SystemHouse Solutions
SMARTER BUILDINGS, BETTER SECURITY

INTEGRA

Access Control- and Security Management System

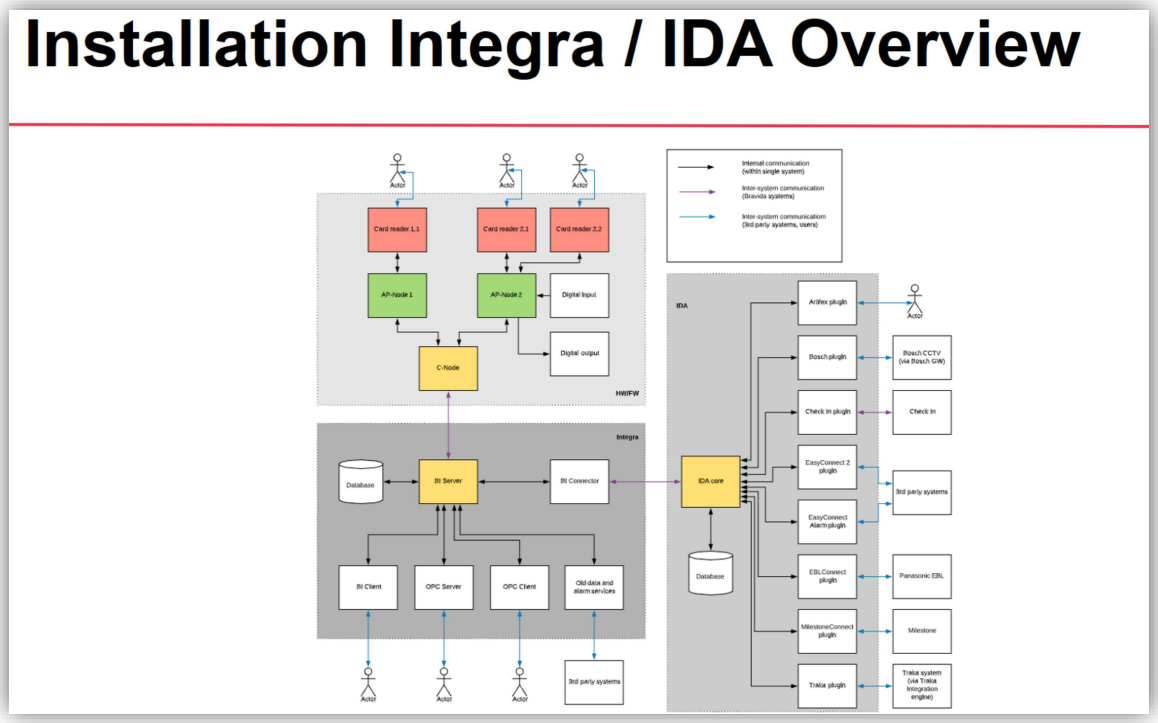
Data Services

1-986-4115-GB, 2023-05-05
SystemHouse Solution AB

Table of contents:

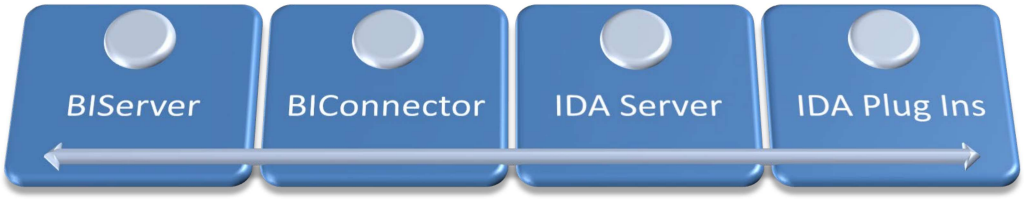
1 BIConnector

1.1 System description/overview IDA



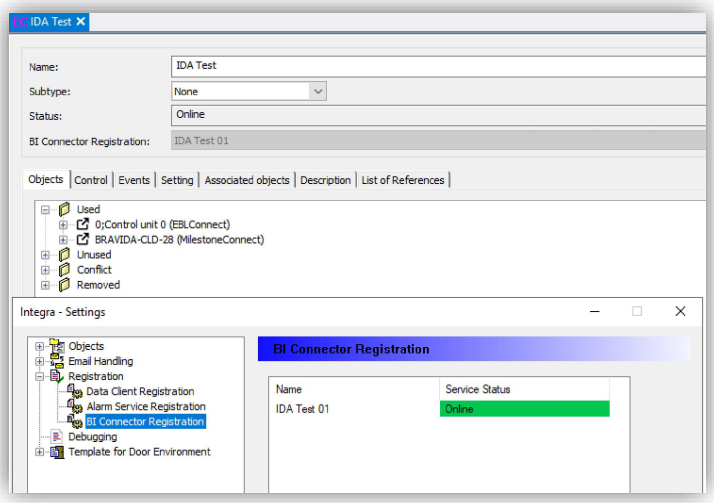
1.1.1 General Description BIConnector

The BIConnector is a component used exclusively for communication between Integra and IDA Server, hence is utilized only if IDA Server is going to be used. Installation of BIConnector is done by Integra Setup so no additional installation is required.



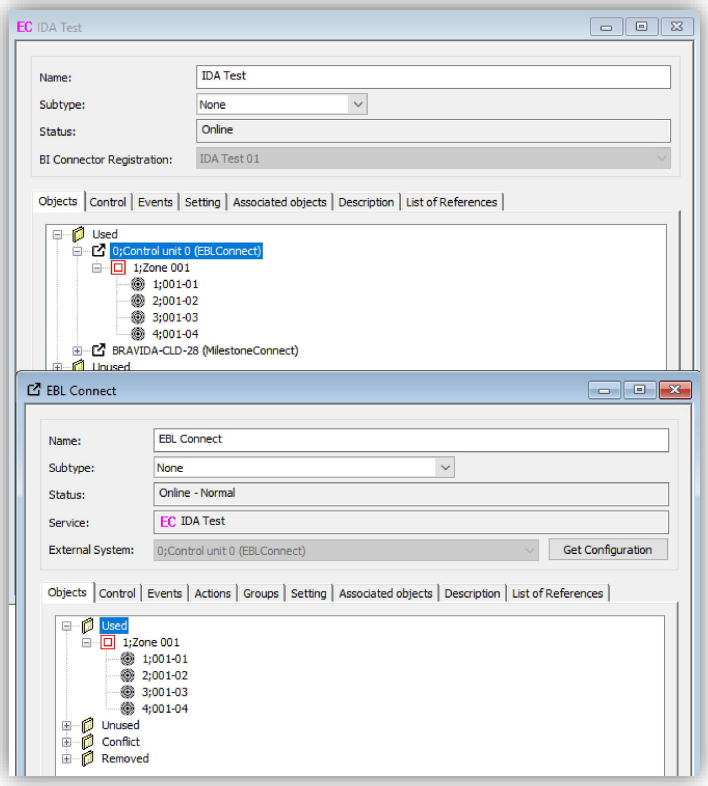
1.1.2 General description External Client

External Client handles all external systems that should be added into that IDA Server. You can have several External Clients which are connected to separate BIConnector services. Each External Client then handles external systems configured in IDA config file.



1.1.3 General description External System

Each Plug In in IDA is represented by an External System object in Integra. You can have several External systems created, also as same type. External Systems can belong to different External Clients. It handles all communication to External Systems underlying supported objects.



1.2 System Requirements

The following requirements must be fulfilled:

- Integra version: Same Integra version as BIConnector
- Client OS: Microsoft Win10 or later
- Server OS: Windows Server 2016 or later
- SQL Server version: SQL 2017 Server or later
- .Net Framework 4.8 or later

1.3 Installation & Configuration BIConnector

For installation and configuration of BIConnector please read User Manual *Installation Integra Software* chapter, *Installation BIConnector*

2 IDA Server

2.1 General Description

IDA server is a service that acts as a manager for plug-ins such as Artifex, Easy Connect, Check-In and integration with other 3:rd party services. It provides a Configuration GUI for all available Plug-Ins. It supports message encryption and configuration file is encrypted.

2.2 System Requirements

IDA Server requires BIConnector and it needs to have admin rights on server where it is installed. IDA Server have its own database. IDA server require a service account to be allowed to create database on SQL Server and to be its database owner. For setting up IDA Server database you need an SQL account with rights to create database.

The following requirements has to be fulfilled:

- IDA version is depended on Integra version. Please use IDA from same Setup as Integra
- Database on same SQL Server as Integra database is running
- BIConnector installed
- Client OS: Microsoft Win10 or later
- Server OS: Windows Server 2016 or later
- SQL Server versions: MSSQL 2017 or later. It is always recommended to install the latest SP of MSSQL Server.
- Microsoft .NET Framework 4.8 or later

For Artifex plugin:

- Desktop Browser: Chrome (latest release), Safari or Firefox
- Mobile Browsers: Android and IOS

2.3 Installation & Configuration IDA Server

For installation and configuration of IDA Server please read User Manual *Installation Integra Software* chapter, *Installation IDA Server*

3 IDA Server Plug Ins

3.1 Plug In; Easy Connect 2

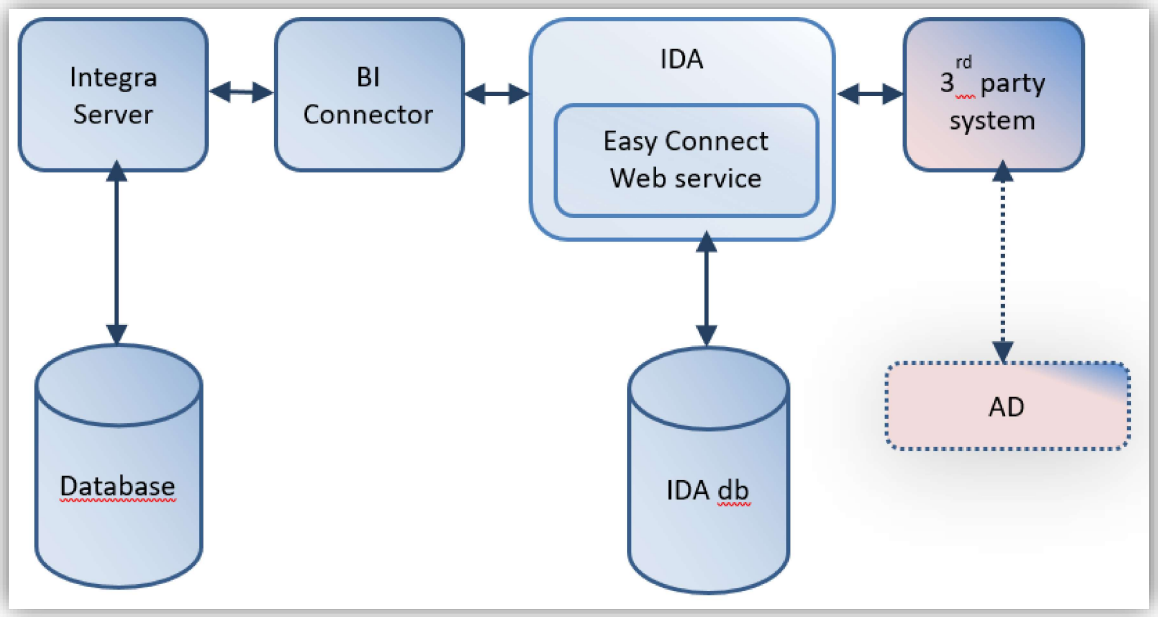
3.1.1 Easy Connect 2 General Description

Easy Connect 2 is a web interface plug-in to IDA, the main purpose for the interface is to enable 3rd party systems to communicate with Integra and exchange data.

Easy Connect 2 communicate with 3rd party systems using *SOAP (*Service Oriented Architecture Protocol*)* protocol. Easy Connect fulfill requirement for *SOAP* version 1.2 and the *WSDL* (*Web Services Description Language)* is compatible with *WSDL* version 2. There is possible to generate a *WSDL* file from the browser which you also can use to create a describing document in *html* format by using a 3rd party *SOAP* client (e.g. *SOAPUI* by Smartbear), the *html* document will describe all supported methods.

There are two different license options, *Basic and Advanced*. All functions will be performed regardless of license, but any attempt to call a function which is not supported by license will return an error.

Please read User Manual *Easy Connect 2 Description* for more information



3.1.2 Easy Connect 2 System Requirements

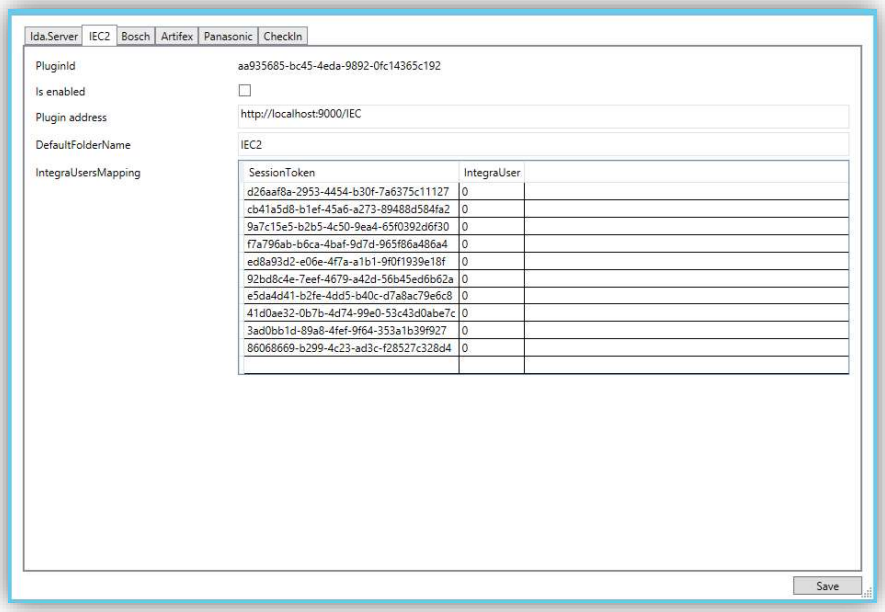
- BIConnector installed
- Client OS: Microsoft Win10 or later
- Server OS: Windows Server 2016 or later

3.1.3 Easy Connect 2 Installation and Configuration

To be able to get Easy Connect up and running you need to do some configuration. All configurations are done from a graphical user interface named *Ida.Server.Config.exe*.

See chapter *Configuration IDA Server* to open configuration tool.

To configure Easy Connect go to tab *IEC2*



- **Is enabled –** Checked if it should be enabled
- **Plugin address –** Easy Connect Listening address and port for 3:rd party system
- **DefaultFolderName -** Default Folder within Integra for import of objects if Folder is not specified within methods. Value should be unique folder name. If value starts with \\ it is treated as a folder path
- **IntegraUserMapping:**
  - **SessionToken –** A token that must be entered when data are sent to Easy Connect. This Token represents an Integra User, see Integra User
  - **IntegraUser –** Database ID of Integra User with proper access rights
- **Save –** After configuration is complete press *Save* and restart IDA Server

3.1.4 Easy Connect 2 Advanced

3.1.4.1 General Description

For *Advanced license* you will have access to 126 different methods. For more detailed description you must create a document from the *WSDL* file.

3.1.5 Easy Connect 2 Basic

3.1.5.1 General Description

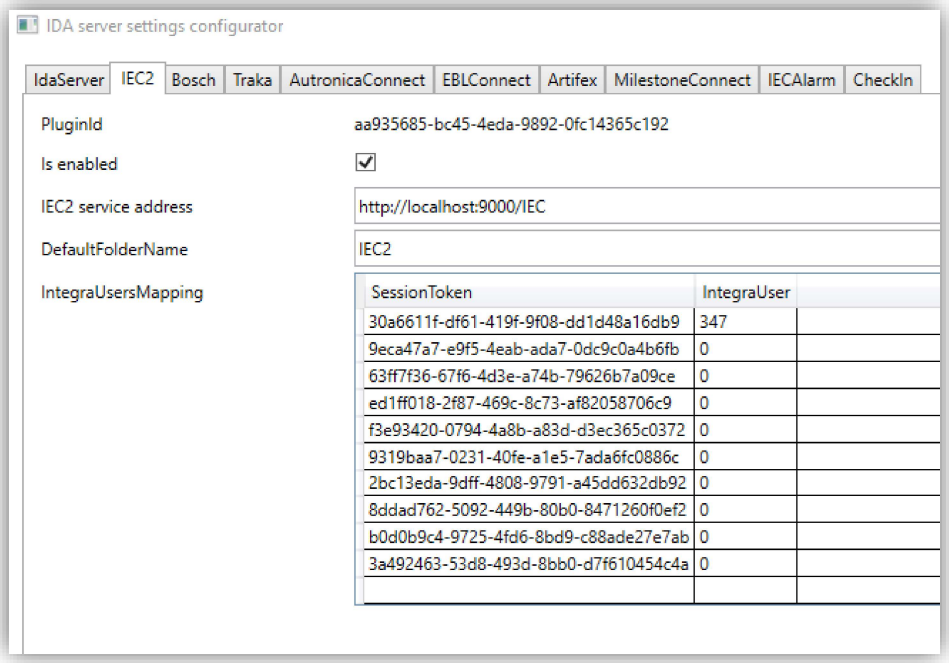
For *Basic license* you will have access to 23 different methods. For more detailed description you must create a document from the *WSDL* file.

3.1.6 Generate WSDL file

3.1.6.1 General Description

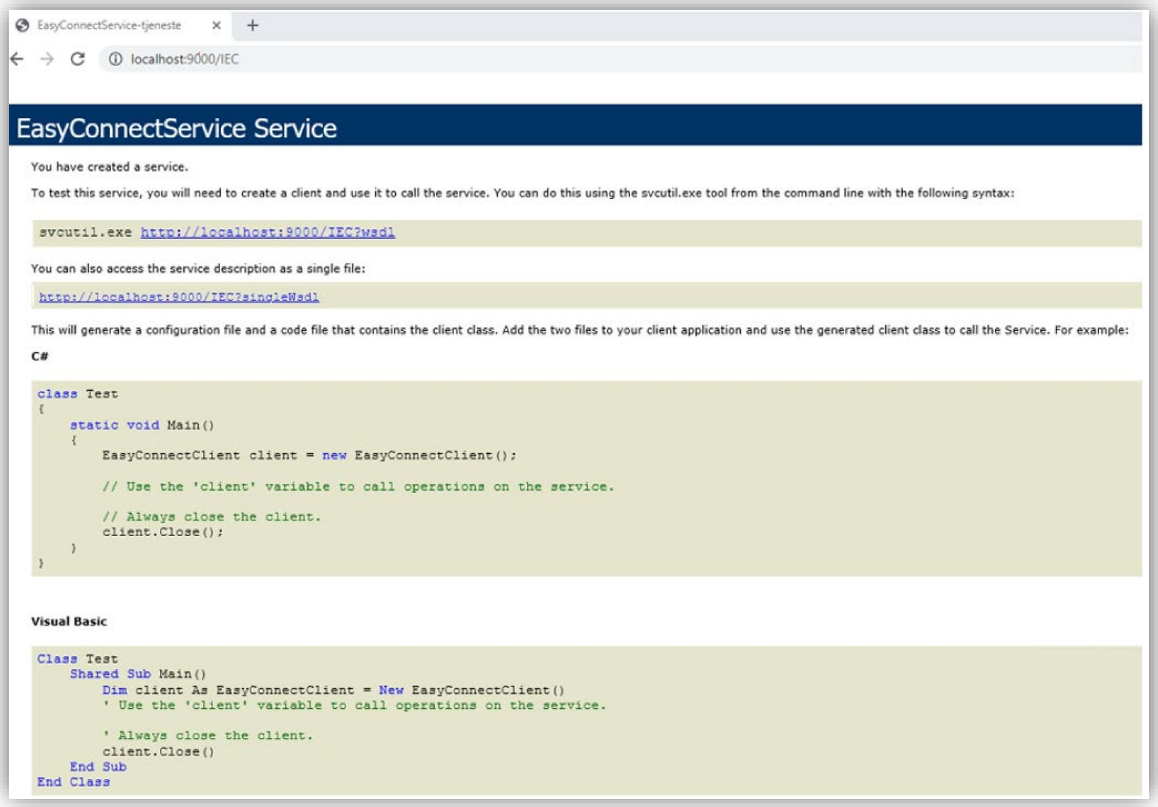
There is possible to generate a *WSDL* file from the browser which you also can use to create a describing document in *html* format by using a 3rd party *SOAP* client (e.g. *SOAPUI* by Smartbear), the *html* document will describe all supported methods.

First you need to open *IDA Server settings configurator* GUI to be able to get the endpoint address (*IEC2 service address*) as shown below. The *IDA Server settings configurator* is located here *C:\Program Files (x86)\Integra\IDA\ Ida.Server.Config.exe* (*Run as Administrator*)



3.1.6.2 Generate the WSDL file from the browser

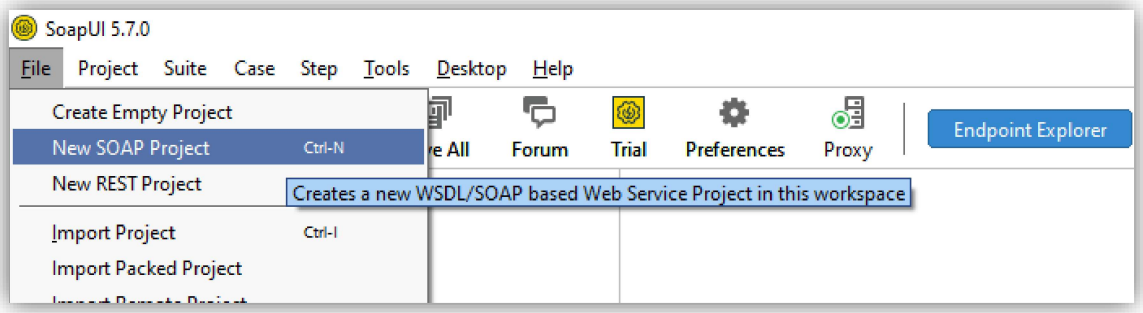
Copy the endpoint (*IEC2 service address*) into your browser address bar as shown below.



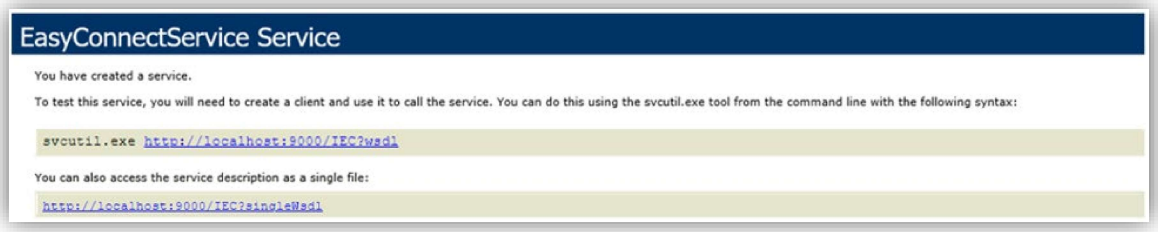
From the page above you can directly download a single *WSDL* file by right clicking on the link and save the file as a xml file.

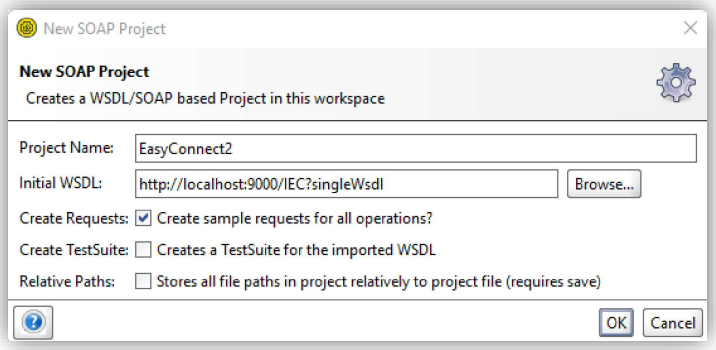
3.1.6.3 Generate SOAP project

To generate SOAP project can one way be to start the *SOAPUI* application (download https://www.soapui.org/) and then create a new *SOAP project* from the *File* menu as shown below.

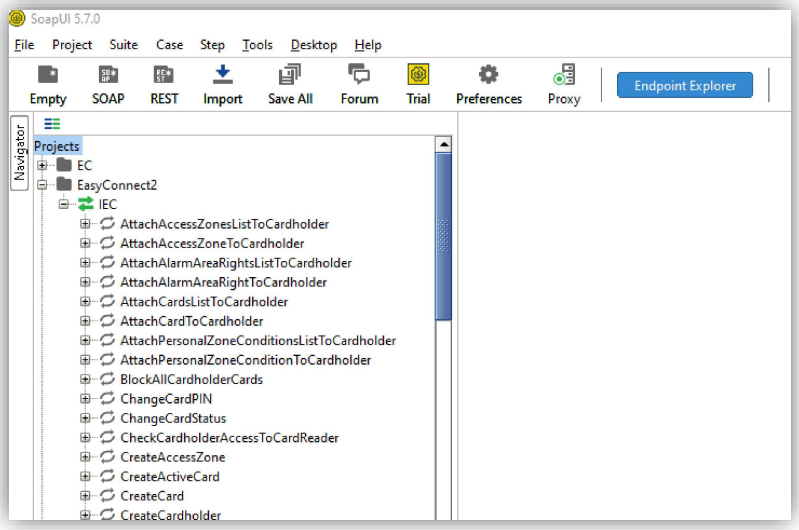


Paste the address (Could be a domain address) from your browser into the "*Initial WSDL*" field as shown below and click *OK*.



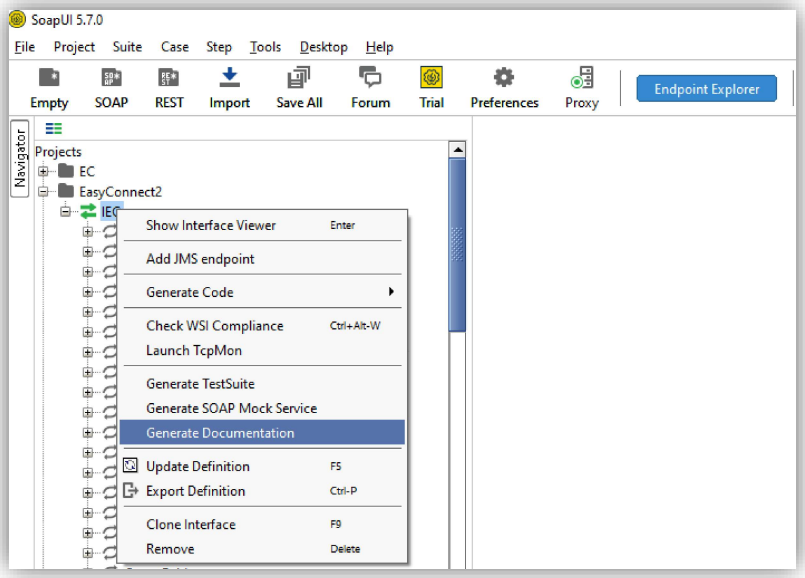


Now you will be able to create test request's from the *SOAPUI*.

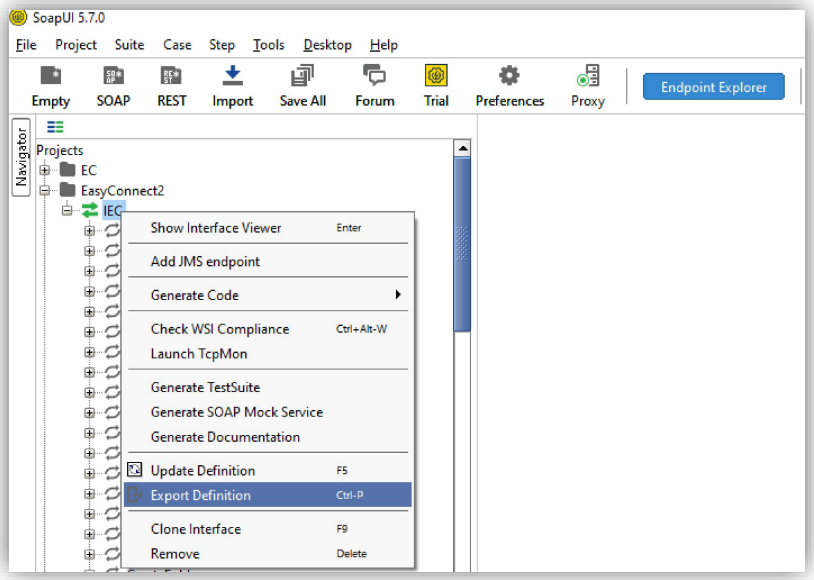


3.1.6.4 Generate a WSDL and HTML file from SOAPUI

To generate a *HTML* file you can right click on the *IEC item* and select *Generate Documentation* as shown below.



To generate a *WSDL* file you can right click on the *IEC item* and select *Export Definition* as shown below.



3.12 Using HTTPS with IDA plugins

In order to guarantee proper security when using IDA plugins that utilize HTTP protocol (Artifex, EasyConnect2/IEC2, IECAlarm), all data transferred between the plugin and web browser/api client should be encrypted. This can be achieved by configuring the plugins to utilize HTTPS endpoints.

3.12.1 Prerequisits

Necessary prerequisite in order to achieve encrypted communication is ownership of SSL certificate. The certificate can be obtained by various ways e.g. create self-signed certificate using command line tools, request certificate via Microsoft Management Console or obtain it from certification authorities (for money, free one can be obtained from Let's Encrypt). We suppose the user who configures HTTPS already has such certificate and it is correctly registered in Windows.

3.12.2 IDA configuration for Artifex

1. Start IDA configuration tool and open Artifex tab
2. Change endpoint address to start with **https** instead of **http** (e.g. https://+:8090, https://artifex:8090 or **Error! Hyperlink reference not valid.**

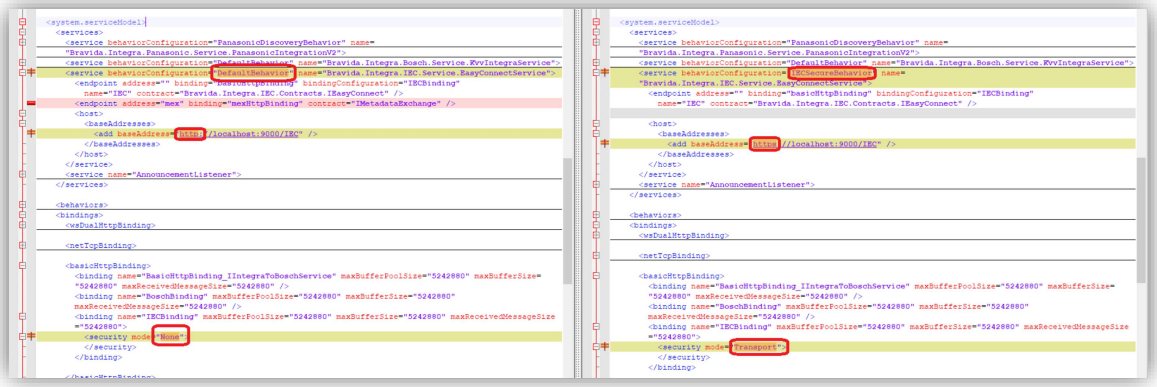
3.12.3 IDA configuration for IECAlarm

1. Start IDA configuration tool and open IECAlarm tab
2. Change endpoint address to start with **https** instead of **http** (e.g. https://+:8070, https://iecalarm:8070 or **Error! Hyperlink reference not valid.**iecalarm.mydomain.com)

3.12.4 IDA configuration for EasyConnect2

1. Start IDA configuration tool and open IEC2 tab
2. Change plugin address to start with **https** instead of **http** (e.g. https://localhost:9000/IEC)
3. Open Ida.server.exe.config file in any text editor and change this:

   For Ida Version 2.1.0-2.5.0



For Ida version 2.5.0 ->

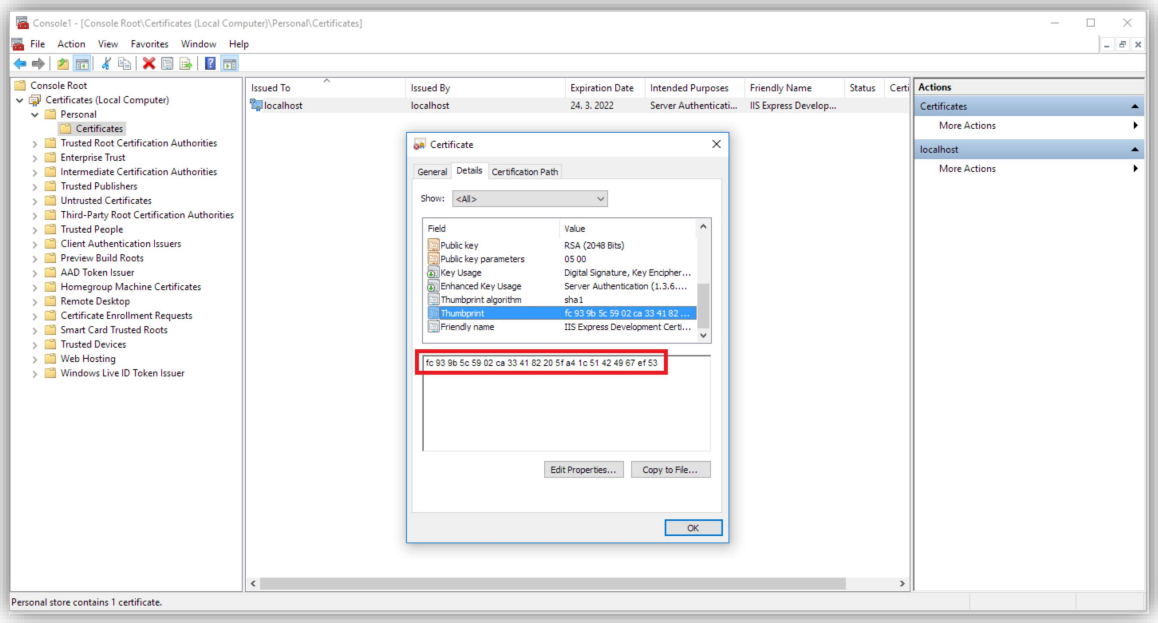
Default (Http):

IECSecureBehavior (Https):

3.12.5 IDA machine configuration

Certificates are strongly tied with an operating system, therefore it is necessary to link the registered certificate with the IDA application itself - specifically to link application TCP port with the certificate.

1. Find the certificate using Microsoft Management Console Certificates snap-in and search for certificate thumbprint



2. Copy certificate thumbprint to any text editor such as Notepad and remove spaces (in this case it will be fc939b5c5902ca334182205fa41c51424967ef53).
3. Register certificate using netsh http add sslcert command

Example:

For Artifex running on port 8090 and the certificate above, the command would be ***netsh http add sslcert ipport=0.0.0.0:8090 certhash=fc939b5c5902ca334182205fa41c51424967ef53 appid={00000000-0000-0000-0000-000000000000}***

For EasyConnect2 running on port 9000 and the certificate above, the command would be ***netsh http add sslcert ipport=0.0.0.0:9000 certhash=fc939b5c5902ca334182205fa41c51424967ef53 appid={00000000-0000-0000-0000-000000000000}***

Info:

The appid parameter is informational only and accepts any GUID value. It is useful for administration of certificates, so the administrator can find easily which application has registered give port and certificate.

4. Start IDA and open Artifex or EasyConnect2 using new URL with https at the beginning.

Example addresses for settings above

Artifex - https://localhost:8090

EasyConnect2 - https://localhost:9000/IEC?singleWsdl (shows WDSL schema)

3.12.6 IDA using Web proxy

It is also possible to configure a web proxy for encrypted communication with IDA plugins using third party tools as NGINX or others.

Please contact support@systemhousesolutions.com for more information regarding this.