SIGINT Systems

HARVESTER COMINT Suite

Version 2.0

Traffic Analysis Workbench
User's Manual

SIGINT Systems

Signals Intelligence Collection Software

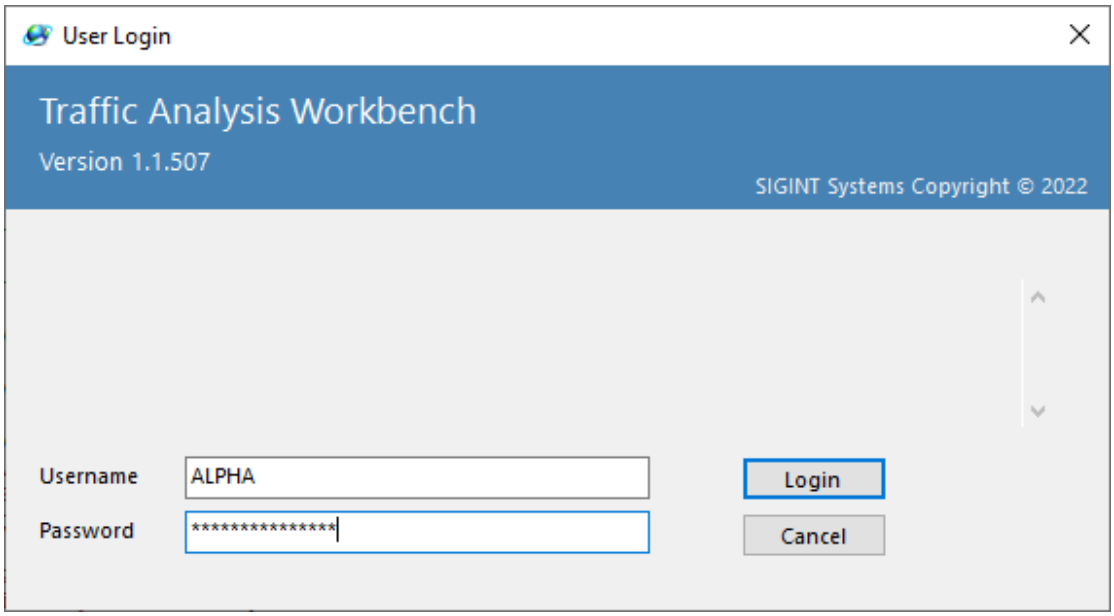
Document Version Control

Version	Description	Date
1.0	Initial Draft	10-Aug-2022
1.1	Minor Corrections	13-Sep-2023
1.2	Case File amendments	27-Jun-2024
1.3	Minor Corrections to TEXTA Database	14-Sept-2024
2.0	Amendments, corrections and Log Analysis Added	16-Jan-2025

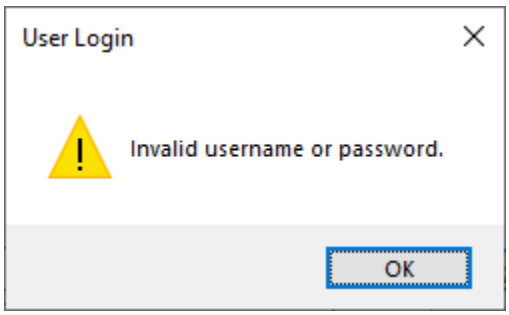
1. Logging Into Traffic Analysis Workbench

When you run any of the HARVESTER COMINT Suite applications, you will first be presented with the standard login screen. The screen will display the name and version of the application being run. It may also display user security warnings and caveats. These notifications are maintained by your system administrator.

The screen will ask you to enter your username and password and once entered, you should click the Login button to proceed with the login process.

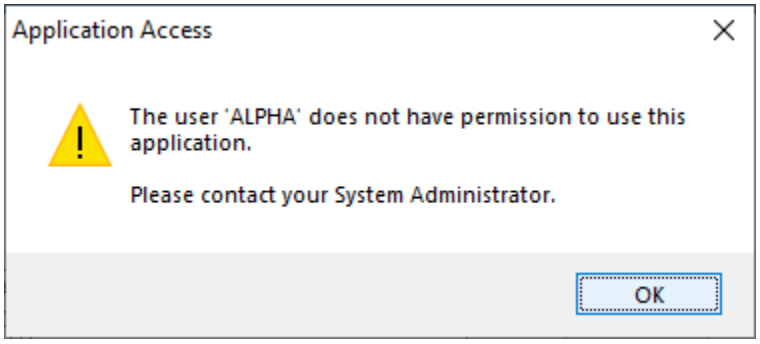


If both username and password are correct, the application will open as normal. However if either or both credentials cannot be authenticated, the following warning message will be displayed:

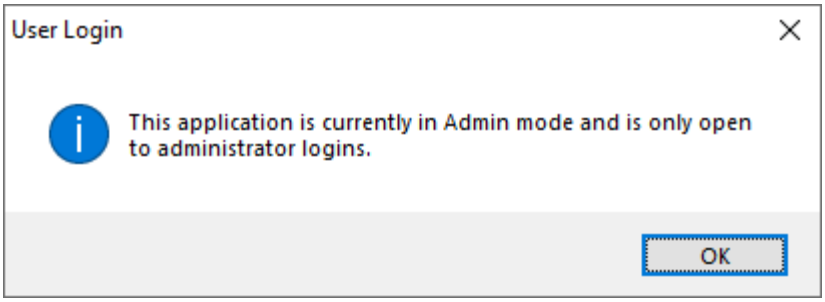


Ensure that both your username and password have been entered correctly and try logging in again. If you are still denied access, contact your system administrator.

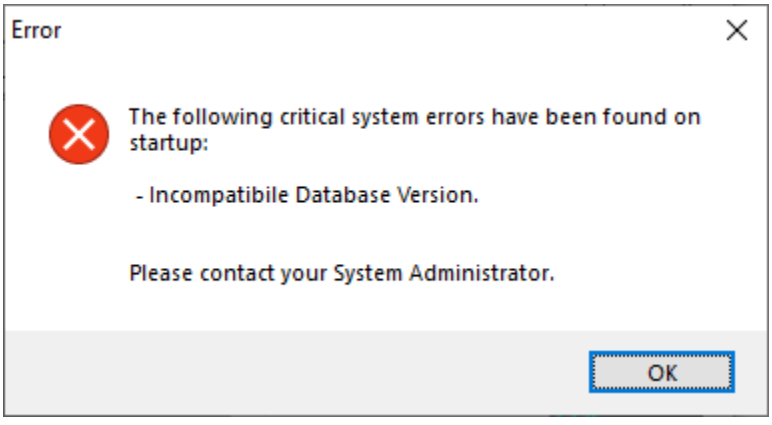
If your credentials are correct and authenticated by the system but you do not have user permissions to run the application, then the login process will be halted and you will be presented with the following warning:



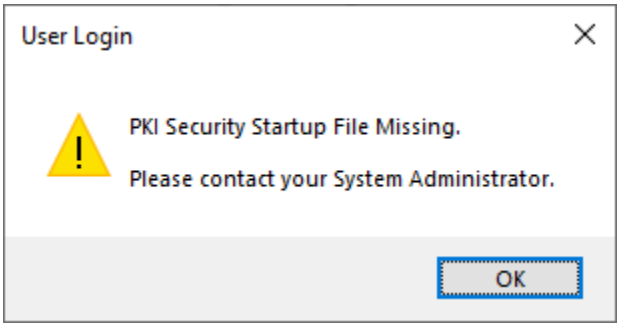
Applications may also be disabled by system administrators for maintenance or other operational reasons. If the application you are trying to log into has been disabled, you will see the following warning:



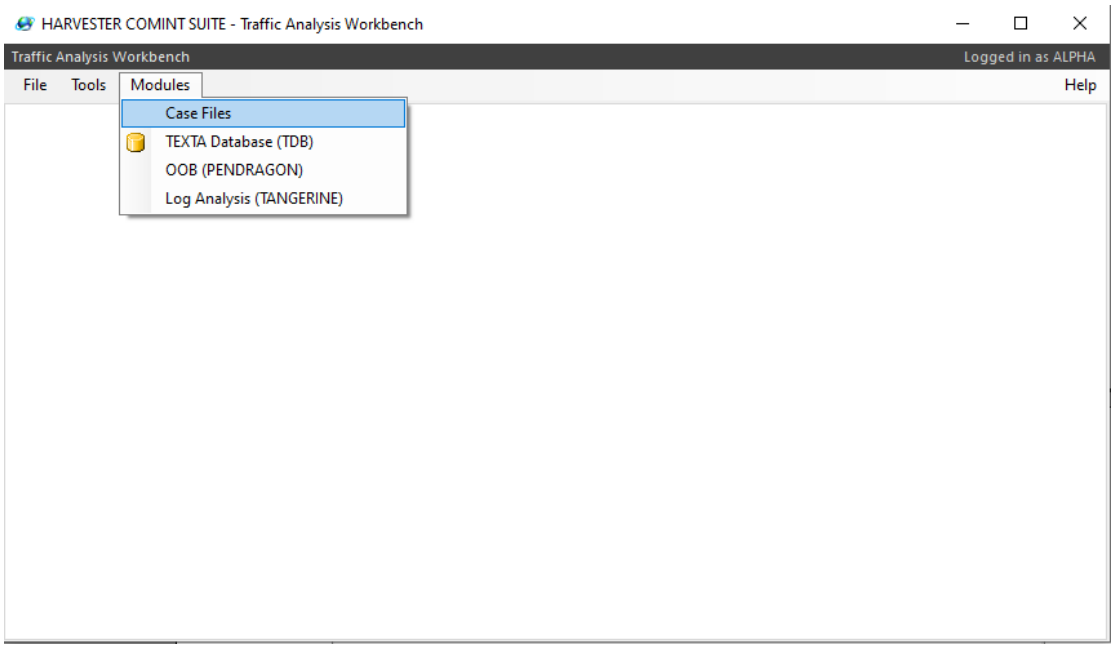
If the HARVESTER COMINT Suite database has recently been upgraded by a System Update and you have not yet deployed updated applications, logging into an application may result in the following warning being displayed:



If the application is started and no PKI security file is present, then following warning message will be displayed. Contact your system administrator and request the *harvester.pki* file to be added to your local installation.



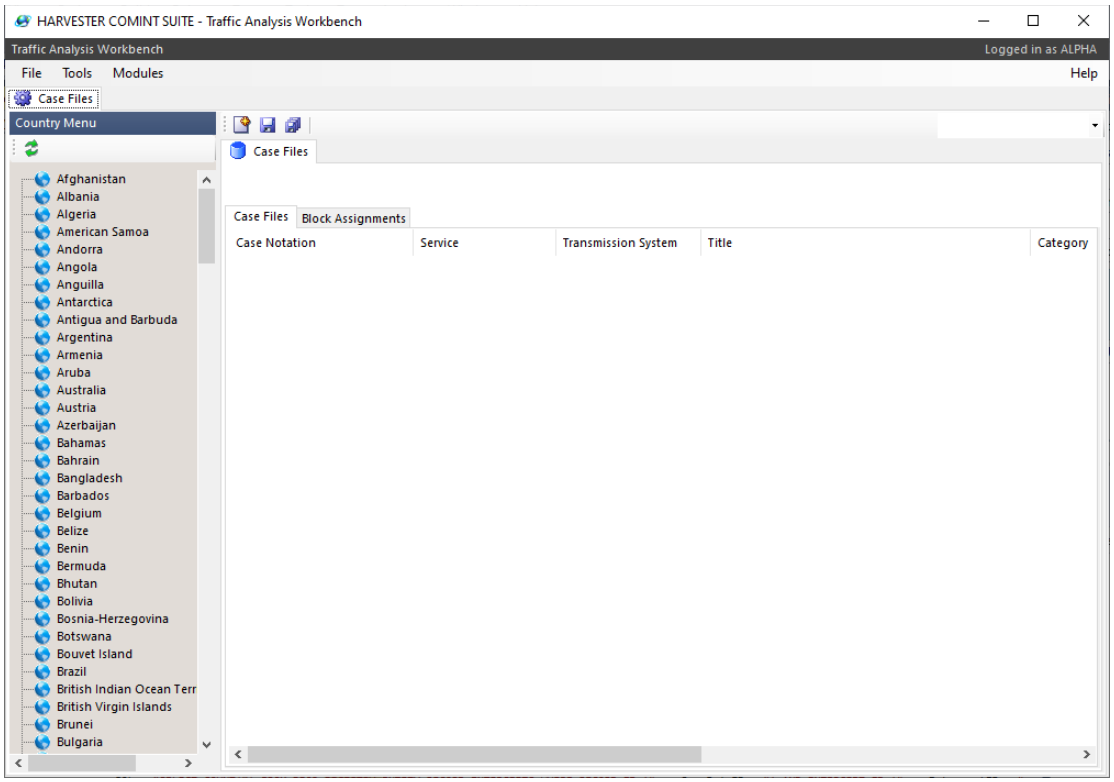
The Traffic Analysis Workbench is a module based application that currently provides access to four separate modules: Case Files, TEXTA Database, Order of Battle and Log Analysis.



Click on the Modules menu and select an option to open a module.

2. CASE FILES

The Case File module is an extremely useful repository for the recording of all the details associated with the operation and behaviours of individual communications nets and networks.



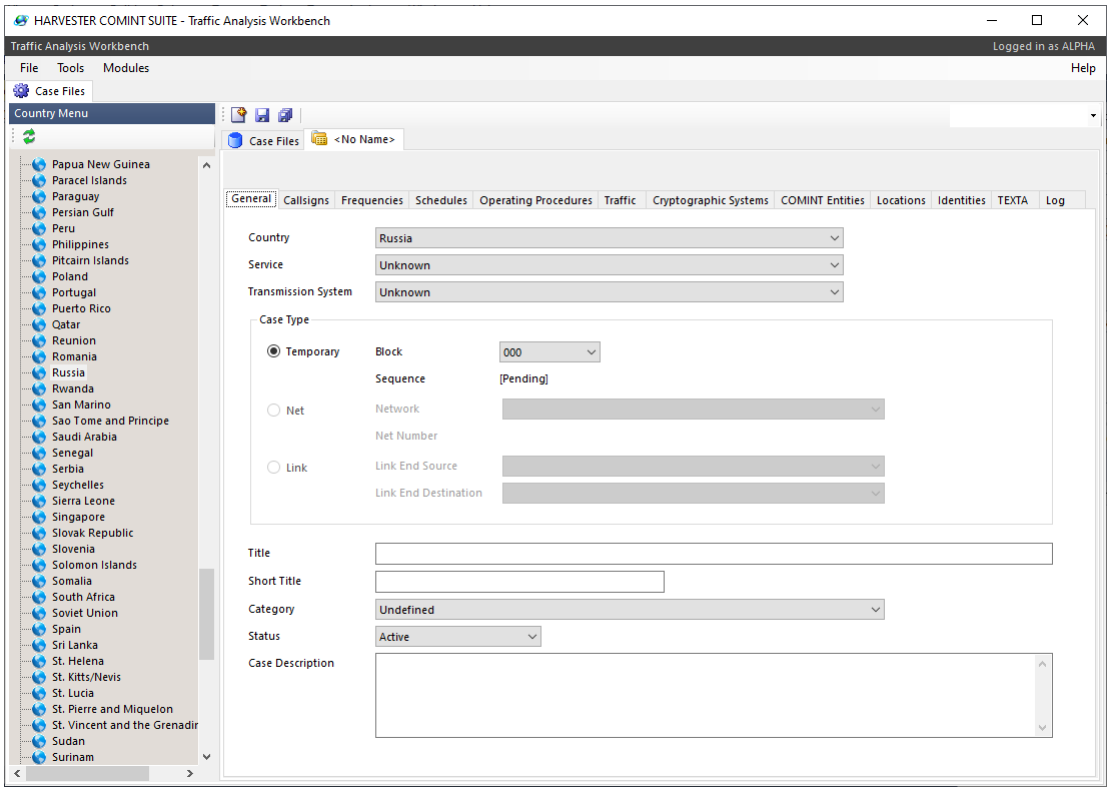
Each Case File record is divided into twelve sections, each dealing with a specific function or behaviour of the network or net being described. These sections are:

- General
- Callsigns
- Frequencies
- Schedules
- Operating Procedures
- Traffic
- Cryptographic Systems
- COMINT Entities
- Locations
- Identities
- TEXTA
- Log

Select the country of interest in the Country Menu list then click the New Temporary Case File button in the toolbar to create a Case File record. The selected country will be automatically populated in the new window.

2.1 General

The General section allows you to record details about the identify and purpose of the network being analysed such as the country of origin, the national service responsible for the network and the types of transmissions that the network uses.



Note that all locally created case files are initially designated as Temporary. Select the appropriate Assignment Block for the case file that best suits the associated collection programme and the sequence number will be automatically generated when the case file is saved.

Enter a title of the network, a short title for quick reference and a brief description of the network. Case files are initially set to the Active status but this can be changed at any time. There are three status options:

1. **Active** – assigned to a Case File that currently reflects the network

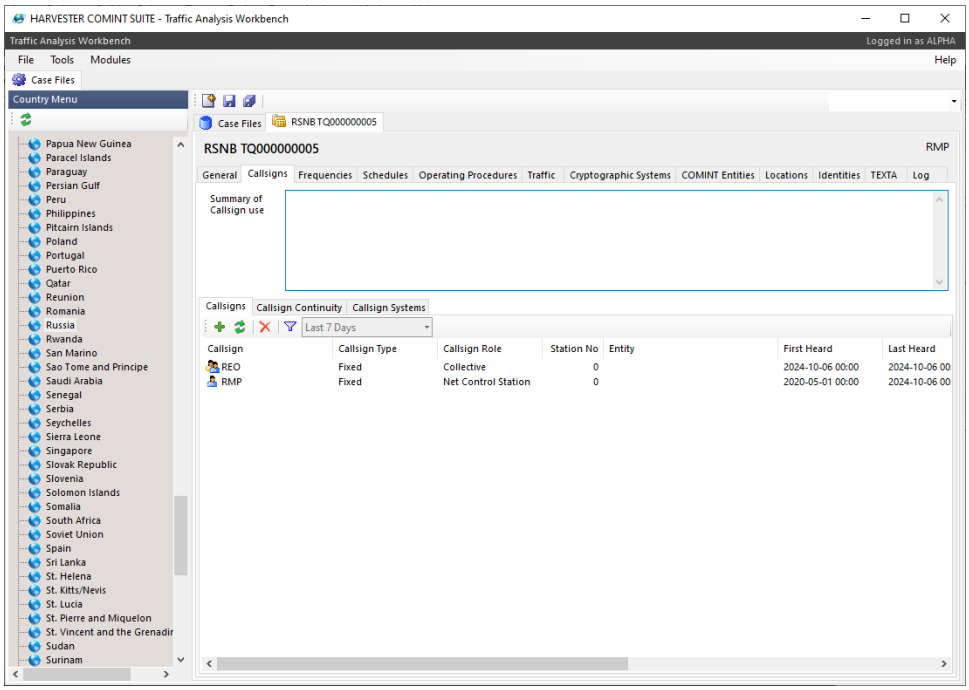
2. **Cancelled** – assigned to a Case File that has been superseded by another Case File

3. **Suspended** – assigned to a Case File that no longer reflects the network

Once all the relevant information has been entered, click the Save button on the toolbar to save the case file.

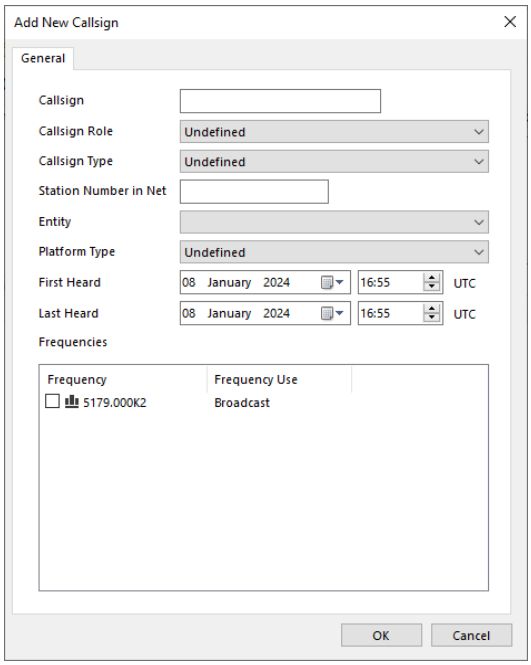
2.2 Callsigns

The Callsign section allows you to record observations about callsign usage, callsign continuity and the typical types of callsigns used by stations on this network.



2.2.1 Callsigns

Select the Callsigns tab and click the Add button on the toolbar to open the Add New Callsign window:



Callsigns are an essential means of identification within any network or net therefore being able to record the types of callsigns in use is a critical tool in the analysis of a network. Callsigns may be fixed, making stations easier to follow and identification much more straightforward, or they could be follow a daily changing random pattern. Whichever method a network uses, it is essential to understand callsign habits and be able to recognise them. This part of the callsign module will allow you to record callsigns by both days of use and the frequencies on which they appear.

Useful fields to note here are:

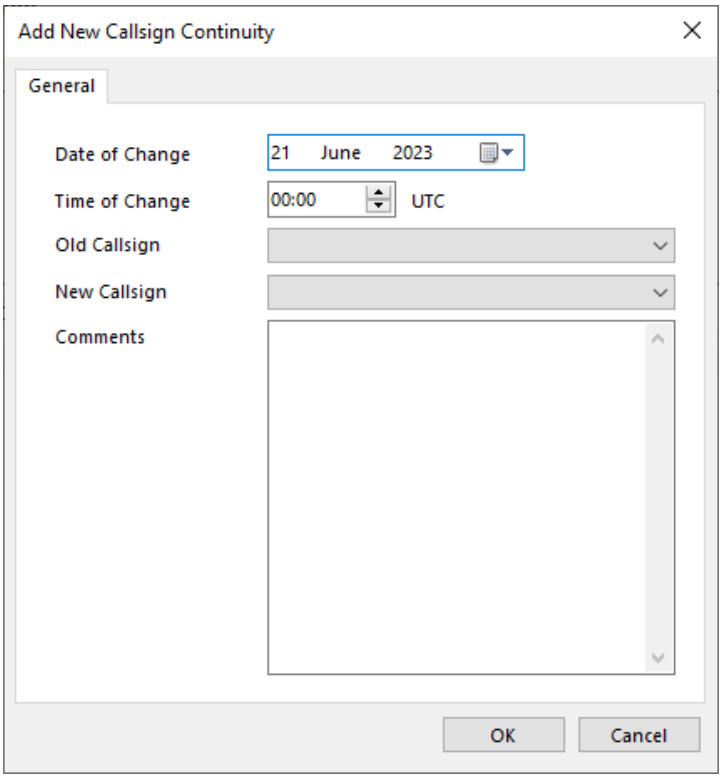
1. **Station Number in Net**. This number reflects that order in which out stations are called up in a network. In some networks, the control station will call up out stations in the same physical station order, irrespective of the callsign order. In such cases, the station number in the net becomes the key to callsign continuity.

2. **Entity**. This dropdown box is automatically populated with all the entities added under the COMINT Entities tab (See Section 2.9)

3. **Frequencies**. This box automatically lists all the frequencies that have been added under the Frequencies tab (See Section 2.3)

2.2.2 Callsign Continuity

Select the Callsign Continuity tab and click the Add button on the toolbar to open the Add New Callsign Continuity window

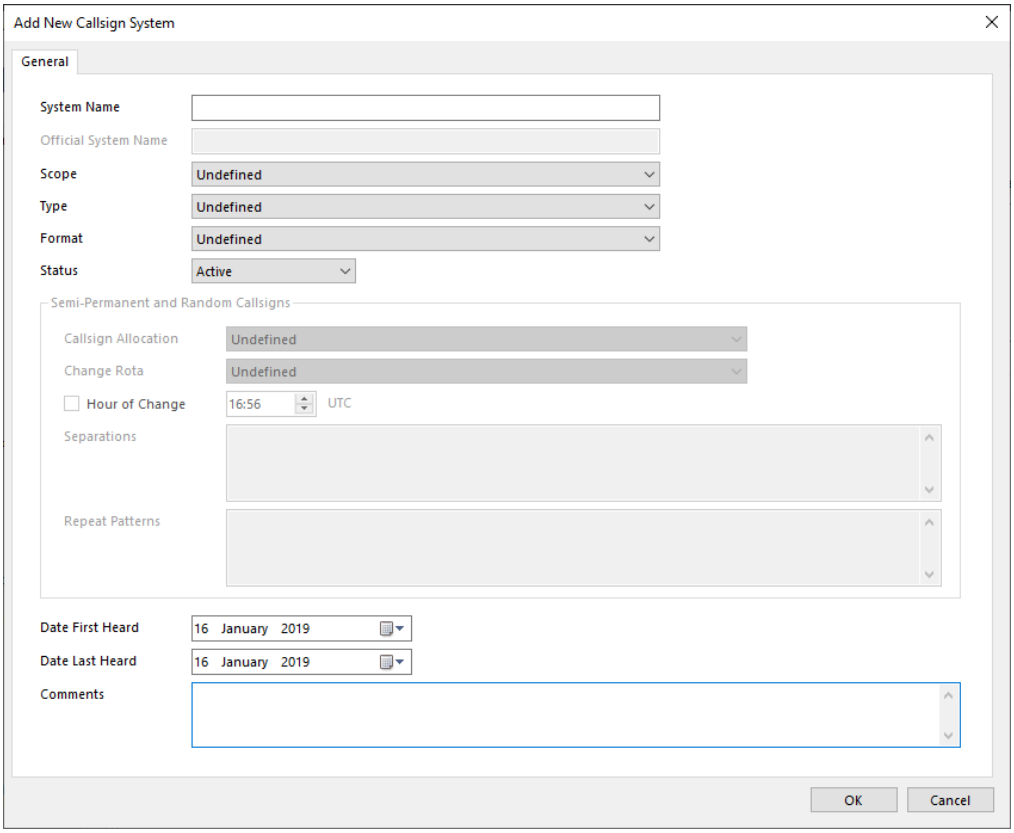


For random and semi-permanent callsign systems, callsign continuity is an important step in attempting to understand the underlaying system being used to generate callsign series, whether they are taken from a book of callsigns or whether they are generated by cryptographic method. The first step in this process of analysis is the collection of as many consecutive daily examples of callsign changes.

Enter in the date and time of the callsign change as well as the old callsign and the new callsign then click the OK button to save the record.

2.2.3 Callsign Systems

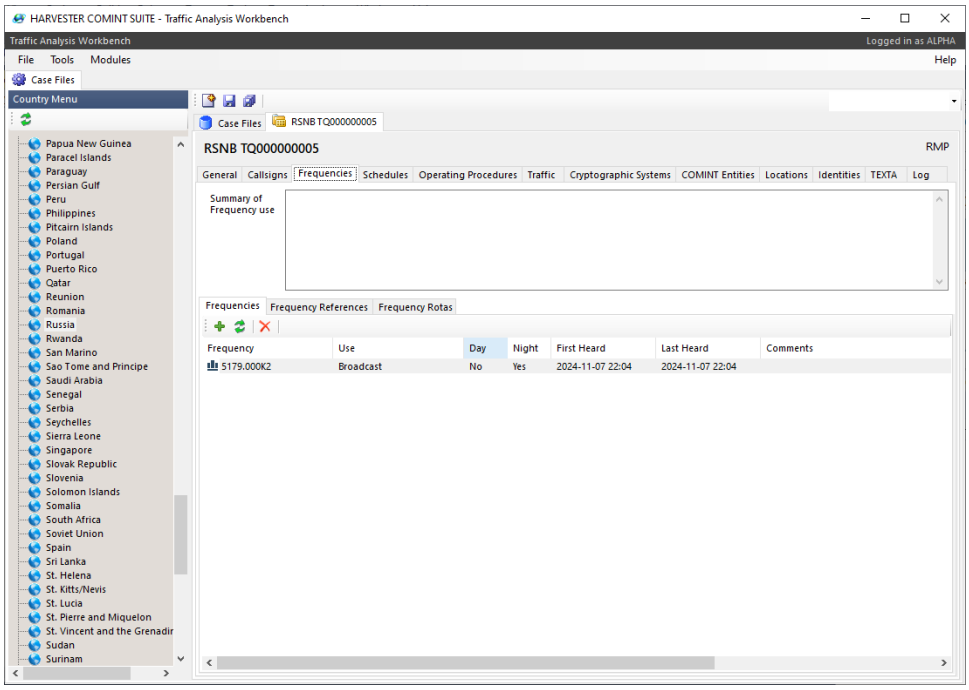
Select the Callsign System tab and click the Add button on the toolbar to open the Add New Callsign System window



Analysis of callsign behaviour within a network will very quickly reveal the type of callsign system that is in use. In most cases, a network will utilize only one callsign system but there any many exceptions where two or more callsign systems are all in operation at the same time. Use the Callsign System window to record all the characteristics of each callsign system in operation then click the OK to save the record.

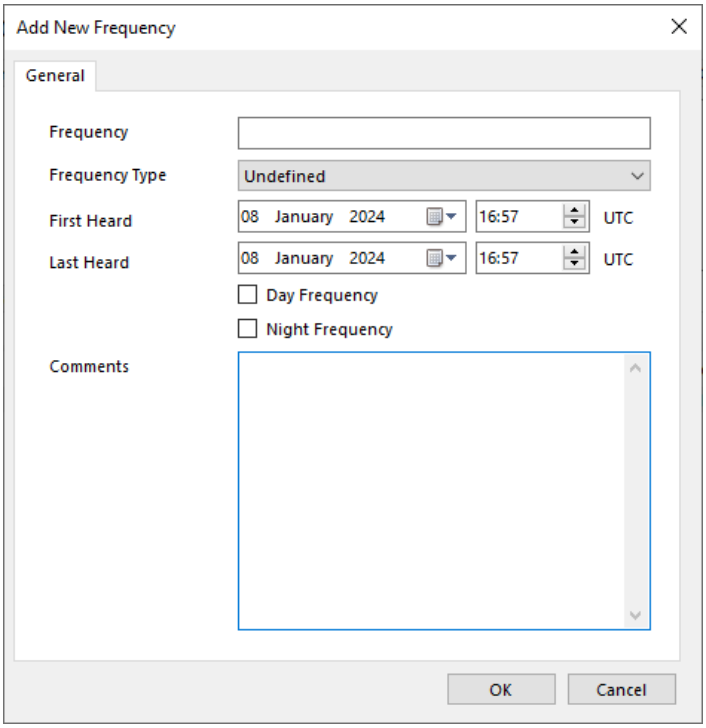
2.3 Frequencies

The Frequencies section allows you to record the various frequencies used by stations in this network.



2.3.1 Frequencies

Select the Frequencies tab and click the Add button on the toolbar to open the Add New Frequency window.



Enter the frequency and select the appropriate frequency type that best describes the frequency's use. Frequency use falls into four categories:

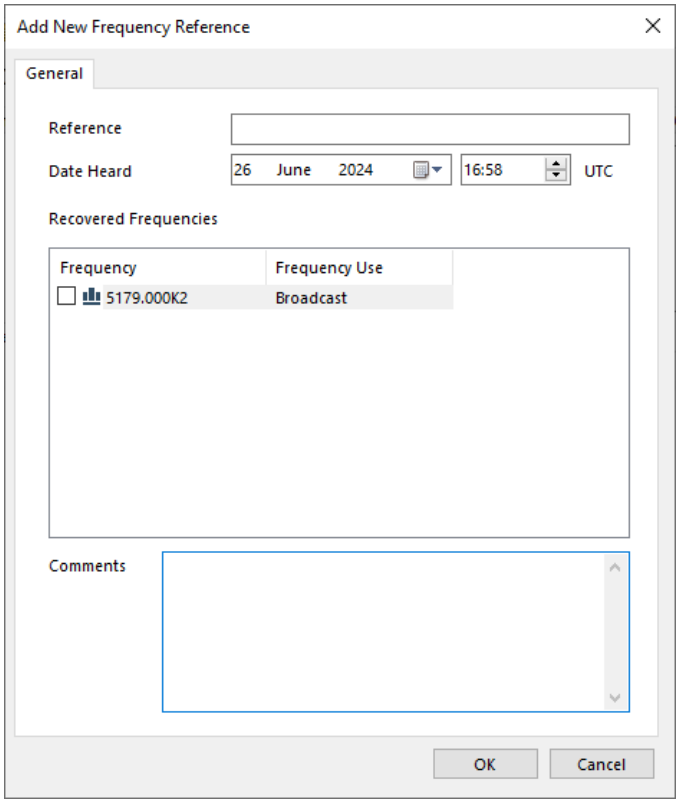
- **Broadcast** – These are frequencies that only support one way transmissions, such as weather stations, fleet broadcasts and analogue pager systems.
- **Net Control Station** – These are frequencies that only support the net control station in a duplex frequency arrangement.
- **Out Stations** – These are frequencies that only support out stations in a duplex frequency arrangement
- **Simplex** – These are frequencies that support both the net control station and any out stations

NOTE: Frequencies entered here will be used throughout the Case File record to populate lists of operating frequencies.

Once the challenge and authentication, and any supporting information has been added, click the OK button to save the record.

2.3.2 Frequency References

Select the Frequency References tab and click the Add button on the toolbar to open the Add New Frequency Reference window.



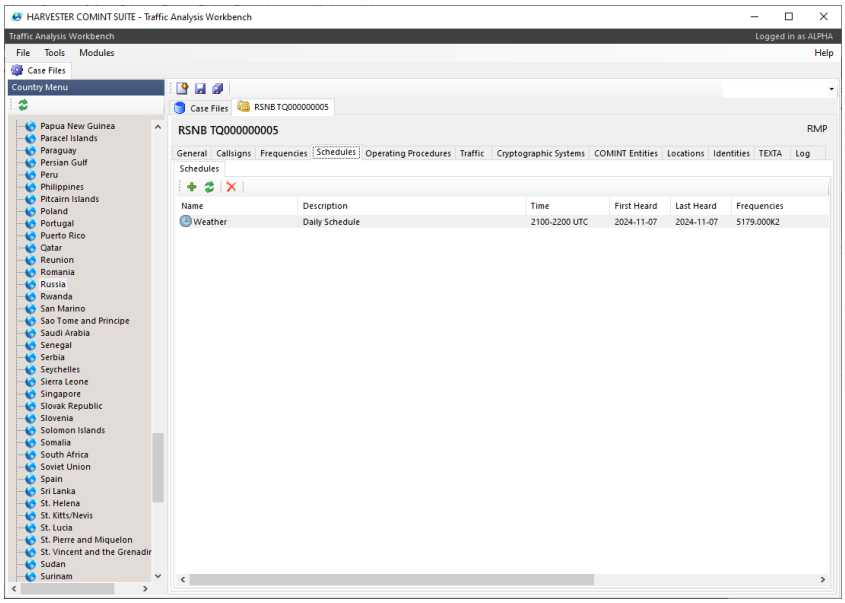
For reasons of brevity and security, many networks may be refer to operating frequencies by some arbitrary code or reference rather than pass the actual dial frequency. The reference may actually be a pre-programmed channel number or a pre-defined channel designator but it could also be an encrypted version of the frequency. In many cases, channel numbers or designators may remain static for extended period of times and these may be determined over time however encrypted frequency references may change on a daily basis and without knowing the corresponding frequency, maintaining continuity on the network following a frequency change can be problematic. It is therefore essential that some attempt to understand a network's scheme of frequency references be made.

Enter any frequency reference that is heard along with the date and time it was used. Add the recovered frequency if known and any other supporting information. Even if the frequency (or in some cases, the frequency pair) cannot be recovered, it is always worth recording the frequency reference for analysis and in case the operating frequency for that exact same transmission is discovered at a later date.

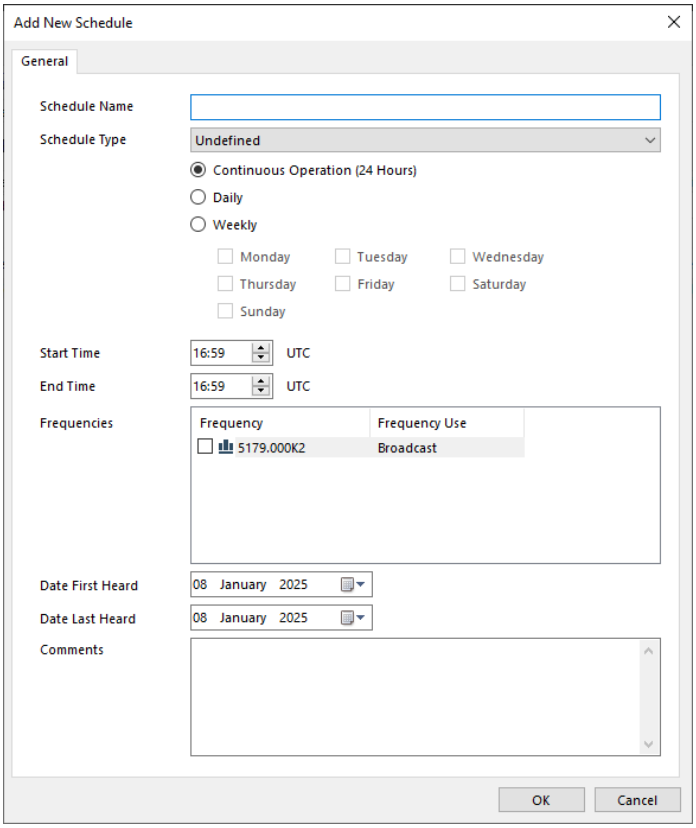
Click the OK button to save the record.

2.4 Schedules

The Schedules section of Case Files allows you to record the working schedules for stations in the network under analysis.



Click the Add button on the toolbar to open the Add New Schedule window.



Determining a network's operating schedules provides both valuable details of the operating procedures of the network and also important data for the management and planning of collection assignments against the network.

Networks may operate numerous schedules combining broadcast-only components as well as station to station exchanges. Schedules may be limited to a few minutes each day or may operate 24 hours per day over a wide range of frequencies. Operating times may vary depending on the time or season of year, or from year to year. Additional schedules may be added to support specific events and removed when operation requirements no longer require them.

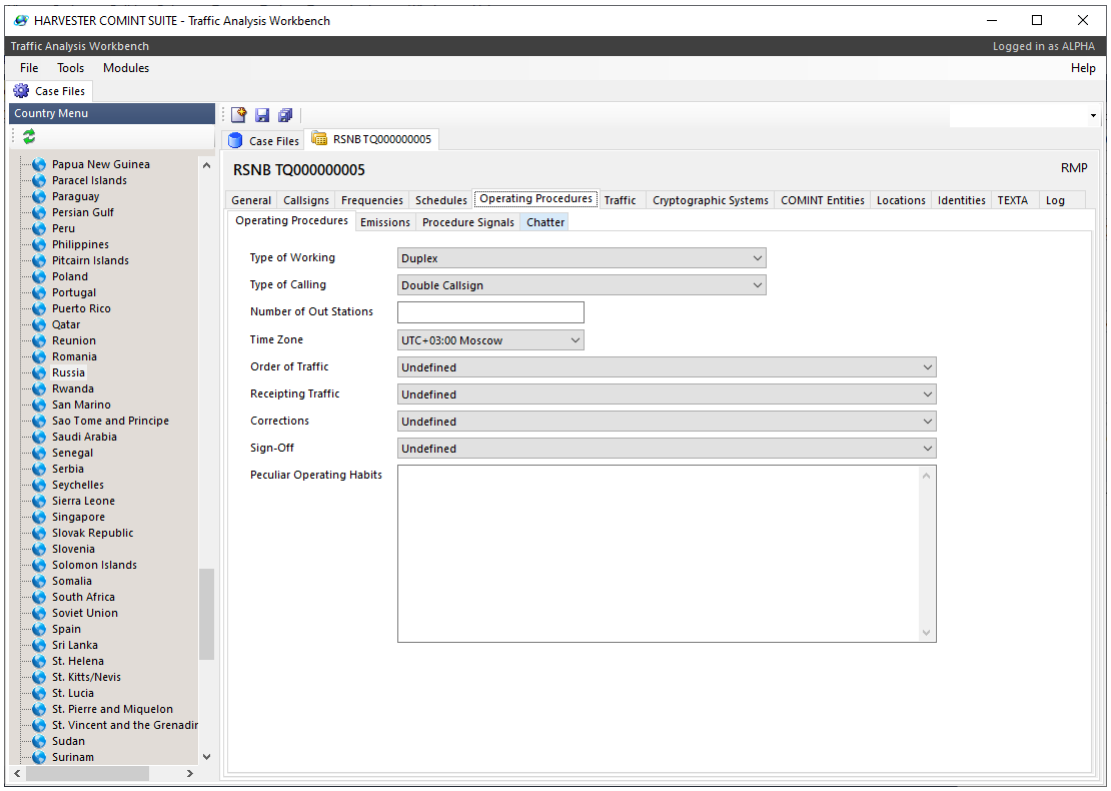
From your analysis of the operating patterns of the network, determine the number of schedules in operation and create a separate schedule record for each one, noting as much information as possible.

Operating frequencies are automatically populated from the case file frequencies entered on the Frequencies tab (Section 2.3)

Once you have entered all the information, click the OK button to save the record.

2.5 Operating Procedures

The Operating Procedures section allows you to record observations about network procedures, operator behaviours and habits by stations in the network.



Select the Operating Procedures tab and provide as much information about that observed procedures of stations in the network. All stations will follow the same procedures and any unusual deviations for that procedure by particulars stations or operators can be noted under Peculiar Operating Habits.

Generally, each network will have a set of procedures that can be categorised as follows:

1. **Type of Working** – describes how the physical net operates in terms of the frequency schemes it uses.
    - Broadcast
    - Complex Receiving
    - Complex Sending
    - Complex Star
    - Duplex
    - Free Star
    - Simplex
    - Star
    - Star with Lateral
    - Undefined

2. **Type of Calling** – describes how stations in the net call each other.
   - Collective Callsign
   - Double Callsign
   - Link Callsign
   - Single Callsign
   - Undefined

3. **Number of Out Stations** – many networks will have a variable number of out stations but others will have a fixed number and this can prove a valuable clue to identification following callsign changes.

4. **Time Zone** – this can often give a clue to the origin of a network though care must be taken as UTC is used by many networks worldwide.

5. **Order of Traffic** – this is almost always in order of priority though can be difficult to assess when single or groups of similar priority messages are sent together.

6. **Receipting Traffic** – this is usually a QSL signal but there are some variations specific to certain networks.

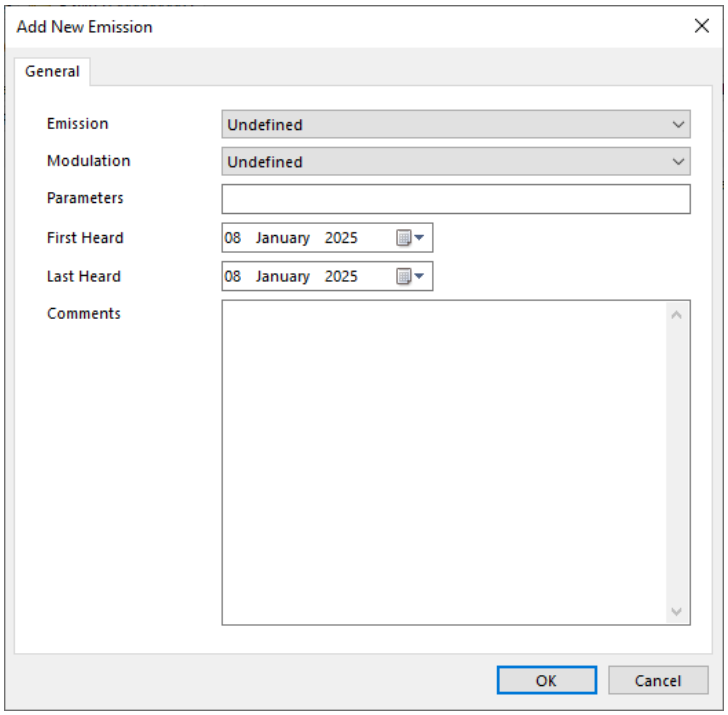
7. **Corrections** – this is more prevalent with voice or Morse communications where errors are more likely. Corrections are less likely in telex messages which are generally pre-prepared. Correction methods are often unique across entire country users which is indicative of well organised training and disciplined operators.

8. **Sign Off** – this can range from a simple QRU to less formal 73.

9. **Peculiar Operating Habits** – this is less obvious with disciplined operators but occasionally an operator will have a very distinctive hand or voice, or may say or send traffic in an unusual manner that is starkly different from other operators or stations.

2.5.1 Emissions

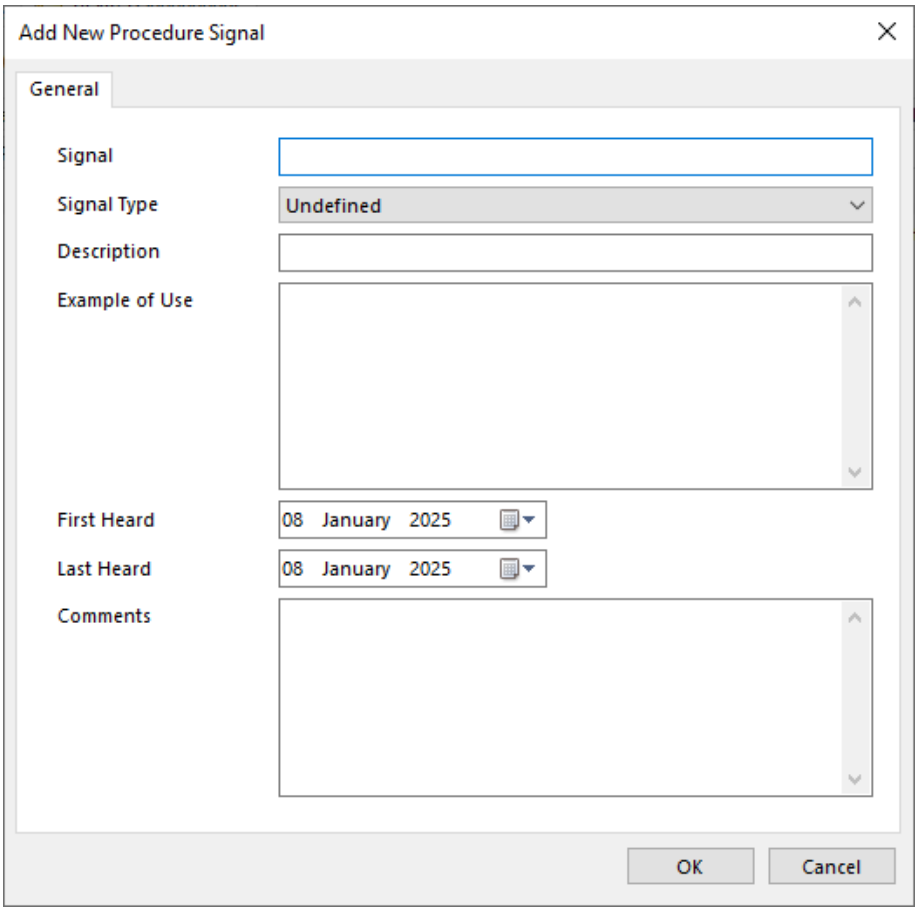
Select the Emissions tab and click the Add button on the toolbar to open the Add New Emission window:



Select emission and modulation types from the dropdown lists. If the emission or modulation type required is not available in the lists, ask your System Administrator to add them to the list. Add emission parameters, if known, and any additional information then click the OK button to save the record.

2.5.2 Procedural Signals

Select the Procedural Signals tab and click the Add button on the toolbar to open the Add New Procedural Signal window:



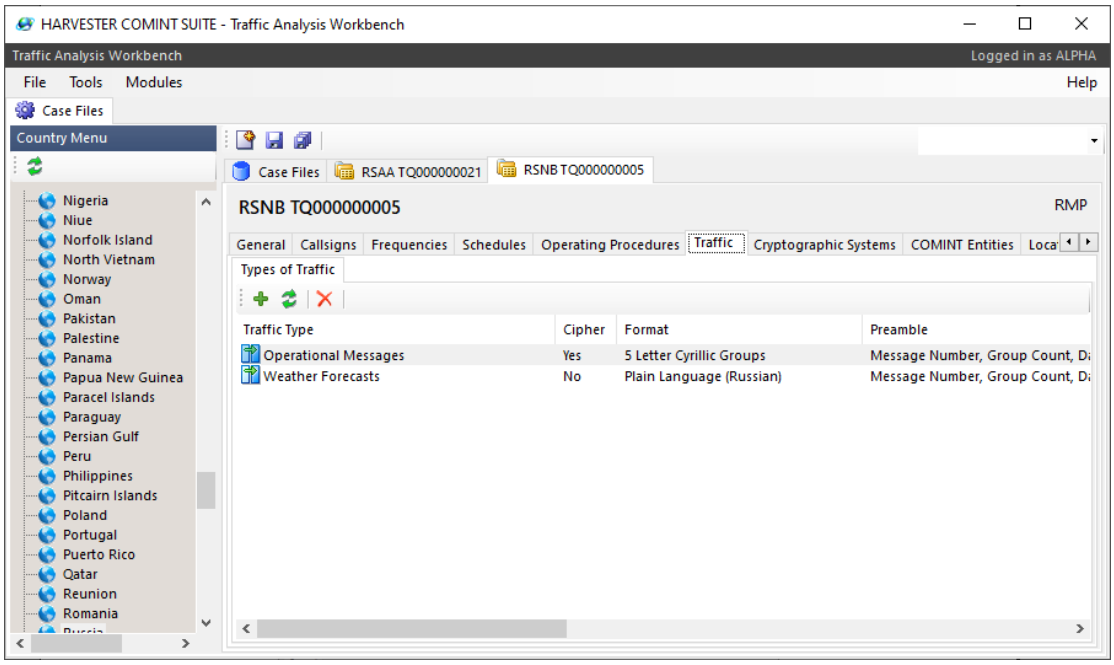
Enter the Procedural Signal and select the signal type from the dropdown list that best describes it. These signal types are

- International
- Q Code
- Undefined
- Z Code

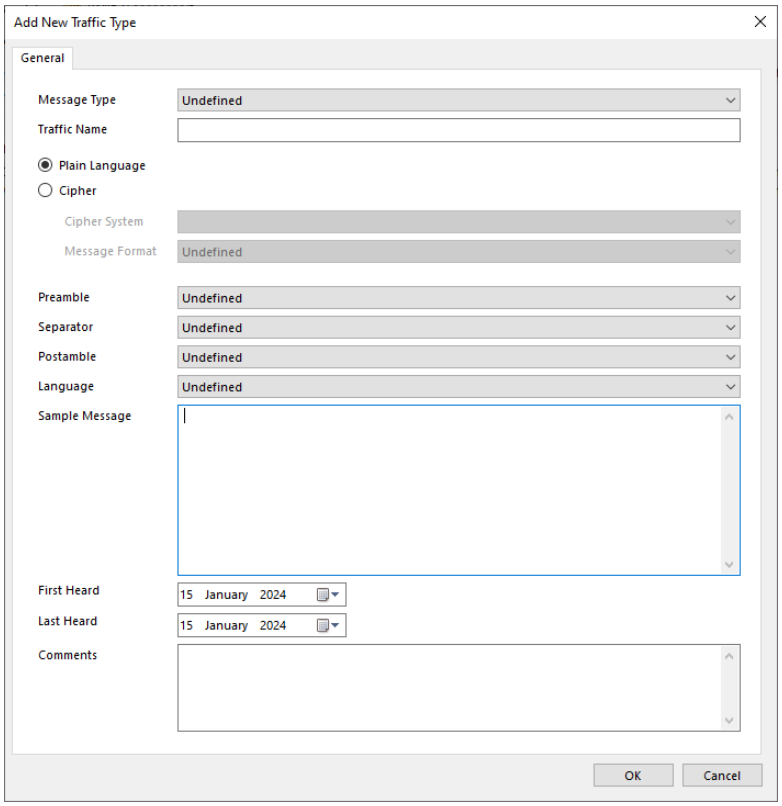
Add a description of the meaning or purpose of the signal. Provide an example of how the signal is used and any additional information then click the OK button to save the record.

2.6 Traffic

The traffic section allows you to record observations about traffic characteristics and the typical types of traffic sent by stations in the network. In most cases, networks use a small number of message types. These types are often similar to other networks so it is essential that each detail about messages types are noted to aid in the identification of any one network.



Click the Add button on the toolbar to open the Add New Traffic Type window:



Message types generally fall into number of general categories

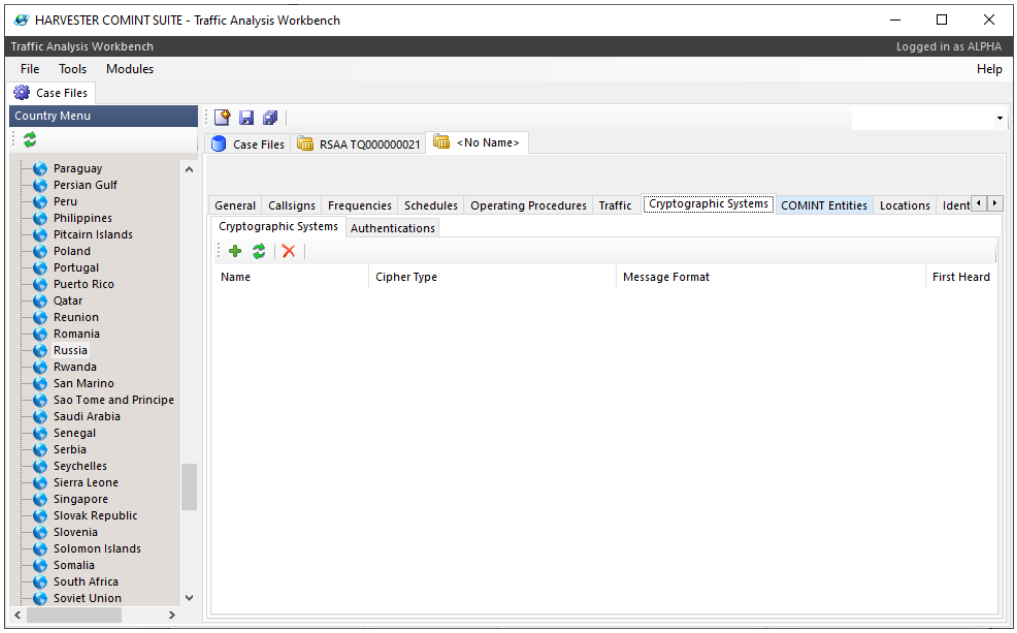
- Navigational Warnings
- Operational Messages
- Radar Tracking Reports
- Situation Reports
- Training Messages
- Undefined
- Weather Forecasts
- Weather Reports

Select the message type from the dropdown and provide a name of the message or broadcast type if know. Note if the message is in plain language or is encrypted, and if encrypted, what type of cryptographic system is being used. These systems can be defined in the Cryptographic Systems tab.

Most messages follow a standard format of preambles, separators and postambles. Select the values that best describe the message, noting the language and add an example of the message.

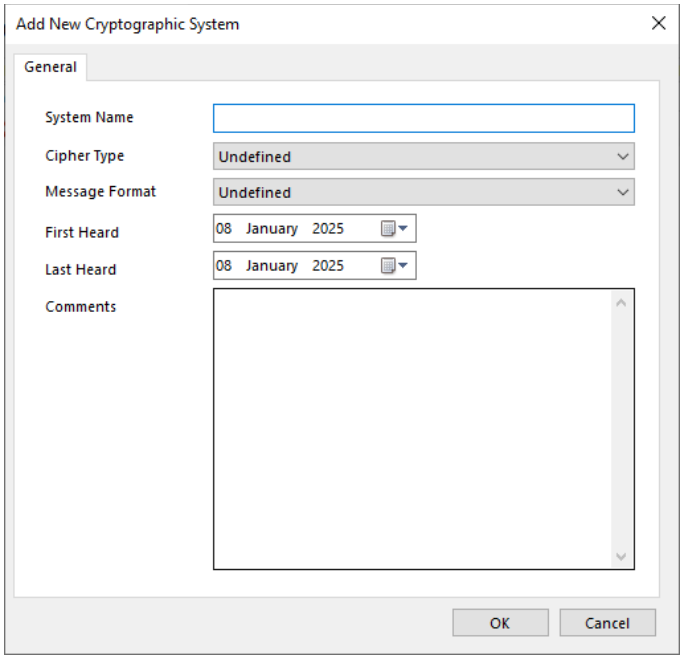
2.7 Cryptographic Systems

The Cryptographic Systems section allows you to record observations about the types of cryptographic systems in use and appearing in traffic send by stations in this network.



2.7.1 Cryptographic System

Select the Cryptographic Systems tab and click the Add button on the toolbar to open the Add New Cryptographic System window:



As the official name of a system is usually unknown, a suitable alias must often to used.

Cipher Types

- Generic Machine Cipher
- Monographic Substitution Cipher
- Polygraphic Substitution Cipher
- Transposition Cipher
- Undefined

Message Formats

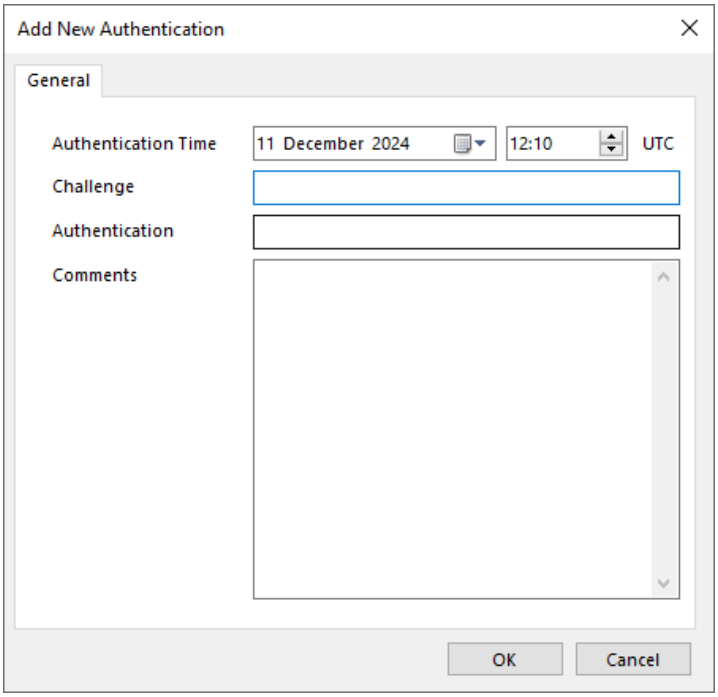
- 4 Digit Groups
- 5 Character Hexadecimal Groups
- 5 Digit Groups
- 5 Letter Cyrillic Groups
- 5 Letter Groups
- Undefined

Select the cipher type and message format that best reflects the cryptographic system then click OK to save the record.

2.7.2 Authentications

Authentication systems form an essential part of net security, and being able to record challenge and authentication parts over time provides a usual resource when attempting to cryptanalytic attack of the system.

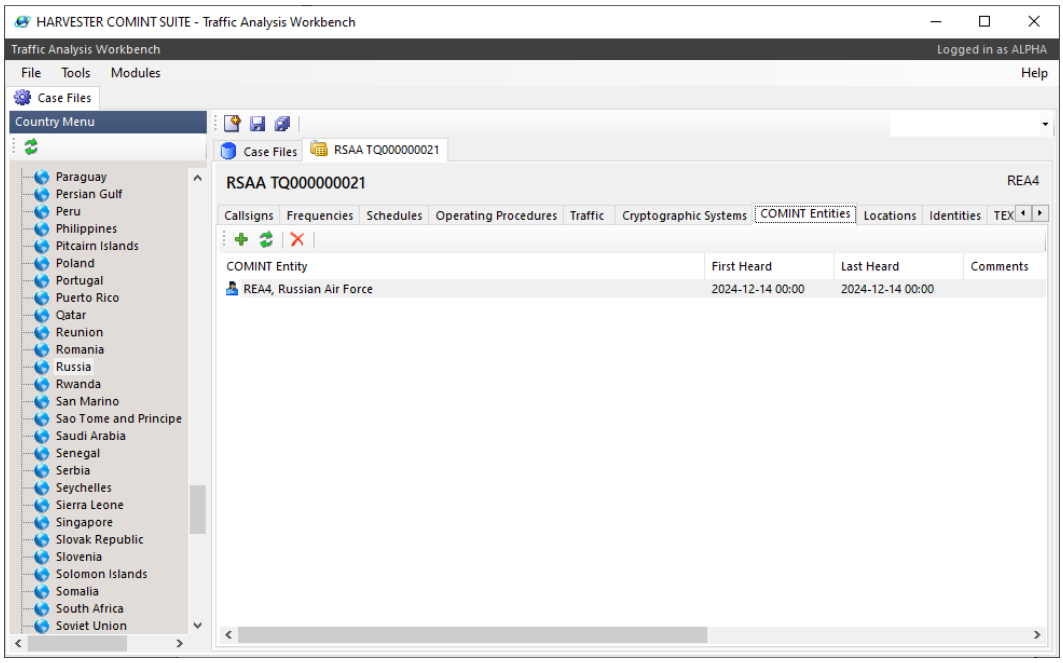
Select the Authentications tab and click the Add button on the toolbar to open the Add New Authentication window:



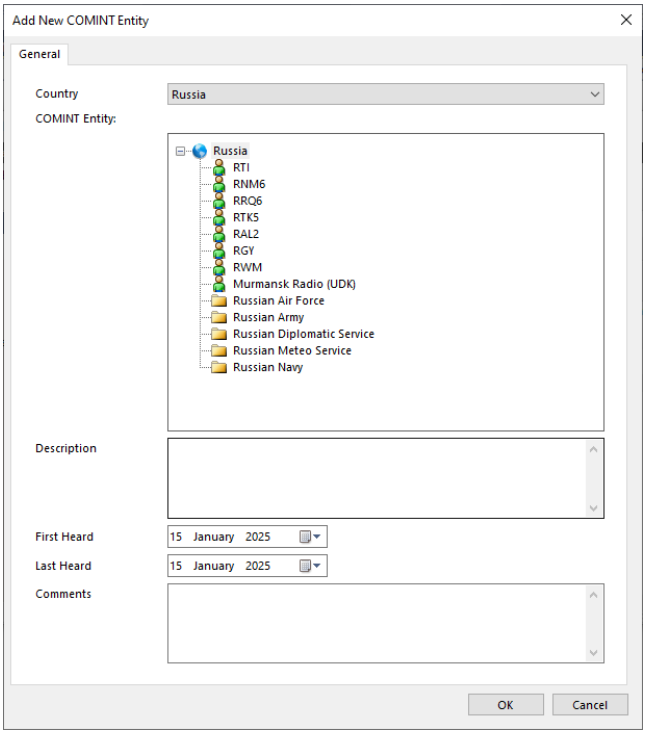
Once the challenge and authentication, and any supporting information has been added, click the OK button to save the record.

2.8 COMINT Entities

The COMINT Entities section allows you to record entities that are connected to individual stations within the network.



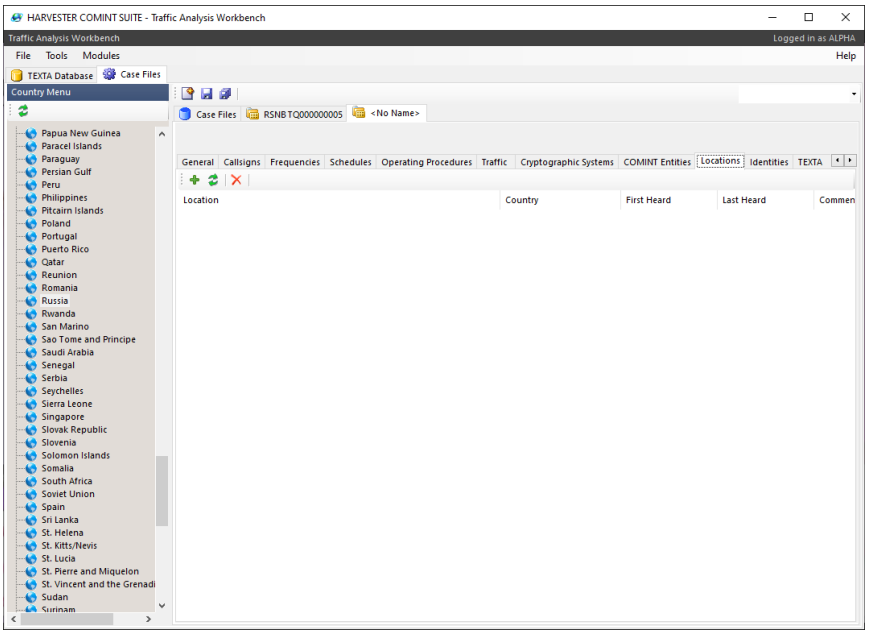
Select the COMINT Entities tab and click the Add button on the toolbar to open the Add New COMINT Entity window



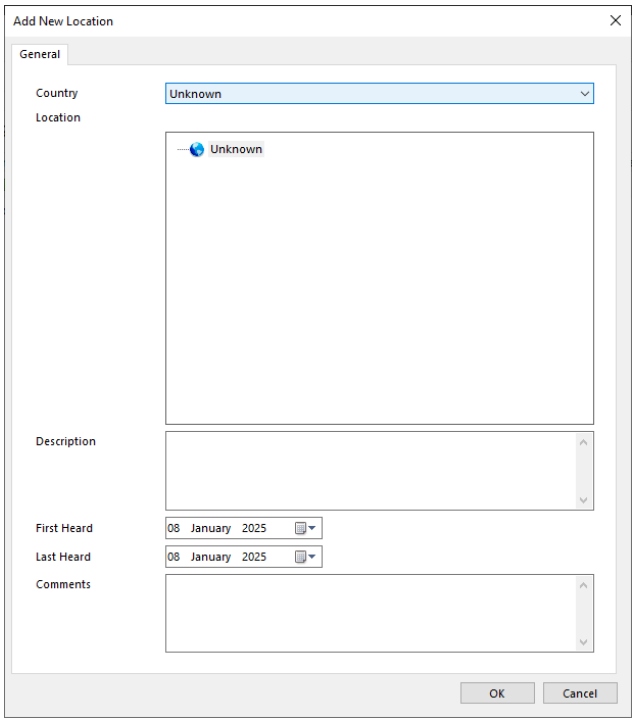
Once the country is selected, the Entity box will be populated with entities from the COMINT Entities module in OOB. Navigate to and select the appropriate entity then click the OK button to save the COMINT Entity.

2.9 Locations

The Locations section allows you to record locations that have been mentioned in intercepts or about have been connected to individual stations within the network.



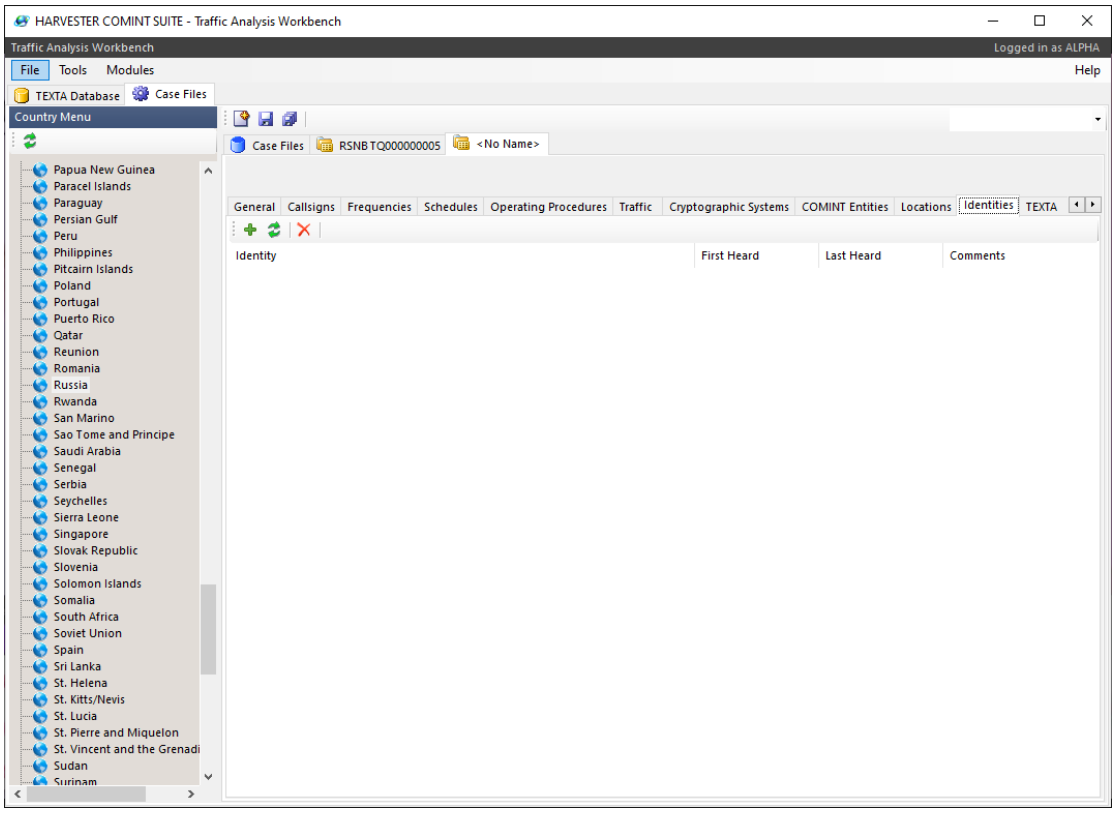
Select the Locations tab and click the Add button on the toolbar to open the Add New Location window



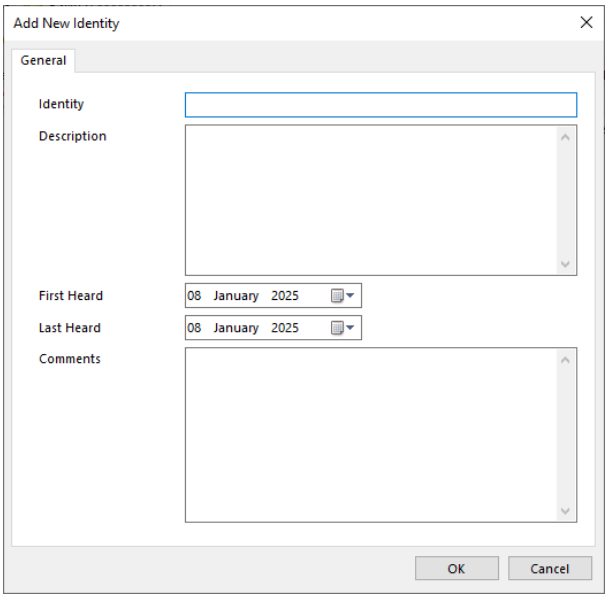
Once the country is selected, the Location box will be populated with locations from the Geolocation module in OOB. Navigate to and select the appropriate location then click the OK button to save the location.

2.10 Identities

The Identities section allows you to record identities that have been mentioned in intercepts or about have been connected to individual stations with the network.



Select the Identities tab and click the Add button on the toolbar to open the Add New Identity window



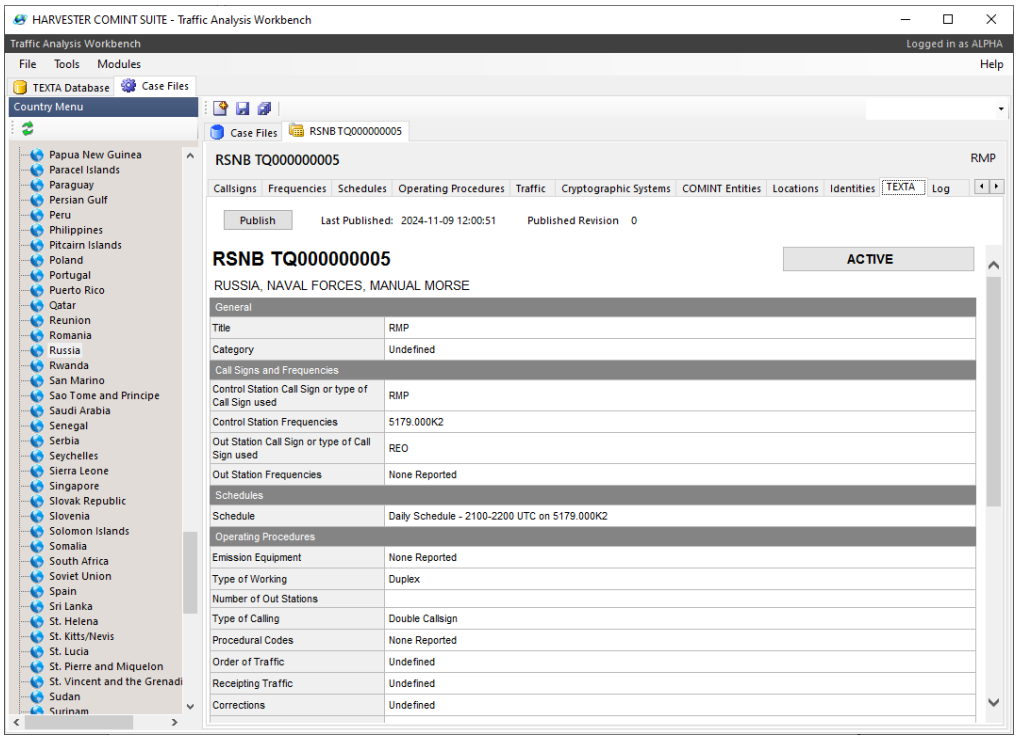
Enter all the available details about the identity then click the OK button to save the record.

2.11 TEXTA

The TEXTA section provides a textual summary, in the form of a TEXTA Page, including all the information that has been entered into the Case File. It should be noted that the TEXTA Page is not a vehicle to list extensive historical information but should be a summary that reflects the current status of a net or network. The information is summarised into seven section, to provide the most up-to-date description of a network or net, and will aid Intercept Operators to rapidly identify the network.

The seven summarised TEXTA areas:

- Case Summary
- Callsigns and Frequencies
- Schedules
- Operating Procedures
- Traffic
- Locations and Identities
- History

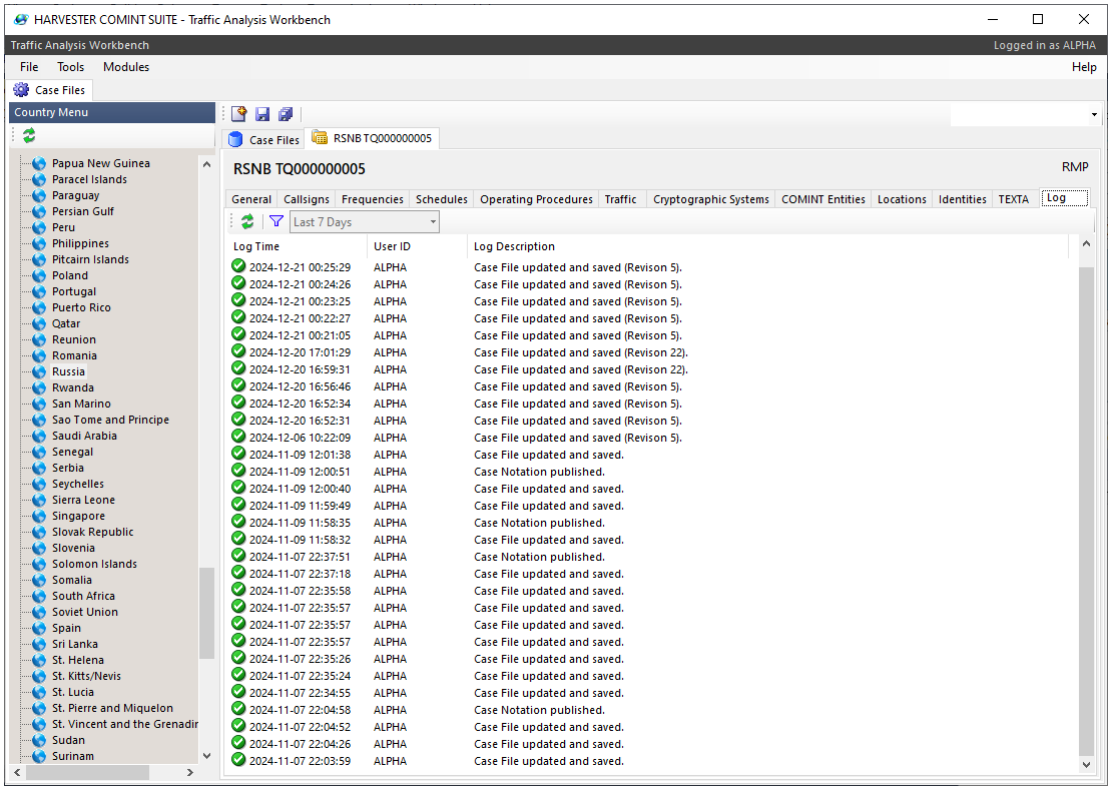


2.11.1 Publishing TEXTA

The TEXTA Page displayed in Case Files shows a summary of all the information added to the case file, and is automatically refreshed whenever the case file is saved. In order to publish the TEXTA Page to the TEXTA Database so that other users, including as Intercept Operators, can view it, click the Publish button. Unpublished and amended TEXTA Pages will not appear in the TEXTA Database once they have been published.

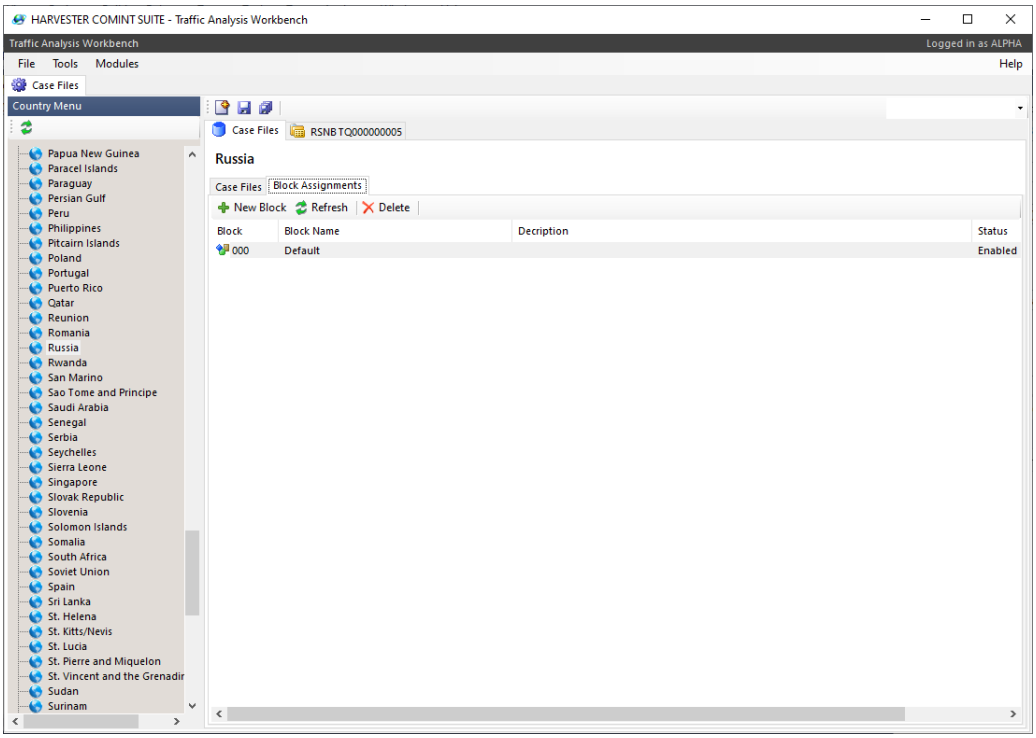
2.12 Logs

The Logs section provides a systems log of major events in the life of each Case File, such as when it was created, when it was updated and when, and what revision number, was published to the TEXTA Database. The log is automatically maintained by the system.

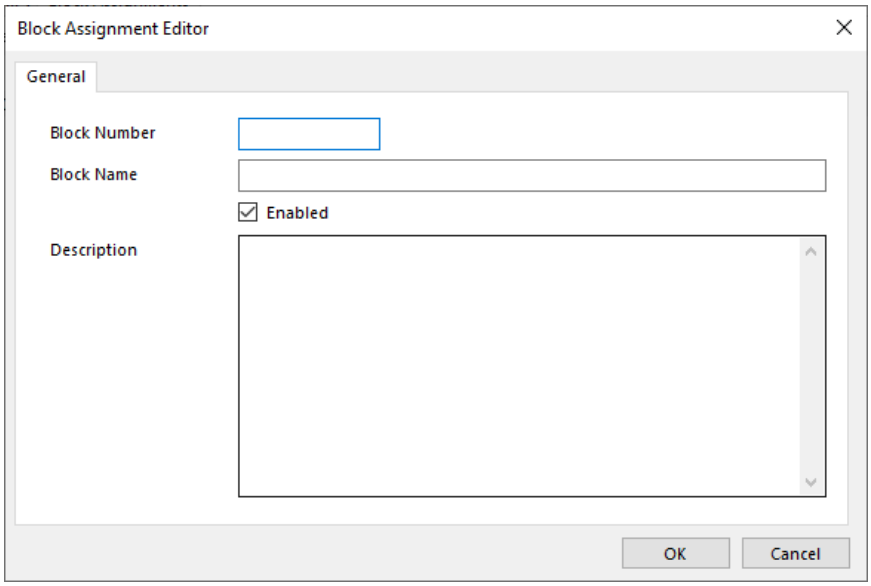


2.13 Block Assignments

Block Assignments provide a useful tool to the Traffic Analyst when managing targeted collection assignments. By defining different blocks for different collection



Click the New Block button in the toolbar to open the Block Assignment Editor window.

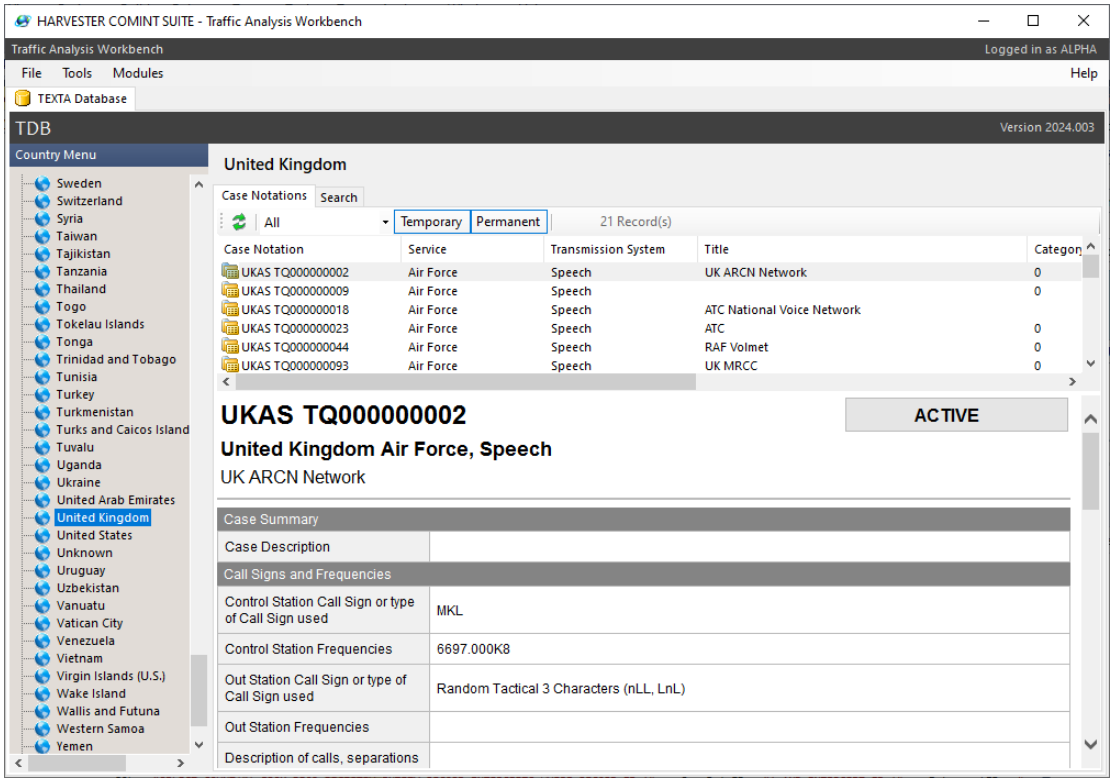


3. TEXTA DATABASE (TDB)

The TEXTA Database (TDB) module provides a country by country list of all the currently published TEXTA for networks and nets currently identified or under analysis. Each TEXTA page is divided into seven specific areas that are organised into topics that will help Intercept Operators rapidly identify communications.

> **NOTE** This module is also available to Intercept Operators in the Collection Operator Terminal.

Select the TEXTA Database option from the menu to open the TEXTA Database module.

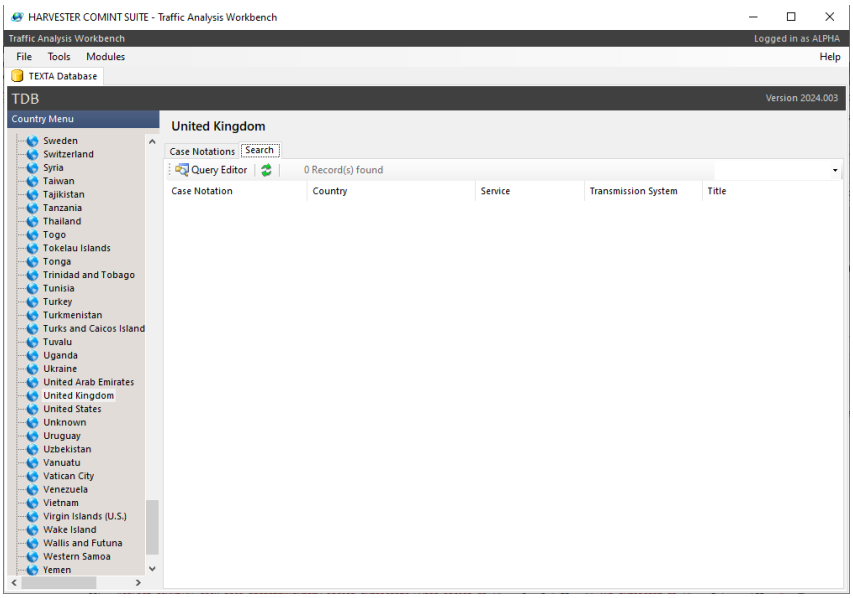


Select the country of interest in the Country Menu and the current list of published TEXTA for that country will be displayed in the right-hand panel. Select a Case Notation from the list to display the TEXTA page. Each TEXTA page is organised into TEXTA areas:

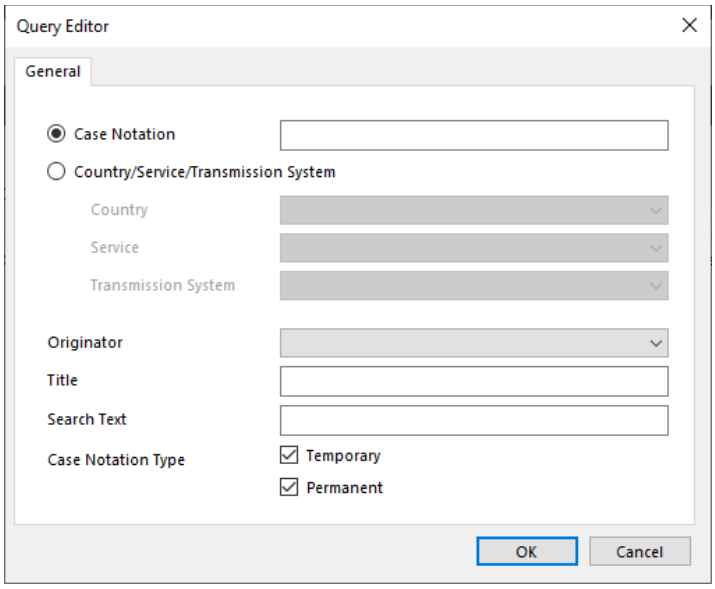
- Case Summary
- Callsigns and Frequencies
- Schedules
- Operating Procedures
- Traffic
- Locations and Identities

- History

TEXTA pages should be viewed as “latest available information” but are works in progress as they constantly evolve as new information is gleaned from Traffic Analysis. It is the responsibility of the Traffic Analysis process to keep TEXTA pages up-to-date. As well as viewing specific countries, the TEXTA Database can also be searched.



Select the Search tab then click the Query Editor button to open the Query Editor window. Here Case Notations can be searched using the wildcard character %, by Country, Service or Transmission System. Results can be further refined by defining the originator of the TEXTA, the Case title and any specific words that might be used in the TEXTA page, again using the wildcard character %.



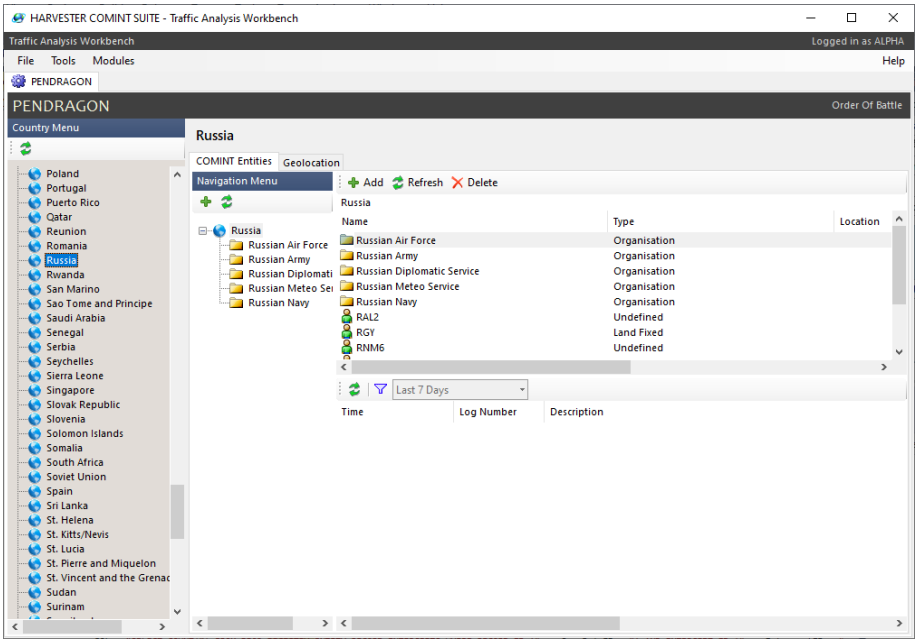
4. ORDER OF BATTLE

The Order of Battle (OOB) module provides a repository for the development and recording of individual organisations and their constituent entities as they are discovered through intercepts and analysis. The hierarchical view allows the internal structures of each organisation to be modelled to produce an Order of Battle for each individual organisation. OOB data is fully integrated throughout HARVESTER COMINT Suite to provide a universal data structure onto which all information gleaned from intercepts, such as intercept logs, messages and callsigns, can be quickly and easily mapped. This level of integration then allows logs from individual COMINT entities to be rapidly retrieved for analysis.

NOTE: The OOB module uses a Query Focussed Dataset which must be periodically refreshed to ensure that the latest logs appear against selected COMINT Entities. The last refresh date is displayed at the right hand side of the module's toolbar. If you need the data refreshed, ask your Systems Administrator to refresh the PENDRAGON dataset.

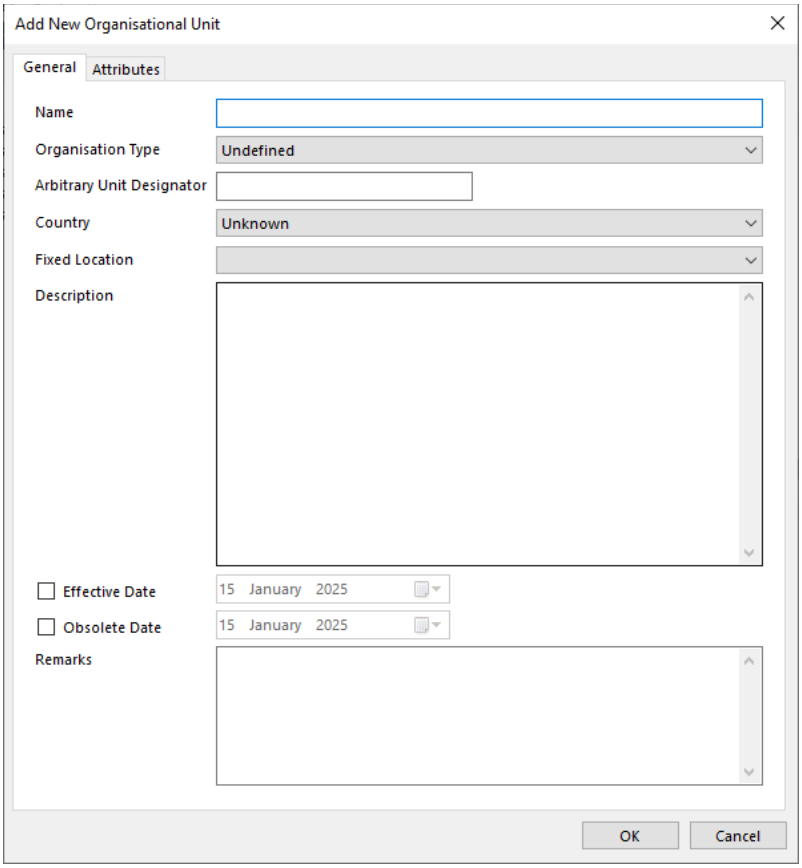
It should be noted that there is an important functional difference between an organisational unit and a COMINT entity. Organisational units reflect the hierarchy of an organisation, its roles and its functions but do not emit COMINT signals. COMINT entities, on the other hand, are physical entities attached to the various levels of an organisational hierarchy that will emit COMINT signals and will be identified by a callsign.

Select the OOB option from the menu to open the Order of Battle module.



4.1 Adding a new Organisational Unit

With the COMINT Entities tab selected, select the country of interest from the Country Menu. This will load the country information into the Navigation Menu. The country icon and name will appear in the country hierarchy view. Click the Add icon in the Navigation Menu to open the Add New Organisational Unit window.



Enter the name of the organisation and any additional information that is known about it then click the OK button to save the new organisational unit. The new unit will be appear in the hierarchy view of the country with the name that was entered in the Name field.

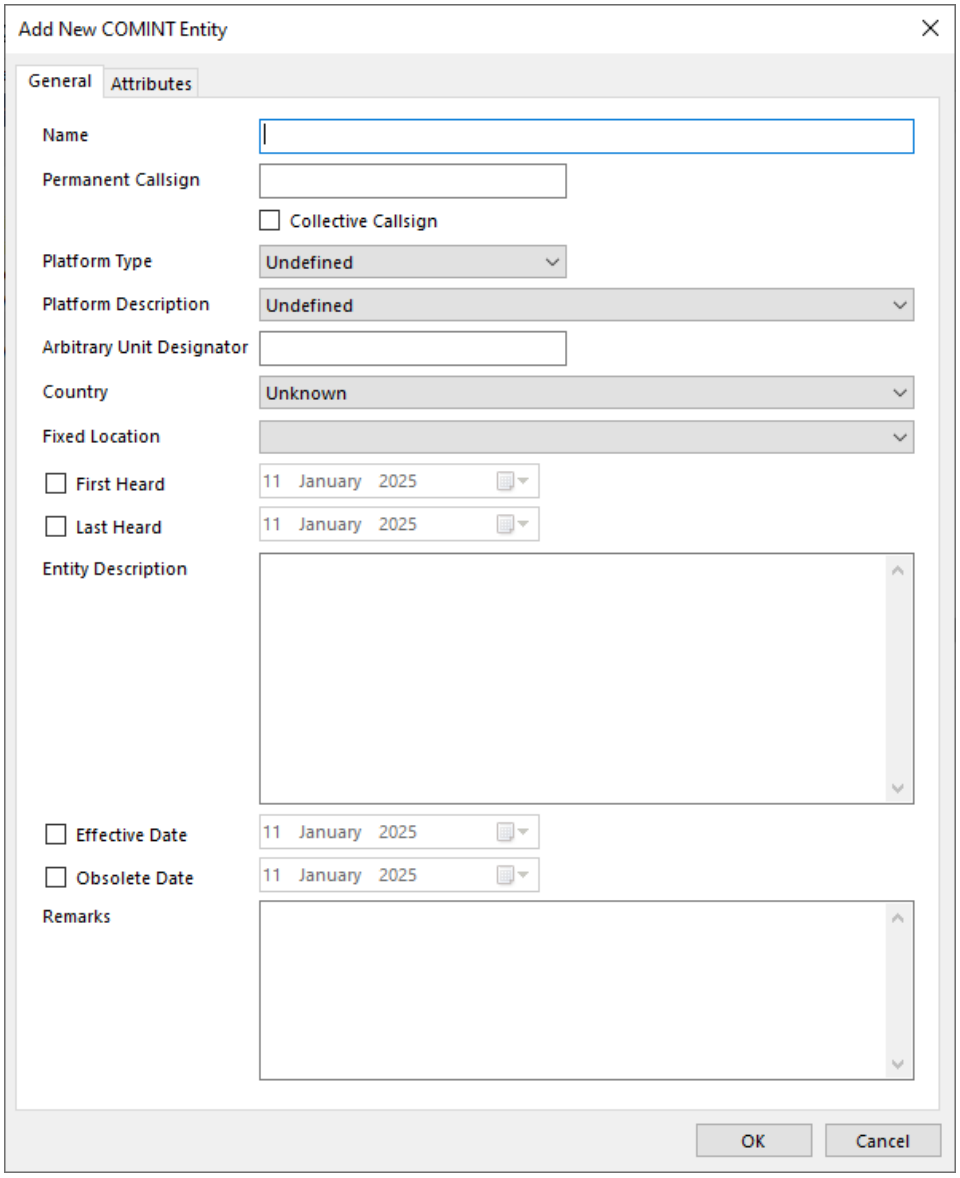
An Arbitrary Unit Designator can be assigned to each individual organisational unit if required to help map the organisational structure and add an additional level of hierarchy and deposition information. This is particularly useful when mapping military organisational structures.

Country can be selected to provide a general location for an organisational unit, and can be further refined by selecting a Fixed Location from the dropdown box. Fixed location are populated directed from Geolocation data.

> **TIP** When building an organisational hierarchy, there can often be some confusion when trying to decide whether a certain type of entry should be defined as either a organisational unit or as a COMINT entity. A good example of this is a military airfield. It will be home to a number of services, each of which may well support COMINT emitters. In this case, it is suggested that the airfield is defined as an organisational unit with each of its services defined as different organisational units. Only the transmitting entities within each organisational unit should be defined as COMINT entities. Another example of this is an embassy. Although the embassy is a physical location, it is also a COMINT emitter therefore would be recorded on the OOB as a COMINT entity.

4.2 Adding a new COMINT Entity

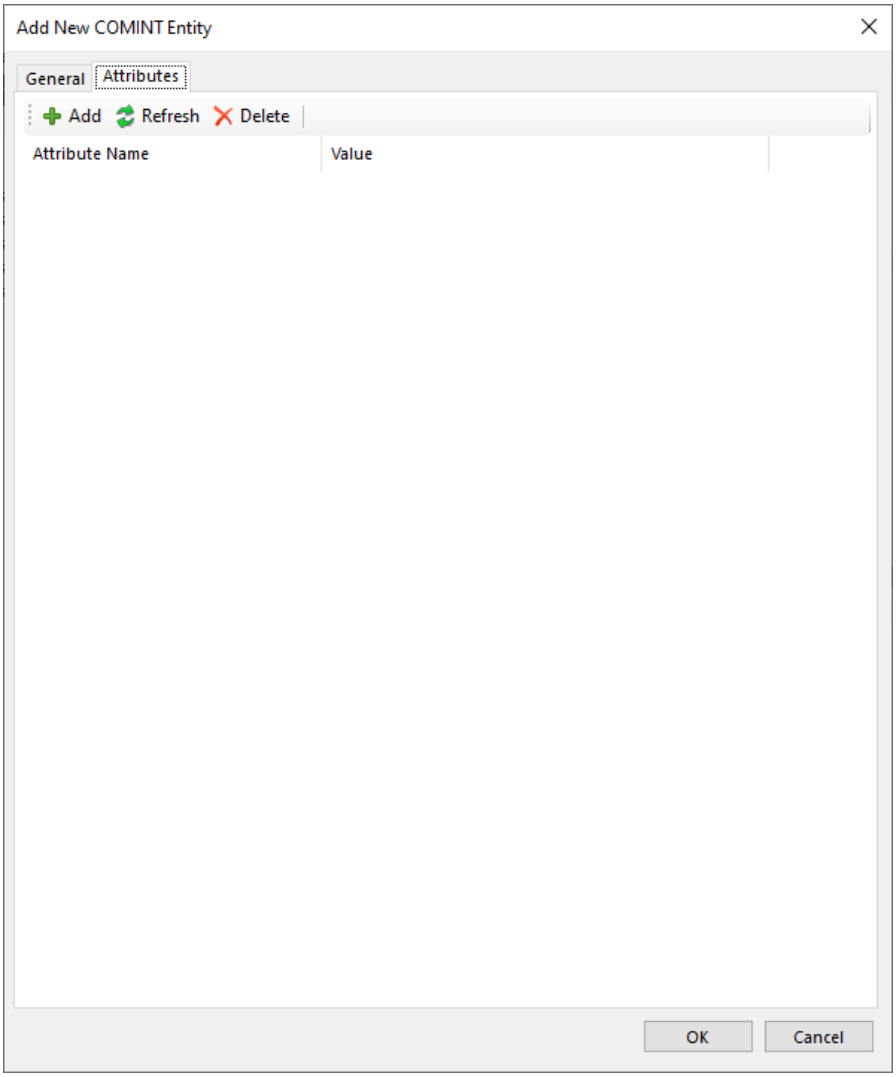
Select the organisational unit in the Navigation Menu that you wish to add the COMINT entity to and click the Add icon in the right hand toolbar to open the Add New COMINT Entity window.



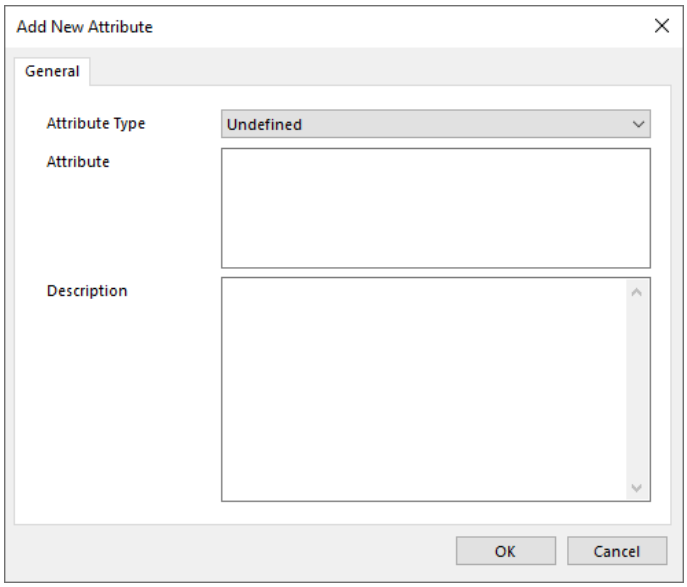
COMINT entities can be identified by either the name of the entity or by its callsign. This allows both known entities that have not yet been heard or intercepted entities that have not yet been fully identified to be added.

To add additional information about the COMINT entity, click the Attributes tab to access the entity attributes module.

Enter as much information about the entity that is known then click the OK button to save the new organisational unit. The new COMINT Entity will be appear in the right-hand entity panel.



To add a new attribute, click the Add button in the toolbar to open the Add New Attribute window.



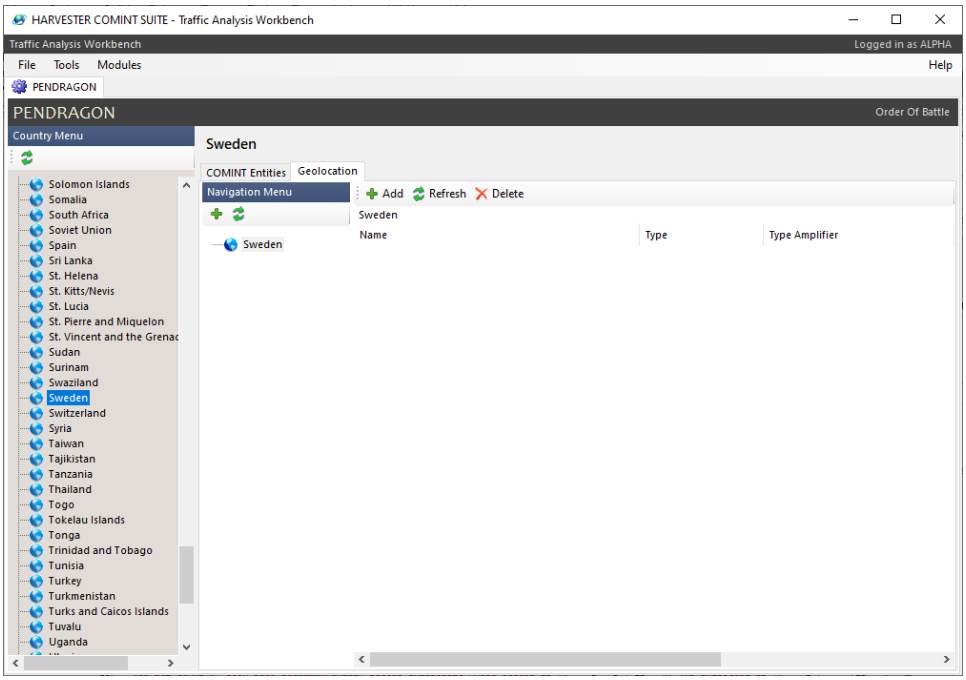
Select the type of attribute being added from the dropdown box, enter the attribute value and a description if required, then click the OK button to save the attribute.

There are currently 29 types of attribute that can be attached to organisational units and COMINT Entities.

Aeronautical Selcal Code (ANNEX 10)
Aircraft Registration
ALE Call Sign
Email Address
Fixed Service Maritime Selcal
Fixed Service Selcal
Home Port
Hull Number
IATA 3-Letter Airfield Code
IATA Airline Code
ICAO 4-Letter Airfield Code
ICAO24 Address
IMO Number
IMSI
INMARSAT Telephone Number
Internal Telephone Extension
IPv4 Address
IPv6 Address
ITU Call Sign
Landline Telephone Number
Maritime Mobile Selcal
MMSI
Mobile Telephone Number
Pager Number
Postal Address
Routing Designator
Undefined
URL
Voice Call Sign
WMO Observing Station Number

4.6 Geolocation

With the Geolocation tab selected, select the country of interest from the Country Menu. This will load the country information into the Navigation Menu. Like OOB data, Geolocation data is fully integrated throughout HARVESTER COMINT Suite and is used in Case Files as a method of correlating the locations of different COMINT entities. Geolocation data is divided into two types: Locations and Installations.



4.6.1 Locations

Locations describe major regions and areas within a country and fall into three main categories: Geopolitical Areas, Population Areas and Geographical Features. These categories are further defined as:

Geopolitical Areas

- Autonomous Region
- Country
- County
- Occupied Territory
- Region
- State

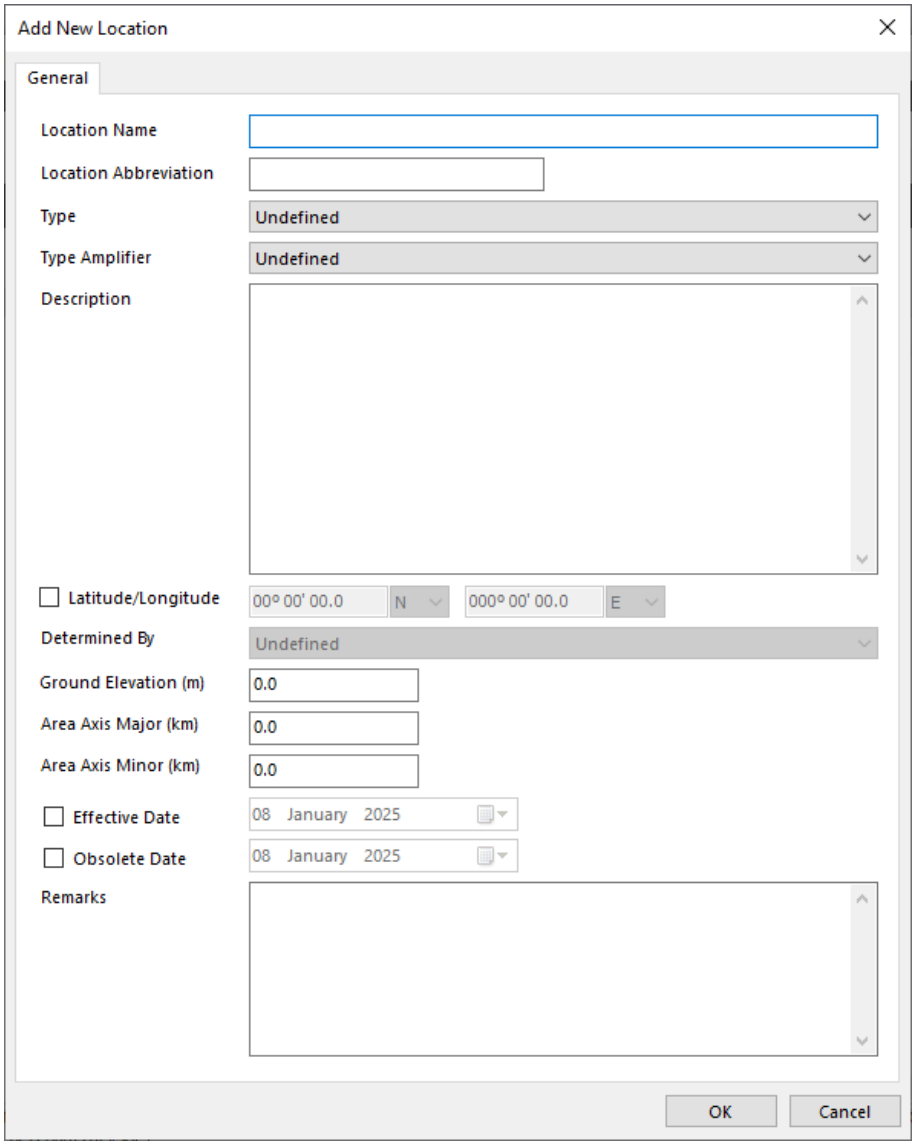
Population Areas

- City
- Suburb
- Town
- Village

Geographical Features

- Hill
- Inland Waterway
- Mountain

To add a new location, click the Add button in the toolbar to open the Add New Location window.

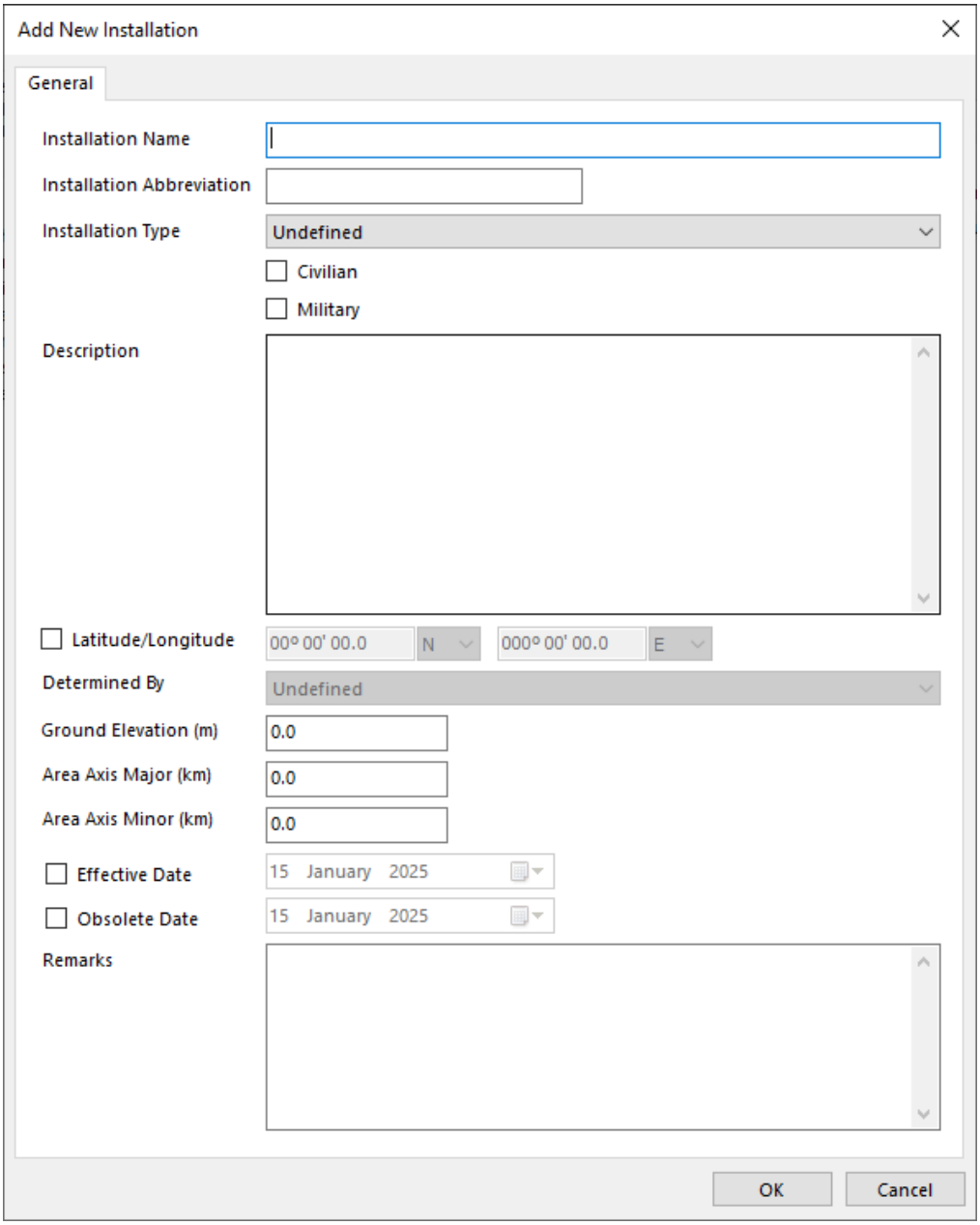


4.6.2 Installations

Installations describe specific physical buildings and structures within a location. There are currently 26 defined types of installation:

Airfield
Airport
Antenna Site
Barracks
Container Storage Facility
Embassy or Consulate
Factory
Fire Station
Government Building
Government Installation
Harbour
Headquarters Building
Hospital
Office Block
Oil Refinery
Oil Storage Facility
Police Station
Port
Power Station (Coal)
Power Station (Gas)
Power Station (Nuclear)
Radar Station
Railway Station
Railway Yard
Research Building
Training Area

To add a new installation, click the Add button in the toolbar to open the Add New Installation window.

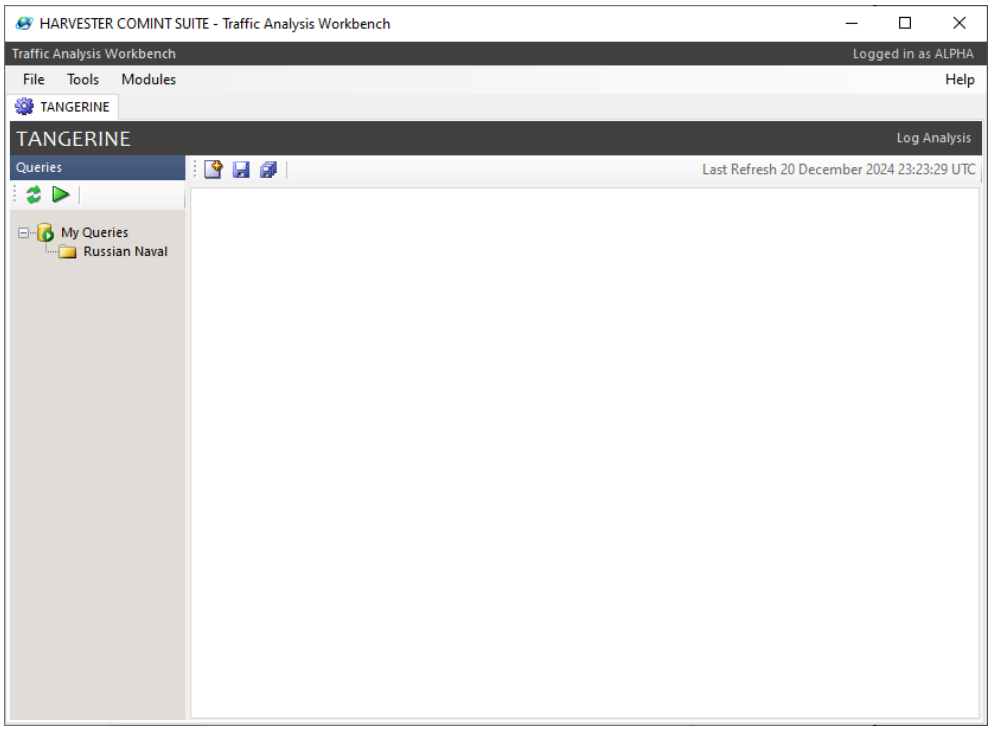


5. LOG ANALYSIS

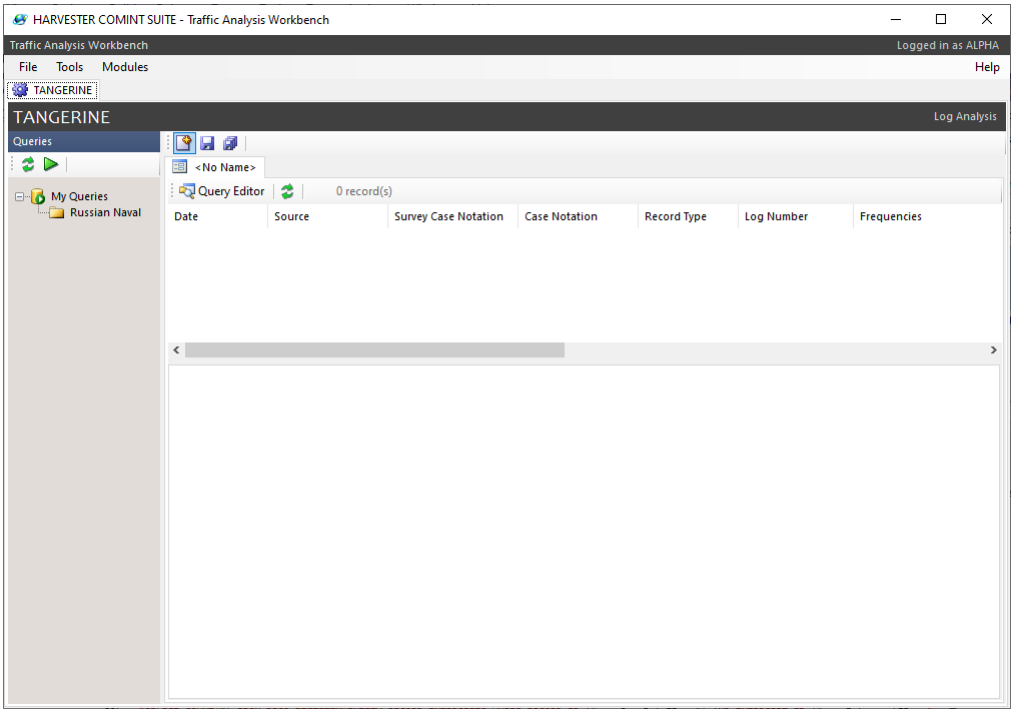
The Log Analysis module is designed to provide traffic analysts with an ability to rapidly search all local logs (Coverage, Intercepts and Message logs) to aid in the analysis task.

NOTE: The Log Analysis module uses a Query Focussed Dataset which must be periodically refreshed to ensure that the latest logs are available for analysis. The last refresh date is displayed at the right hand side of the module's toolbar. If you need the data refreshed, ask your Systems Administrator to refresh the TANGERINE dataset.

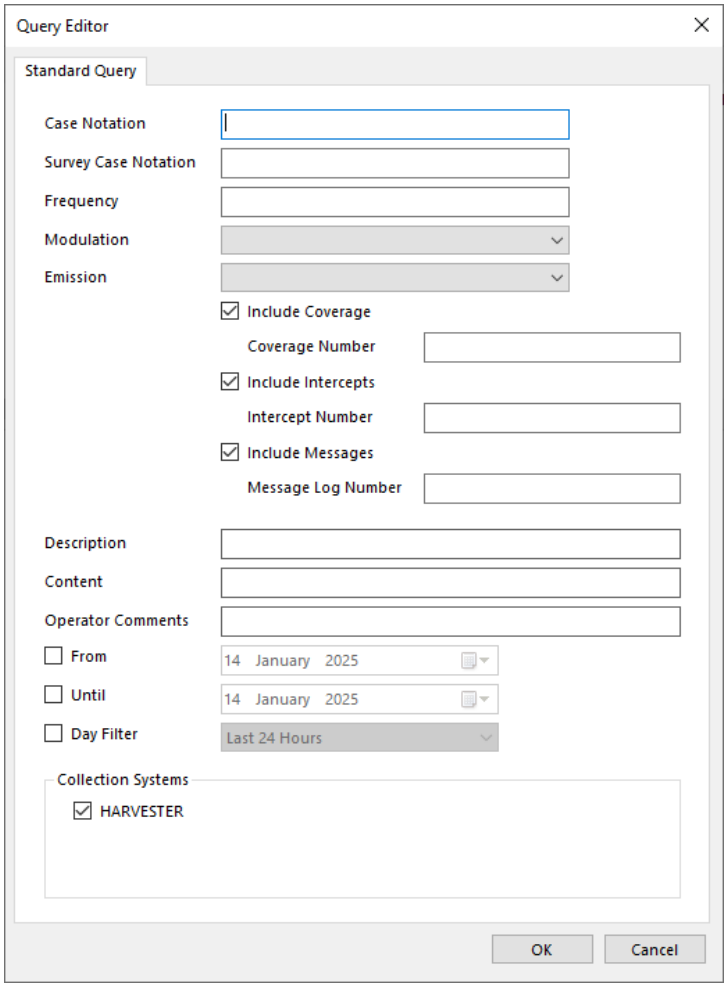
Click on the Modules menu and select the Log Analysis option to open this module.



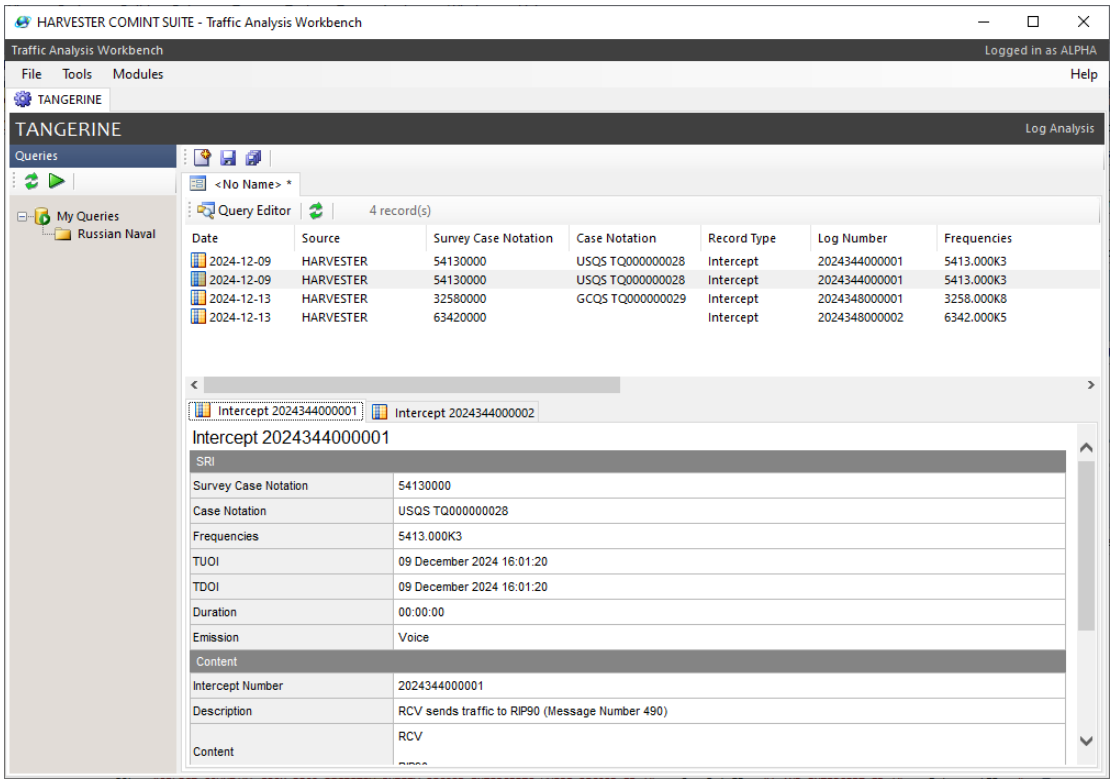
In the Log Analysis module, click on the New Query button on the toolbar bar to open a new Query window:



Click on the Query Editor button on the toolbar to open the Query Editor:



In the Query Editor, you can define a number of parameters to meet your search requirements then click the OK button to run the query. Query results are displayed in the lower section of the query window.



To amend a query, click the Query Editor button to reopen the Query Editor.

If your query if one that you will reuse, it can be saved by clicking the Save button on the toolbar.