default one if applicable. Click "Next >" to proceed with the installation of the software files.



If Windows User Account Control prompts, allow the installer to continue with the installation.



Once the installation is complete, click "Close," and the service will be installed. To ensure the proper functioning of the service, it is necessary to assign write permissions to the directory "C:\Program Files\SGSE\SGSE Maps Service\wwwroot\img\map" for the user "SGSEMaps AppPool."



6. Configuration

Galaxy panel configuration has to match with the Plugin configuration, both configurations share some parameters that must have the same values. This applies to any communication mode, although parameters are different in each case.

6.1 Galaxy configuration

6.1.1 Ethernet module

Firstly, we will have to configure the Galaxy panel to send events to the Milestone Event Server IP address (Primary IP for alarm report, SIA level 4), and then we will have to configure it to allow the Milestone Event Server to connect to the panel and send commands to it (SIA Control).

The mandatory configuration steps to follow in order to configure the Galaxy panel, when using the keypad are described below. Same configuration can be done using Galaxy's configuration software (FrontShell):

6.1.1.1 Enable the engineer mode

Login with the user pin (the default is 12345) and then press the enter key ("ent") Access to the menu 48, option 1, option 1 (menu 48.1.1) and set it to Enabled (value "1") Finally press the escape key ("esc") four times until it escapes completely from the menu. And login as engineer immediately: enter the engineer pin (the default is 112233) and then press the enter key.

6.1.1.2 Configure the Galaxy panel IP address

Login as engineer, access the menu 56.4.01.1 and then assign the IP to the Galaxy panel. The menu options 56.4.01.3 and 56.4.01.4 allow you to assign the gateway IP and the network mask.

6.1.1.3 Configure the SIA level

Login as engineer, access the menu 56.4.02.1.1, **set the value of the SIA level to "4"**. After the enter key is pressed, the panel will request to enable or disable all the events available in the SIA protocol. The Plugin is able to process all of them if it is needed.

6.1.1.4 Configure the primary IP for alarm report

This is the listening IP address where the Plugin receives and process the events. Login as engineer, access the menu 56.4.02.2.1, **set the value to the IP of the Milestone Event Server**. The option 56.4.02.2.2 allows to change the port number if needed. If it is changed, the same value has to be configured in the Milestone Management Client.

6.1.1.5 Account number

Login as engineer, access the menu 56.4.02.4 and assign an account number.

6.1.1.6 Enable TCP

Login as engineer, access the menu 56.4.02.8 and set the value to "1=TCP".

6.1.1.7 Enable the SIA control

This enables the Plugin to send commands to the Galaxy.

Login as engineer, access the menu 56.4.08 and set the value to the IP of the Milestone Event Server, the port is 10005.

6.1.1.8 Encryption

Login as engineer, access the menu 56.4.09 and set all values to "0=OFF"

6.1.1.9 Exit engineer mode

After all configuration is done, configurator user has to exit the engineer mode. Press "esc" until keypad shows the model and then enter the engineer pin and press the "esc" key instead of the "ent" key. It is recommended to do a full restart (unplug power and battery).

6.1.2 Serial to Ethernet converter

If the Galaxy panel is communicating with the plugin through the RS-232 serial port using a serial to Ethernet converter, then configuration is simpler.

6.1.2.1 Galaxy serial settings configuration

To configure the Galaxy to support event signaling and SIA control over RS232, you need to go through the following options:

- INT RS232 mode must be set to Direct (option 56.6.1 Mode, set value 2=Direct)
- Format must be set to SIA level 4 (option 56.6.2.1)
- Set an Account Number (option 56.6.3). It can be 4 or 6 digits.
- Set the baud rate, data bits, stop bits and parity (option 56.6.4 COMMS SET-UP).
By default, baud rate is set to 9600, but can be increased if required.

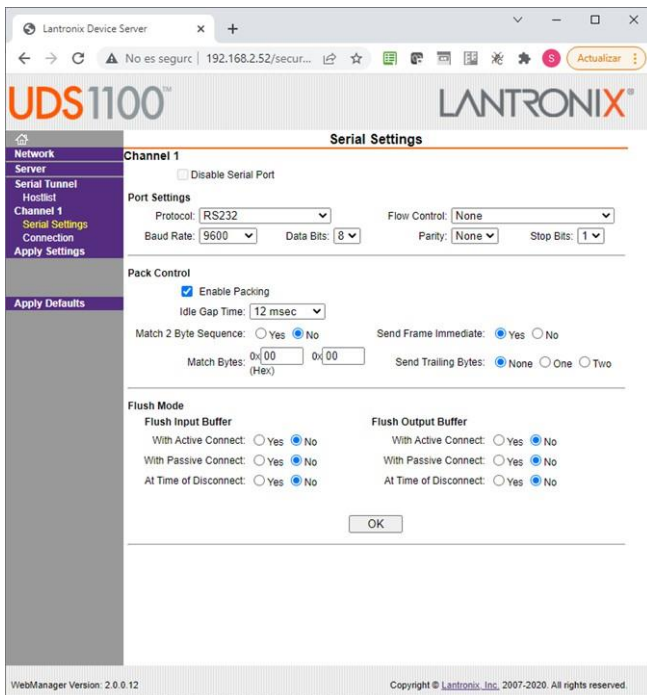
Then, you need to configure the serial parameters of the converter to match the parameters of the Galaxy serial port, and the operating mode so that it acts as a tunnel for data in both directions. The serial converter will act as a web server and the plugin will actively connect to it to send messages and retrieve events.

We are showing some configurations of the verified serial converters (Lantronix UDS-1100 and Moxa NPort 5110)

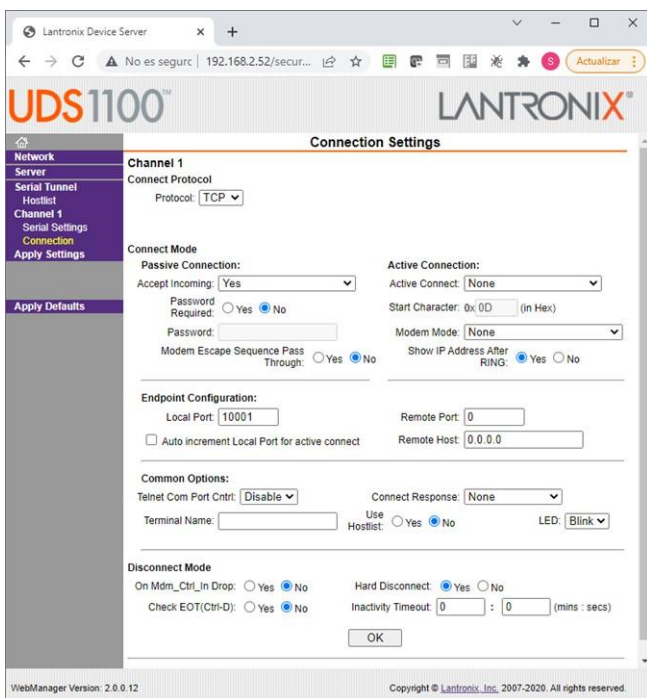
6.1.2.2.1 Lantronix UDS-1100

Access the configuration web page and establish a static IP address to the device.

Then, go to **Serial Settings** and set the serial parameters that match the Galaxy RS-232 port configuration:



Then go to **Connection** settings, and configure **TCP Protocol**, and set Passive Connection. You have to configure in **Local Port** the port in which the converter will listen for connections.

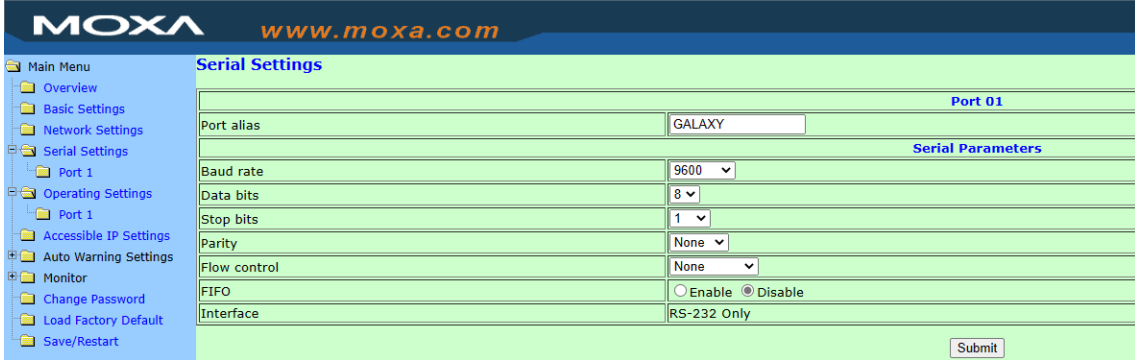


Then, at the plugin, you will have to select **RS232_Socket** as Communication module and set the corresponding parameters.

6.1.2.2.2 Moxa NPort 5110

Access the device configuration web page and give it a static IP address.

Then go to Serial Settings > Port 1 and establish the parameters that match the Galaxy configuration.



The screenshot shows the MOXA web interface for Serial Settings. The left sidebar contains a navigation menu with options like Overview, Basic Settings, Network Settings, Serial Settings, Port 1, Operating Settings, Accessible IP Settings, Auto Warning Settings, Monitor, Change Password, Load Factory Default, and Save/Restart. The main content area is titled 'Serial Settings' and shows configuration for 'Port 01'. The 'Serial Parameters' section includes the following fields:

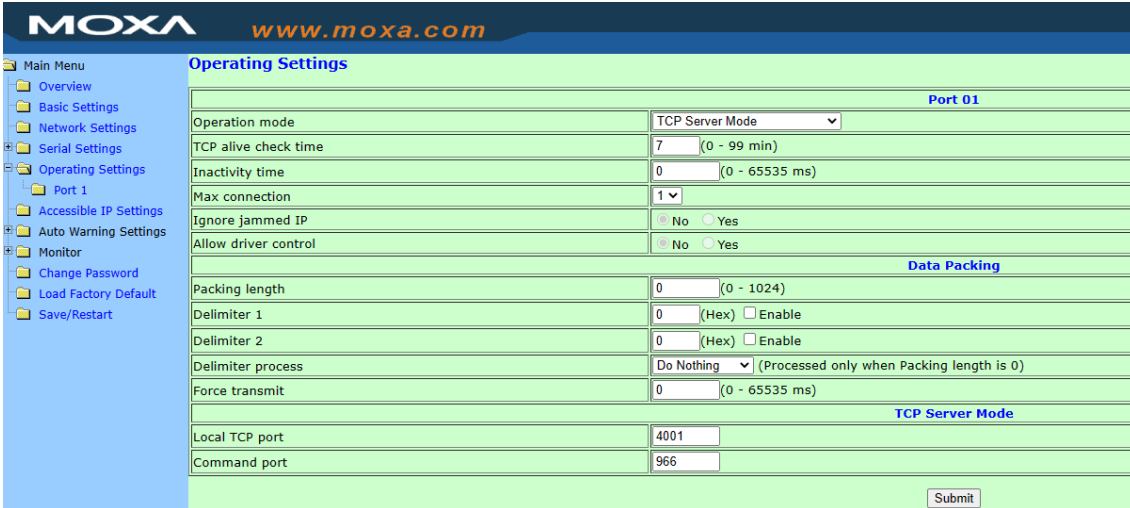
Port alias	GALAXY
Baud rate	9600
Data bits	8
Stop bits	1
Parity	None
Flow control	None
FIFO	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Interface	RS-232 Only

A 'Submit' button is located at the bottom right of the form.

After that, go to Operating Settings > Port 1 and focus in the following parameters:

- Operation Mode: must be TCP Server Mode
- Local TCP Port: This is the port that the plugin will try to connect to.

Keep the rest of parameters with their default values, as seen in the following picture:



The screenshot shows the MOXA web interface for Operating Settings. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Operating Settings' and shows configuration for 'Port 01'. The 'TCP Server Mode' section includes the following fields:

Operation mode	TCP Server Mode
TCP alive check time	7 (0 - 99 min)
Inactivity time	0 (0 - 65535 ms)
Max connection	1
Ignore jammed IP	<input type="radio"/> No <input type="radio"/> Yes
Allow driver control	<input type="radio"/> No <input type="radio"/> Yes

The 'Data Packing' section includes:

Packing length	0 (0 - 1024)
Delimiter 1	0 (Hex) <input type="checkbox"/> Enable
Delimiter 2	0 (Hex) <input type="checkbox"/> Enable
Delimiter process	Do Nothing (Processed only when Packing length is 0)
Force transmit	0 (0 - 65535 ms)

The 'TCP Server Mode' section includes:

Local TCP port	4001
Command port	966

A 'Submit' button is located at the bottom right of the form.

6.2 Configuration of SGSE Avigilon Integration Service

Firstly, it is necessary to create an administrator user. This can only be set the first time the service is run, and its information can be modified afterward.

Access the site created in IIS (by default, <http://localhost:8765>) and click on the link "Register as a new user."

Iniciar sesión.

Nombre de
usuario

Contraseña

¿Recordar cuenta?

Iniciar sesión

Registrarse como usuario nuevo

Create a new user by filling in the details on the form, and click the "Register" button.



Crear una cuenta nueva.

Nombre de
usuario

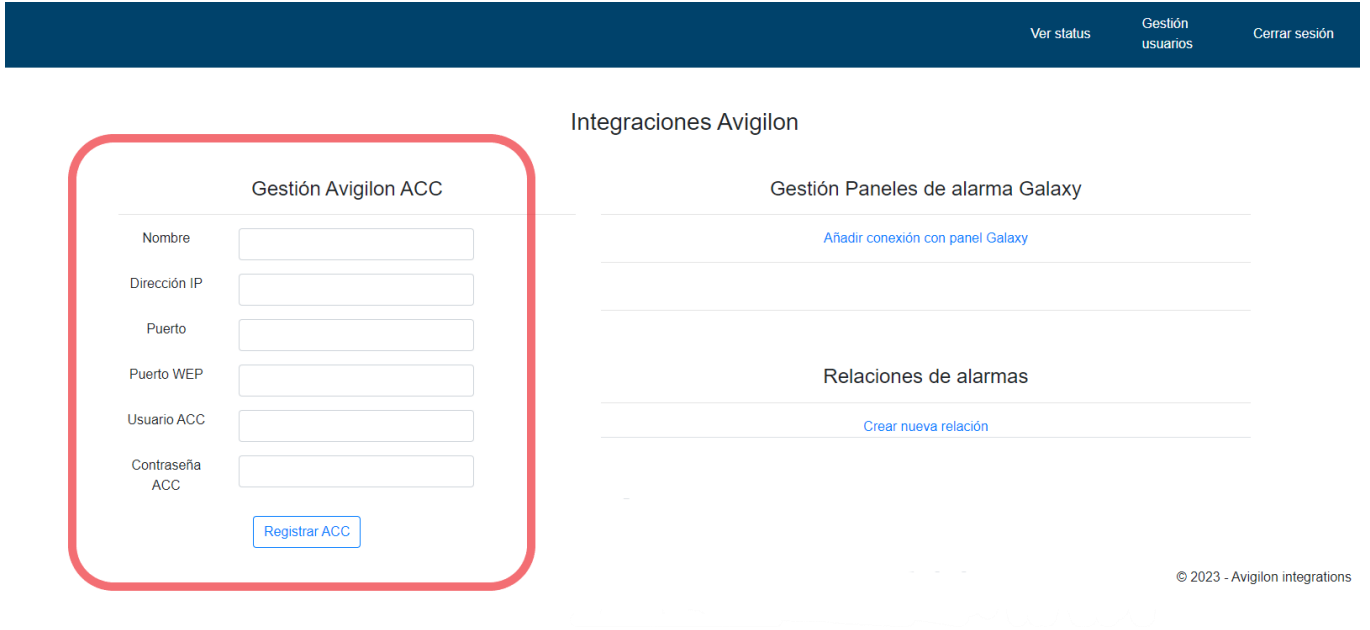
Contraseña

Confirmar
contraseña

Registrarse

With the Administrator user data set, you can access the main configuration page of the service.

First, you need to connect to your Avigilon Control Center by adding the connection details.



Ver status Gestión usuarios Cerrar sesión

Integraciones Avigilon

Gestión Avigilon ACC

Nombre

Dirección IP

Puerto

Puerto WEP

Usuario ACC

Contraseña ACC

[Registrar ACC](#)

Gestión Paneles de alarma Galaxy

[Añadir conexión con panel Galaxy](#)

Relaciones de alarmas

[Crear nueva relación](#)

© 2023 - Avigilon integrations

We add the details and click the "Register ACC" button.

Next, we proceed to add a connection to a Galaxy panel by clicking on the "Add Galaxy Panel Connection" link.



Ver status Gestión usuarios Cerrar sesión

Integraciones Avigilon

Gestión Avigilon ACC

Nombre

Dirección IP

Puerto

Puerto WEP

Usuario ACC

Contraseña ACC

[Registrar ACC](#)

Gestión Paneles de alarma Galaxy

[Añadir conexión con panel Galaxy](#)

Relaciones de alarmas

[Crear nueva relación](#)

© 2023 - Avigilon integrations

Configure the different Galaxy panels based on the panel model and communication type.

Create

GalaxyPanel

Name

ModelCode

CommunicationModuleType

ProtocolPIN

[Back](#)

Groups

Select All

- A1
- A2
- A3
- A4
- A5
- A6
- A7
- A8

Zones

Select All

- 1001
- 1002
- 1003
- 1004
- 1005
- 1006
- 1007
- 1008
- 1011
- 1012
- 1013
- 1014
- 1015
- 1016
- 1017
- 1018

Outputs

Select All

- 1001
- 1002
- 1003
- 1004
- 1011
- 1012
- 1013
- 1014
- 1021
- 1022
- 1023
- 1024
- 1031
- 1032
- 1033
- 1034

With both sections completed and connections established with both ACC and a Galaxy panel, you can set up alarm relationships in the "Relationships" section.

Ver status
Gestión usuarios
Cerrar sesión

Integraciones Avigilon

Gestión Avigilon ACC

Nombre

Dirección IP

Puerto

Puerto WEP

Usuario ACC

Contraseña ACC

Gestión Paneles de alarma Galaxy

[Añadir conexión con panel Galaxy](#)

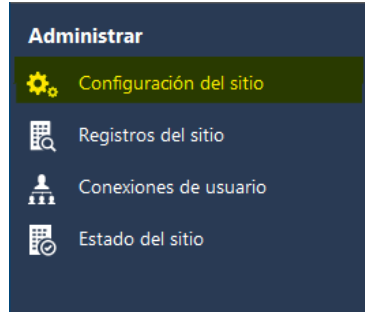
Relaciones de alarmas

[Crear nueva relación](#)

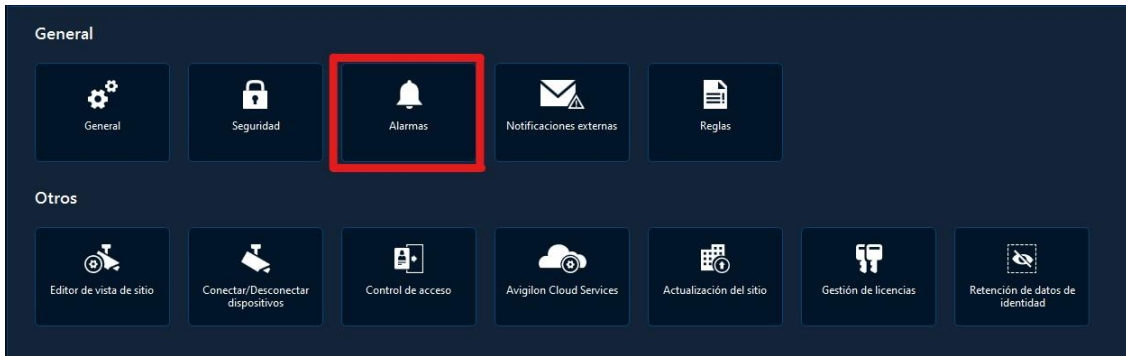
© 2023 - Avigilon integrations

To establish relationships, it is necessary to create alarms in the Avigilon platform first.

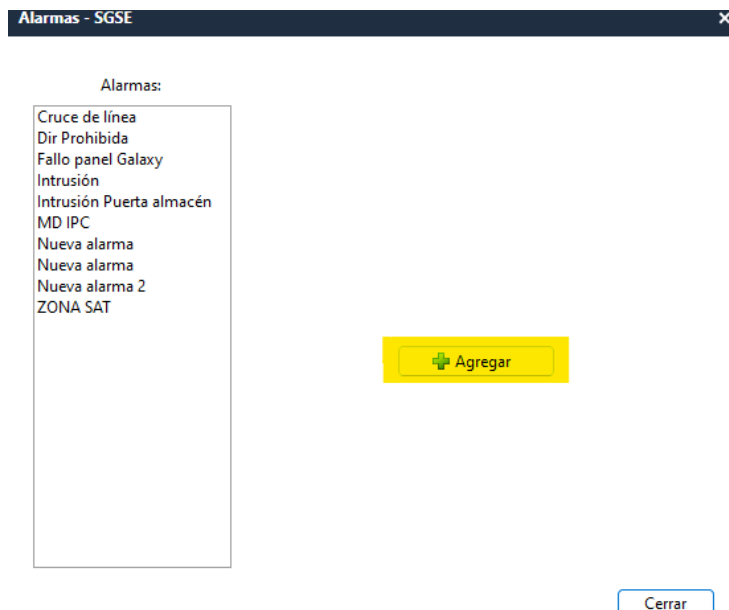
Access the site configuration:



Access the alarm management:



Follow the steps to generate a new alarm:



Once you have parameterized alarms in Avigilon, you can proceed with creating relationships. Select the Galaxy panel event that will trigger alarms in Avigilon.

Crear relación Cancelar

Panel Galaxy (Galaxy panel 1)	Zona de acción Galaxy Zona <input type="checkbox"/> Select All <input checked="" type="checkbox"/> Cristal exterior	Evento SIA (Galaxy) <input type="checkbox"/> ACPower_Trouble <input checked="" type="checkbox"/> Burglary_Alarm <input type="checkbox"/> Burglary_Trouble <input type="checkbox"/> Closing_ClosingReport <input type="checkbox"/> Fire_Alarm <input type="checkbox"/> Fire_Trouble <input type="checkbox"/> Holdup_Alarm <input type="checkbox"/> Holdup_Trouble <input type="checkbox"/> PhoneProgram_LineTrouble <input type="checkbox"/> Opening_OpenReport	Alarma Avigilon Dir Prohibida	<input type="button" value="Crear"/>
----------------------------------	---	--	----------------------------------	--------------------------------------

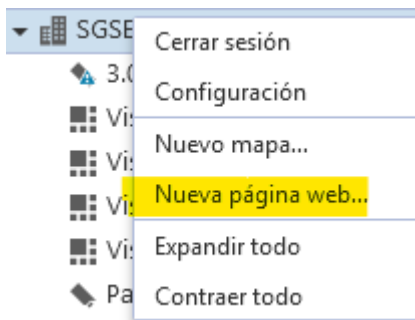
6.3 Configuration of the "Floor Plan" web service

By default, the web service will have the following configuration values: Database connection string: By default, it will try to connect to the local machine with the credentials created during installation. This connection string can be changed in the appsettings.json file located at "C:\Program Files\SGSE\SGSE Maps Service."

7. Operation

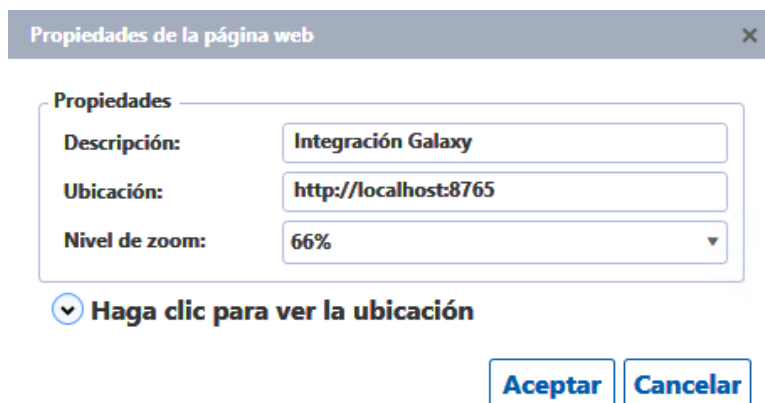
Operation on the Avigilon platform

In ACC, you can establish multiple views that load a web page, and you can configure the URL for accessing your management application.



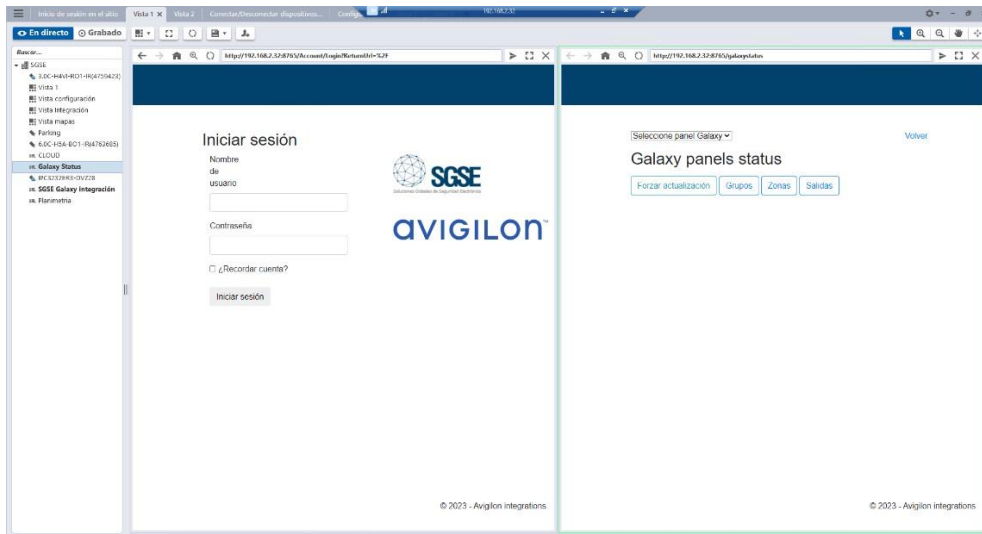
In the "Location" text, change the URL to access your service.

Thanks to this action, you will see all the alarm panel management from ACC.



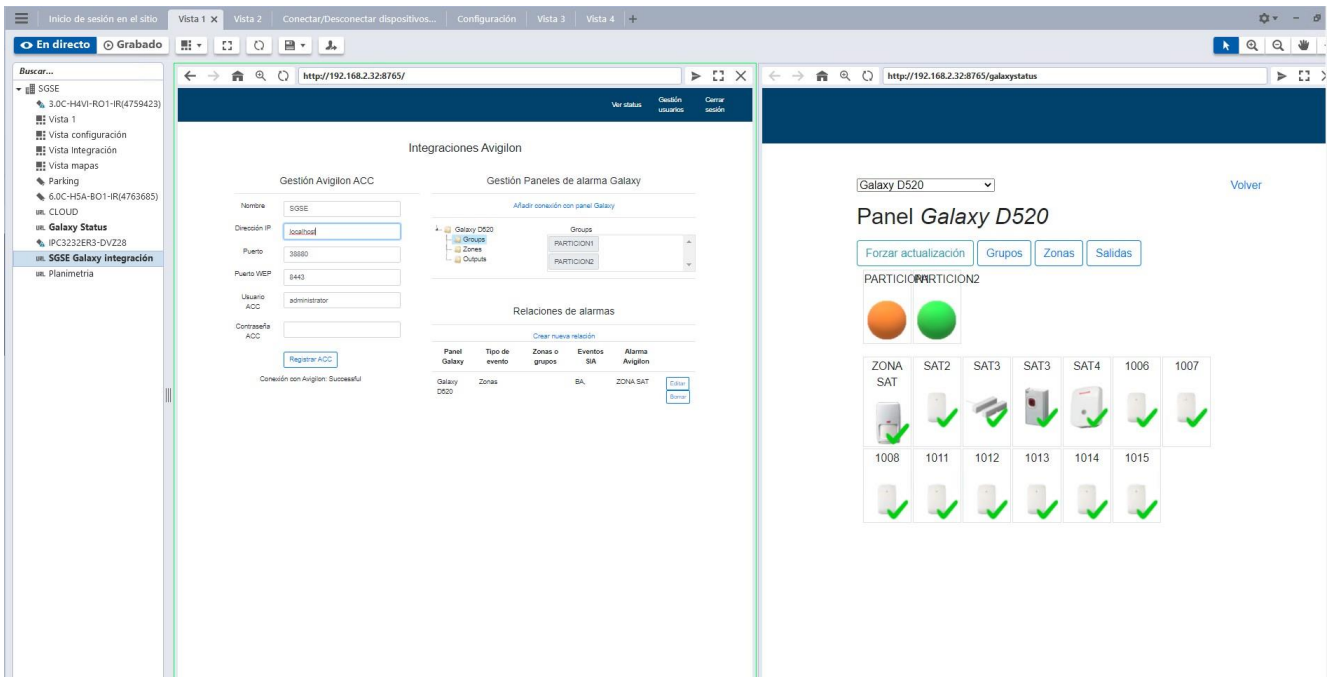
Once the view is established, you can drag it to any quadrant to display the information.

To access the view of the synoptic that displays the alarm panel states, simply enter the URL..



<https://{{URL or DNS}}:8765/galaxystatus>

In this view, you will see the current state of the zones, groups, and outputs configured on the panel, and you can take actions on these elements.



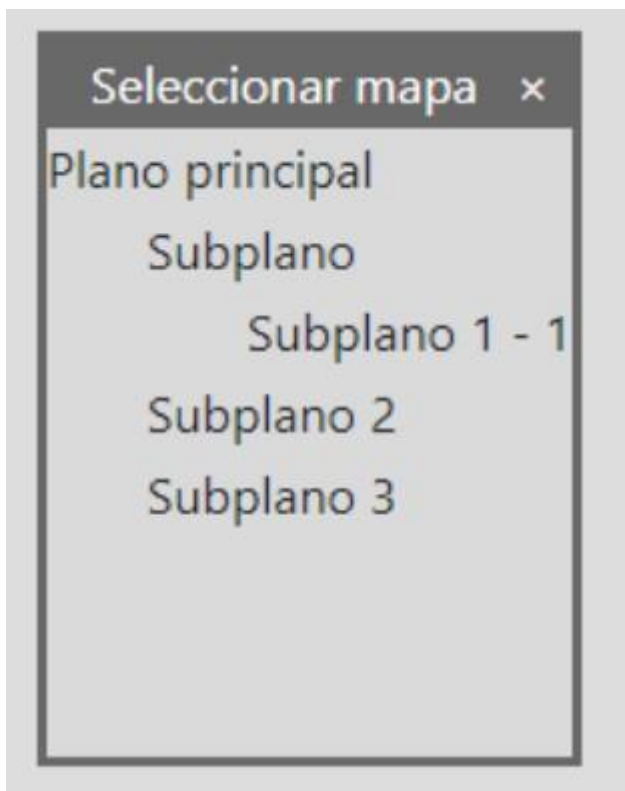
Operation with the Floor Plan Manager

You can access the application via the URL <http://<hostname>/SGSEMaps/> or embedded within another application. If the user is not authenticated, they will be presented with a login screen where they can log in with a username and password..

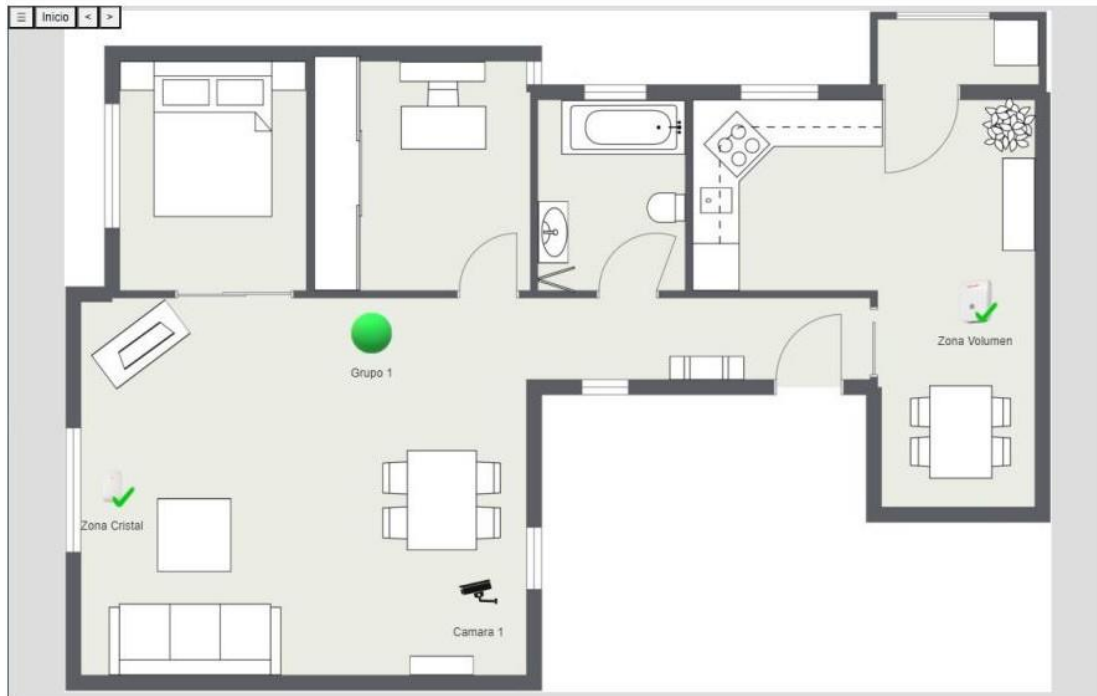
By default, there will be an admin user with the password Admin-123. There are two user profiles: administrator and user.

User Profile

If you access the user interface without specifying any floor plan, a popup will appear to select the main floor plan.


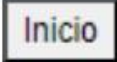




Once a floor plan is selected, the chosen plan will be displayed on the screen.

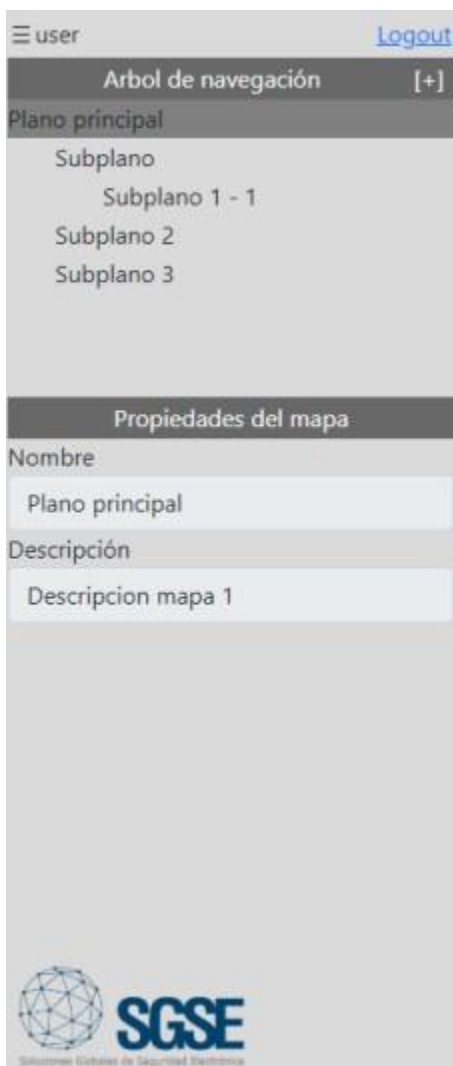


Navigation Buttons

In the upper-left corner, you will find the following buttons.

	Muestra u oculta el panel lateral
	Sitúa la navegación en el plano inicial
	Sitúa la navegación en el plano anteriormente seleccionado
	Sitúa la navegación en el siguiente plano si anteriormente se usó el botón de atrás

Sidebar



The sidebar displays user information and the navigation tree containing the main floor plan and its sub-plans.

Clicking the button **[+]** will close the current navigation tree and display a popup to select a new main floor plan.

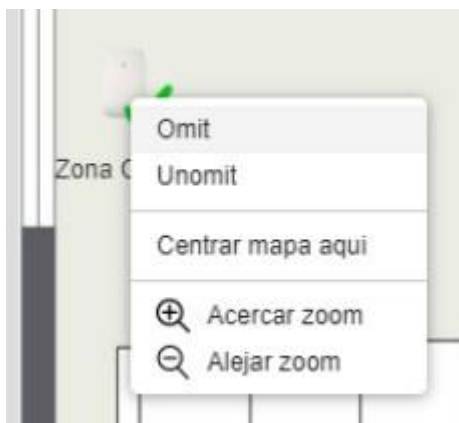
In the navigation tree, the names of the floor plans may appear marked with a color depending on the state of the devices contained in that map.

Below the navigation tree, information associated with the currently selected floor plan will be displayed

Within the Floor Plan

Within the floor plan, two types of elements may exist: the devices themselves and hot zones. Devices are categorized by type and may have commands. To send a command to a device, hover the mouse over the icon and right-click.

A contextual menu will appear with various actions.



When you click on one of the actions, an indicator will appear over the icon to show that the command has been sent. It will disappear once the action is completed.



If the device supports video preview, placing the mouse over it will display the live image.

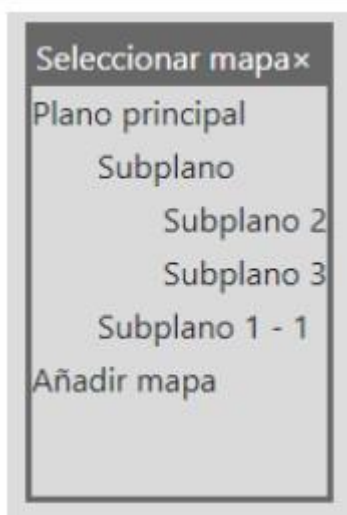


Hot zones represent an area on the floor plan and allow you to navigate to that plan by clicking on them.



Administrator profile

The administrator profile has all the functionalities of the user profile, but it also includes tools for creating and modifying floor plans. Both the popup window and the navigation tree will have the option to add a new floor plan.



Clicking on "Add Map" will create a new map that will be a child of the currently selected floor plan. If you create it in the popup window, it will become a main floor plan.

Once a floor plan is selected, it will be displayed on the screen with an interface similar to the user profile.

Sidebar

Within the sidebar, in the map properties section, there will be an option for the background image among the floor plan details. This option allows you to select a new image for the floor plan background. The image will not be set until the floor plan is saved.



Editing Mode

In the upper-right corner, you will find the **Editar** button.

Clicking on it will activate the editing mode for the currently selected floor plan.

In edit mode, the **Editar** button will be replaced by the following buttons:

Borrar	Elimina el plano actual
Descartar	Descarta los cambios efectuados en el plano y sale del modo edición
Guardar	Guarda los cambios efectuados en el plano y sale del modo edición

A tool window will also appear to enable the addition of new elements to the floor plan.



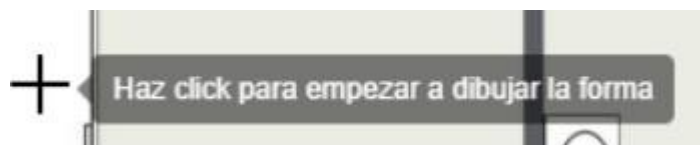
The content of this window depends on the various types of devices specified through the integration API. When you click on one of the types, another window will appear with a list of registered devices of that type.



From this window, you can drag a device to the area of the floor plan where you want to place it. To remove an element from the floor plan, click on it and then press the delete key on the keyboard.

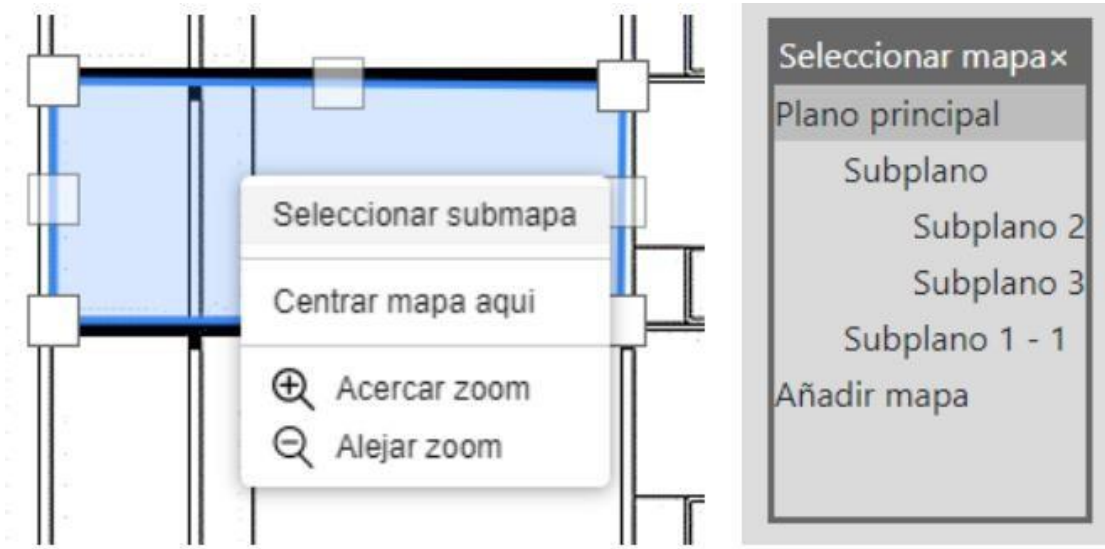
The "Hot Zone" option is independent of the integration, and its operation is as follows:

After clicking the "Hot Zone" button, the mouse cursor will turn into a cross, and the following message will appear next to it.



In this mode, you can define polygonal areas by clicking multiple times on the floor plan. It is mandatory to select the first point created as the last point to close the polygon. Once the polygon is created, clicking on it will display boxes at the vertices that allow you to modify the polygon. Like with icons, the polygon can be deleted by pressing the delete key on the keyboard while it is selected for editing.

Right-clicking on a polygon will show the option "Select Submap," which opens a popup to choose the map to which the user will be redirected upon clicking on the area.



8. Troubleshooting

The service does not seem to connect with Avigilon:

Verify that the connection details, username, and password are correct.

Failure to connect to different alarm panels:

Confirm that the connection data and connection type are accurate.

Unable to create relationships:

Ensure that Avigilon is connected, and various connections to alarm panels are established.

Avigilon alarms do not appear when creating relationships:

Check the accuracy of the connection details with Avigilon ACC, including the username and password.

Verify in ACC that there are created alarms to associate with events.

The service remains loading without fully executing:

Review the communication status with both Avigilon ACC and the panels.

Ensure that ports are accessible and IP addresses are correct.

Error al cargar la imagen de fondo

If an error "Error loading the background image" occurs after selecting an image for the floor plan, ensure that the web service has write permissions for

Additional Information

For further information: Please refer to the online documentation or contact SGSE via email at info@sgse.eu.