AIS MEDITERRANEAN REGIONAL SERVER

National AIS proxy user manual

Submitted by Italy

Executive summary	The present document contains the national proxy user manual ed. 1 rev. A
Action to be taken	Take note to document
Related documents	STIRES 6/MED/1 - Consolidated document containing requirements and specification agreed by the MED AIS EWG

INDEX

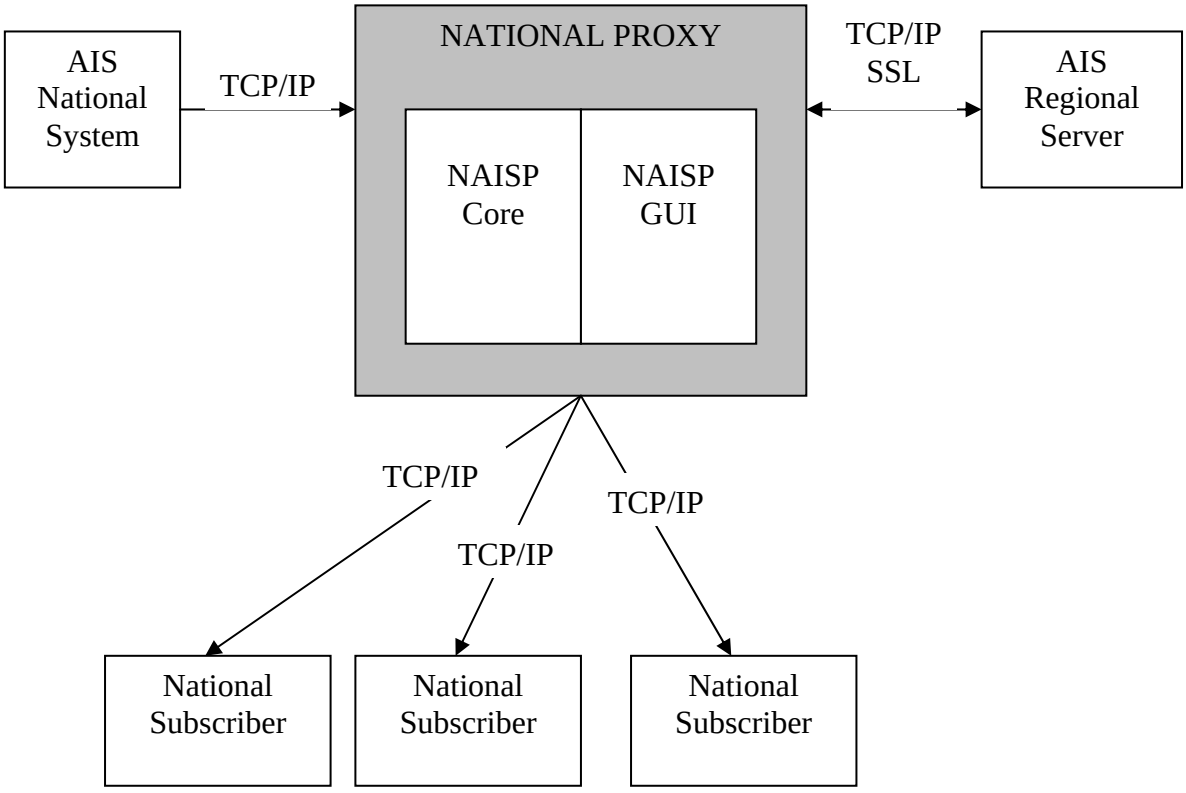
CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

The “AIS Mediterranean server” has been developed to be the main system for collection, distribution, storage and display of AIS data acquired from the individual Mediterranean AIS National systems.

The main service that a Regional AIS server provides is collection of AIS data in real time and their storage into databases. To achieve this, a Regional AIS server requires permanent connections with all the National AIS servers to exchange data among the systems involved.

This connection is performed by a component named National Proxy. The National Proxy will take care of the management of all the issues related with physical connection, exchange and down-sampling of the messages sent from each AIS National system to the Mediterranean Regional server.



1.2 PURPOSE OF THIS DOCUMENT

This document is the installation guide and user's manual for NAISP (National AIS Proxy), which serves as a National Proxy defined in the "AIS Mediterranean server" project.

1.3 DESCRIPTION OF NAISP

NAISP is made up by two modules. One module, NAISP Core, takes care of establishing, managing and terminating connections required for the exchange of AIS data among the National AIS System, the Regional AIS Server and the Subscriber Applications. The other module, NAISP GUI, provides a graphical interface for the user intended to monitor and configure NAISP Core.

CHAPTER 2
INSTALLING NAISP

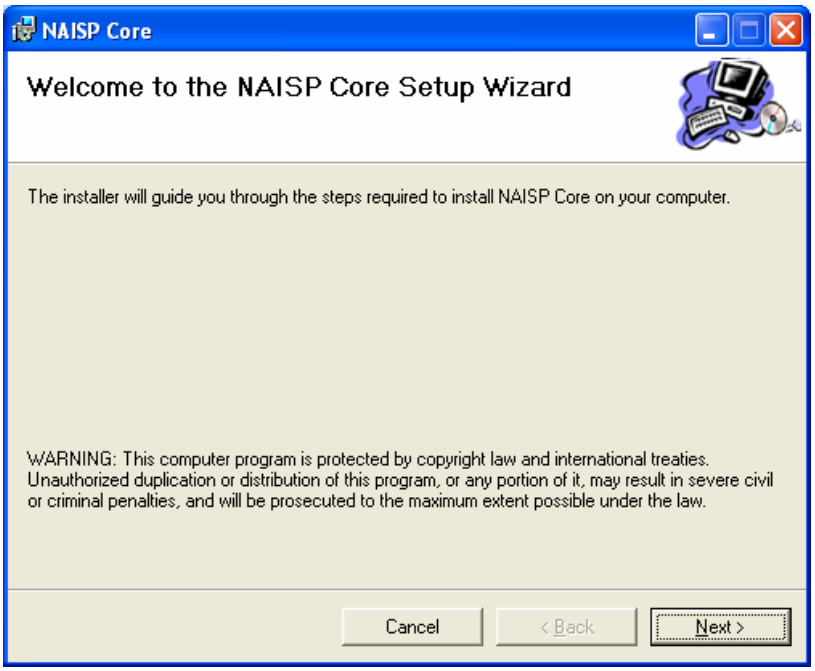
The NAISP install CD contains installation files for the NAISP Core and GUI modules. In addition to these, you can find executable files which install the runtime core licensing environment, which is required to be installed on the machine running the NAISP Core application, and the .NET 2.0 and 3.0 frameworks, which are needed in order for the NAISP GUI module to work.

The Core and GUI modules are installed independently from each other. While it is possible to install both modules on the same machine, it is not required to do so. This allows controlling and monitoring of the NAISP Core from a machine different from the one on which it is running. You can obviously install multiple copies of the GUI on different machines, to allow simultaneous monitoring from different places. However, only one machine can take control of the Core at any given time.

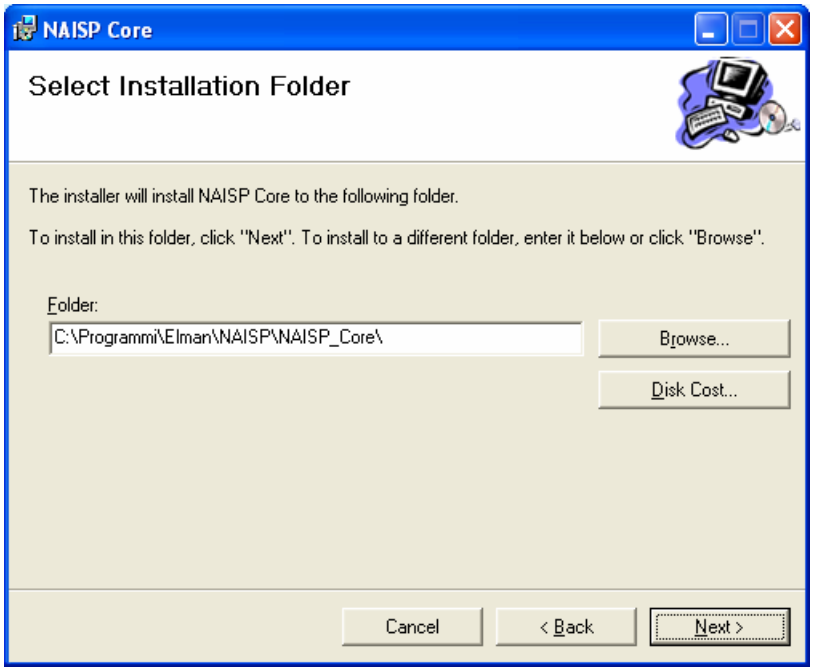
2.1 INSTALLING THE NAISP CORE

Follow these steps to install the NAISP Core:

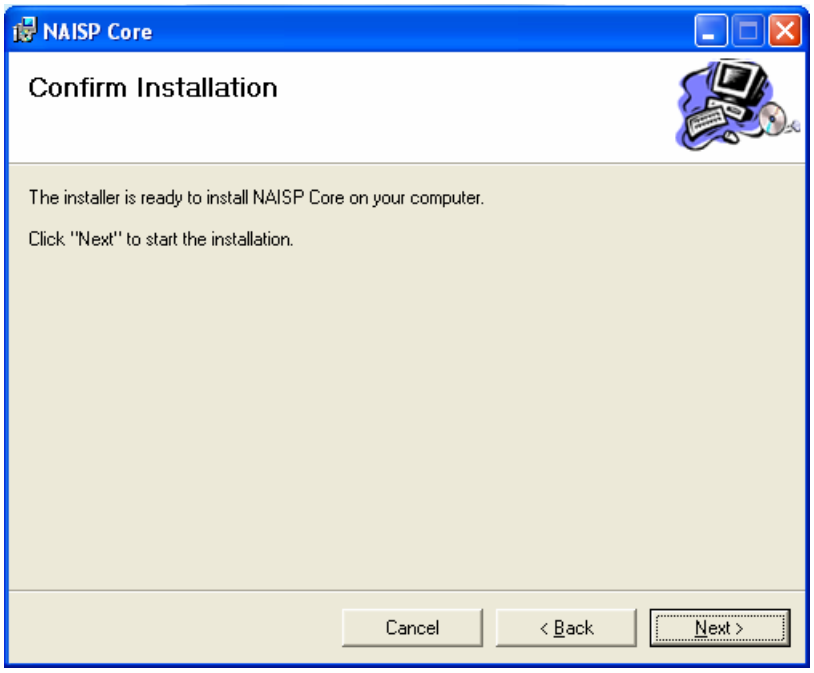
1. Start the *setup.exe* executable file located in the *NAISP_Core* folder in the install CD. A wizard will guide the user during the installation as shown below.



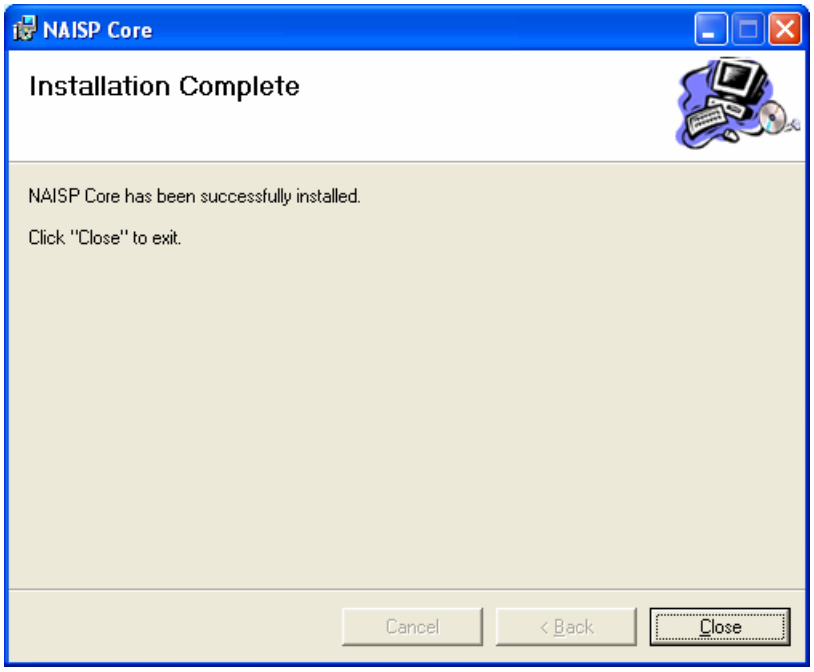
2. Click on **Next**.



3. Click on **Next**.



4. Click on **Next**.



5. Click on **Close**. The program has now been installed.

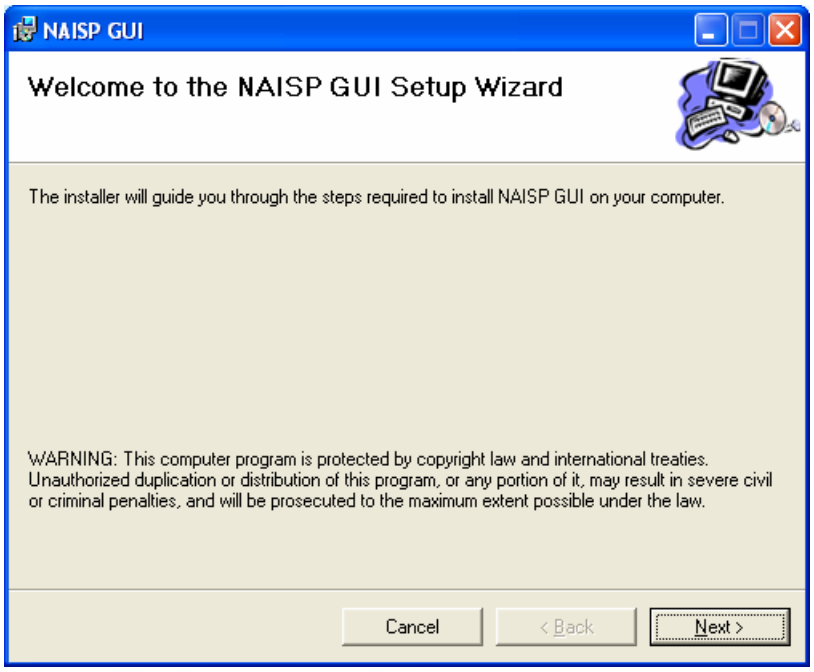
The NAISP Core application uses license checking through a USB dongle (protection key) supplied together with the install CD. Before the Core module can be used, you need to install the runtime environment required to enable the protection key to run and communicate with the protected application. To install the runtime environment, start the *HASPUserSetup.exe* executable file located in the *HAS_ SRM_Runtime* folder. A wizard will guide the user during the installation.

2.2 INSTALLING THE NAISP GUI

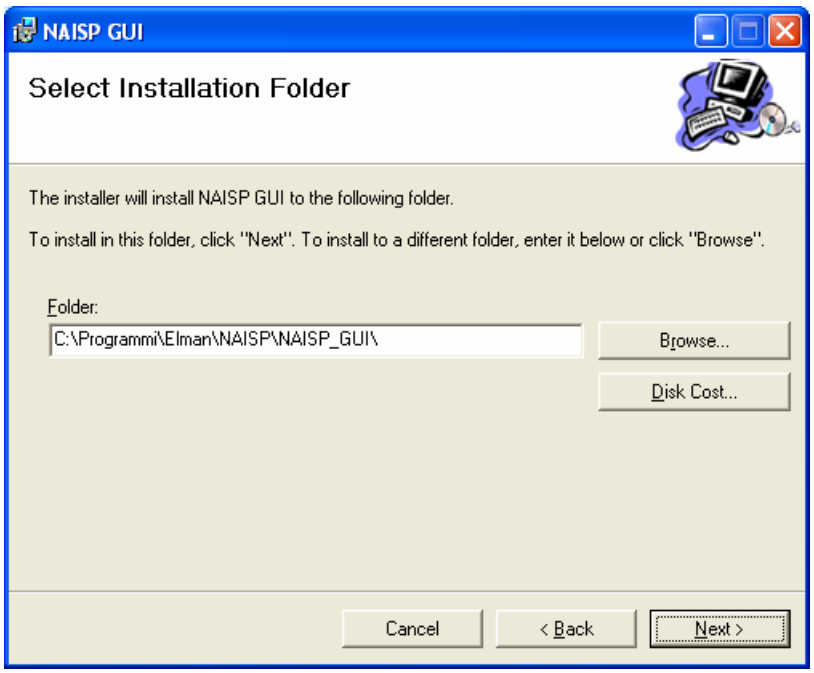
To install the GUI module, the .NET framework version 2.0 and 3.0 must be present on the target machine. If they are not already present, you can install them by starting the executable files present in the *Framework_2_0* and *Framework_3_0* folders in the install CD.

Follow these steps to install the NAISP GUI:

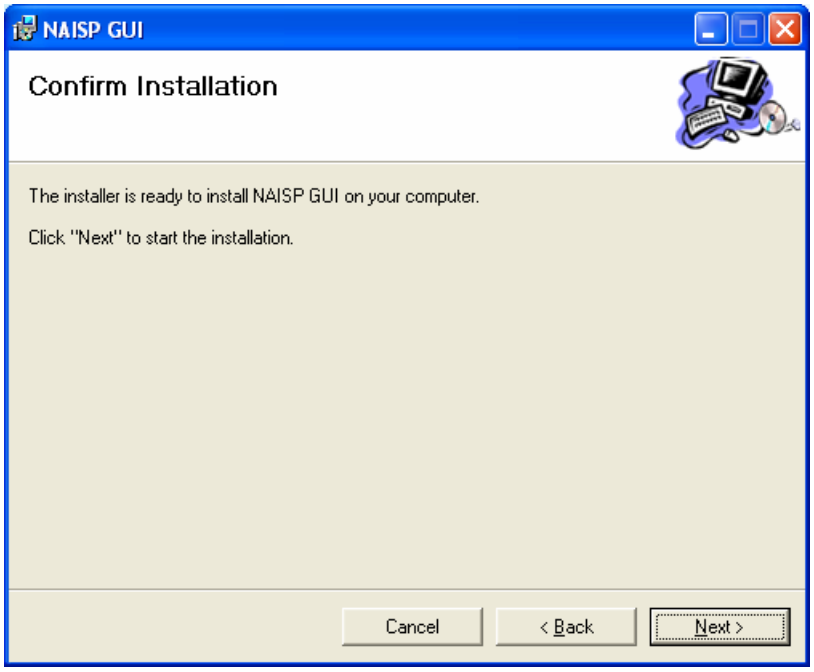
1. Start the *setup.exe* executable file located in the *NAISP_GUI* folder in the install CD. A wizard will guide the user during the installation as shown below.



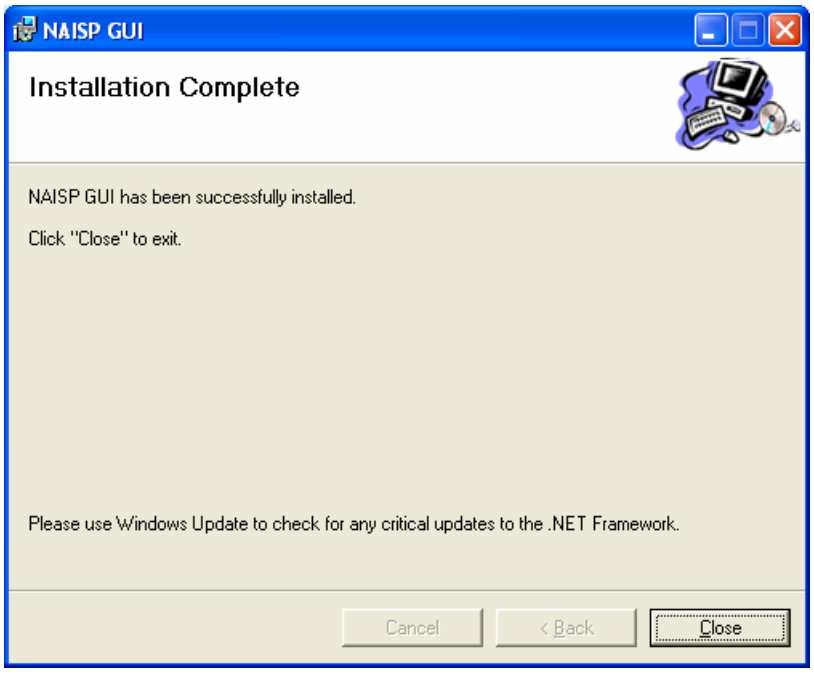
2. Click on **Next**.



3. Click on **Next**.



4. Click on **Next**.



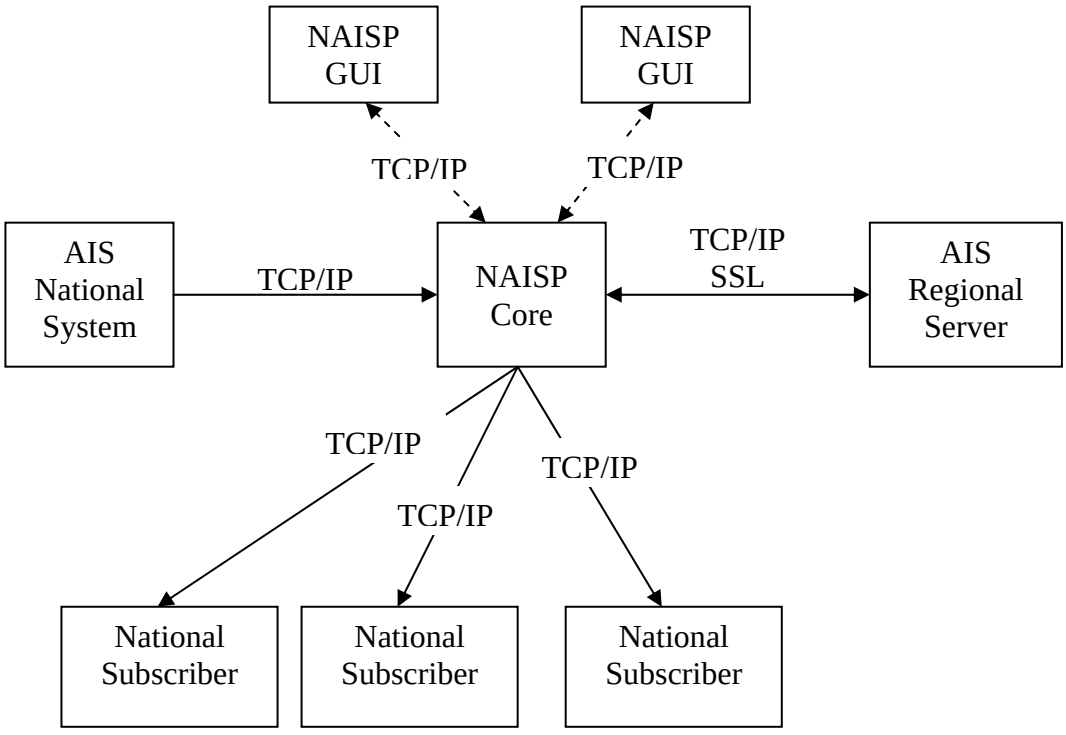
5. Click on **Close**. The program has now been installed.

CHAPTER 3
USE

NAISP is an application for the exchange of AIS data in the IEC standard format. It consists of two modules, NAISP Core and NAISP GUI.

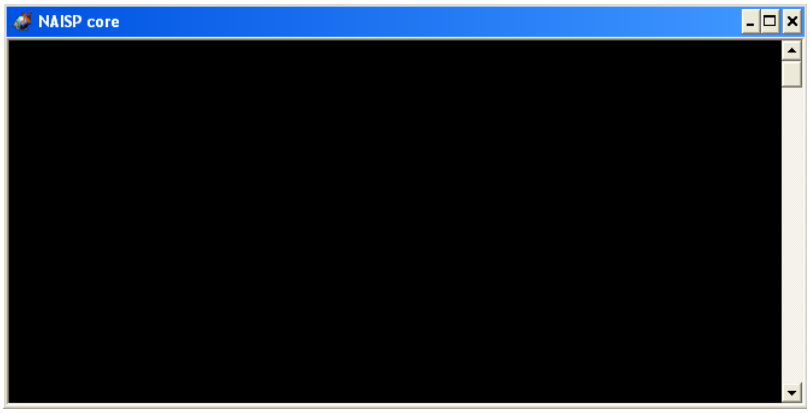
NAISP Core is a module that manages the following connections:

- 1 connection towards the AIS Regional Server (RAS). This is a secure TCP/IP SSL one-way handshake connection.
- 1 connection towards the national AIS data system (NAS). This is an unencrypted TCP/IP connection.
- Up to 3 simultaneous connections towards the national subscriber applications (NSAs) receiving the AIS data coming from the RAS. These are unencrypted TCP/IP connections.
- 2 connections towards the NAISP GUI modules. These are unencrypted TCP/IP connections.



Start the application by clicking on the *NAISP_Core.exe* in the folder *C:\Program Files\Elman\NAISP\NAISP_Core*.

When NAISP Core is running, a console window similar to the one in figure is shown. Closing this window terminates the application.



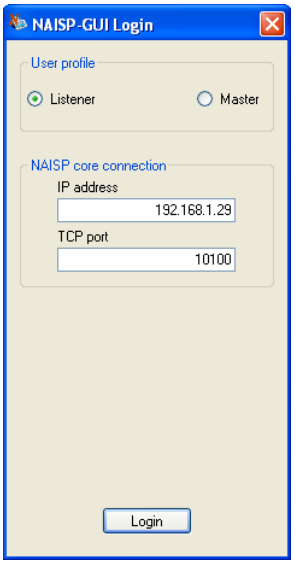
NAISP Core can be controlled and monitored through the use of the **NAISP GUI** module, which provides a graphical interface for the user.

NAISP Core may execute without the need for NAISP GUI to be running. In this case, NAISP Core will use the settings in the most recently saved configuration.

3.1 CONNECTION BETWEEN NAISP GUI AND NAISP CORE

NAISP GUI and NAISP Core interact through a TCP/IP socket connection in which NAISP GUI acts as a client while NAISP Core acts as a server.

When NAISP GUI is started, a login window appears through which the user can connect to the Core.



To establish a connection, you need to set the following parameters in the ***NAISP Core Connection*** frame:

- ***IP address:*** The IP address of the machine on which NAISP Core is running.
- ***TCP port:*** The TCP port on which NAISP Core is listening for connection requests from the NAISP GUI. NAISP Core by default will listen for connections on ports 10100 and 10200; these values are stored in the files *MASTER_settings_connection_1.txt* and *MASTER_settings_connection_2.txt* stored in the NAISP Core installation directory and can be changed by the user.

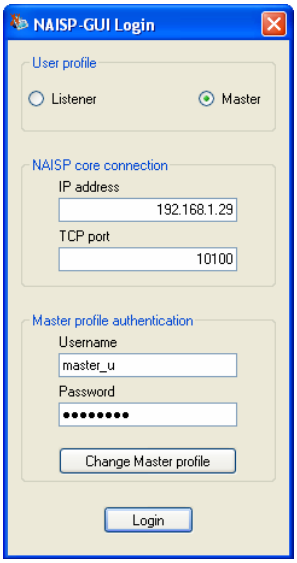
The ***User Profile*** radio buttons determine the profile the GUI will use when connecting to the Core.

Two choices are possible for the profile:

- ***Listener:*** To monitor NAISP Core's active connections and status.
- ***Master:*** To take full control over NAISP Core's activities.

If the Master profile is selected, an additional frame named ***Master profile authentication*** will appear in the login window. This frame contains the two text boxes shown:

- ***Username:*** The username for the Master profile.
- ***Password:*** The password for the Master profile.



After the program installation, the Master profile is as follows:

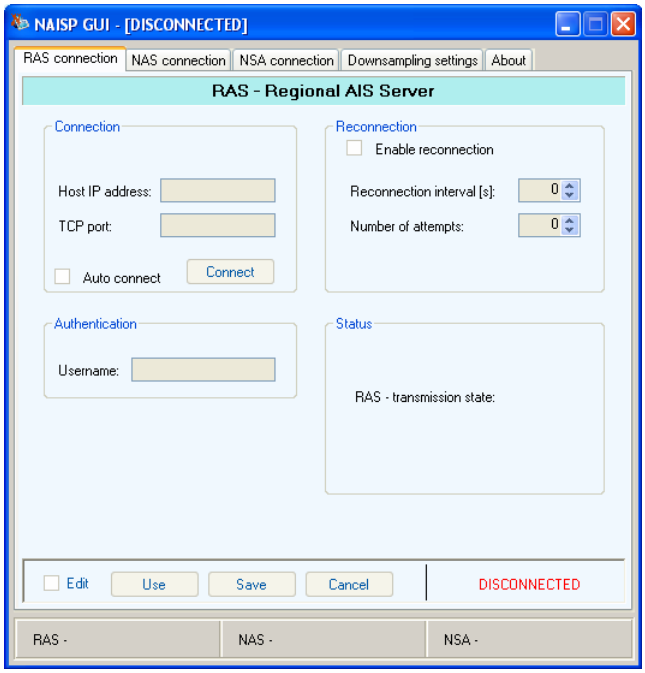
- **Username** → master_u
- **Password** → master_p

You can change this profile at any time by following this procedure:

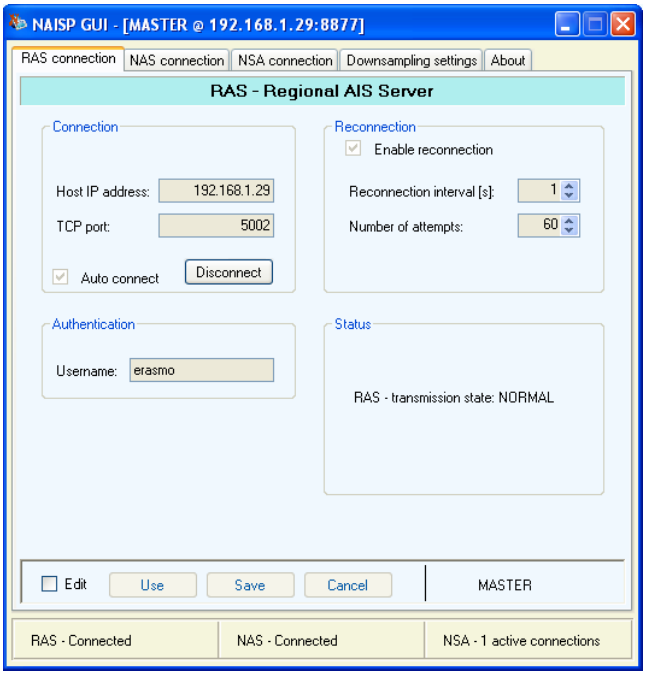
- In the ***Master profile authentication*** frame, enter the current values for username and password.
- Press the button ***Change Master profile*** in the bottom of the same frame. The ***Change master profile*** window will open as shown in figure.
- Enter the new username chosen for the Master profile in the ***New Username*** box and the new password in the ***New Password*** and ***Confirm Password*** boxes.
- Press ***OK*** to confirm the changes. A confirmation window will appear if the operation is performed correctly.

Once the desired profile has been picked and the parameters for connection towards the NAISP Core have been set, pressing the ***Login*** button will open the main NAISP GUI window and the GUI will attempt connection to the Core.

Until the connection between GUI and Core is not established, the writing ***DISCONNECTED*** will be shown in the bottom right corner of the window.



When the connection is established, the window changes its colour. The address of the machine on which the core is running and the user profile will be shown.



It may happen that, even though a Master profile was chosen, the GUI is connected with a Listener profile. This occurs when another Master user is connected to the Core. When this

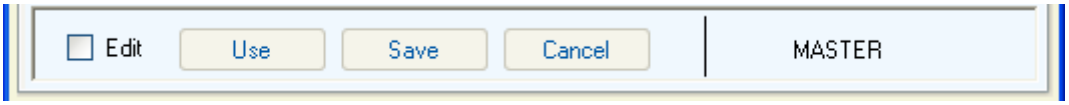
user disconnects, the profile will automatically be changed to Master, as requested. This is meant to ensure that only one user can connect to the Core as a Master, avoiding the eventuality that changes made by one user may be cancelled by another user.

3.2 NAISP GUI USAGE

The main function of NAISP GUI is to monitor the status and configuration of NAISP Core. For this purpose, a connection status bar is displayed on the bottom of NAISP GUI's window.

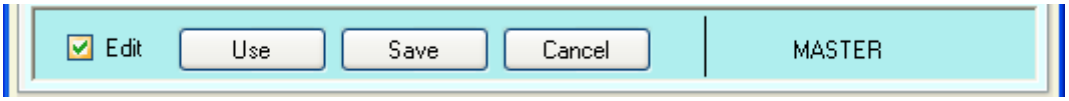
This bar enables the user to check the status of the connections at a glance, so that it is possible to know immediately which connections are working and which ones have issues. In the example shown in the figure above the NAISP Core is connected to the RAS, to the NAS and to one NSA, while in the example shown in the figure below the connection to the NAS is inactive, and the red writing helps the user to notice the problem immediately.

Another job of the NAISP GUI is to manage the NAISP Core and its activities. Each activity can be managed through one of the tabs of the NAISP GUI. All the tabs present an edit mode bar at their bottom.



Only the Master user may enter edit mode. When it is activated, the parameters shown in the corresponding tab can be changed, enabling modification of the settings of the NAISP Core.

Edit mode can be entered by selecting the ***Edit*** checkbox in the edit mode bar.

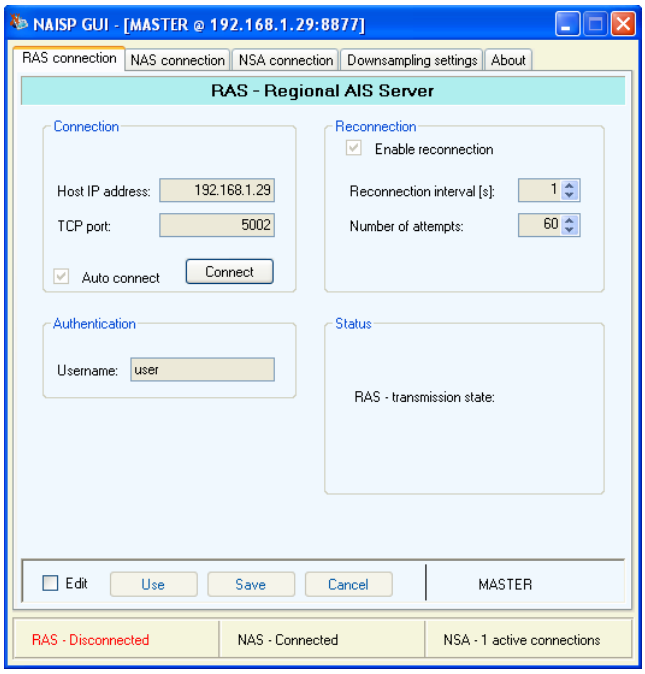


When edit mode is entered, the ***Use***, ***Save*** and ***Cancel*** buttons are enabled. Their functions are the following:

- ***Use:*** The new settings are transmitted to the NAISP Core, which will start using them without saving them. If the NAISP Core is shut down, the new settings will be lost.
- ***Save:*** The new settings are transmitted to the NAISP Core, used immediately and saved. If the NAISP Core is shut down, the new settings will be also used at its next start.
- ***Cancel:*** The modifications to the settings are cancelled and the configuration previously in use is restored.

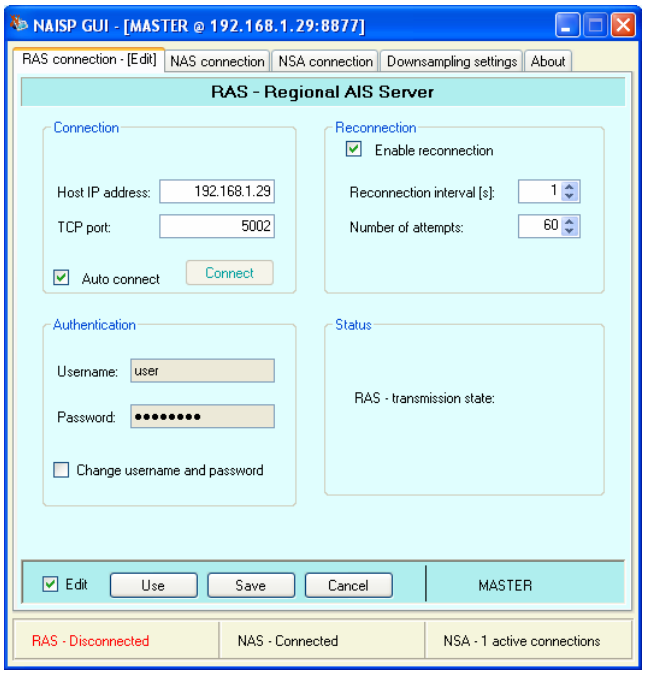
3.3 RAS CONNECTION

The ***RAS Connection*** tab is dedicated to the settings for the connection towards the Regional AIS Server.



When edit mode is inactive, the only operation possible is starting and stopping the connection towards the RAS; this is done using the button in the ***Connection*** frame. If, as shown in figure, the connection is not active, the button will show the word ***Connect***, otherwise it will be marked as ***Disconnect***.

Changing all other parameters of the RAS connection tab requires entering edit mode.

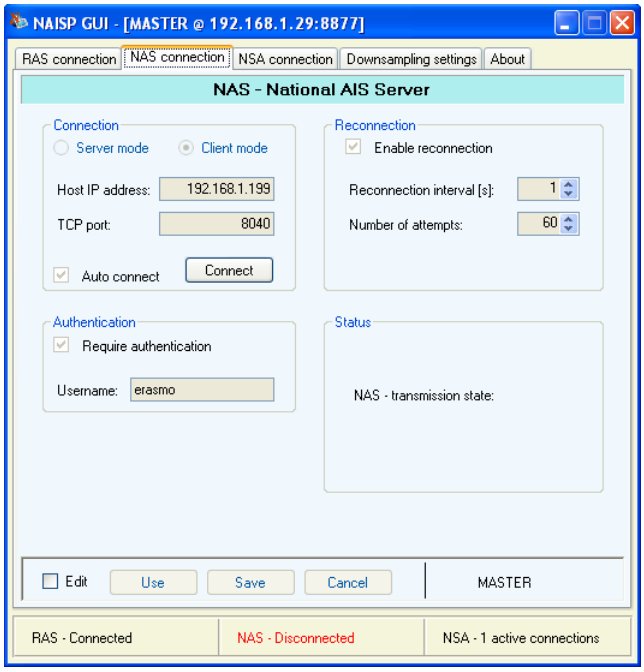


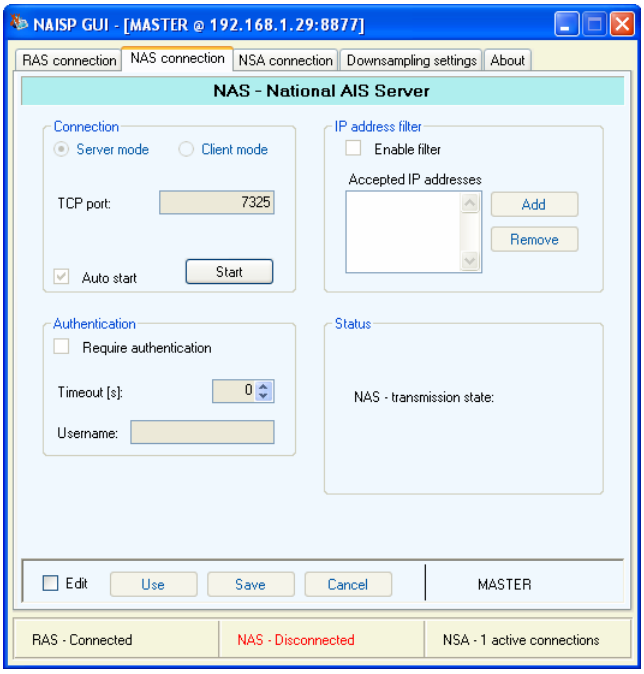
Settings may be changed in the RAS connection tab are:

- ***Host IP address:*** The IP address of the AIS Regional data Server.
- ***TCP port:*** The TCP port on which the Regional Server is listening for connection from the NAISP Core.
- ***Auto connect:*** If this checkmark is selected, the Core, when started, will automatically attempt connection to the RAS.
- ***Enable reconnection:*** If selected, the Core will automatically attempt to reestablish connection to the RAS in case of disconnection.
- ***Reconnection interval:*** The time interval in seconds that occurs between two successive reconnection attempts towards the RAS (this is only valid if ***Enable reconnection*** is checked).
- ***Reconnection attempts:*** The maximum number of times the Core will attempt reconnection towards the RAS (this is only valid if ***Enable reconnection*** is checked).
- ***Username*** and ***Password:*** The login data that NAISP uses to authenticate to the Regional Server. These must be chosen by the administrator of the Regional Server and must be known to the administrator of the NAISP. Note that to change the username and password used by the NAISP the ***Change username and password*** checkbox must be selected when the changes are confirmed by pressing the ***Use*** or ***Save*** button.

3.4 NAS CONNECTION

The NAS connection tab enables configuration of the settings used for connection towards the National AIS System. The NAISP Core can connect to the NAS either in client or in server mode. The NAS connection tab changes according to the connection mode chosen.



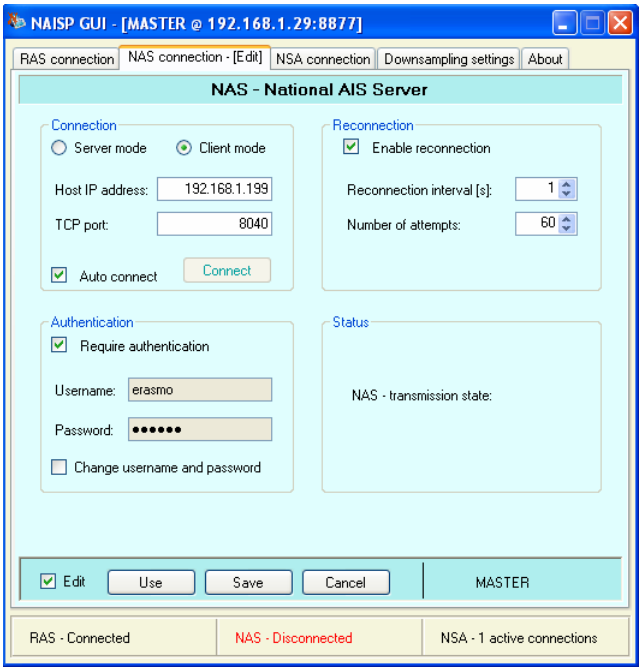


When edit mode is inactive the only operation allowed is starting or stopping the connection towards the NAS. In client mode, the button in the ***Connection*** frame will show the marking ***Connect*** or ***Disconnect***, depending on the state of the connection. In server mode, the button label will be ***Start*** to start listening for the connection from the NAS on the TCP port chosen, and ***Stop*** to shut down the connection, if active, and stop listening.

The settings in the tab may be changed by activating edit mode. Settings are described below.

3.4.1 CLIENT MODE

When in client mode, NAISP Core connects to the National AIS System using an IP address and a TCP port.



The following settings can be configured:

- ***Host IP address:*** The IP address of the AIS National Data Server.
- ***TCP port:*** The TCP port on which the National Server listens for connections from the NAISP Core.
- ***Auto connect:*** If checked, the Core will automatically attempt connection towards the NAS at startup.
- ***Enable reconnection:*** If checked, the Core will automatically attempt to reconnect to the NAS in the case that the connection should fail.
- ***Reconnection interval:*** The time interval in seconds that occurs between two successive attempts of reconnection to the NAS (this is only valid if ***Enable reconnection*** is selected).
- ***Reconnection attempts:*** The maximum number of times the Core will attempt reconnection towards the RAS (this is only valid if ***Enable reconnection*** is checked).
- ***Require authentication:*** This must be checked if the NAS requires authentication of the user that connects to it to read AIS data.
- Username and Password: The logindata that NAISP uses to authenticate to the National Server. These must be chosen by the administrator of the National Server and must be known to the administrator of the NAISP. The format that NAISP uses to send the

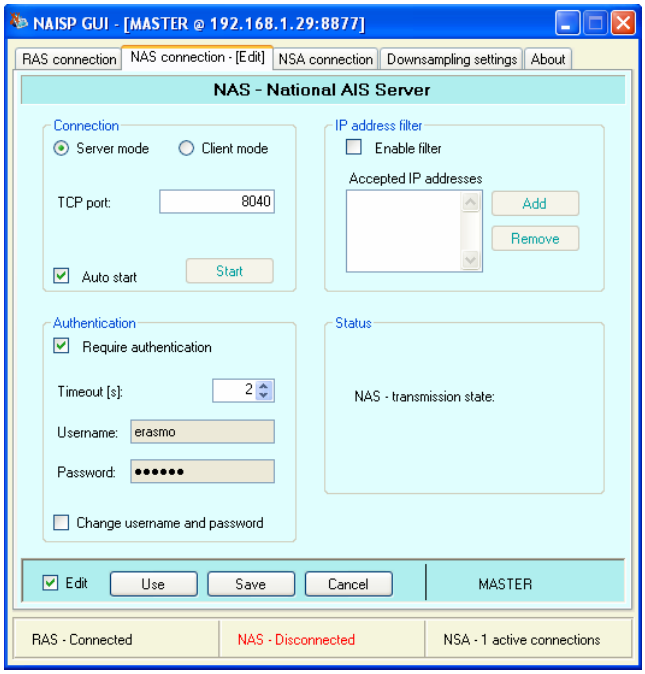
authentication data is defined in the file *NAS_template_auth_str.txt* located in the NAISP Core installation directory. The format of this file is defined in appendix A. The default format consists of the username and password preceded, separated and followed by single non-printable ASCII characters of value, respectively, 1, 0 and 0. For example, if the username is *MedProxy* and the password is *EMSA*, the following sequence of bytes would be sent to the National Server:

<1>MedProxy<0>EMSA<0>

where <x> stands for the non-printable ASCII character of value x.

3.4.2 SERVER MODE

When in server mode, NAISP Core opens a TCP socket on a chosen port and waits for connection from the National AIS System.



Settings can be configured as follows:

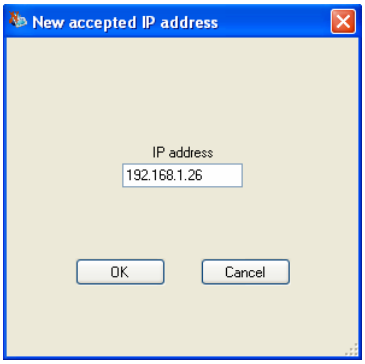
- ***TCP port:*** The TCP port on which the NAISP Core listens for connections from the National Server.
- ***Auto start:*** If checked, the Core will automatically attempt to open the port listening for NAS connection requests upon startup.
- ***Require authentication:*** When this checkbox is selected, the NAS connecting to the NAISP is required to authenticate.
- ***Timeout:*** The maximum time that NAISP will wait to receive the NAS authentication after accepting its connection request.

- ***Username*** and ***Password:*** The login data that the National AIS Data Server needs to send to authenticate. The format that NAISP expects for the authentication data is defined in the file *NAS_template_auth_str.txt* located in the NAISP Core installation directory. The format of this file is defined in appendix A. The default format consists of the username and password preceded, separated and followed by single non-printable ASCII characters of value, respectively, 1, 0 and 0. For example, if the username is *MedProxy* and the password is *EMSA*, the following sequence of bytes needs to be sent by the National Server:

  <1>MedProxy<0>EMSA<0>

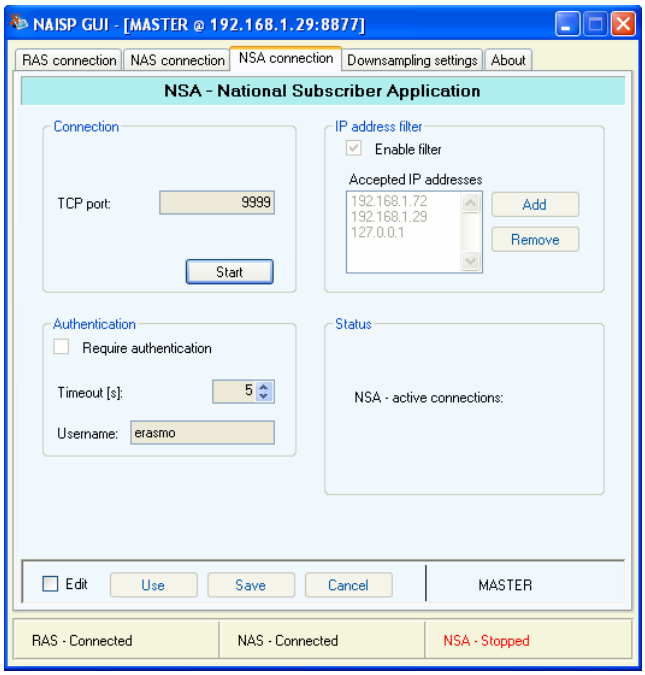
  where <x> stands for the non-printable ASCII character of value x.

- ***Enable filter:*** If checked, the NAISP will only accept connection requests from the IP addresses included in the ***Accepted IP Addresses*** listbox. Addresses may be added to or removed from the list using the ***Add*** and ***Remove*** buttons. To remove an address, select it and press ***Remove***. To add an address, press the ***Add*** button: the ***New accepted IP address*** window will open; enter the IP address in the ***IP address*** box and press ***OK***.



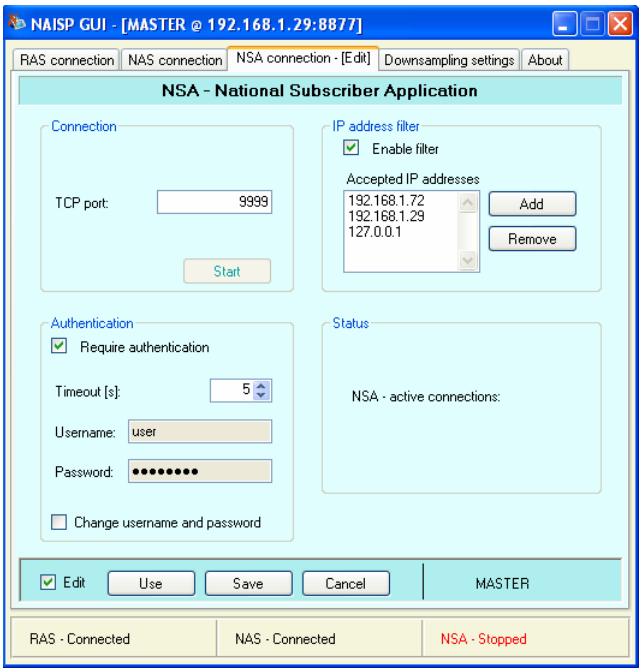
3.5 NSA CONNECTION

The NSA connection tab contains the settings for the connections towards the national subscriber applications; these are applications (as for example an AIS target display application) that connect to the NAISP Core to receive AIS data coming from the Regional Server.



As for the two tabs seen before, if edit mode is inactive the user may only start or stop connections using the button in the ***Connection*** frame. In this case, similarly to the NAS connection tab in server mode, the button will show ***Start*** or ***Stop*** depending on the status of the connection to the subscriber applications.

The remaining settings in the tab may be changed in edit mode.



Settings can be configured as follows:

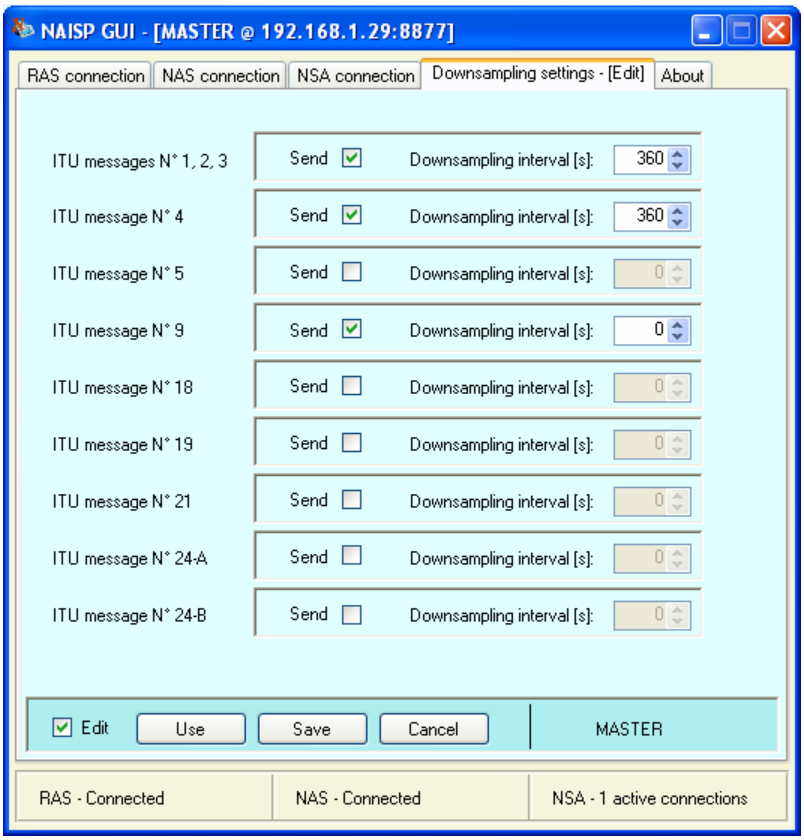
- ***TCP port:*** The TCP port on which NAISP Core listens for connection requests from subscriber applications.
- ***Require authentication:*** When this checkbox is selected, NSAs connecting to the NAISP are required to authenticate to be granted access to AIS data.
- ***Timeout:*** The maximum time NAISP will wait for authentication from the NSA after accepting its connection request.
- ***Username*** and ***Password:*** The login data that the subscriber application needs to send to authenticate. The format that NAISP expects for the authentication data is defined in the file *NSA_template_auth_str.txt* located in the NAISP Core installation directory. The format of this file is defined in appendix A. The default format consists of the username and password preceded, separated and followed by single non-printable ASCII characters of value, respectively, 1, 0 and 0. For example, if the username is *MedProxy* and the password is *EMSA*, the following sequence of bytes needs to be sent by the subscriber application:

  <1>MedProxy<0>EMSA<0>

  where <x> stands for the non-printable ASCII character of value x.
- ***Enable filter:*** This checkbox has the same function as in the NAS connection tab in server mode.

3.6 DOWNSAMPLING SETTINGS

One function of the NAISP is getting AIS messages from the NAS and forwarding them to the RAS. NAISP handles a subset of the different AIS message types defined by the ITU-R M.1371-3 recommendation; message types belonging to this subset are shown in the ***Downsampling settings*** tab.



Depending on the requirements of the application, filtering and downsampling criteria may be applied to the messages to be sent to the RAS. *Filtering* means that all messages of a certain type must not be sent to the RAS; *downsampling* means imposing a minimum time that must occur between consecutive transmissions of messages of the same type coming from the same AIS target. Settings for these operations may be made in the ***Downsampling settings*** tab.

When edit mode is active, an AIS message type may be enabled for transmission by selecting the corresponding ***Send*** checkbox. If a message type is enabled, a downsampling value may be set for that type by entering the desired value in seconds in the ***Downsampling interval*** box. If this value is set to zero, downsampling for that type of message will not be performed and all messages available will be sent.

In the configuration example shown in figure, the message types enabled are 1, 2, 3 and 4, with a downsampling interval of 360 seconds (the default value), and 9, without downsampling. All other messages are not sent to the RAS.

APPENDIX A: FORMAT OF AUTHENTICATION DATA TEMPLATES

The authentication data templates define the format that NAISP uses to send, or in which expects to receive, the username and password to perform authentication. These templates are stored in files which can be modified to suit individual needs.

The files contain text that defines the format of the authentication string. If the % character is encountered in the text, the % itself and the following two characters are interpreted as a token, which is replaced by the application according to the following rules:

- `%un`: Username;
- `%pw`: Password;
- `%xx`, where `xx` is a 2-digit hexadecimal number: The ASCII character of value xx.

For example, if the file contains the following template:

```
%01username:%un%00password:%pw%00
```

and if the username is *MedProxy* and the password is *EMSA*, the authentication string will be defined as:

```
<1>username:MedProxy<0>password:EMSA<0>
```

where `<x>` stands for the non-printable ASCII character of value x.