



IntegriTAS
THREAT ASSESSMENT SYSTEM

IntegriTAS User Manual





IntegriTAS User Manual

International Institute for Democracy and Electoral Assistance

© 2018 International Institute for Democracy and Electoral Assistance

International IDEA publications are independent of specific national or political interests. Views expressed in this publication do not necessarily represent the views of International IDEA, its Board or its Council members.



The electronic version of this publication is available under a Creative Commons (CC) Attribution-NonCommercial-ShareAlike 3.0 licence. You are free to copy, distribute and transmit the publication as well as to remix and adapt it provided it is only for non-commercial purposes, that you appropriately attribute the publication, and that you distribute it under an identical licence.

For more information visit the Creative Commons website:
<<http://creativecommons.org/licenses/by-nc-sa/3.0/>>.

International IDEA
Strömsborg
SE-103 34 STOCKHOLM
SWEDEN
Tel: +46 8 698 37 00
Email: info@idea.int
Website: www.idea.int

Design and layout: International IDEA

Contents

Introduction	6
1. Getting the system up and running	7
2. Help	16
3. Knowledge Resources Module.....	17
4. Analytical Instrument Module	26
5. Creating and editing an analytical model	37
6. Adding data to an analytical model	43
7. Mapping	47
8. Settings	51
9. Saving work	54
10. Cumulative factors	59
11. Static markers	64
12. Charting	72
13. Keyhole mark-up language and Google Earth	74
14. Threat and Action Register (TAR)	76
15. Prevention and Mitigation Module	80
About IntegriTAS	87
About International IDEA	88

Introduction

This User Manual provides advice for users of the IntegriTAS Threat Assessment System. It presents the steps required to get the system up and running, including system requirements, installation and user administration. It also describes how the user can access help, and what knowledge resources can be accessed as part of the system, including ways in which the user can add, modify, delete or reorder factors.

The Manual also features instructions on the software's analytical instrument's module, particularly how to import and download maps, how to create maps in the software and, more broadly, how to create and edit an analytical model, add data to an existing one, and perform mapping with the software. Importantly, the Manual provides instructions on various software settings, such as connecting to new servers, dealing with maps or charts, and saving the work by creating backups, restoring, exporting or importing a model. Users are also guided on how to create and add cumulative factors, as well as static markers and charting. Since the system includes the potential usage of Google Earth, this Manual provides instructions to implement this. On prevention and mitigation, the Manual indicates how the user can make use of the Threat and Action Register (TAR) by creating a threat alert and a master TAR. Finally, the Manual helps users to add and manage responses and action points.

The IntegriTAS Threat Assessment System as a whole focuses on the threats that transnational organized crime poses to democracy by supporting the users' capacity to design prevention and mitigation strategies. The system helps identify threats by looking into its driving factors on two separate—albeit related—dimensions: (a) democratic vulnerabilities; and (b) presence of organized crime networks. The software supports this analytical process by mapping and creating trend charts based on a series of selected indicators that measure each factor under the two dimensions, and crafting an action register to design related prevention and mitigation strategies.

1. Getting the system up and running

1.1. System requirements

To install the IntegriTAS Threat Assessment System, you will need a licence that can be accessed from the International IDEA website. After receiving the license, you can download the IntegriTAS installer.

IntegriTAS works on a server-client based system, with the following requirements:

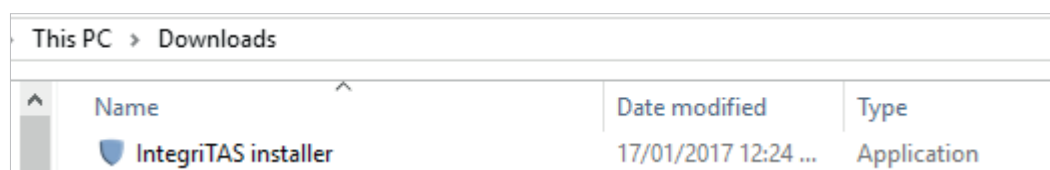
- Windows 7 and above (32/64 bit)
- .Net Framework 4.5 (automatically installed by the installer)
- Microsoft SQL 2012 (automatically installed by the installer)
- Hard disk storage: up to 1 GB

1.2. Installation steps


Step 1

Locate the IntegriTAS Installer. If you downloaded the tool from the Internet, it will usually be in the 'Downloads' folder. If not, it will be on a flash drive or elsewhere on the computer's hard drive. Find the installer as shown in Figure 1.1.

Figure 1.1. Installer location



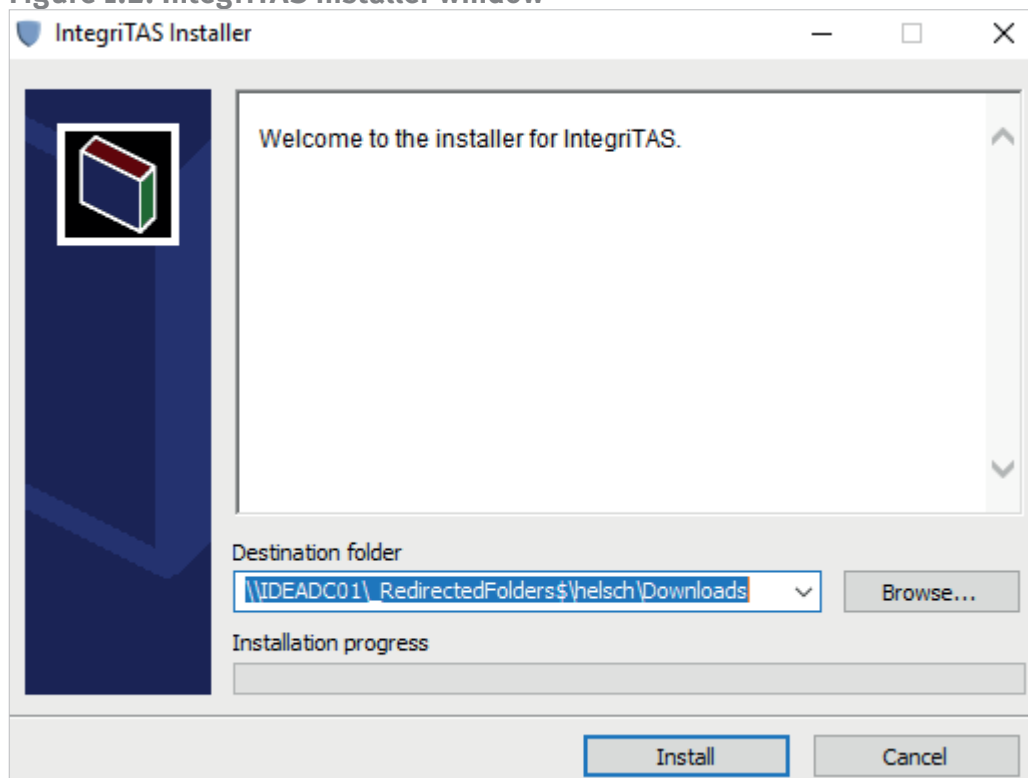
The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Downloads'. The main area displays a table of files. The table has three columns: 'Name', 'Date modified', and 'Type'. There is one file listed: 'IntegriTAS installer', which has a date modified of '17/01/2017 12:24 ...' and is of type 'Application'.

Name	Date modified	Type
 IntegriTAS installer	17/01/2017 12:24 ...	Application

Step 2

After you locate the installer, double click on the 'IntegriTAS Installer'. Then click on 'Install', as shown in Figure 1.2. The system extracts all the required files to the same location as the installer, and it may take one or more minutes to complete.

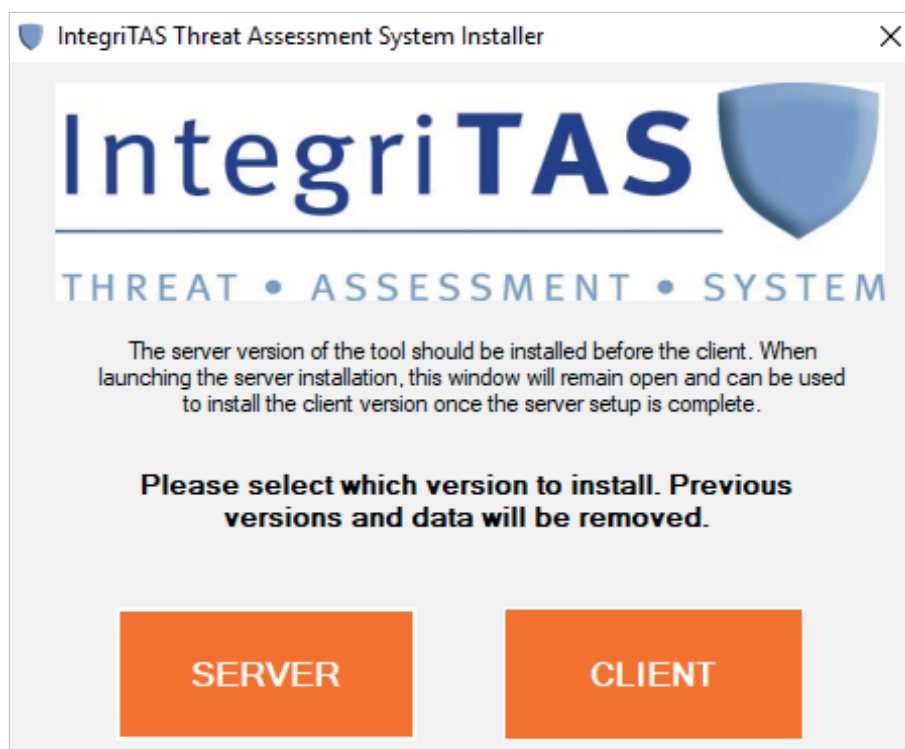
Figure 1.2. IntegriTAS installer window



Step 3

After the IntegriTAS installer has completed the download, it opens automatically as a launcher, as shown in Figure 1.3.

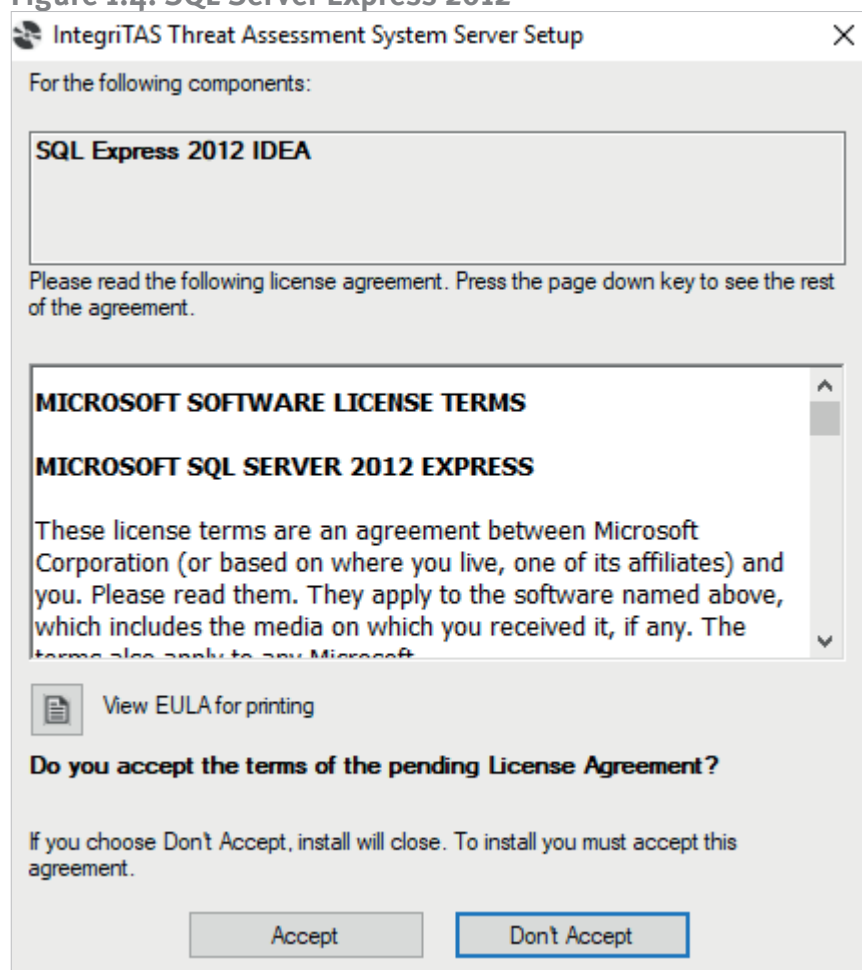
Figure 1.3. IntegriTAS launcher



Step 4

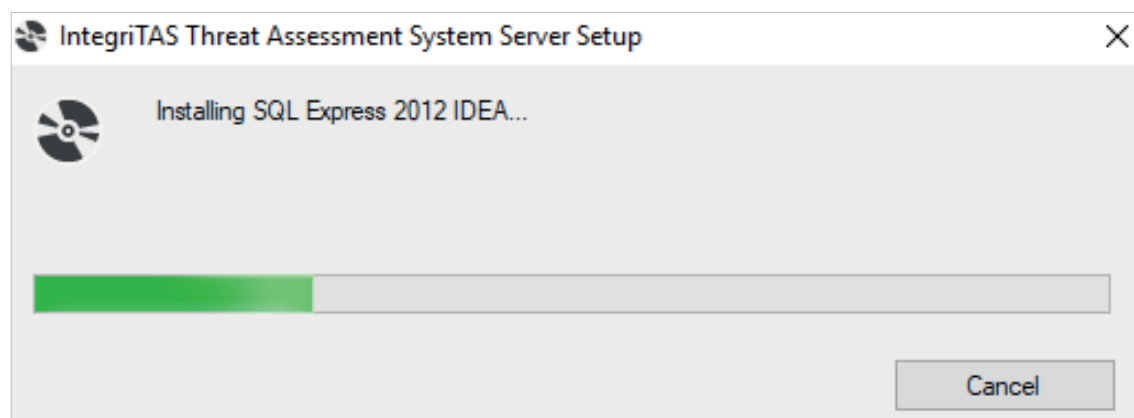
As IntegriTAS is a server-client based system, you must click on 'Server' to initiate the IntegriTAS installation. After you click on 'Server', a new window pops up to install SQL Server Express 2012, after which you must click on 'Accept' as shown in Figure 1.4.

Figure 1.4. SQL Server Express 2012



This installation takes approximately 10 minutes. If the system asks for any further information, you accept by clicking 'Yes' or 'Ok' as required. Figure 1.5 appears on your desktop.

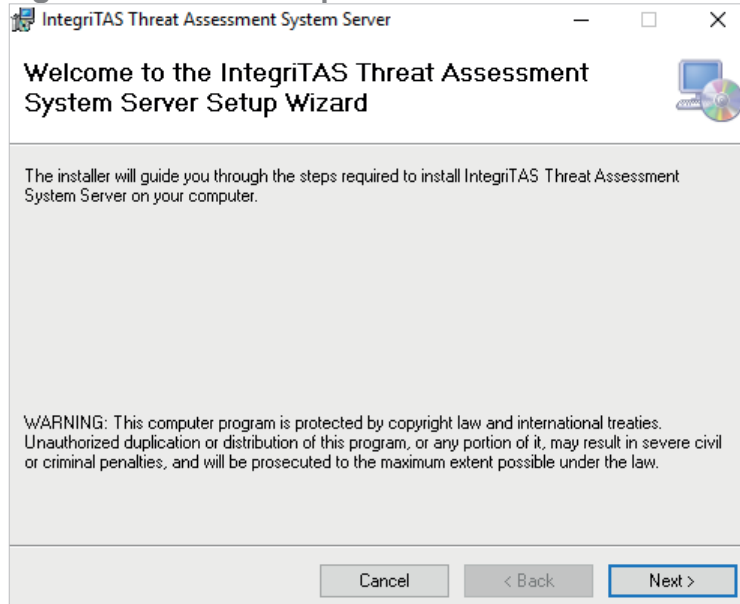
Figure 1.5. SQL Server Express 2012 progress report



Step 5

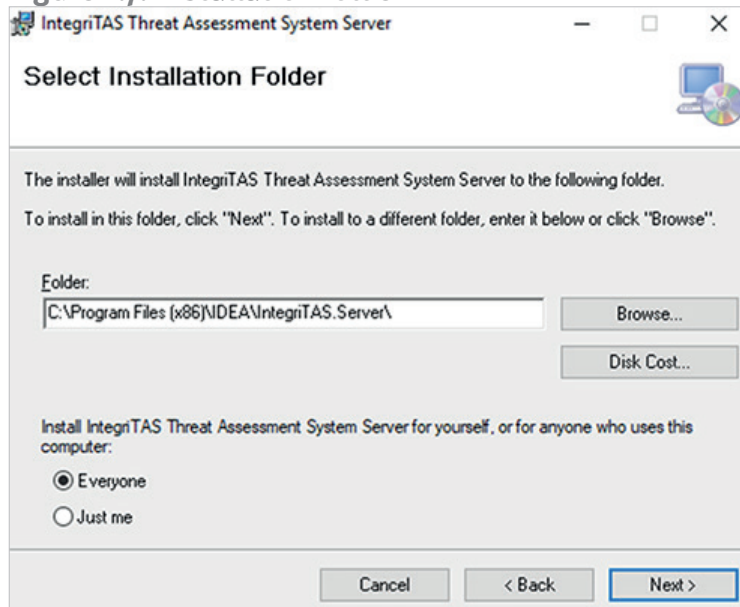
Once the first phase of the installation is complete, the IntegriTAS installer requests to install the server on the system. When Figure 1.6 appears on your screen, click 'Next'.

Figure 1.6. Server setup wizard



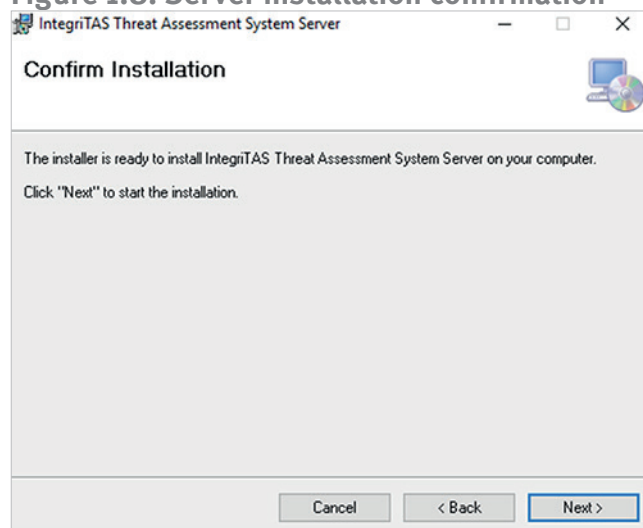
Click 'Next' again and the system specifies where the IntegriTAS Server will be installed, as in Figure 1.7.

Figure 1.7. Installation folder



To confirm and continue with the installation, click 'Next', as shown in Figure 1.8.

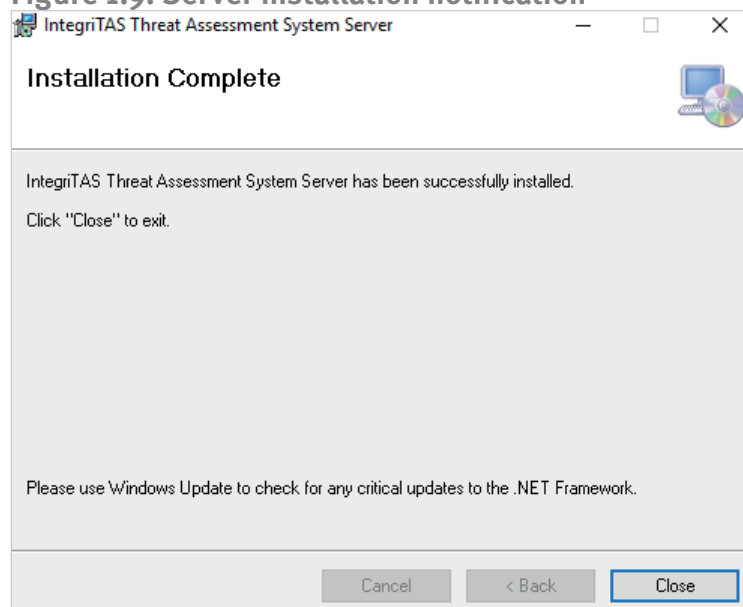
Figure 1.8. Server installation confirmation



Now click 'Next' again to confirm your installation of the IntegriTAS Server. Then click 'Yes' or 'Ok' when asked by the operating system for any information shown in the screen.

It takes less than a minute to install the IntegriTAS Server on your system. Once this is done, the message in Figure 1.9 appears with a confirmation of the successful completion of the installation. Click 'Close' to finish the IntegriTAS Server installation.

Figure 1.9. Server installation notification



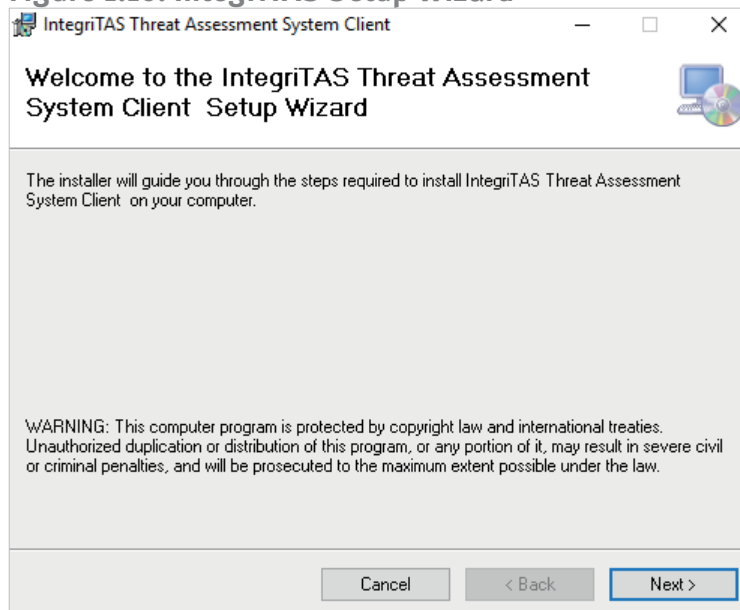
Step 6

To install the client after you finish installing the server, click 'Client' on the launcher. Click 'Yes' or 'Ok' when required.

If your system does not have .Net or other necessary components required by IntegriTAS, the installer installs automatically. If asked, click 'Yes' or 'Ok'.

Click 'Next' to proceed, as shown in Figure 1.10.

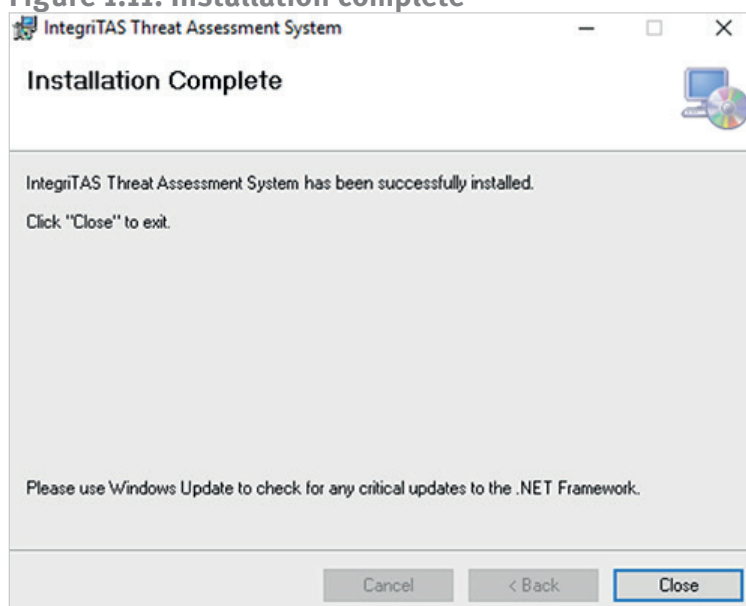
Figure 1.10. IntegriTAS Setup Wizard



Just as in the Server installation, the installer shows where the IntegriTAS Client is installed. Click 'Next' to proceed, and 'Next' again to begin installation.

Once the installation is complete, click 'Close', as shown in Figure 1.11.

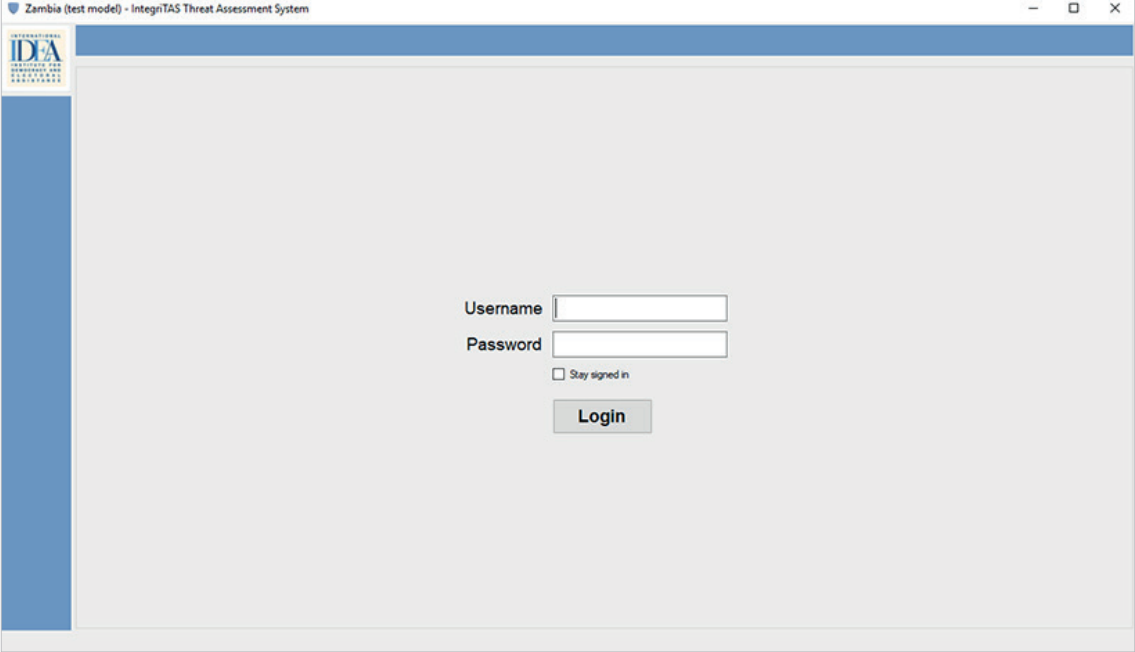
Figure 1.11. Installation complete



Step 7

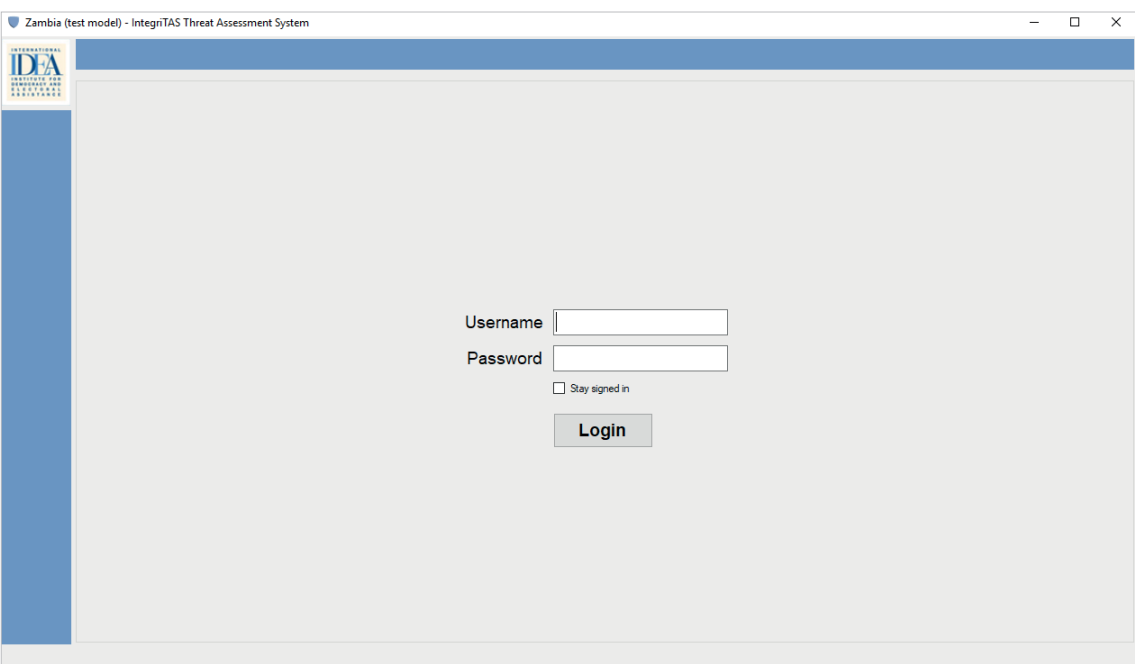
When you have successfully installed IntegriTAS on the system, you will see the IntegriTAS logo on your desktop. Double click it to open IntegriTAS. When Figure 1.12 appears, enter the ‘Username’ and ‘Password’. The default username is ‘admin’ and password is ‘123456’.

Figure 1.12. Login screen



Click ‘Login’. Figure 1.13 appears, with the Side Bar, Menu Bar, Module Selection, and Current User information.

Figure 1.13. IntegriTAS content menu



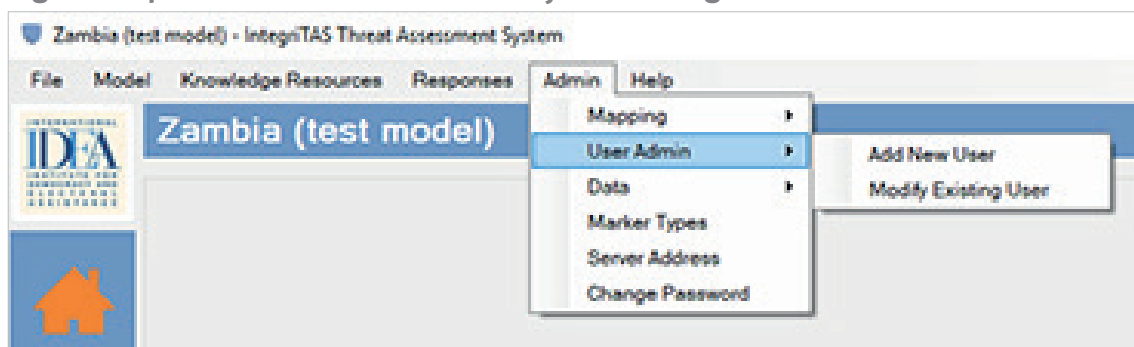
1.3. User administration

You can change the account settings, which are designed to increase data security. You can set privileged settings, such as 'reader', 'data entry', 'country administrator' or 'super administrator'.

Step 1

To create a new user or modify an existing user, as shown in Figure 1.14, go to the 'Admin' menu → 'User Admin' → 'Add new user' to add new user, or 'Modify existing user' to update information about the user.

Figure 1.14. Create a new user or modify an existing user



Step 2

Once you click 'Add new user', Figure 1.15 appears, and you can add the user's First Name, Last Name, desired username and password, email and specific user privileges. Afterwards, click 'Save'.

Figure 1.15. Add user details

 The screenshot shows the 'Add new user' form within the IntegriTAS Threat Assessment System. The form contains the following fields: First Name, Last Name, Username, Password, Confirm Password, Email, and Role (a dropdown menu currently set to 'Super Administrator'). There are 'Save' and 'Cancel' buttons at the bottom right of the form. The interface includes a top menu bar with 'File', 'Model', 'Knowledge Resources', 'Responses', 'Admin', and 'Help'. A sidebar on the left contains icons for home, documents, globe, and mail.

Step 3

To modify the user's information, click on 'Modify Existing user' and Figure 1.16 appears. You must log in as the Super Administrator to modify user details.

You can select the user and change their First Name, Last Name, desired username and password, email and privileges. Then click 'Save'.

Figure 1.16. Modify user

The screenshot shows the 'User modify' window of the 'Zambia (test model) - Electoral Risk Management Tool'. The window has a menu bar with 'File', 'Model', 'Knowledge Resources', 'Responses', 'Admin', and 'Help'. A sidebar on the left contains icons for home, documents, a globe, a circular arrow, a folder, and an envelope. The main area is titled 'User modify' and contains a 'Users' dropdown menu set to 'admin'. Below this is a form with the following fields: 'First Name' (Admin), 'Last Name' (Admin), 'Username' (admin), 'Password' (masked with asterisks), 'Confirm Password' (masked with asterisks), and 'Email' (admin@idea.int). A 'Role' dropdown menu is open, showing a list of roles: 'Super Administrator', 'Super Administrator', 'Country Administrator', 'Data Entry', and 'Reader'. The 'Cancel' and 'Delete' buttons are located at the bottom right of the form.

Step 4

To change the current user password, go to 'Admin' -> 'Change Password'. Figure 1.17 appears. Add the new password and confirm it. Click 'Save' to update the new password.

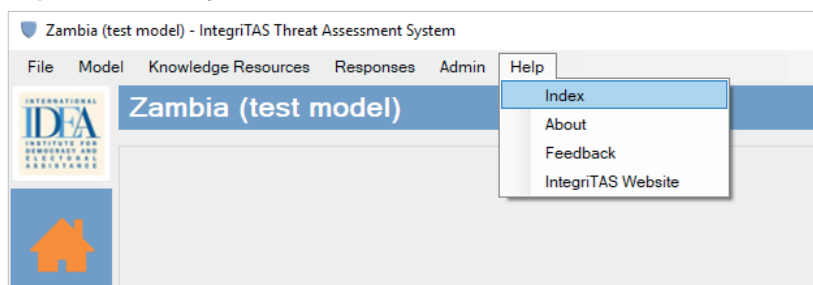
Figure 1.17. Change password

The screenshot shows the 'Change Password' dialog box. It has a title bar that says 'Change Password'. Inside the dialog, there are two text input fields. The first is labeled 'New password' and the second is labeled 'Confirm new password'. Below these fields are two buttons: 'Save' and 'Cancel'.

2. Help

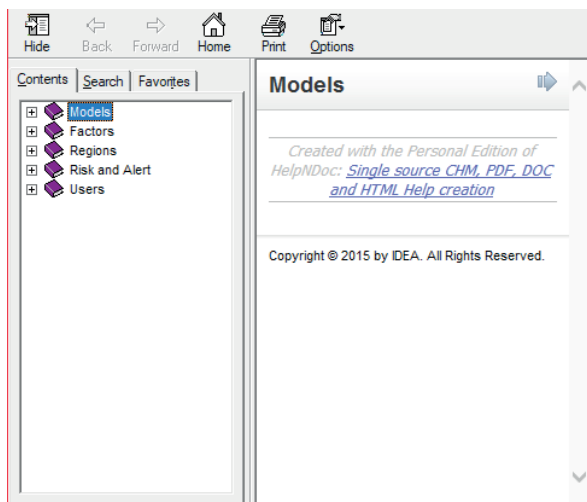
You can access self-help resources such as the Help Index, which covers all the main tool features and is divided into six main folders: Models, Factors, Regions, Threat and Alert, Copying and Pasting, and Users. To access the Help Index, click on 'Help' → Index, as shown in Figure 2.1.

Figure 2.1. Help menu



The Help file appears in a new window, as shown in Figure 2.2.

Figure 2.2. Help file



3. Knowledge Resources Module

The IntegriTAS threat assessment system helps identify the threat that organized crime poses to democratic politics. Focusing on the threat allows you to map and focus on the factors that contribute to this type of corruption, and identify related strategies to prevent or mitigate the threat.

IntegriTAS uses a bi-dimensional approach to examine the incentives and drivers of these relationships under a political economy analysis that considers the relevant stakeholders by focusing first on the democratic structure and given vulnerabilities at different geographical levels according to the various phases of the electoral cycle. Second, the tool focuses on the presence and scope of organized crime networks in the given geographical area. Coupling the analysis of these two dimensions allows you to identify, map and monitor the threat factors, and subsequently plan and implement evidence-based prevention and mitigation strategies.

The Virtual Knowledge Resource Library (VKRL) provides a list of factors that increase the threat of organized crime distorting democratic politics. The factors are divided into two parallel dimensions: (a) democratic vulnerabilities and (b) organized crime. In each dimension you can customize the list of factors according to the specific geographical area or local context.

The VKRL is based on the 21 factors described in the IntegriTAS Process Guide and the IntegriTAS Action Guide. Each of these 21 factors includes: (a) a general definition and explanation of the context in which it can contribute to the nexus between organized crime and politics; (b) empirical evidence of countries and examples in which the factor contributed to the nexus between organized crime and politics; and (c) observable indicators. Once the knowledge resources are customized, you can create analytical models by selecting the factors you wish to monitor.

Factors presented in the Knowledge Resources module are compiled from various research papers, reports and other relevant publications. The VKRL can consist of two kinds of factors—colour-coded factors (marks different features of threat level with different colours) and cumulative factors (numerical representation of the factor).

By default, only colour-coded factors are included from the guides on the threats and vulnerabilities posed by the political–criminal nexus.

3.1. Accessing the Virtual Knowledge Resource Library (VKRL)

Step 1

You can access the VKRL from:

- The Menu Bar: Knowledge Resources → View Factors
- The Side Bar
- The Module Selection Bar

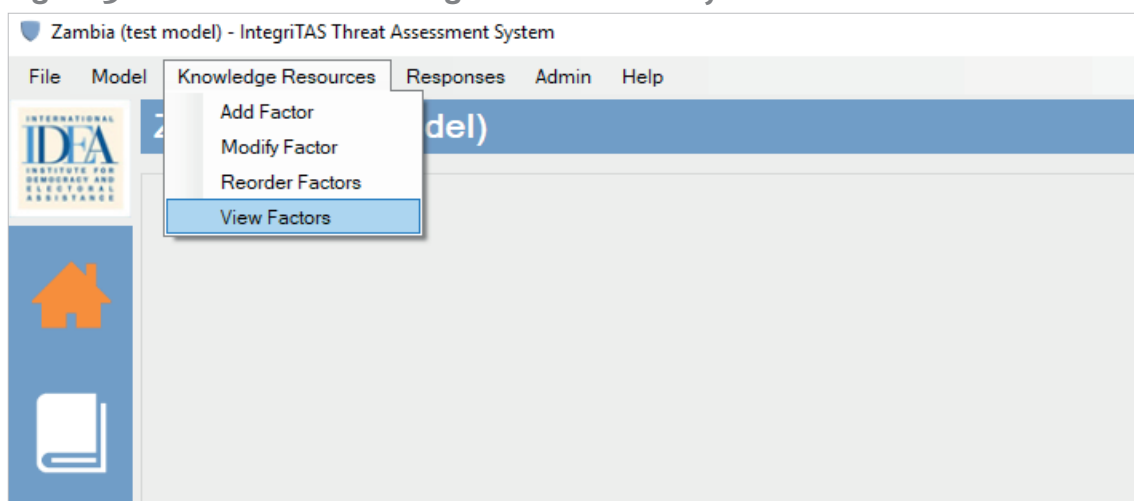
Figure 3.1 displays these options.

Figure 3.1. Access the Virtual Knowledge Resource Library



Figure 3.2 shows how to access the VKRL through the Menu Bar.

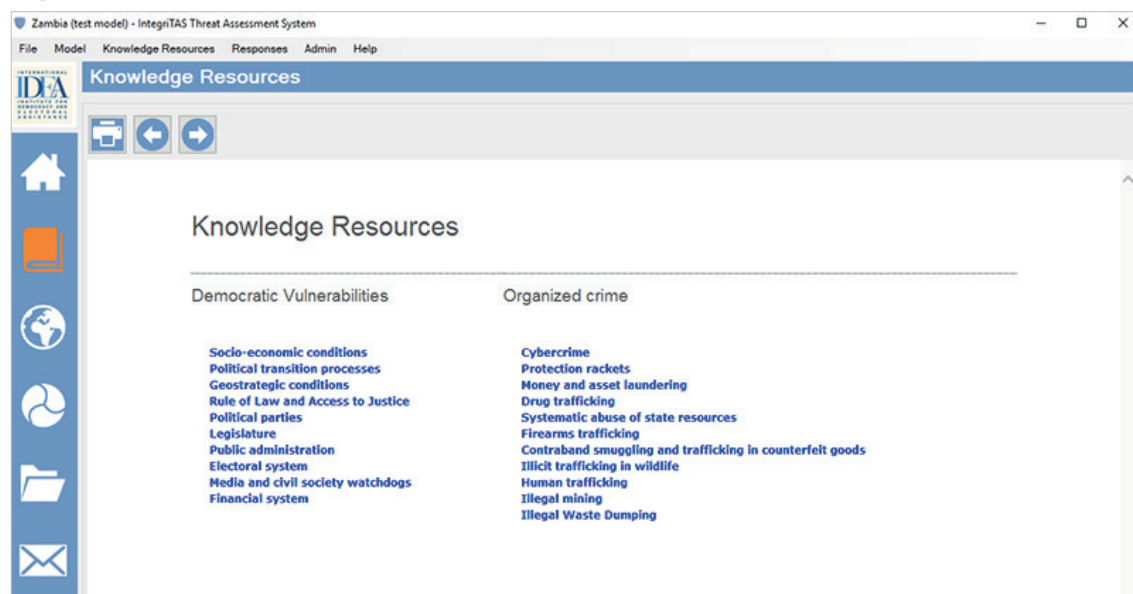
Figure 3.2. The Virtual Knowledge Resource Library in the menu bar



Step 2

Click on the VKRL, and 10 democratic vulnerability factors and 10 organized crime factors appear, as shown in Figure 3.3. The VKRL icon is highlighted in the side bar.

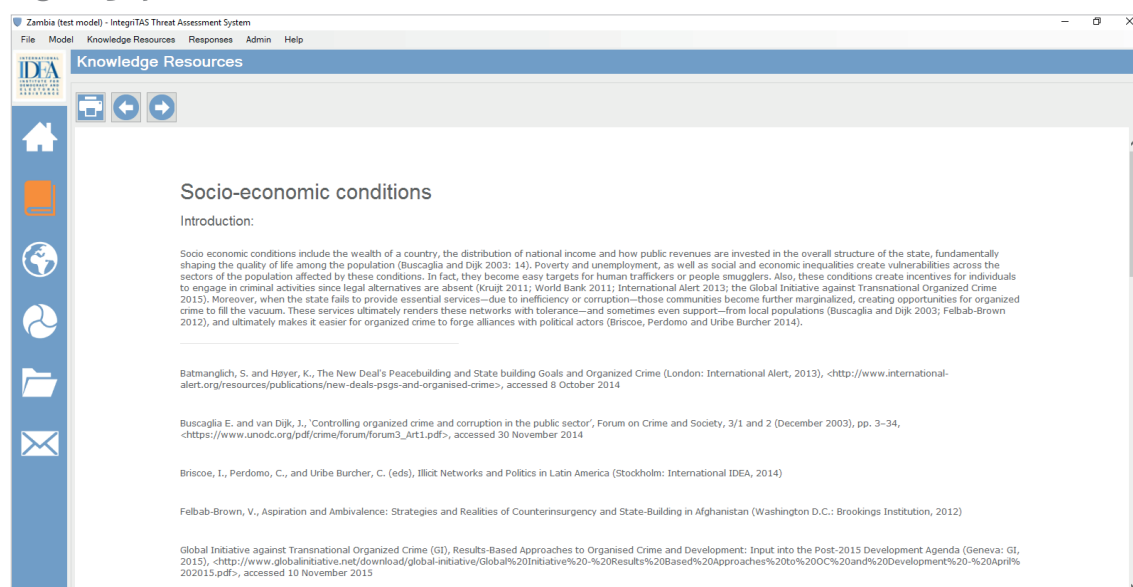
Figure 3.3. List of factors



Step 3

Click on a factor (e.g. Socio-economic conditions), and the introduction, empirical cases and interrelated factors, and observable indicators will appear, as in Figure 3.4.

Figure 3.4. The content of an individual factor



3.2. Adding, modifying and reordering factors

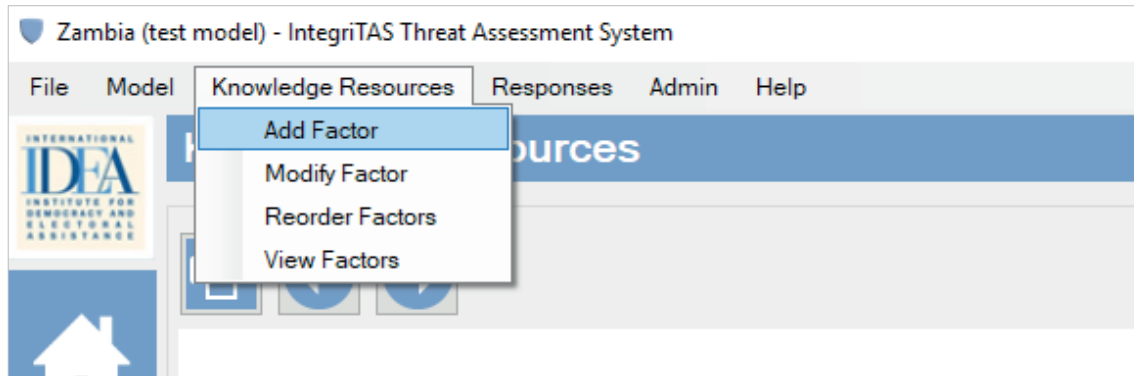
Customize the tool by adding new factors, modifying factors, removing factors and re-ordering factors. The factor added in the tool is shown on the VKRL and Create new model. This feature adds to the tool's flexibility, as analytical models can include country- and election-specific factors that were not originally included in the VKRL. All factors in IntegriTAS can be modified or deleted, thus adding to the tool's flexibility.

3.2.1. Adding new factors

Step 1

To create a new factor, click on Knowledge Resource → Add Factor, as in Figure 3.5.

Figure 3.5. Add factor in dropdown menu



Step 2

Click 'Add factor'. A new window opens, as shown in Figure 3.6.

Figure 3.6. Add factor popup window

 The screenshot shows the 'Add new factor' window. It contains the following fields and controls:

- Factor Name:** A text input field.
- Factor Type:** A dropdown menu with 'Scale' selected.
- Scale:** A dropdown menu with 'Cumulative' selected.
- Democratic vulnerabilities:** A dropdown menu.
- Min:** A numeric input field with the value '1'.
- Interval:** A numeric input field with the value '1.0'.
- Max:** A numeric input field with the value '5'.
- Factor Texts:** A section with a dropdown menu set to 'Introduction'.
- Introduction:** A large text area for entering the factor's description.
- Documents:** A section with four buttons: 'Preview', 'Link Document', 'Add Document to Library', and 'Delete Document from Library'.
- Save/Cancel:** Two buttons at the bottom right.

 The window title is 'Zambia (test model) - IntegriTAS Threat Assessment System'.

Step 3

Fill in the spaces for Factor Name, Factor Type (Scale for colour-coded factor), Democratic Vulnerability or Organized Crime, as shown in Figure 3.7.

Select values for Minimum, Maximum and Interval. Minimum value represents the lowest threat level for that factor. Maximum value represents the highest threat level for that factor. Interval represents the numerical scales in which intervals have the same interpretation throughout.

Figure 3.7. Factor properties

The screenshot shows the 'Add new factor' form in the IntegriTAS Threat Assessment System. The form is titled 'Add new factor' and has a sidebar with icons for Home, Knowledge Resources, Responses, Admin, and Help. The main form area contains the following fields and controls:

- Factor Name:** A text input field.
- Factor Type:** A dropdown menu with 'Scale' selected.
- Scale:** A dropdown menu with 'Democratic vulnerabilities' selected.
- Scale:** A dropdown menu with 'Democratic vulnerabilities' selected.
- Min:** A text input field with '1'.
- Interval:** A text input field with '1.0'.
- Max:** A text input field with '5'.
- Factor Texts:** A dropdown menu with 'Introduction' selected.
- Introduction:** A text area for the factor's introduction.
- Documents:** A section with buttons for 'Preview', 'Link Document', 'Add Document to Library', and 'Delete Document from Library'.
- Save and Cancel:** Buttons at the bottom of the form.

Step 4

You can add a Factor Name, Factor Type or Scale. From the dropdown menu under Factor texts, select 'Introduction' and add a brief description of the factor, as shown in Figure 3.8. Empirical cases on the factor can also be added. Observable indicators, data collection methodology and questionnaires can also be added using this dropdown menu.

Figure 3.8. Factor texts

The screenshot shows the 'Add new factor' form in the IntegriTAS Threat Assessment System, with the 'Factor Texts' dropdown menu open. The dropdown menu lists the following options:

- Introduction
- Empirical Cases
- Observable Indicators
- Data Collection
- Questionnaire

The form also includes the same fields and controls as Figure 3.7, including the 'Factor Name', 'Factor Type', 'Scale', 'Min', 'Interval', 'Max', 'Introduction' text area, and 'Documents' section with buttons for 'Preview', 'Link Document', 'Add Document to Library', 'Delete Document from Library', 'Save', and 'Cancel'.

Step 5

To save the factor, click 'Save'.

Other options include:

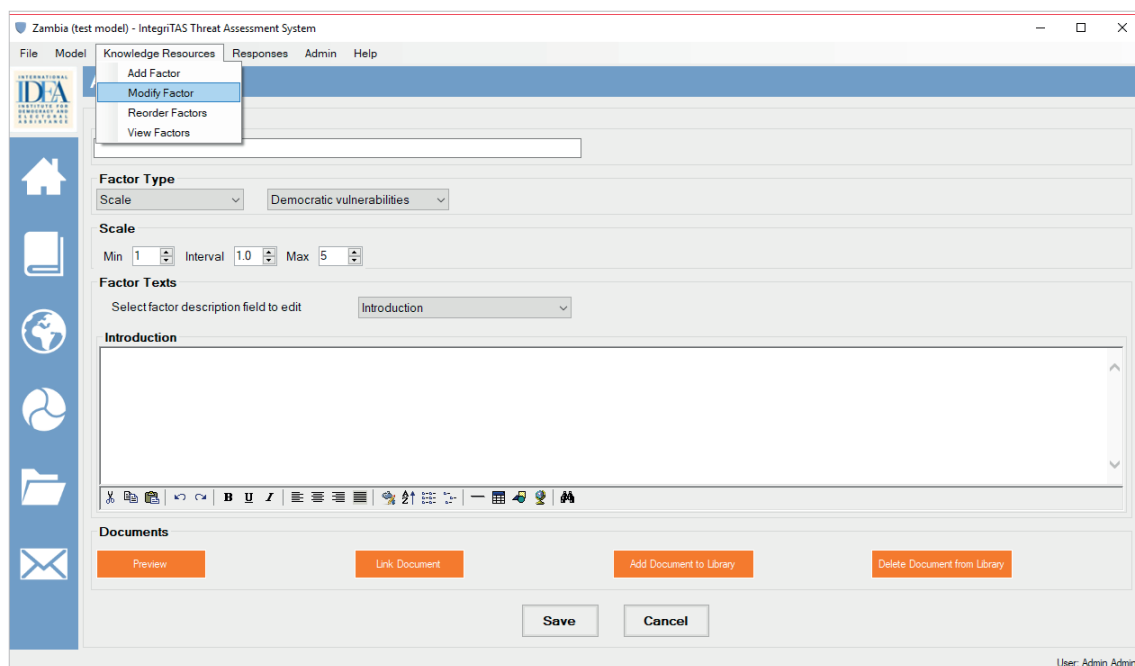
- 'Link Document' creates a hyperlink to the document(s).
- 'Add document to Library' enables you to attach documents to the tool.
- 'Delete documents from Library' removes particular documents from the tool.

3.2.2. Modifying, editing or removing a factor

Step 1

To modify a factor, go to Knowledge Resources → Modify Factor, as shown in Figure 3.9.

Figure 3.9. Modify factor in dropdown menu



Step 2

Select the factor to modify from the Factor list in the dropdown display, as shown in Figure 3.10.

Figure 3.10. Factor selection dropdown menu

Once the factor is selected to modify, you can change the following characteristics:

- Factor Name;
- Factor Type (Democratic Vulnerability or Organized Crime);
- Scale; and
- Factor text (Introduction, Empirical Cases, Observable Indicators, Data Collection and Questionnaires).

Step 3

After modifying the factor, click 'Save' to save the changes.

3.2.3. Deleting a factor

To delete a factor, click Knowledge Resource – Modify Factor. Select the factor that you want to delete from the dropdown menu. Click 'Delete' and confirm it, as in Figure 3.11.

Figure 3.11. Deleting a factor

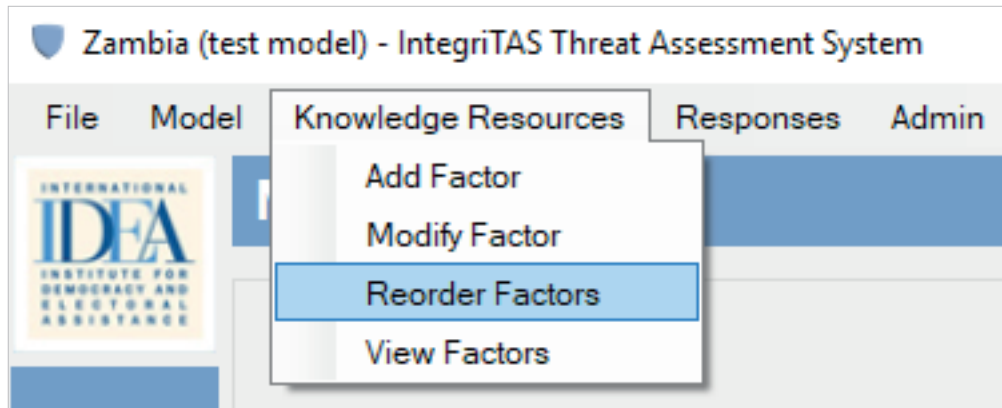
3.2.4. Reorder a factor

You can also rearrange the factors.

Step 1

Click on the Knowledge Resources menu → Reorder Factors, as in Figure 3.12 below.

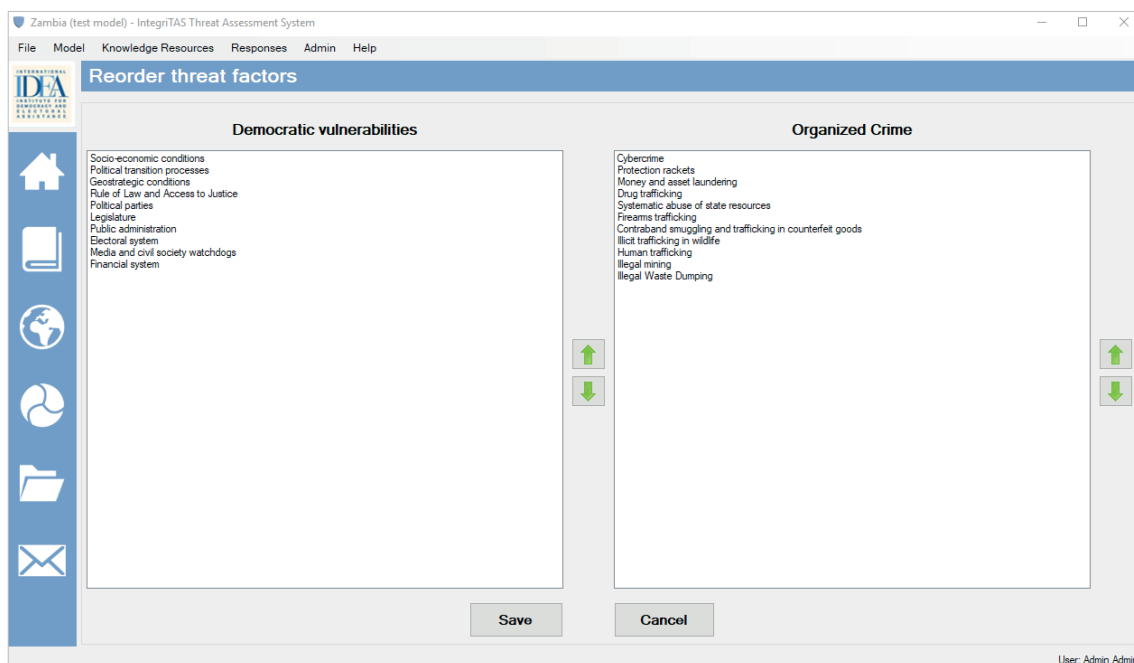
Figure 3.12. Reorder factors in dropdown menu



Step 2

A new window opens, as shown in Figure 3.13. The Democratic Vulnerability factors are displayed on the left side of the window, and Organized Crime factors on the right.

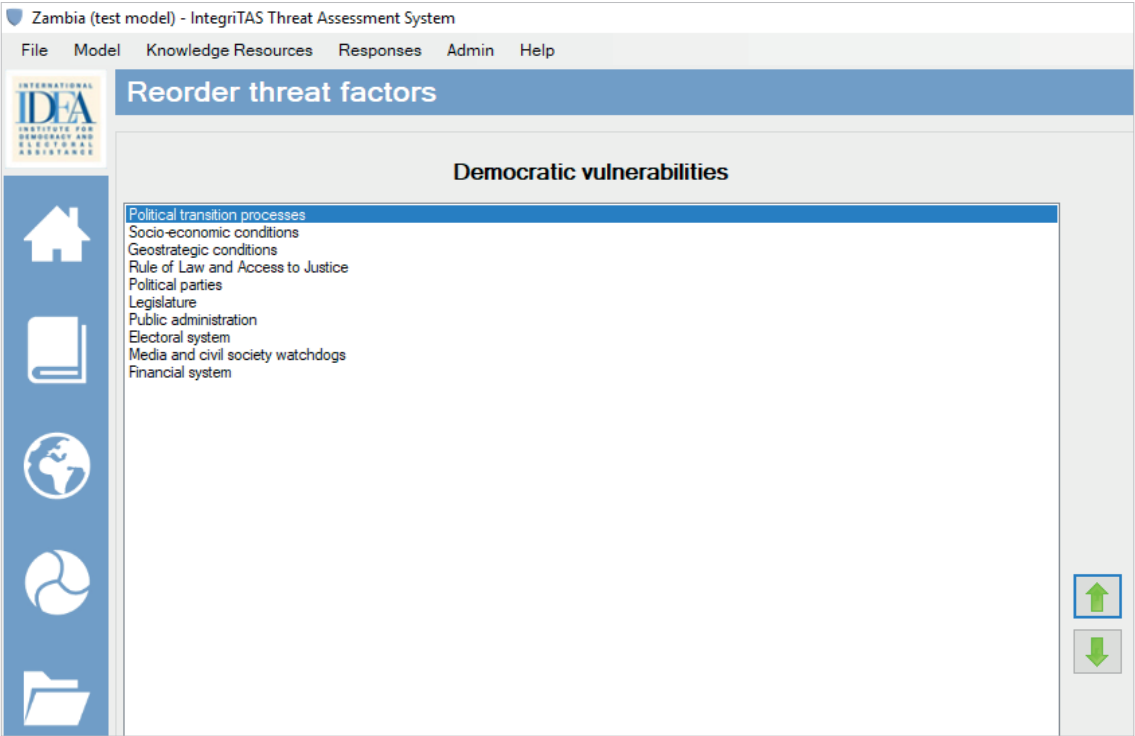
Figure 3.13. Reorder factors popup window



Step 3

To change the order, click to select the specific factor. Click the ‘up’ or ‘down’ arrow, based on the criminal threats or democratic vulnerabilities. As an example, ‘Political transition processes’ have been selected from democratic vulnerabilities in Figure 3.14.

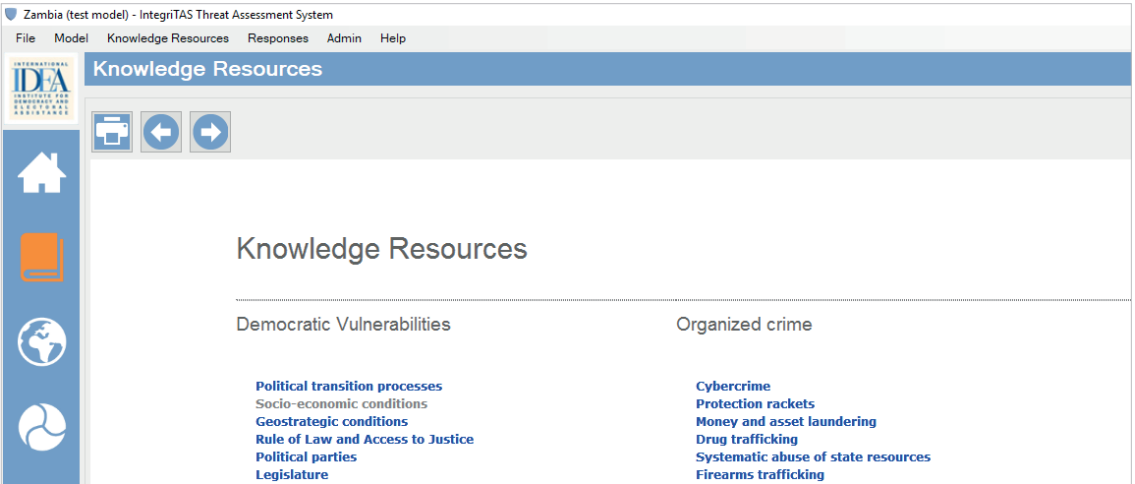
Figure 3.14. Reorder factors using arrows



Step 4

Click ‘Save’ to save the changes. Go back to the VKRL page, and you can see the factor on the top of the window has changed, as shown in Figure 3.15.

Figure 3.15. Virtual Knowledge Resource Library with reordered factors



4. Analytical Instrument Module

4.1. Introduction

The Analytical Instruments Module allows you to upload and analyse data by drawing threat maps and charting threat trends. Before creating an analytical model, all maps and threat factors to be used must be completed in advance.

After creating an analytical model, you can generate and maintain a threat and action register that details threat alerts issued and actions taken. IntegriTAS allows you to export, import or delete analytical models. Maps can be saved within the model and exported as high-resolution pictures or VKML files, which are Google Earth compatible.

The Analytical Instruments Module allows you to: create country- and election-specific analytical models, upload data in order to generate threat maps and trend charts, and create a register of threats and actions.

4.2. Map import

IntegriTAS does not include maps for countries or administrative divisions, provinces, counties or municipalities. Therefore, you must add these maps manually, immediately after installing the application.

The shape maps (.shp files) are typically available from an electoral management body's boundaries department (cartographer) that uses GIS application, on the Internet or from reputable companies producing digital maps. The loading time is reduced when the number of child regions is limited.

4.2.1. Downloading maps

This section provides a guide on how to download and import shape files from the Internet onto a computer, using the example of the website DIVA-GIS as a source and Australia as an example.¹ These steps are only applicable if you are using similar means to import shapefiles for building IntegriTAS models.

Step 1

From a shapefile source, download the Administrative Areas spatial data files of the selected country. For example, DIVA-GIS provides free geographic (GIS) data per country and subject. Find the country you wish to use and click 'OK' to select, as shown in Figure 4.1.

**Figure 4.1. Example download of administrative areas spatial data files:
DIVA-GIS: country selection**



Step 2

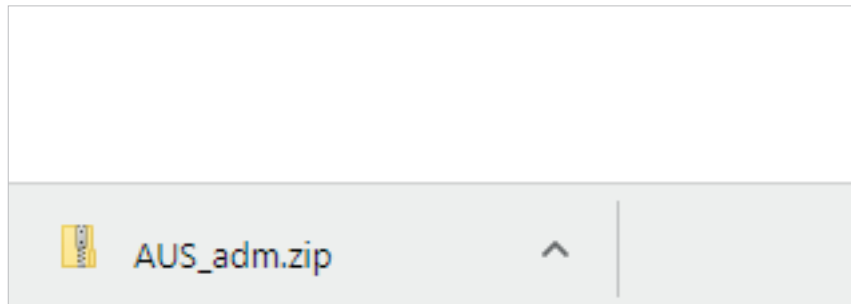
Click 'Download' to begin downloading the zip file in the browser, as shown in Figure 4.2.

**Figure 4.2. Example download of administrative areas spatial data files:
DIVA-GIS zip file download**



A zip file begins downloading in the browser, as shown in Figure 4.3.

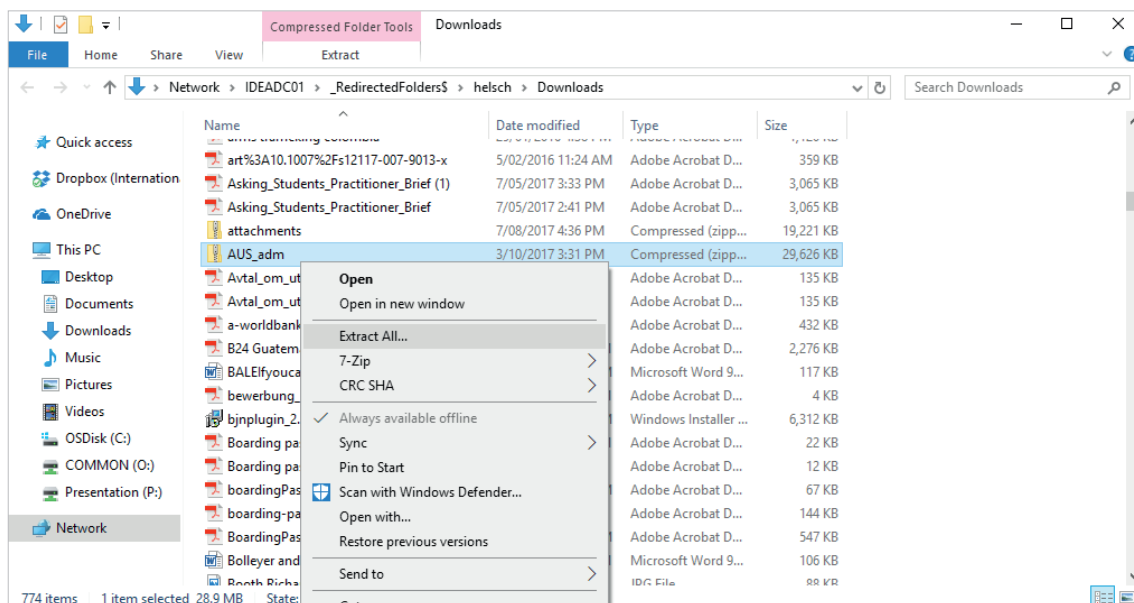
Figure 4.3. Example download of administrative areas spatial data files: DIVA-GIS zip file download progress



Step 3

Locate the zip files in your 'Downloads' folder, and right click to select 'Extract all', as shown in Figure 4.4.

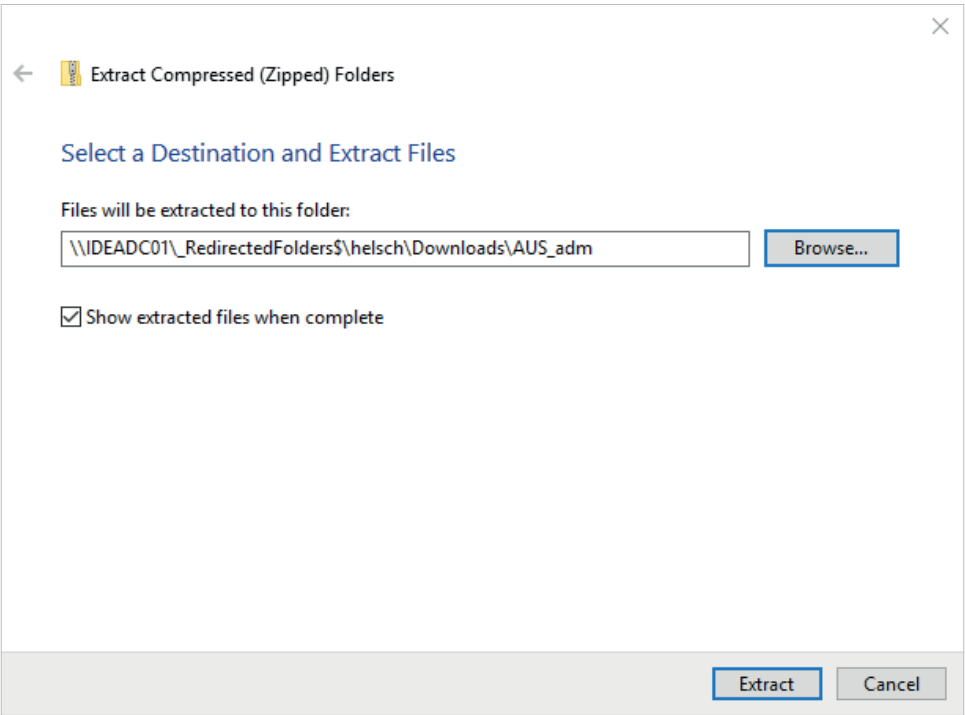
Figure 4.4. Example download of administrative areas spatial data files: DIVA-GIS -zip file extract



Step 4

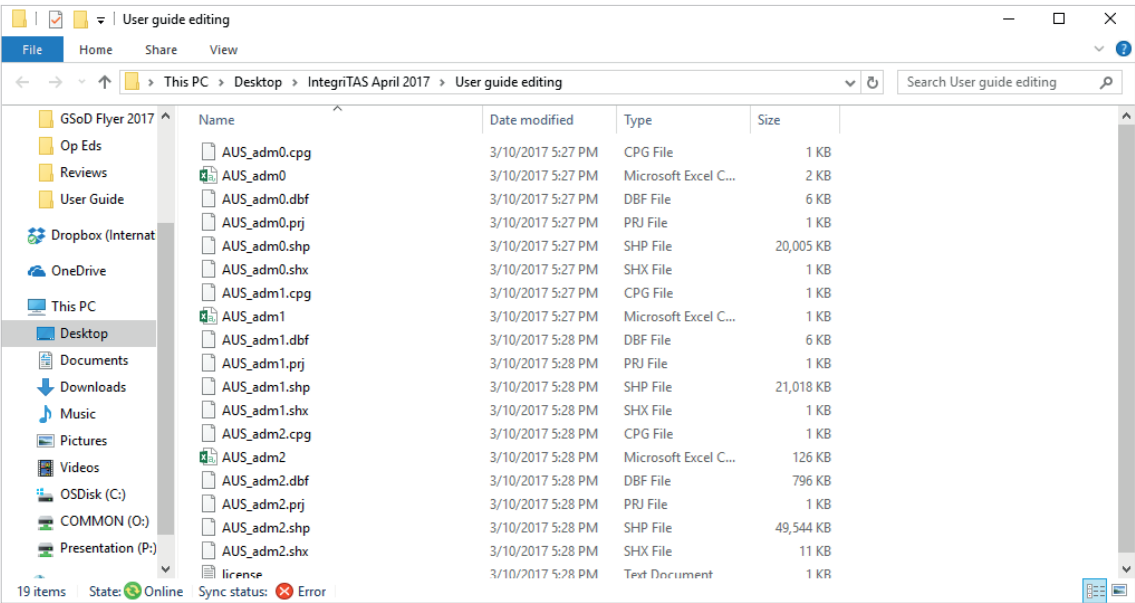
Select where on the computer to save the files by finding the appropriate folder via the ‘Browse...’ button. Click ‘Extract’, as in Figure 4.5.

Figure 4.5. Example download of administrative areas spatial data files: DIVA-GIS-zip file extract destination



The files download into the selected folder within a few seconds, as shown in Figure 4.6. These files will be used in the following section when creating maps.

Figure 4.6. Example download of administrative areas spatial data files: DIVA-GIS zip file extract folder

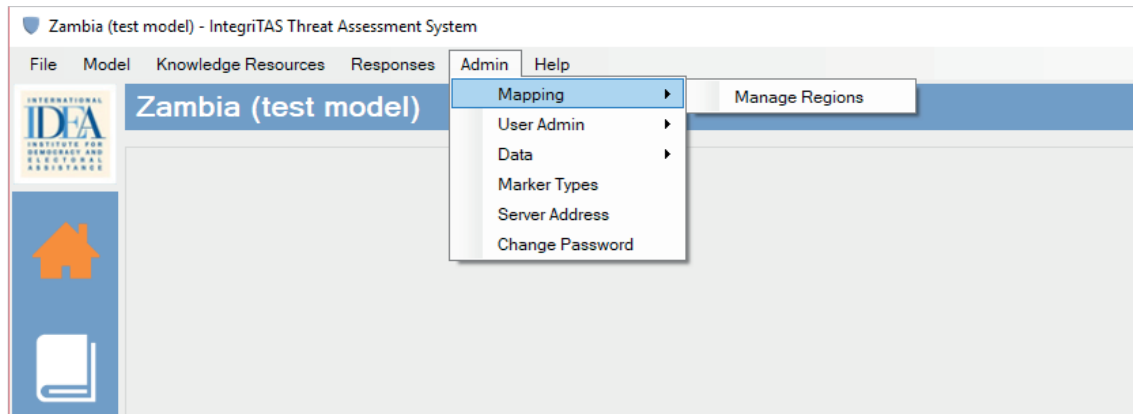


4.2.2. Creating maps in IntegrITAS

Step 1

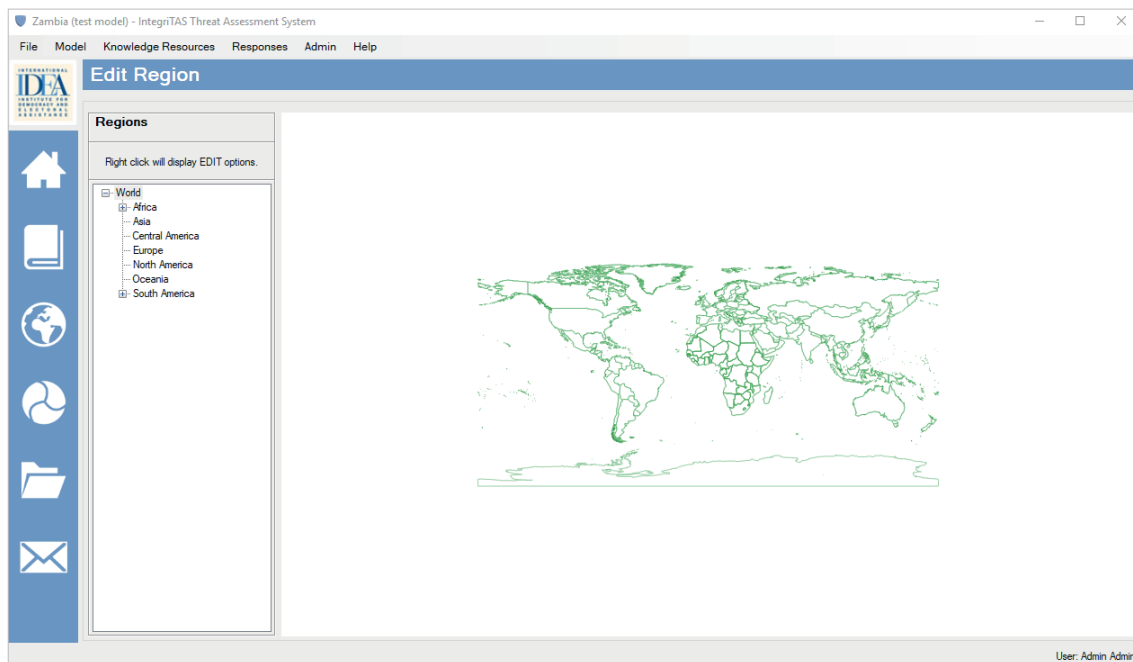
Go to Admin Menu → Mapping → Manage Regions, shown in Figure 4.7.

Figure 4.7. Manage regions' button in 'Admin' dropdown menu



The screen should change to that shown in Figure 4.8.

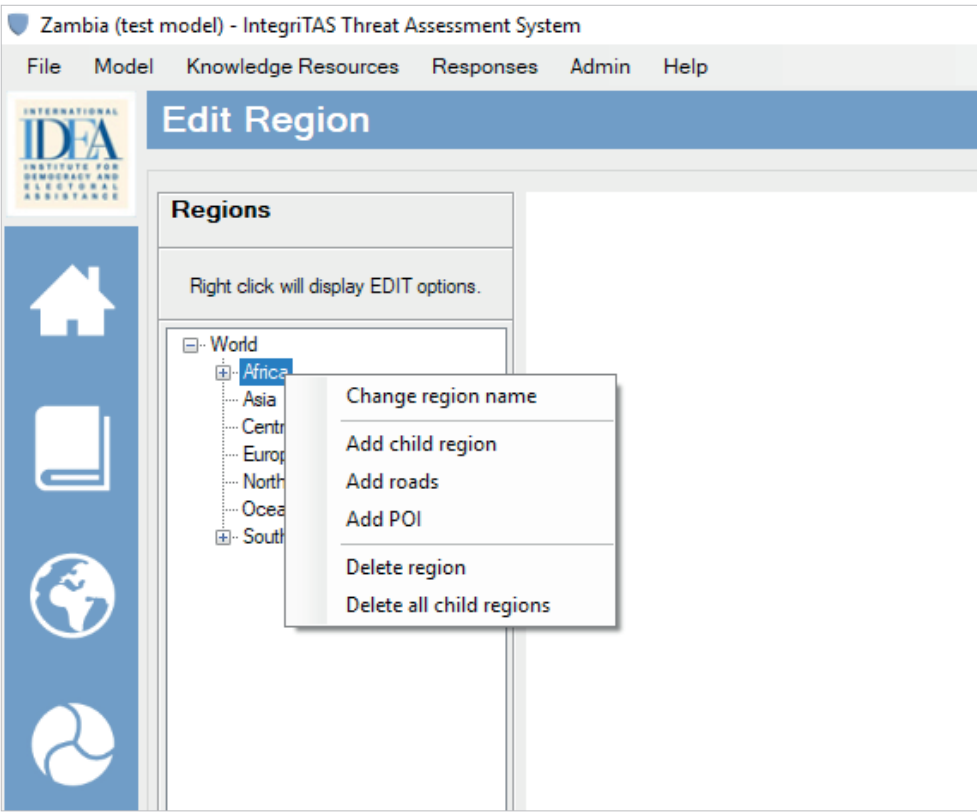
Figure 4.8. Edit region popup window



Step 2

To add more detailed maps of a country, first you need to add regions.
To add regions, right click on the correct region and a menu will appear, as shown in Figure 4.9.

Figure 4.9. Add regions



This right click menu functionality can be used in every level, from the country level to lower levels.

‘Change regions name’: Allows you to rename a region (you can also use their script as part of the customization).

‘Add child region’: Add new regions to the tool (using .shp file).

‘Add roads’: If you have a road .shp file, you can attach it to the tool.




‘Add Point of Interest (POI)’: If you have a POI .shp file, you can attach it to the tool. (For example, if you have a POI .shp file for polling locations you can view it on the tool).

‘Delete region’: Delete a specific region.

‘Delete all child regions’: Delete all the child regions under the parent regions.

This example uses Australia, with three administrative levels, as shown in Figure 4.10.

Figure 4.10. Example of administrative levels: Australia

Name	Date modified	Type	✓
 AUS_adm0.shp	3/10/2017 5:27 PM	SHP File	
 AUS_adm1.shp	3/10/2017 5:28 PM	SHP File	
 AUS_adm2.shp	3/10/2017 5:28 PM	SHP File	

‘Adm0’ – country-level shapefile (boundary level of Australia).

‘Adm1’ – First administrative level (11 states and territories).

‘Adm2’ – Second administrative level (1,395 districts).

Step 3

Right click on the Region, here taking ‘Oceania’ → ‘Add child region’, as shown in Figure 4.11.

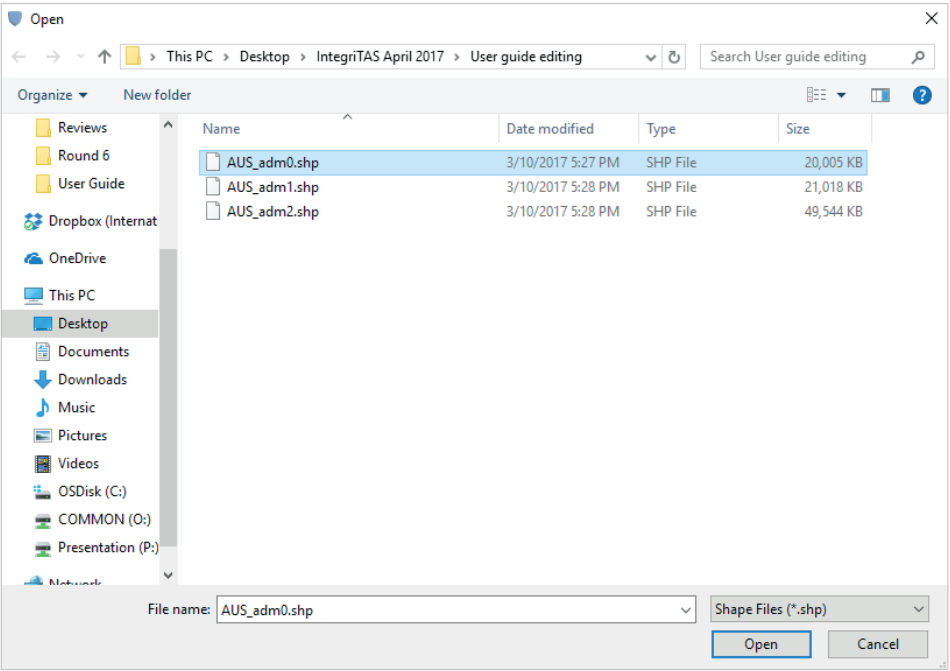
Figure 4.11. Example of adding a child region: Oceania



Step 4

Locate the file on your computer and select the country-level shapefile for the boundary or country level. In the example used in Figure 4.12, the shapefile Aus_Adm0 for Australia is selected.

Figure 4.12. Example of country-level shapefile for the boundary or country level: Australia

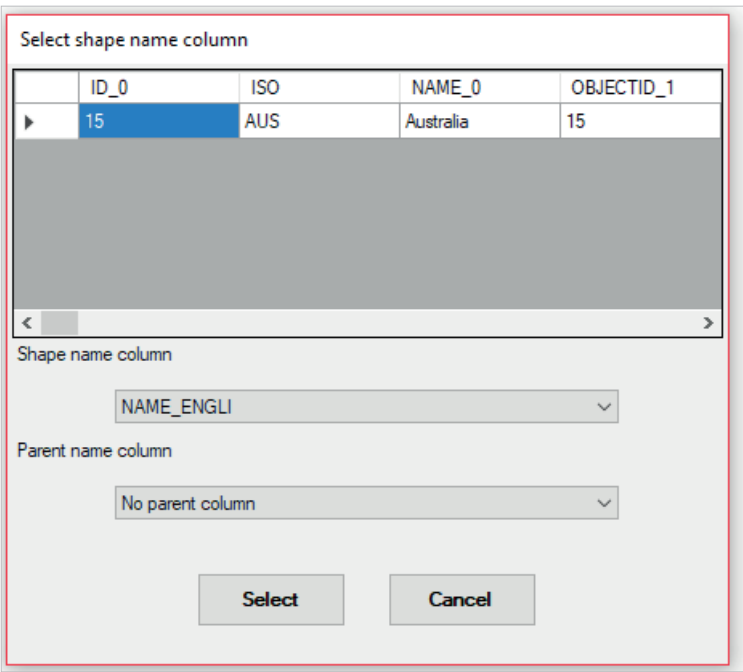


The window below appears. Select the shape name column from the dropdown menu as 'Name_Engli', as in Figure 4.13. For this, you do not need to select Parent Name Column.

Then click 'Select'. You see Australia under Oceania.

The shape name column may change depending on your shapefile attributes.

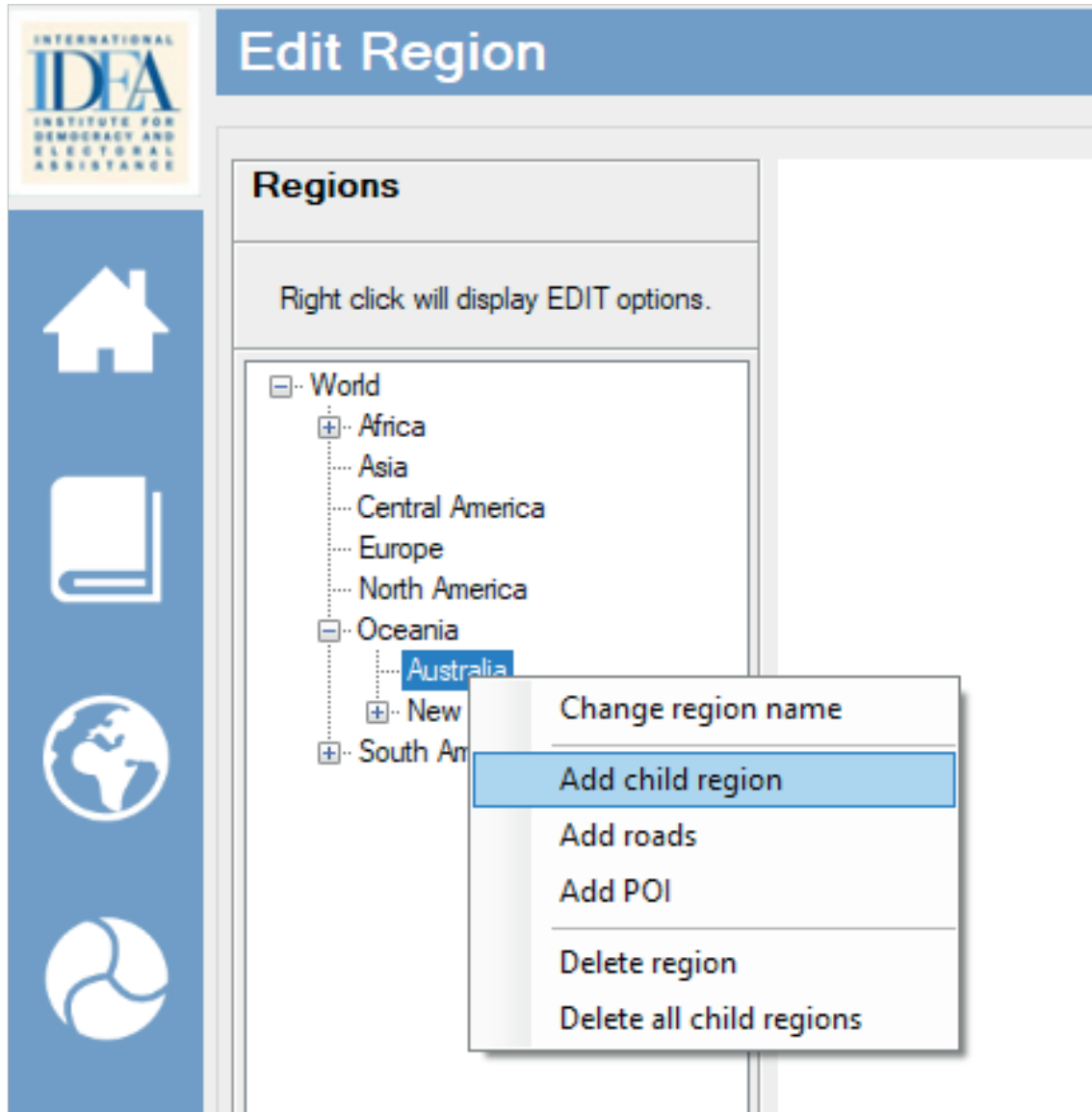
Figure 4.13. Shape name column from the dropdown menu



Step 5

You now have 'Australia (Country Name)' on the map. Right click on 'Australia (Country Name)' and then select 'Add Child region', as illustrated in Figure 4.14.

Figure 4.14. Example of adding a child region: Australia

**Step 6**

Locate the file on the computer and click 'Ok'. Under 'Shape Name' column select 'Name1', and under 'Parent Column Name' select 'Name0'. Click 'Select'. You see the next administrative level under country name.

To link the two levels of shapefiles, 'Name1' is the first administrative level and 'Name0' is the country name.

In the example in Figure 4.15, 'Aus_Adm1' is selected to import the 'First Administration Level' (states and territories).

Figure 4.15. Example of importing the first administration level: states and territories

	ID_0	ISO	NAME_0	ID_1
▶	15	AUS	Australia	1
	15	AUS	Australia	2
	15	AUS	Australia	3
	15	AUS	Australia	4
	15	AUS	Australia	5
	15	AUS	Australia	6

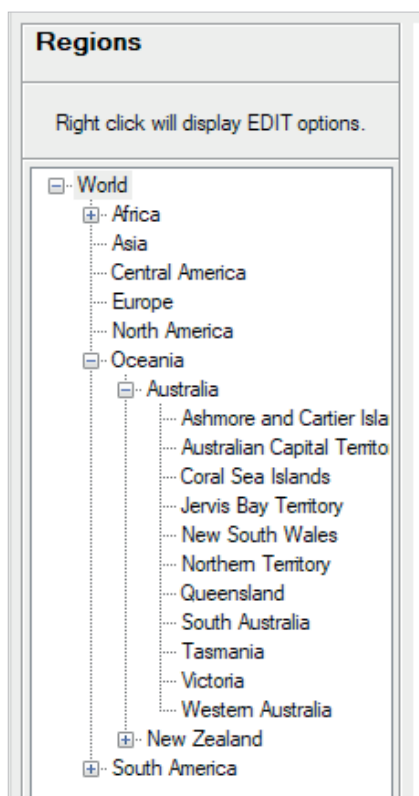
Shape name column
NAME_1

Parent name column
NAME_0

Select Cancel

Under the country (Australia), the states and territories now appear, as in Figure 4.16.

Figure 4.16. Examples of states and territories in regions' popup window



Step 7

To continue, repeat these steps to import the amount of detail you require for your model.

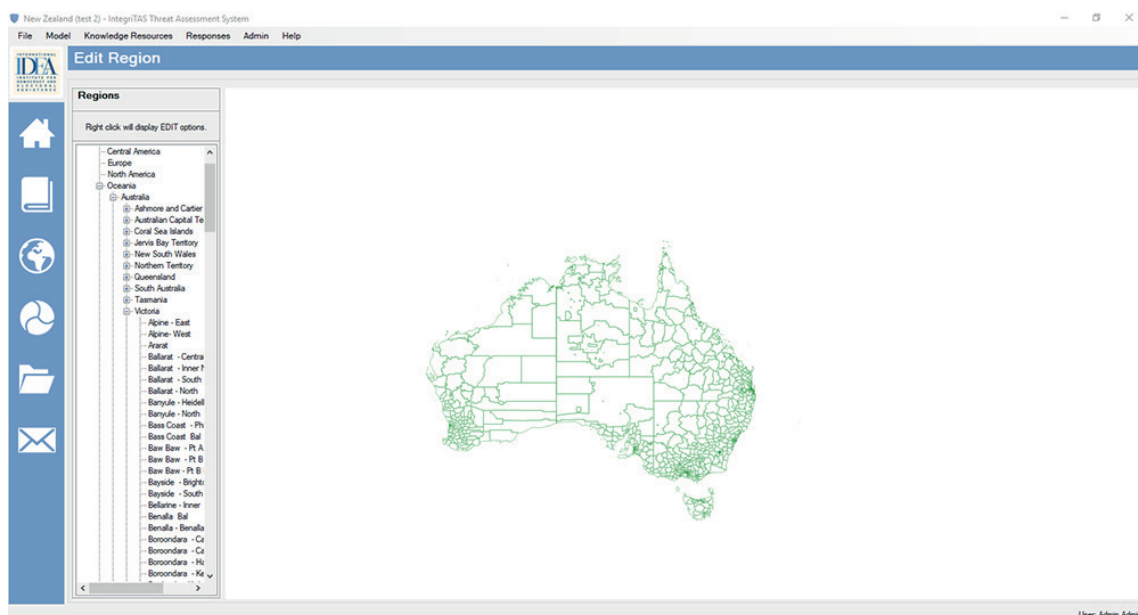
For the second administrative level, select 'Name2' under the 'Shape Name' column and 'Name1' under the 'Parent name' column and click 'Select'.

For the third administrative level select 'Name3' under the 'Shape Name' column and 'Name2' under the 'Parent name' column and click 'Select'.

In Figure 4.17, you see three administrative levels from the country to the second administrative level.

If you have more administrative levels, continue the procedure until you have imported all the shapefiles.

Figure 4.17. Example of three administrative levels from the country to the second administrative level



Endnote

1. Examples of websites providing shapefiles for free download include: DIVA-GIS (<http://www.diva-gis.org>). Free GIS Data (<https://freegisdata.rtwilson.com/>) provides depository of similar pages (both sites visited October 2017). Note that this site and example were functioning and relevant at the time of writing (October 2017) but may have changed since that time.

5. Creating and editing an analytical model

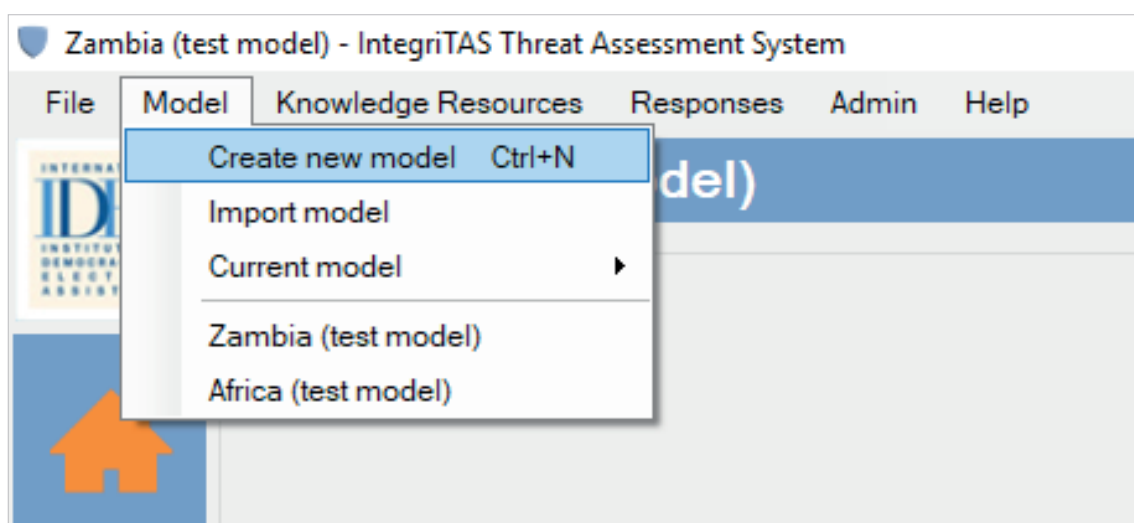
You can create an analytical model by selecting factors that are relevant in a country and electoral context. A model can include several factors. You can also change the scale range, interval and weight on the 'Create New Model' page. You can add or remove factors from the model at any time. But changing the scale, interval or weight of a pre-selected factor in Edit Current Model results in the loss of all data added in Table by Factor or Table by Region. The lists are mirrors of factors included in the VKRL, including newly added factors from 'Adding a New Factor', as explained in Section 3.2.1. You can also edit the model as required.

5.1. Creating an analytical model

Step 1

To create a new model, click 'Model Menu' → 'Create New Model (Ctrl + N)', as in Figure 5.1.

Figure 5.1. Create new model in 'Model' dropdown menu

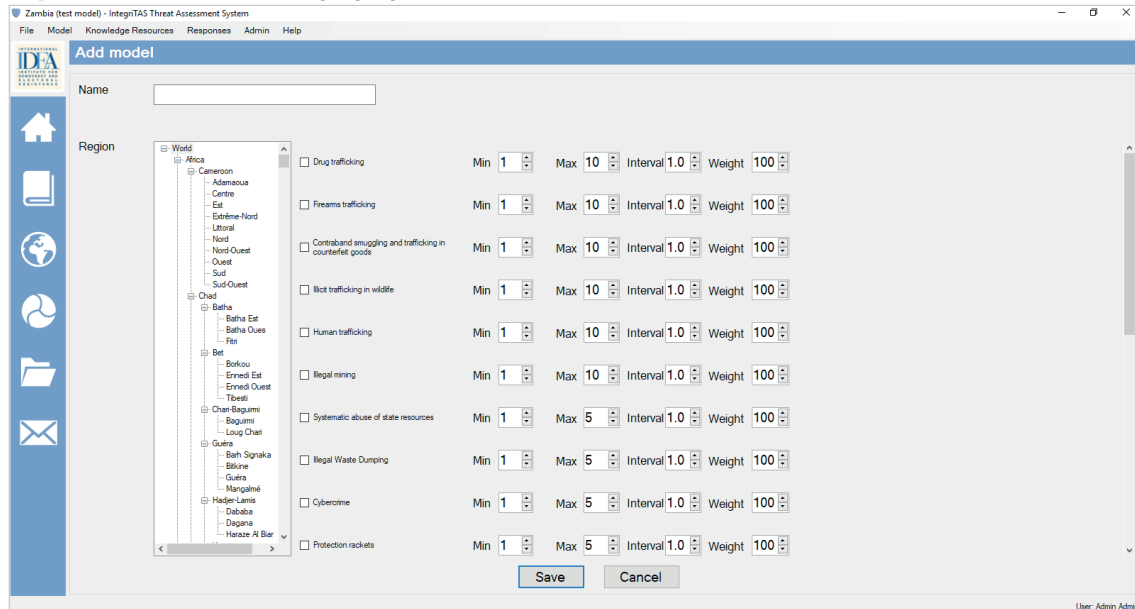


Step 2

By clicking ‘Create New Model’, the screen shown in Figure 5.2 appears.

Regions are displayed on the left side, and factors on the right (scroll down to see the factors you have created).

Figure 5.2. Add model popup window



Step 3

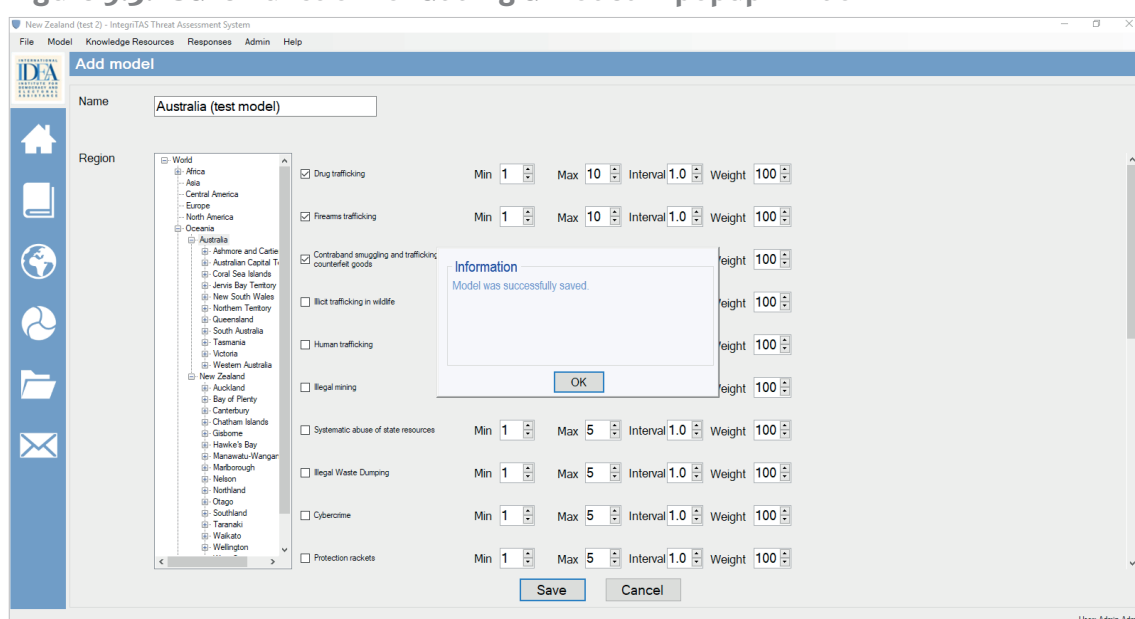
Add the title of the model (for this example ‘Australia (test model)’). Check the box to select factors including scale, weight and region (part of a region or a whole region, i.e. Australia).

You can create a single factor model or a multiple factors model, depending on your requirements.

Step 4

Click ‘Save’ to save the model. A window such as in Figure 5.3 appears.

Figure 5.3. ‘Save’ function for adding a model in popup window



Once you save the model, you select the model from either:

- 1. Model Menu (Figure 5.4)
- 2. Model Dropdown Menu (Figure 5.5)

After selecting the model, the model name appears in the Title Bar and Home Screen. Figure 5.6 shows that ‘Australia (test model)’ is now the name appearing in both.

Figure 5.4. Model menu

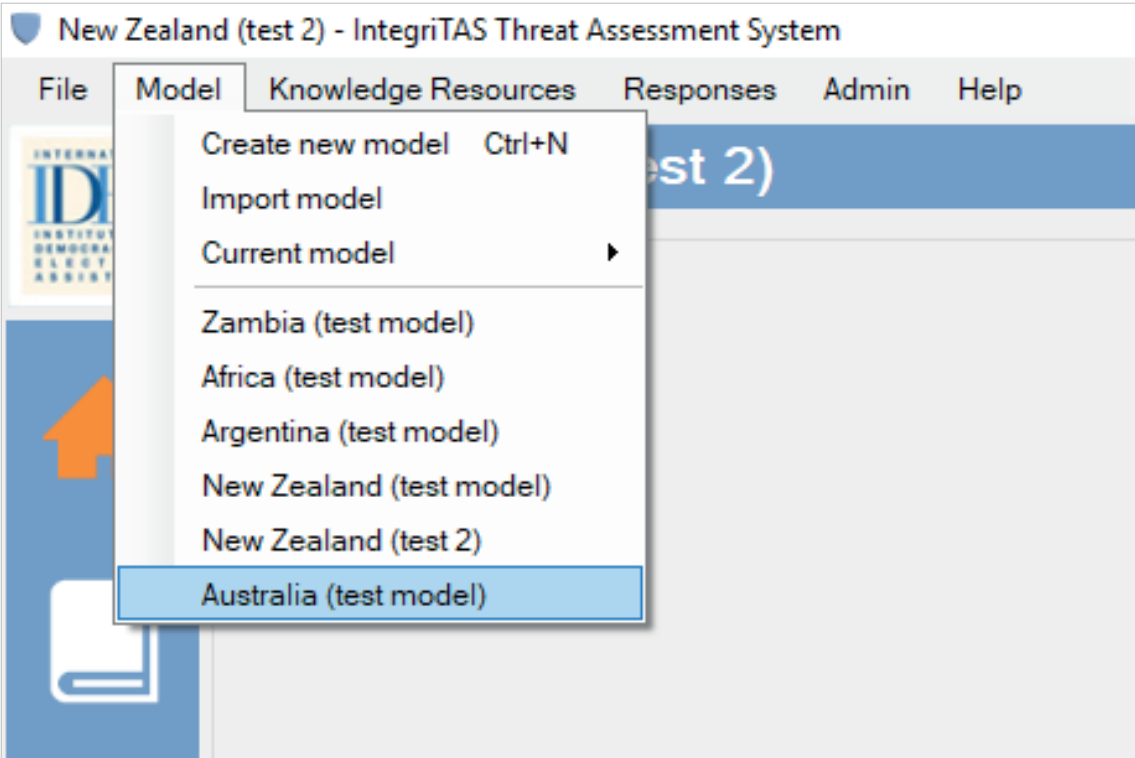
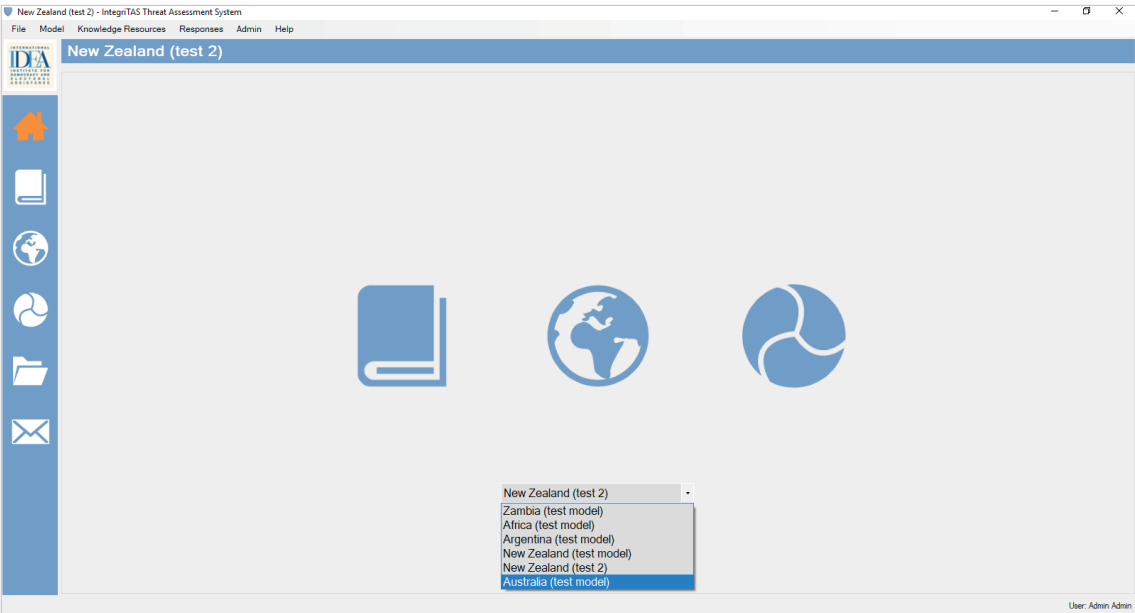


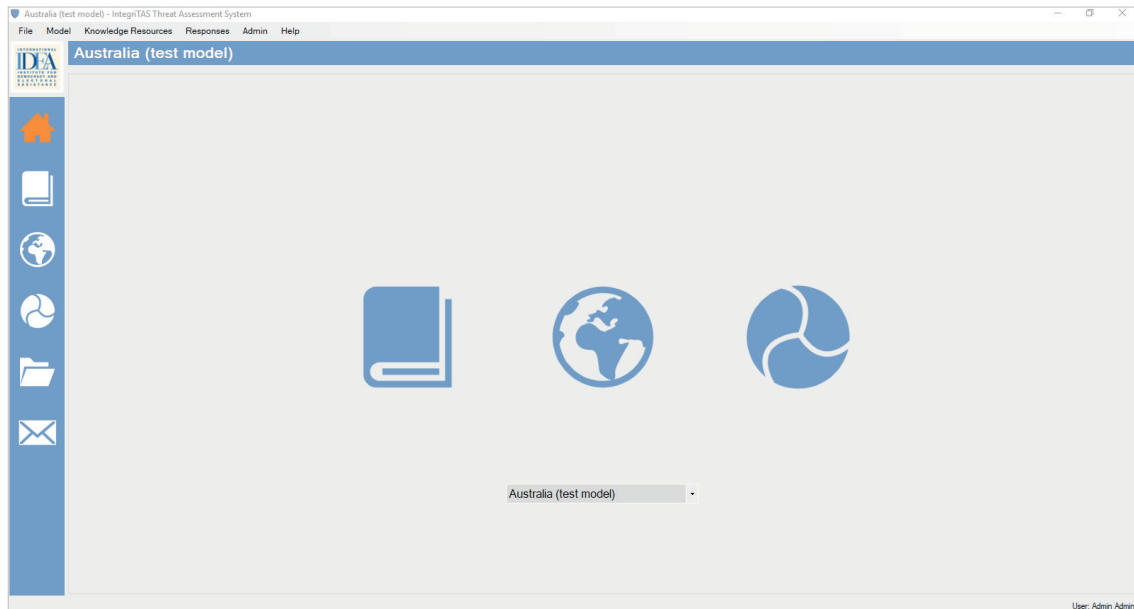
Figure 5.5. Model dropdown menu



Step 5

Access the model for analysis by clicking on either the globe image on the Home Screen or the house icon on the Side Bar as shown in Figure 5.6.

Figure 5.6. Globe image in home screen

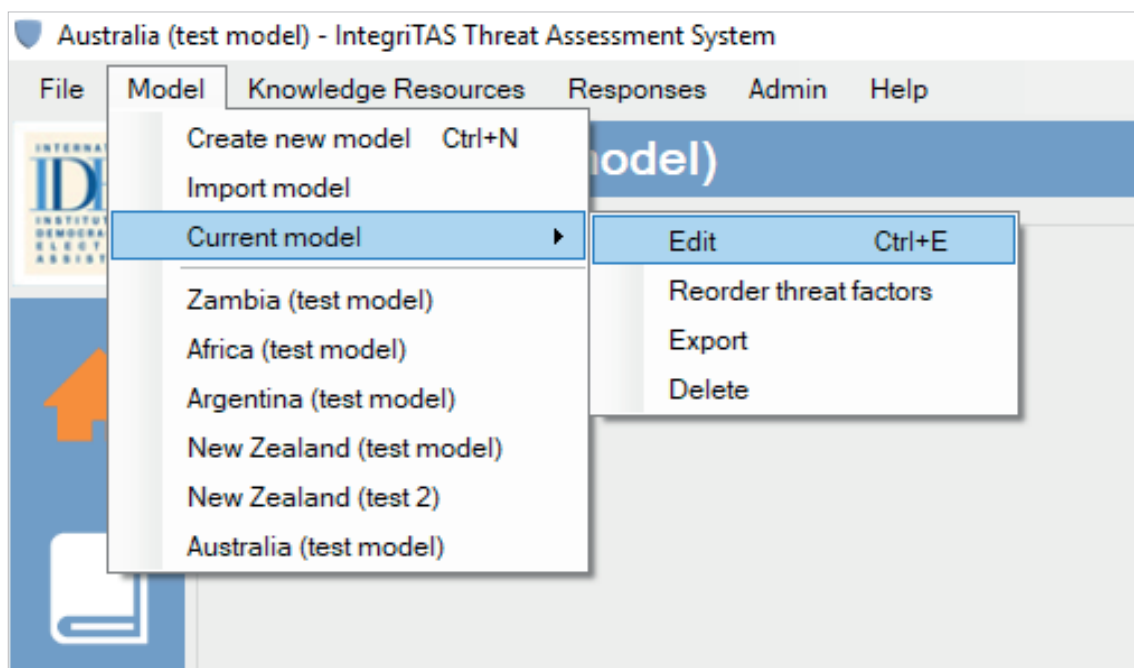
**5.2. Editing an analytical model**

The model can be edited by adding or removing factors.

Step 1

Click on 'Model' -> 'Current model' -> 'Edit (Ctrl +E)', as shown in the window of Figure 5.7.

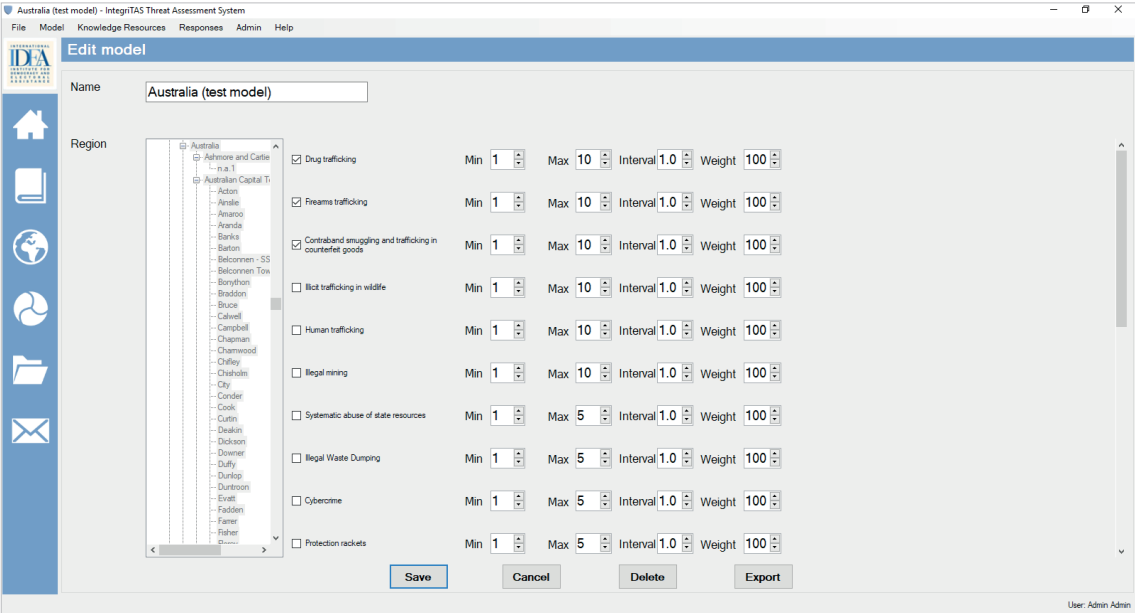
Figure 5.7. Current model dropdown menu



Step 2

A new window will appear, such as in Figure 5.8.

Figure 5.8. Edit model popup window

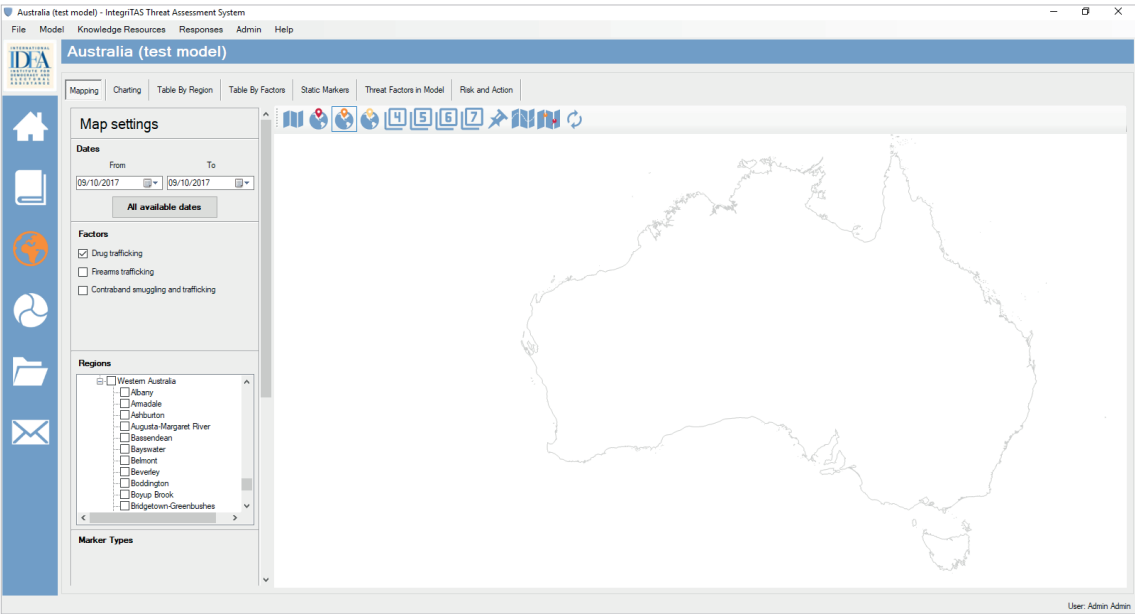


You can edit the title and add or remove factors. You can also change the scale, interval and weight. However, you cannot select the regions while editing a model.

While editing, if any factor(s) previously added to the model has data under changing the scale, interval and weight, the data is lost.

Click on 'Analytical Instrument' (Globe icon) on either the Home Screen or Side Bar. The screen as in Figure 5.9 appears.

Figure 5.9. Analytical instruments popup window



The screen is divided into four sections:

Map Settings: This enables you to select the date, factor(s), region(s), marker(s) and colour scheme, and save or load settings.

Tab Bar: This enables you to switch between different tabs (mapping, charting, table by regions, table by factor, static markers, model in factor, and threat and action).

Toggle Bar: This enables you to select the administrative layers (continent to lower division of country), static markers, roads, POI and refresh the map.

Map Interface: This interface helps you view the maps, with the help of the map settings selection and toggle bar.

6. Adding data to an analytical model

You can add data through ‘Table by Factor’ or ‘Table by Region’. The type of data being entered depends on what factor is being observed. For example, an observable indicator of drug trafficking might be seizures of narcotic drugs across the country, such as found in reports by Australian Federal Police on the volume, type, and street value of drug seizures across the country. Data can be collected on the same observable indicator, over a long period of time. Data relating to trust in the drug trafficking example can be collected on separate occasions and can be projected in mapping and trend analysis. Data requires some coding before entering into IntegriTAS according to either a scale (which can be modified under the ‘Edit Model’ functionality demonstrated above), or the cumulative parameters (see Section 10, ‘Cumulative Factors’). For large data sets, it may be worthwhile to add data into an Excel sheet and then paste it into the application. Data can also be saved by clicking on ‘Export All Tables’.

You can add data using two methods in IntegriTAS. You can either go to ‘Table by Region’, shown in Section 6.1, or ‘Table by Factor’, shown in Section 6.2 on the ‘Tab Bar’.

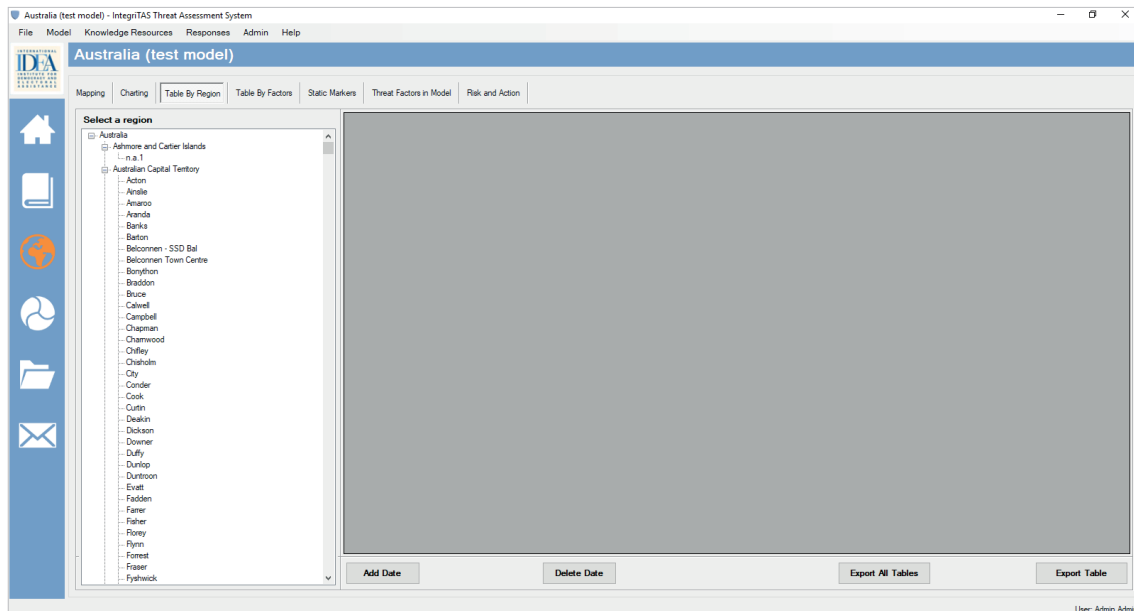
6.1. Table by Region

This data entry method is used when data are collected over regions, which helps to enter data for a specific region.

Step 1

Access this functionality by clicking on ‘Table by Region’ as highlighted in Figure 6.1.

Figure 6.1. Table by region functionality

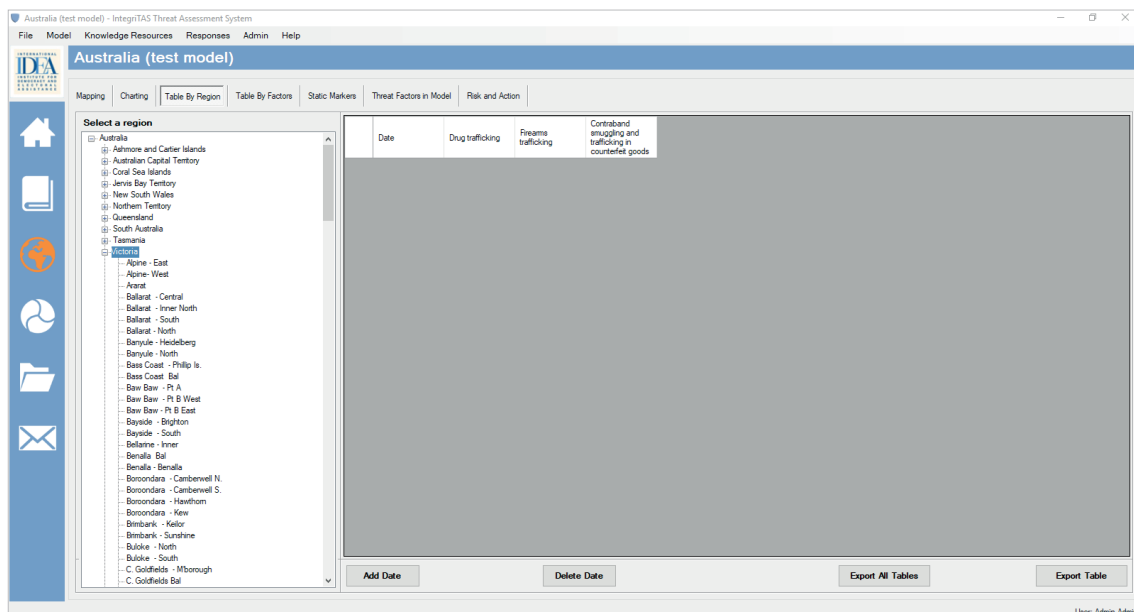


Select a region by clicking on it. All the factors in the model are then shown on the right side of the window, as seen in Figure 6.1.

Step 2

To add the date, click ‘Add Date’, and a line with the current date appears below the factor, as shown in Figure 6.2.

Figure 6.2. Add date in table by region

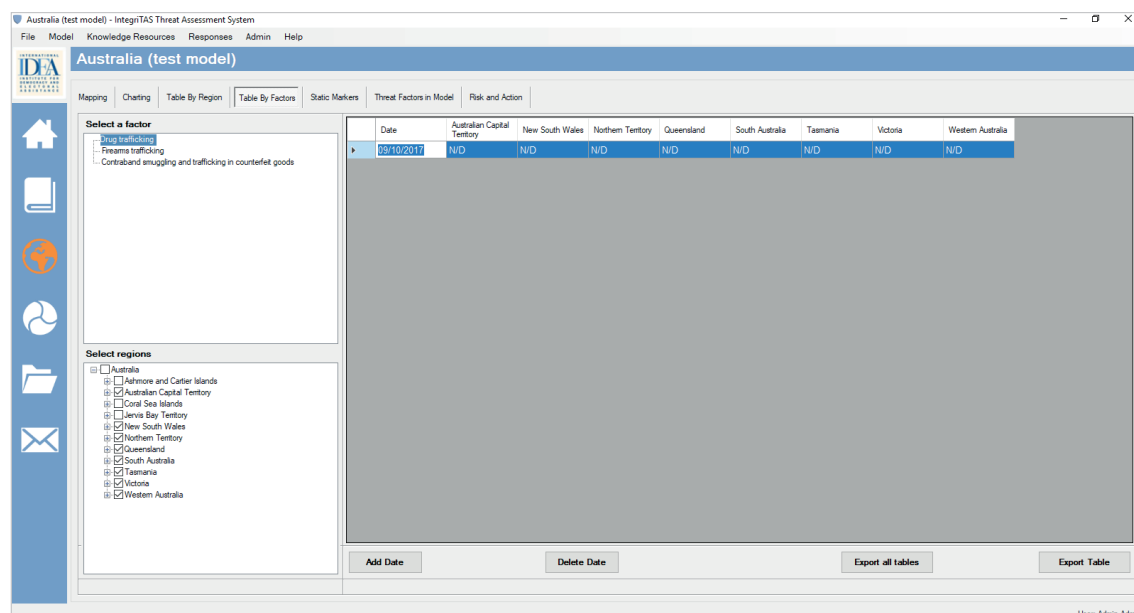


Step 3

Add the data for a particular factor. You can add data for more than one factor as required. You can also change the date, if data are available for the previous data date.

In the Australia example shown in Figure 6.3 below, dummy data have been entered.

Figure 6.3. Example of data: Australia



Step 4

Once data are added, the tool automatically saves it. For this reason, no 'Save' button is on the screen, as seen in Figures 6.2 and 6.3.

To edit the value, click on the value below the factor and make changes.

To delete the values for a region or date, click 'Delete Date'.

6.2. Table by Factor

The second method of entering data into the tool is by selecting the tab 'Table by Factor' from the Tab Bar. This is more useful for entering data for a factor(s) and for all the regions.

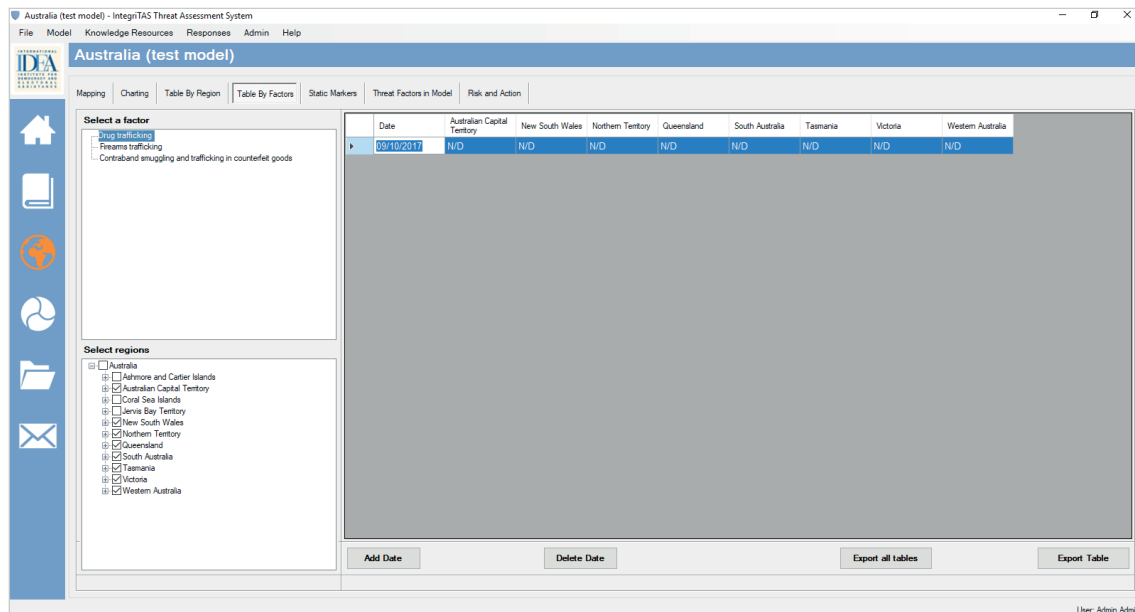
The size of the shapefiles (maps) impacts the loading time.

Step 1

Click to select the appropriate region and factor in the two panels on the left, as seen in Figure 6.4. Then click 'Add Date'.

The region selected appears on the right side. Enter the data. It saves automatically, as is done in the 'Table by Region' option.

Figure 6.4. Region and factor selection in table by factors



Step 2

Right click on a region to display the menu.

This gives you the following options:

'Select all child regions': This menu helps select all the child regions that fall under the selected parent region.

'Select all regions on this level': This menu helps select all the regions on the same level.

'Deselect all child regions': This menu helps deselect all the regions that fall under the selected region.

'Deselect all regions on this level': This menu helps deselect all the selected regions on the same level.

'Export Table': This function enables you to export the current factor to Excel.

'Export All Tables': This function enables you to export all the factors to Excel.

7. Mapping

Once you have entered the data into the application, it can be manipulated and viewed in the mapping interface. The different-coloured regions represent variance in threat.

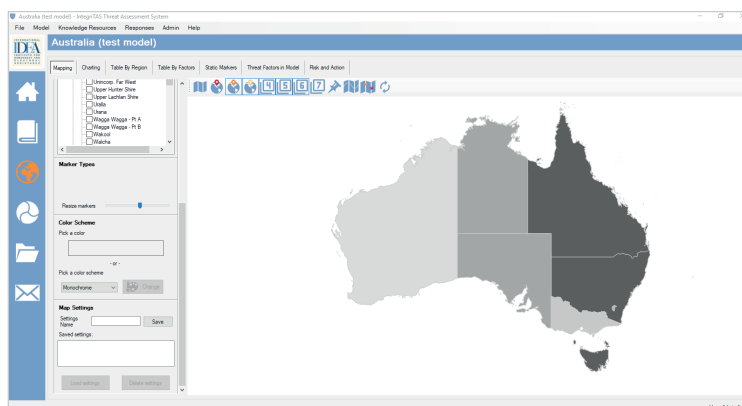
The map displays an average threat level per region. This function is useful when looking at threats over a given time period.

Step 1

Within 'Analytical Instruments', click on the 'Mapping Tab'. The country map will be displayed, as shown in Figure 7.1.

Select the date (from and to) according to your requirements.

Figure 7.1. Country map in mapping tab



Step 2

Select the factors according to your requirements.

Step 3

Right click on 'Country name' (here, Australia) and either click to select all the regions, or click to select the specific regions to be included.

Go to the toggle tab to select the layer to be drawn (in this case the First Administrative Layer is selected).

Step 4

You select the regions or administrative level depending on data availability.

You see a monochrome display of data. If you want to change the colour scheme, you can select a colour from 'Pick a color' (highlighted in Figure 7.2) or use a default colour scheme such as monochrome, traffic light, temperature. Alternatively, you can select a custom colour for each threat level.

Select the colour scheme from the dropdown list.

Figure 7.2. Pick a colour in dropdown menu

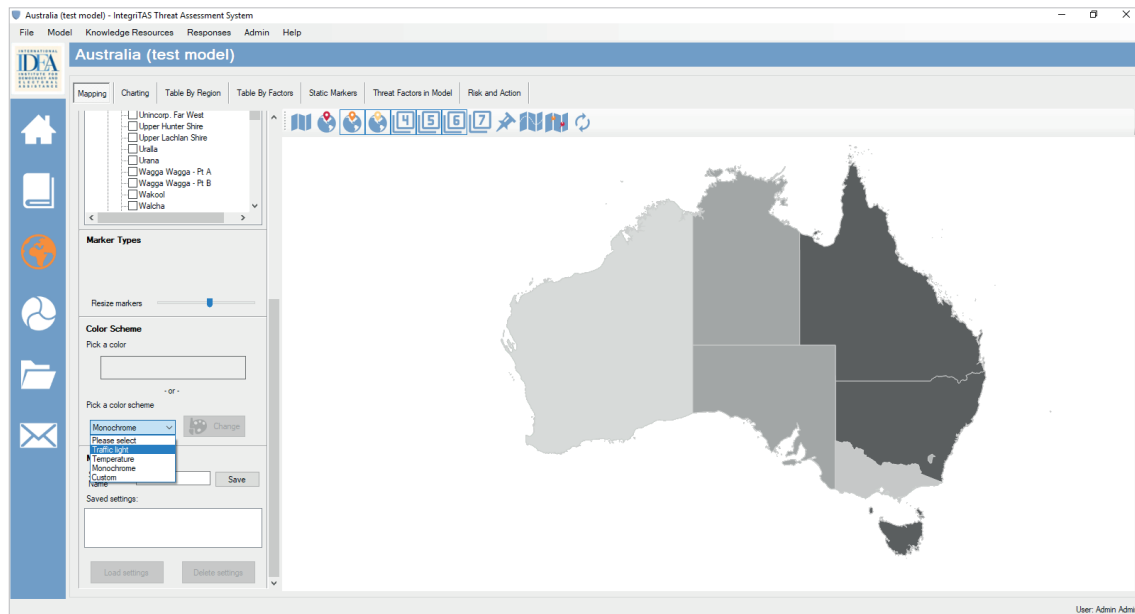
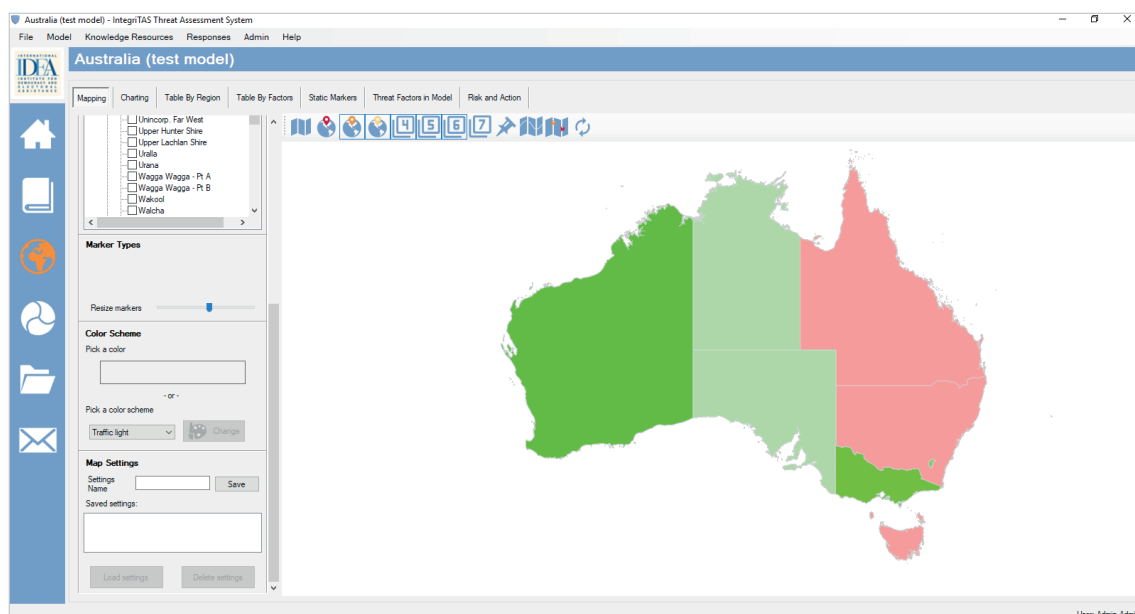


Figure 7.3 is an example of the traffic-light colour scheme.

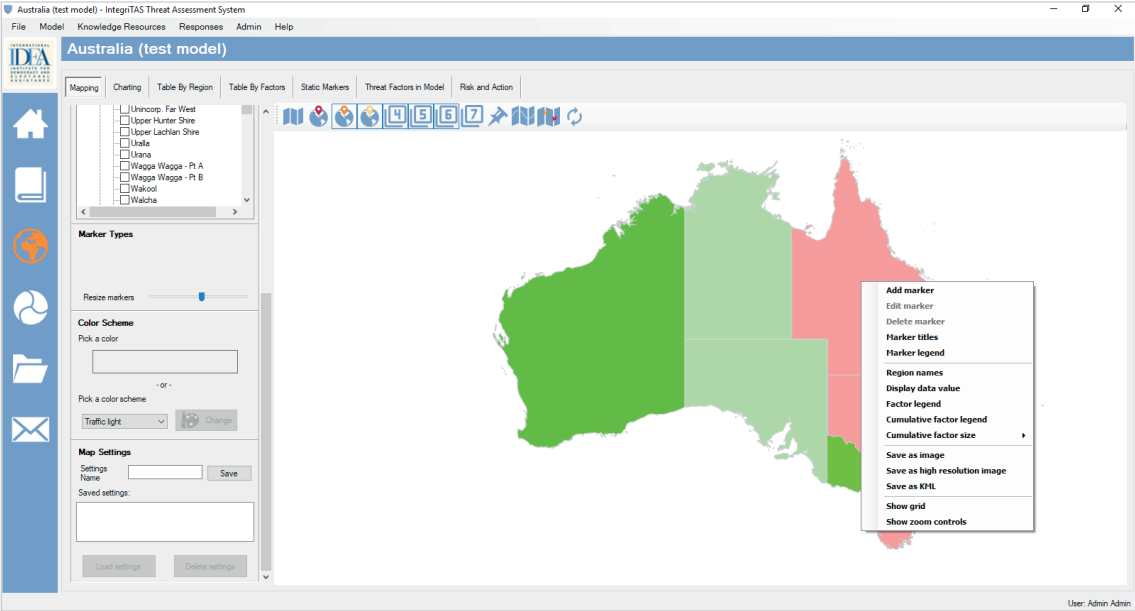
Figure 7.3. Example of traffic light colour scheme



Step 5

Right click to select from various functionalities on the Map Interface. The menu will appear, as shown in Figure 7.4.

Figure 7.4. Functionalities dropdown menu in map interface



This menu provides the following functionality:

- ‘Region Name’: Displays the name of the region selected.
- ‘Display data value’: Shows the colour-coded value for each region. (If more than one factor has been selected, the mean value is displayed).
- ‘Factor legend’: Shows the value and the colour representing the value.
- ‘Show grid’: Displays the geographical grid on the map.
- ‘Show zoom controls’: Displays the zoom controls to help zoom in or out.

Figure 7.6 illustrates what applying these functionalities looks like.

Figure 7.5. Functionalities dropdown menu

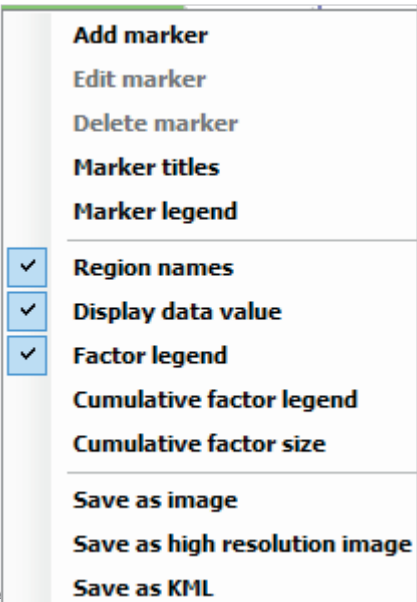
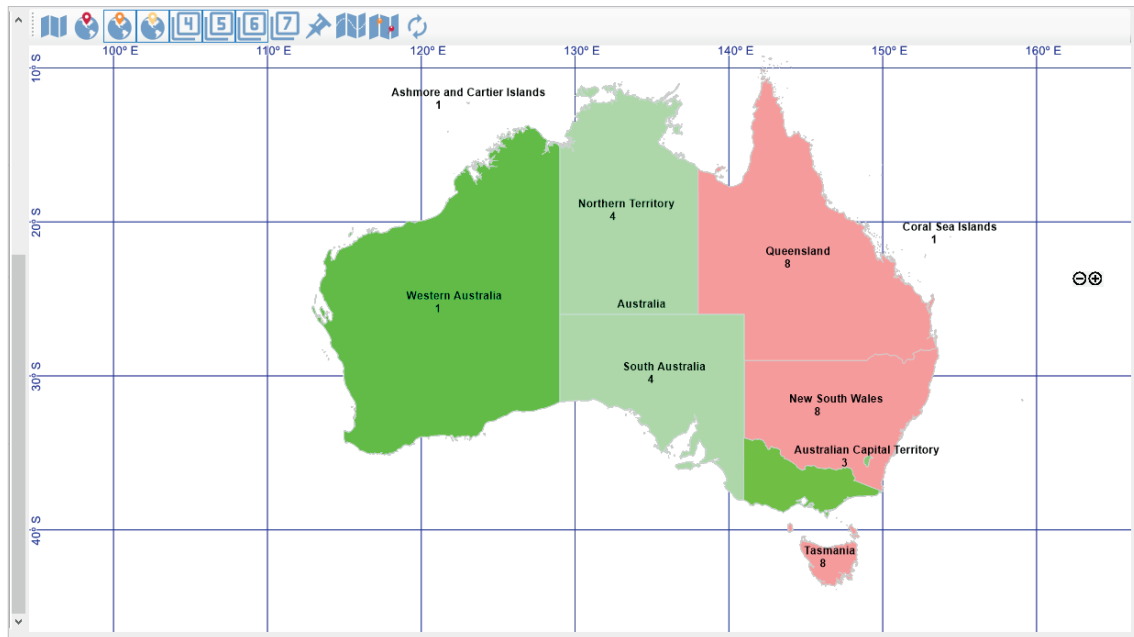


Figure 7.6. Example of application of mapping functionalities

8. Settings

You can use different settings from the tool to ease its use while working on multiple threat alerts.

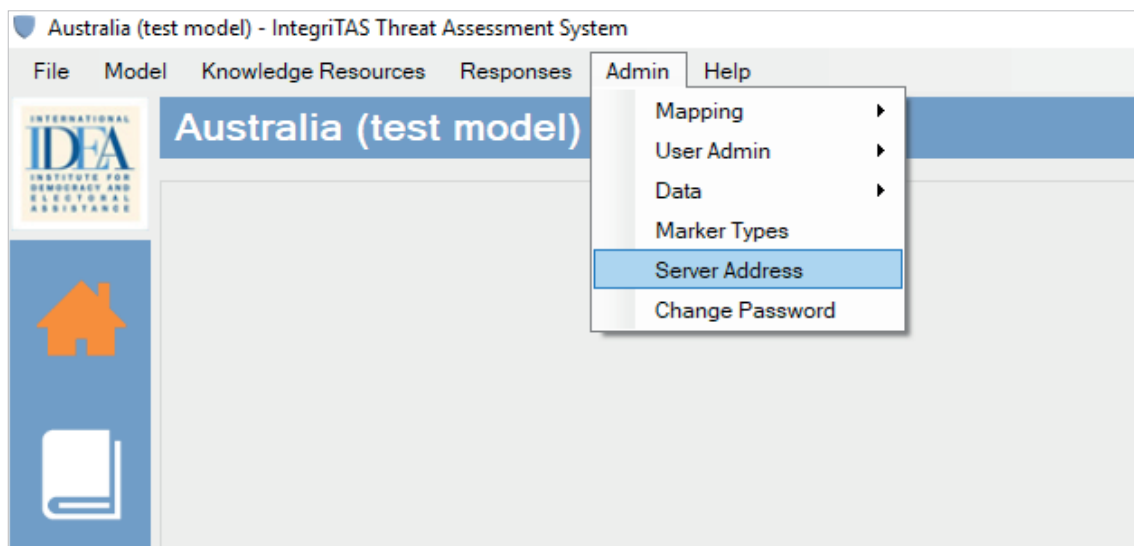
Map and chart settings are mostly useful when you are working on more than one map. You can save the current settings and work on other maps, and can alternate between maps as required.

8.1. Connecting to new or other servers

Step 1

Click on 'Admin' – 'Server Address', as shown in Figure 8.1.

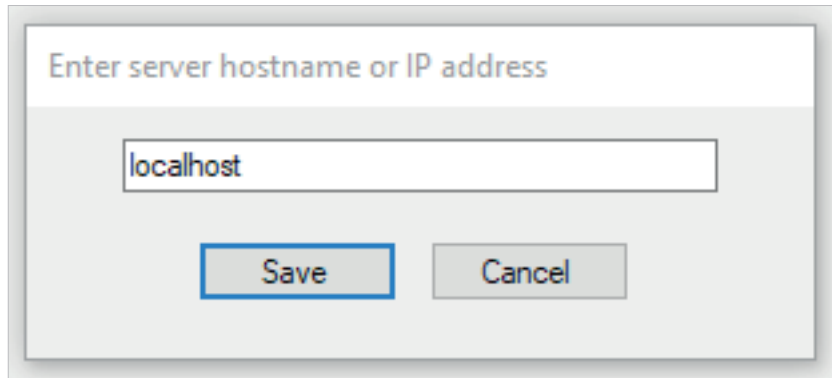
Figure 8.1. Server address in 'Admin' dropdown menu



Step 2

A window appears, as shown in Figure 8.2. Enter the IP address or computer name of the server to connect to the new server.

Figure 8.2. Server hostname or IP address popup window

**Step 3**

Click on 'Save' to save the changes.

Restart the tool to connect to the new server.

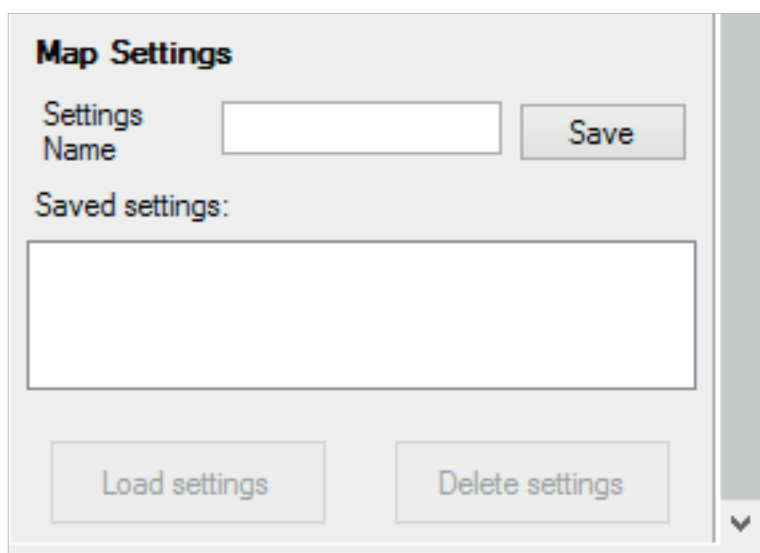
The local host in the tool refers to where the server and client are both installed in the same system.

8.2. Map or chart settings

Step 1

On the 'Mapping Tab', scroll down to the section 'Map Settings', as shown in Figure 8.3.

Figure 8.3. Map settings in mapping tab



Step 2

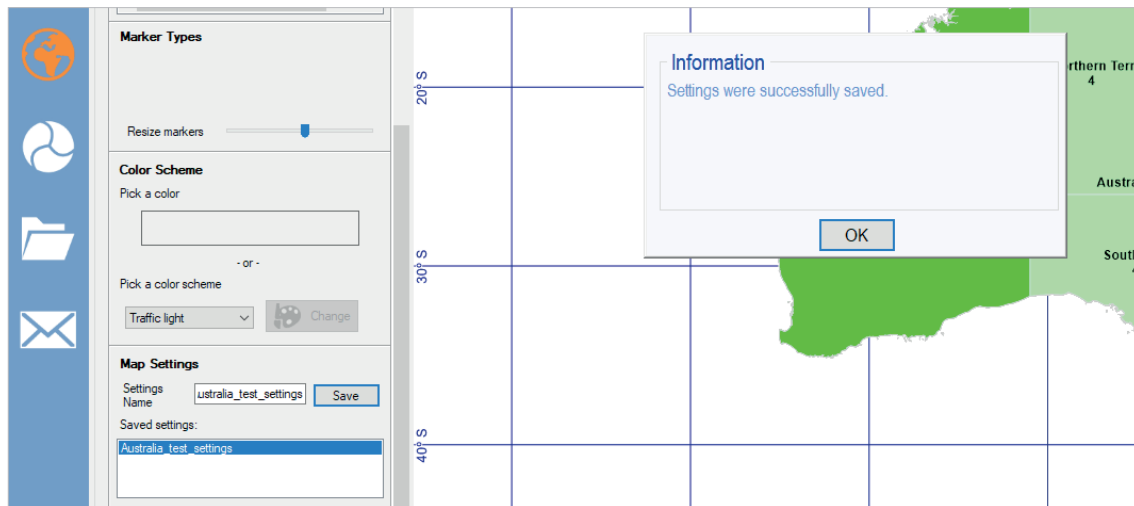
Enter the name to save the current settings and click 'Save' and 'OK' to confirm the save. A window will appear to confirm, as shown in Figure 8.4.

Once saved, the name appears on the saved setting box in the Map Settings Section.

To load a previously saved setting, select the setting and click 'Load Settings'.

To delete a setting, select the setting and click 'Delete Settings'.

Figure 8.4. 'Save' functionality and confirmation popup window for map name



9. Saving work

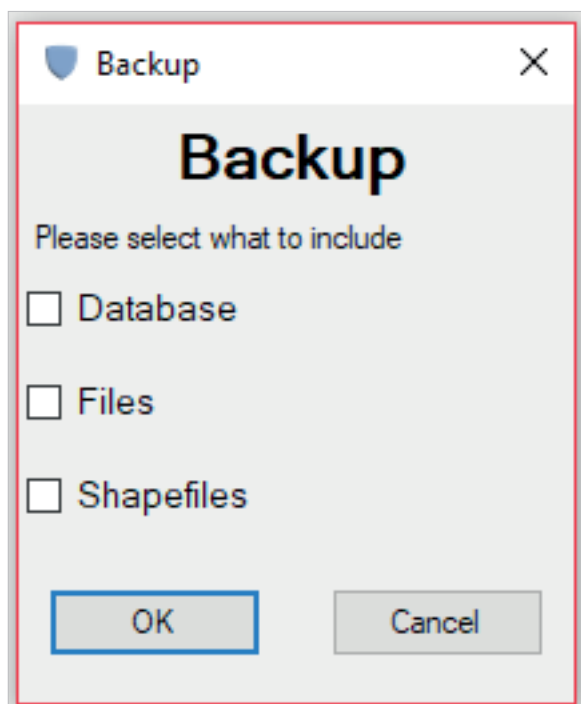
It is recommended that you frequently save models and databases to minimize the risk of losing data if the system becomes unstable. The tool acts as a depository for threat data during and between elections, and saving work should be a common practice for all users in case the IntegriTAS application runs into critical errors or a new version requires installation. To save the work, you can either back up or export. 'Backup' saves all the models included in the tool, while 'Export only' saves the current model selected.

9.1. Backup

Step 1

Go to 'Admin menu' -> 'Data' -> 'Backup'. A window appears, as shown in Figure 9.1.

Figure 9.1. Backup popup window



Step 2

Select the required options. You can back up only the database or files added to the tool, the shapefiles (i.e. GIS datasets) or all three. It is recommended to select all three.

Click 'OK'.

Step 3

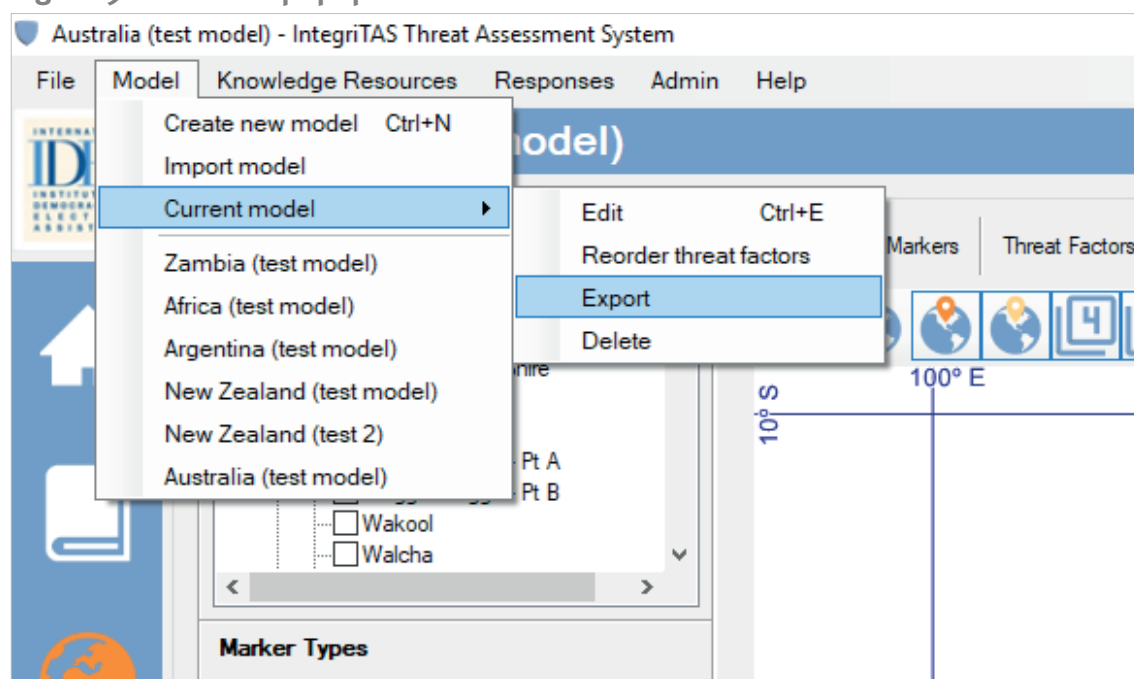
A dialogue box opens. Provide a name for the backup file and location on your hard drive. It takes some time to back up the database. After the database backup is completed successfully, you receive a confirmation.

9.2. Restore

You need the computer's administrative privileges to restore the database.

Go to 'Admin' -> 'Data' -> 'Restore'. A window appears, as shown in Figure 9.2.

Figure 9.2. Restore popup window



You must remember how the backup (Section 9.1) was done previously. If all three options were selected for backup, again select all three options or use the selected option to restore the database.

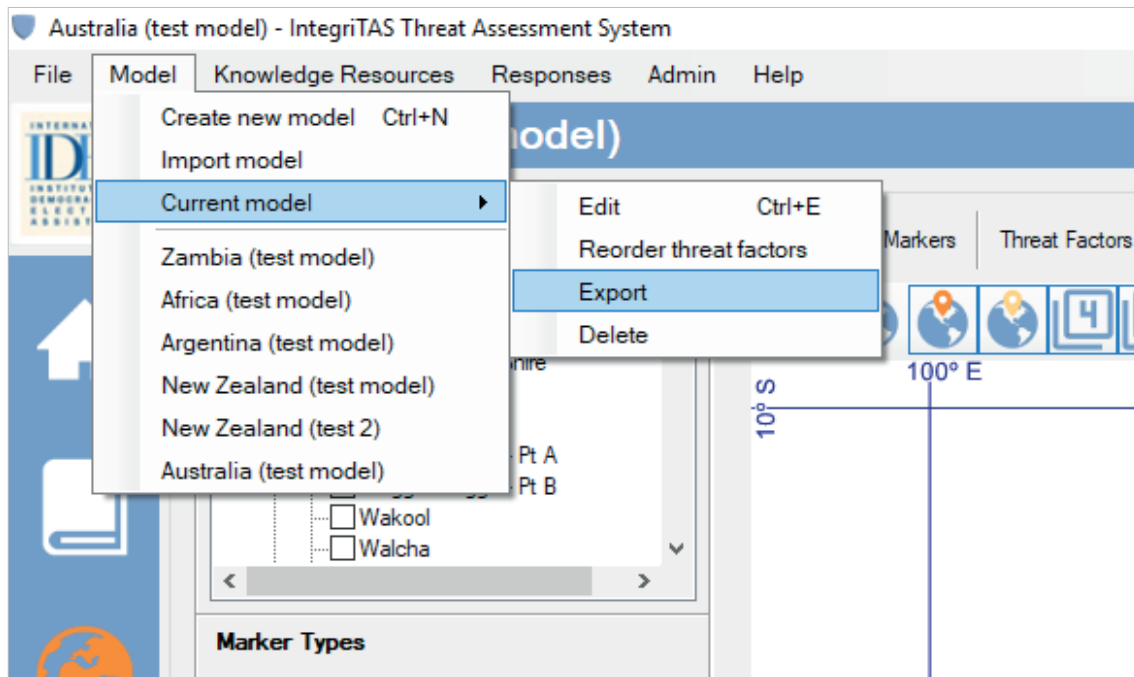
Click 'OK' and locate the previously saved database. This can take a few moments.

9.3. Exporting a model

Step 1

To export the model, go to 'Model Menu' → 'Current' → 'Export', as shown in Figure 9.3.

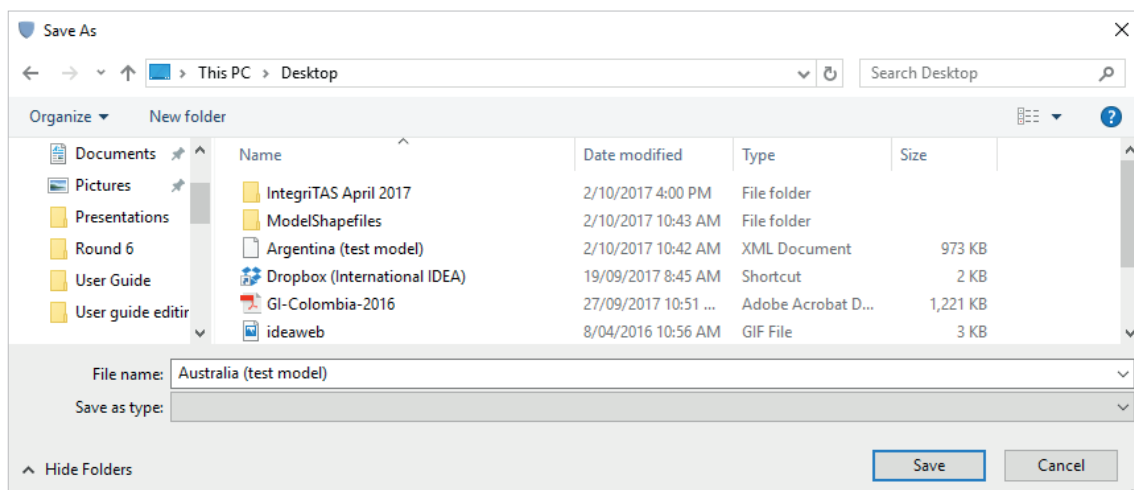
Figure 9.3. Export in current model dropdown menu



Step 2

A new dialogue box appears, as shown in Figure 9.4.

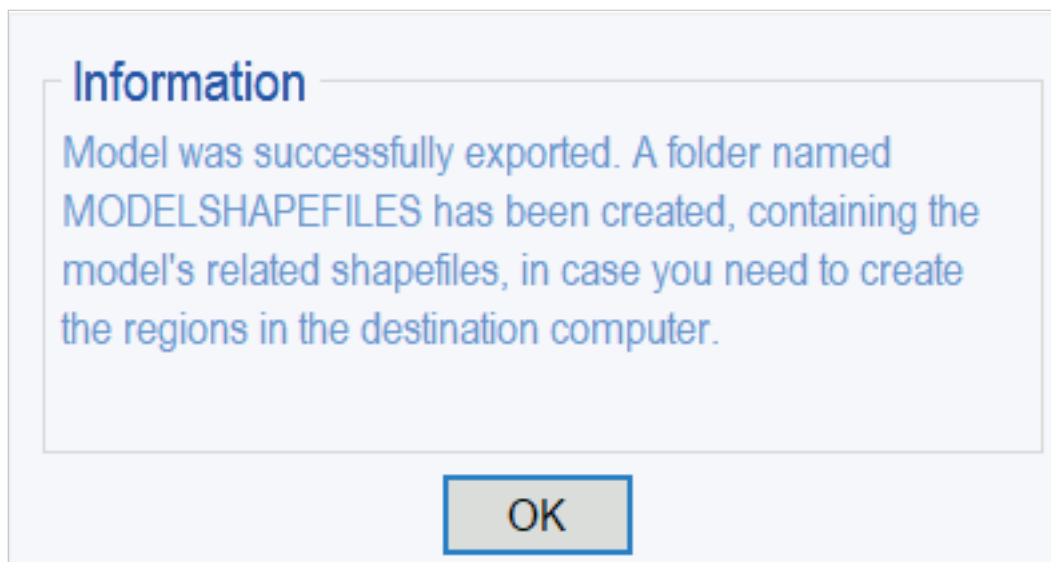
Figure 9.4. Export dialogue box



Step 3

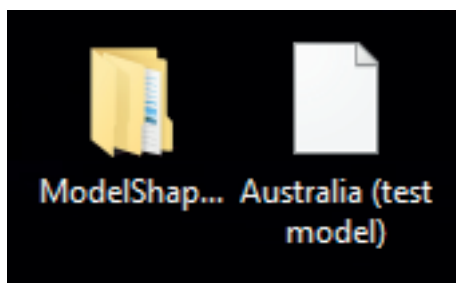
Select a location on your hard drive and click 'Save' to export the desired model. A window such as the one shown in Figure 9.5 will appear.

Figure 9.5. Export save information popup window



The shapefiles associated with the model are also exported to the same location in a folder named 'ModelShapeFiles' to which the model is exported, as shown in Figure 9.6.

Figure 9.6. Location for exported shapefiles associated with the model

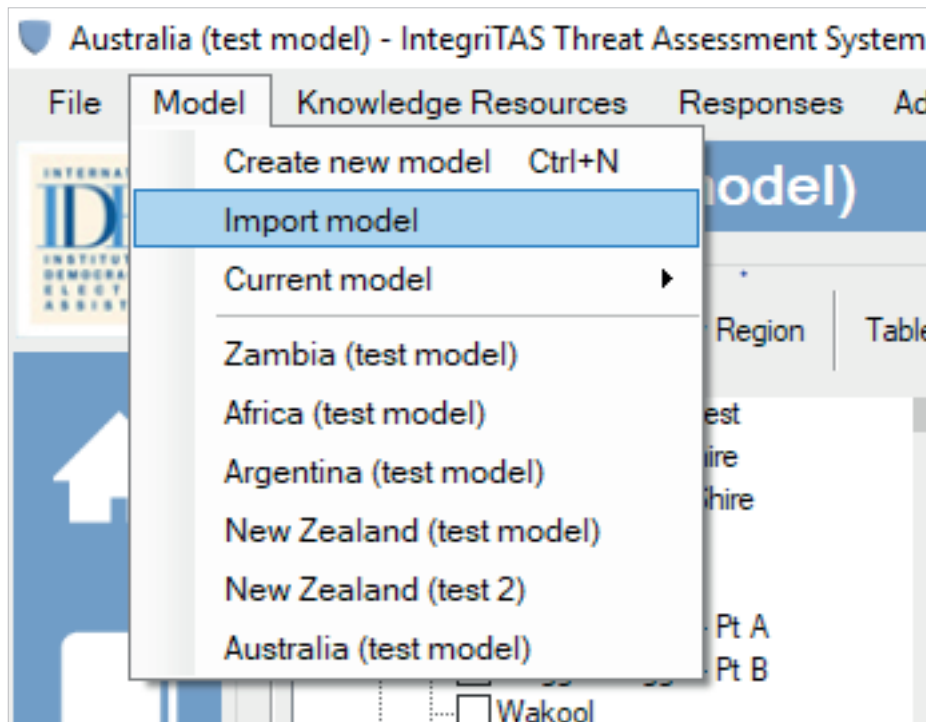


9.4 Importing a model

Step 1

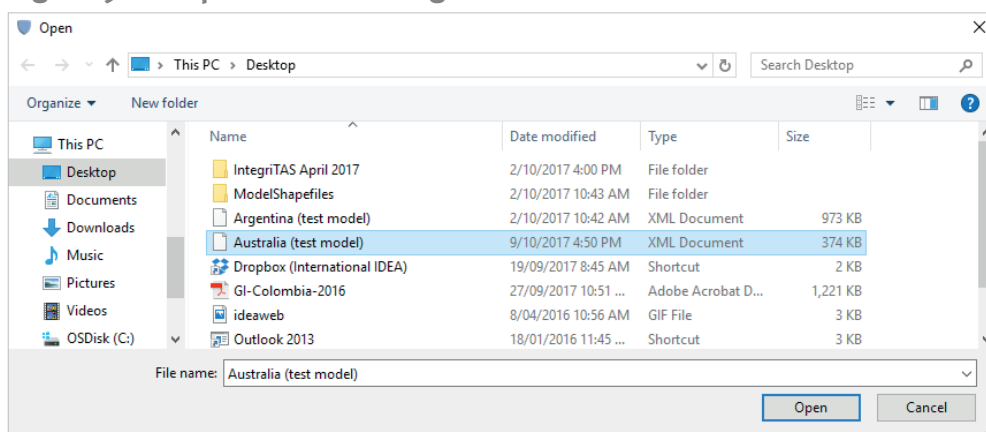
Go to 'Model Menu' → 'Import Model', as shown in Figure 9.7.

Figure 9.7. Import model in model dropdown menu



A new dialogue box appears, as shown in Figure 9.8.

Figure 9.8. Import model dialogue box



Step 2

Locate and select the model to be imported and click 'Open'. The model is imported and is shown on the 'Model Selection Drop Down Menu'.

If the model you are importing does not have the shapefile, you must import the shapefile first and then import the model.

If a model with the same file name as a previous model is imported, the tool automatically renames the model by adding a number after the model name.

10. Cumulative factors

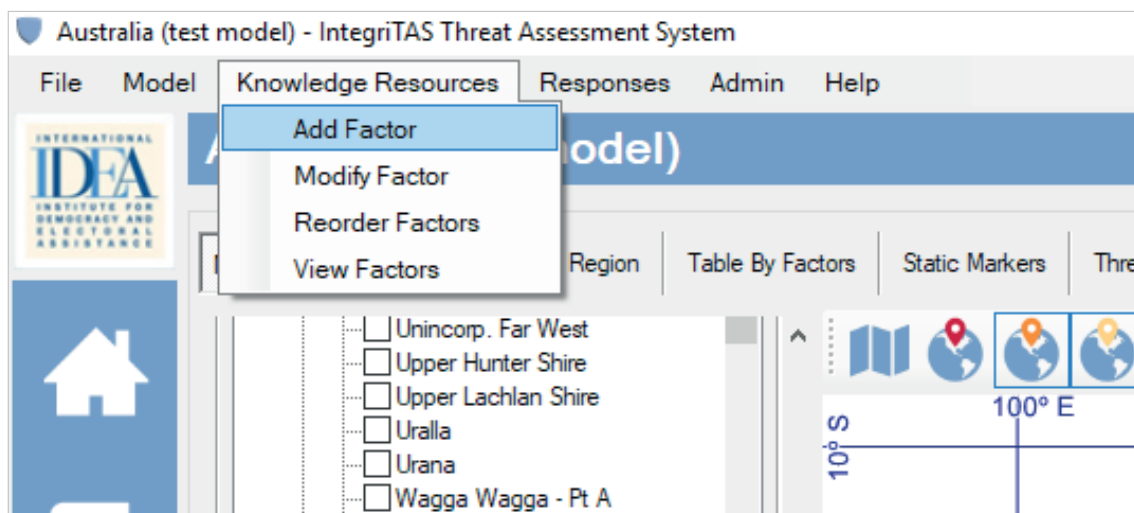
Cumulative factor(s) are used to present numerical data such as a security incident or complaint. If more than one numerical entry is made for the same factor or region under different dates, the numbers are aggregated. Cumulative factor(s) can be combined with colour-coded factors, providing two levels of information. Several cumulative factors can be displayed in the map at the same time.

10.1. Creating cumulative factors

Step 1

Go to 'Knowledge Resources' – 'Add Factor', as shown in Figure 10.1.

Figure 10.1. Add factor in knowledge resources dropdown menu



A new window opens within the tool, as shown in Figure 10.2.

Figure 10.2. Add new factor popup window

Step 2

Enter the name for the factors. For the example in Figure 10.3, the title for the cumulative factor is 'Methamphetamine seizures'.

Figure 10.3. Example of name of new cumulative factor

Step 3

Under the ‘Factor Type’ dropdown menu, select ‘Cumulative’, and specify the factor as ‘Democratic Vulnerabilities or Organized Crime’. See Figure 10.4.

Figure 10.4. Example of colour selection for a cumulative factor

The screenshot shows a form with the following sections:

- Factor Name:** A text input field containing "Methamphetamine seizures".
- Factor Type:** Two dropdown menus. The first is set to "Cumulative" and the second is set to "Organized Crime".
- Cumulative Factor Colors:** This section includes three color selection controls: "Back color" (a red square), "Font color" (a white square), and a "Preview" area showing the number "2" in white font on a red background.
- Factor Texts:** A label "Select factor description field to edit" is followed by a dropdown menu currently showing "Introduction".

Step 4

Select the colours under ‘Cumulative Factor Colors’. Select the ‘Back color’ and ‘Font color’ as required. The example in Figure 10.4 uses a red back colour with a white font.

Step 5

To fill in the factor text, select from the dropdown menu of the description field, as shown in Figure 10.5.

You can enter text for the introduction, empirical cases, observable indicators, data collection and questionnaires to the factor, as is done in the colour-coded factor.

Figure 10.5. Factor text dropdown menu

This screenshot is similar to Figure 10.4 but with the dropdown menu for the "Factor Texts" section open. The menu lists the following options: "Introduction", "Introduction", "Empirical Cases", "Observable Indicators", "Data Collection", and "Questionnaire". The first "Introduction" option is highlighted in blue. Below the dropdown, a text area is visible with the word "Introduction" at the top.

Step 6

Click 'Save' to create a new cumulative factor.

You can also view the cumulative factor(s) in the Knowledge Resource Library.

10.2. Adding cumulative factors to the model

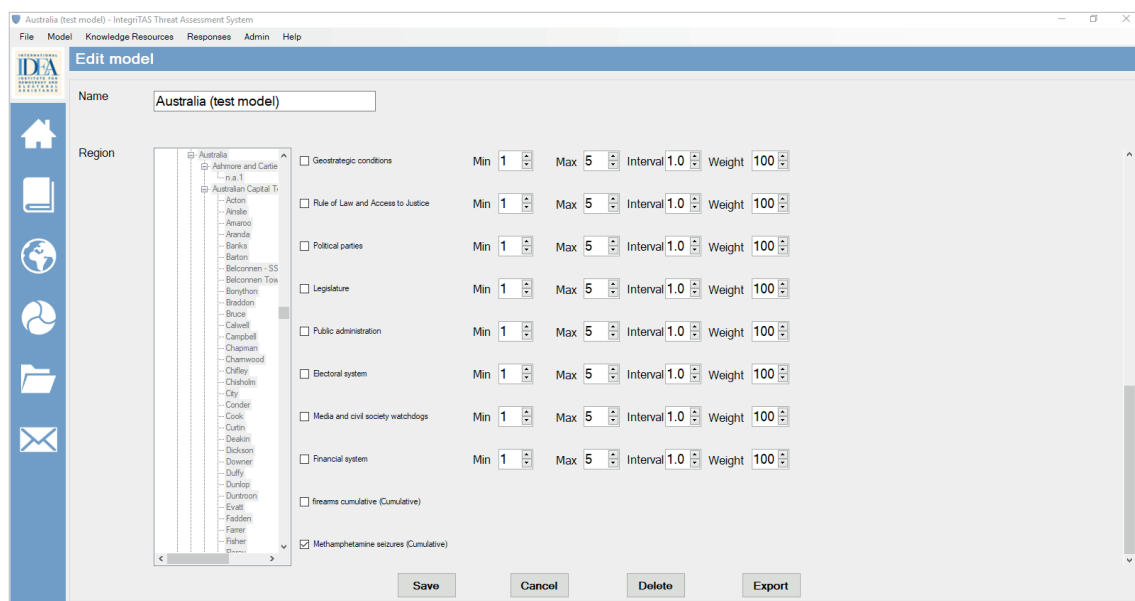
After you have created the cumulative factor, it is time to add the factor to the model.

Step 1

Go to 'Model Menu' → 'Current Model' → 'Edit'.

Add the factor to your current model by selecting it. Added factors appear at the bottom of the list, as seen in Figure 10.6.

Figure 10.6. Factor added to current model



Step 2

Click 'Save' to add the cumulative factor to the model. Adding data to the cumulative factor is the same as adding data in the colour-coded factor.

Step 3

Add the data for the required factor.

Figure 10.7 and 10.8 show the six functionalities for adding the required data into the model.

1. Open 'Analytical Instruments'
2. Add data by either 'Table by Region' or 'Table by Factor' from the Tab Menu
3. Select the region(s) for the data
4. Select the Cumulative factor
5. Click 'Add Date'
6. Enter the data

Figure 10.7. Functionalities for adding data into the model

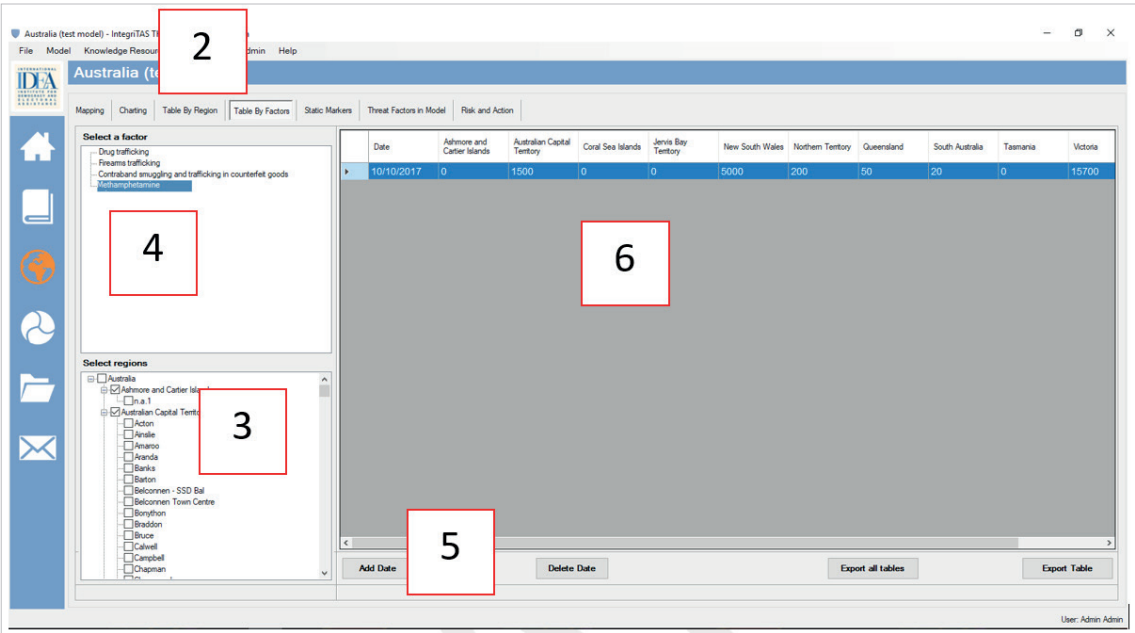
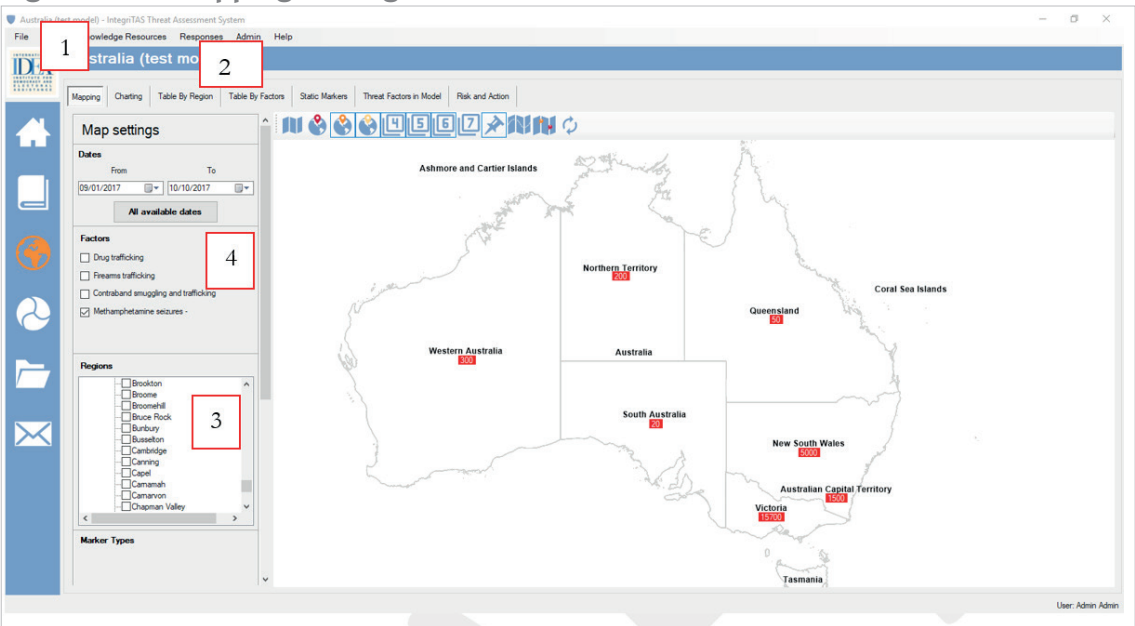


Figure 10.8. Mapping settings functionalities



Step 4

After the data have been entered, go back to the 'Mapping Tab'.

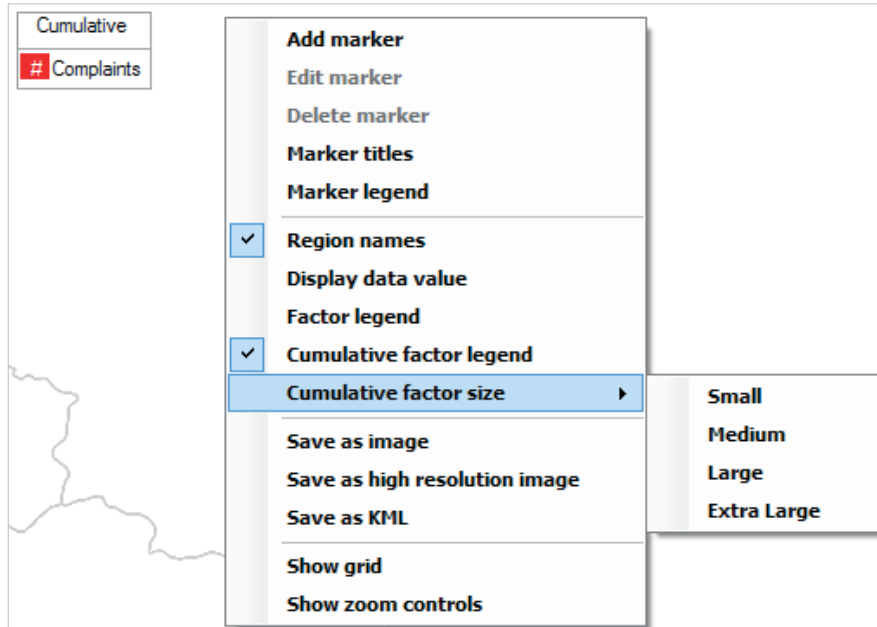
Select the date, factor and region to be drawn.

You can add more than one cumulative factor to the model. You can show the legends by using the right click menu.

Step 5

To increase the size of the cumulative factors, right click on the mapping interface. Select the required size (Small, Medium, Large or Extra Large) as shown in the menu in Figure 10.9.

Figure 10.9. Cumulative factor size dropdown menu



11. Static markers

Static markers can be used in a number of ways, such as to display the location of a facility (polling station, police station, warehouse), events or incidents (political party rally, hate speech, human rights violation), material (sensitive or non-sensitive electoral material, small arms) or actor (political party, police, election monitors, election officials). They can also be used to denote threat factors or vulnerabilities particular to a location. The static marker feature can use GPS coordinates.

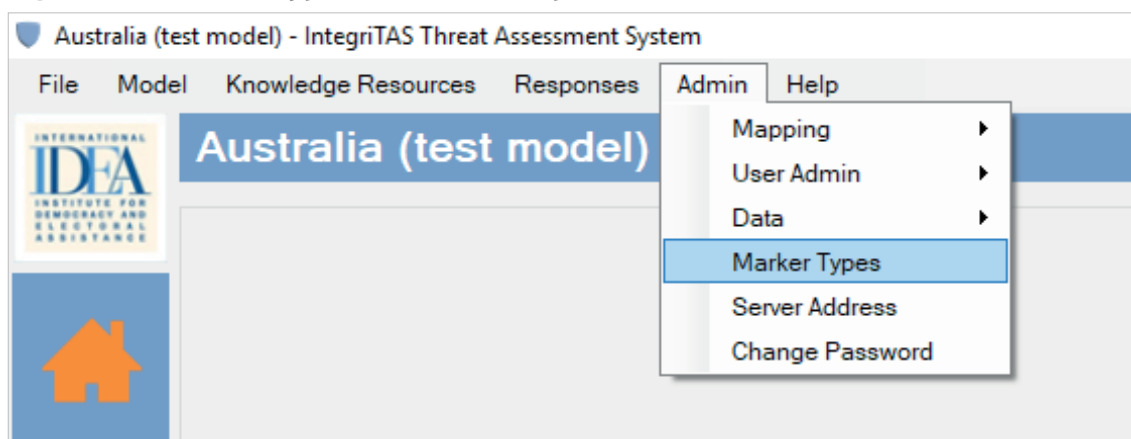
By default, the tool comes with two static markers, but you can also create a new static marker. You can select marker(s) from the list or use your own marker (Note: the static marker should be in .png image format)

11.1. Adding new static markers

Step 1

Go to 'Admin Menu' → 'Marker Types', as shown in Figure 11.1.

Figure 11.1. Marker types in 'Admin' dropdown menu



A new window appears, as in Figure 11.2.

Figure 11.2. Marker types popup window

Step 2

Enter the name of the new marker.

Step 3

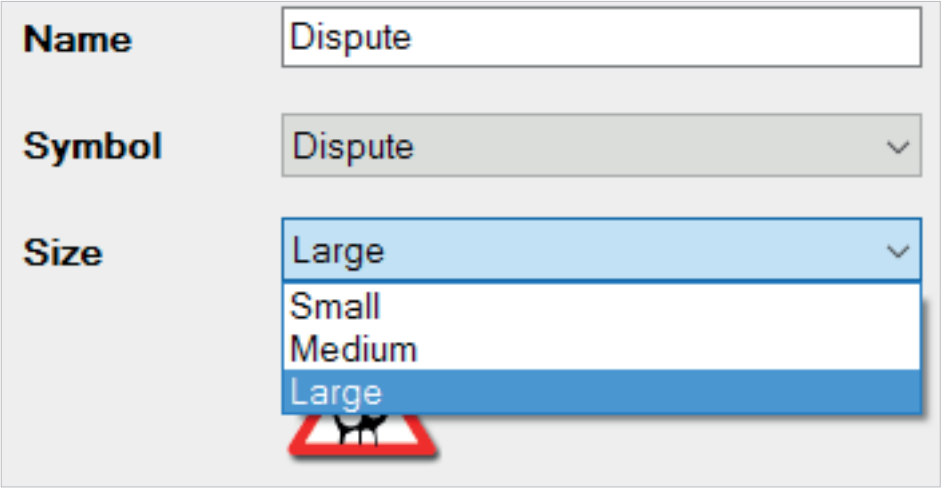
Select 'Symbol' from the dropdown menu. There are around 40 static markers to be selected, as seen in Figure 11.3.

Figure 11.3. Static markers options

Step 4

Select the size (Small, Medium or Large), as shown in Figure 11.4.

Figure 11.4. Static marker size options



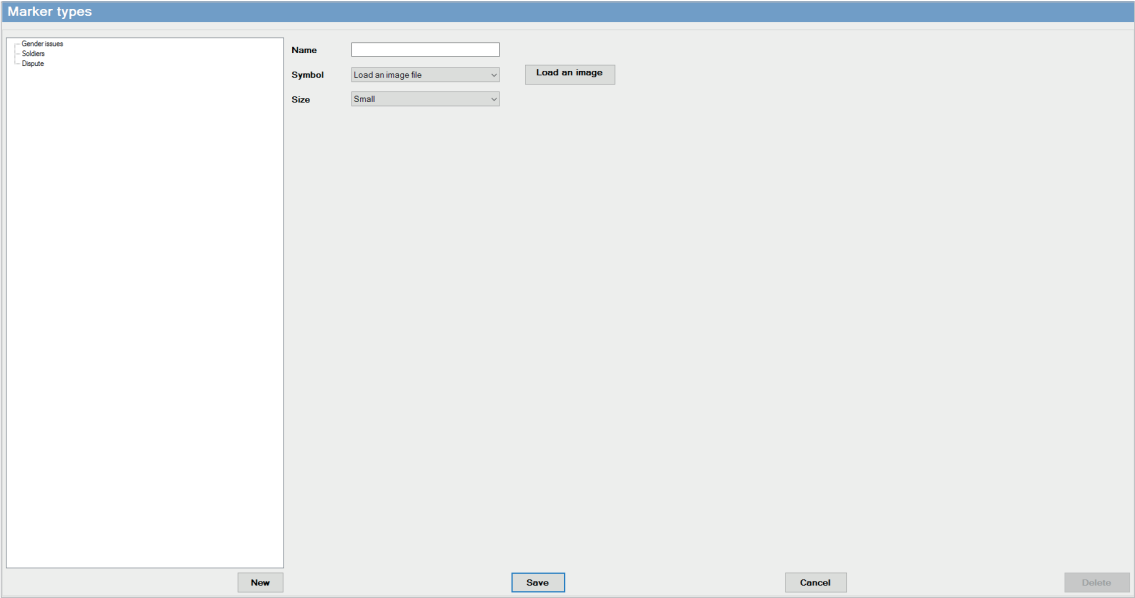
The screenshot shows a configuration window for a static marker. It has three main sections: 'Name', 'Symbol', and 'Size'. The 'Name' field contains the text 'Dispute'. The 'Symbol' dropdown menu also shows 'Dispute'. The 'Size' dropdown menu is open, showing three options: 'Large' (highlighted in blue), 'Small', and 'Medium'. Below the 'Size' dropdown, there is a small red triangular warning sign icon with a black silhouette of a person inside.

Step 5

Click 'Save' to add the new marker to the tool.

After saving, the name of the marker appears on the left side of the window (the markers list), as shown in Figure 11.5.

Figure 11.5. Static marker saved



The screenshot shows the main application window titled 'Marker types'. On the left, there is a list of marker types: 'Gender issues', 'Soldiers', and 'Dispute'. The 'Dispute' marker is selected. On the right, there is a configuration panel for the selected marker. It has fields for 'Name' (empty), 'Symbol' (set to 'Load an image file'), and 'Size' (set to 'Small'). There is a 'Load an image' button next to the 'Symbol' field. At the bottom of the window, there are four buttons: 'Now', 'Save', 'Cancel', and 'Delete'.

Step 6

You can also create your own marker to add to the tool using the 'Load an image' button. You can edit the marker name, symbol and size by selecting the marker from the markers list. You can delete the marker(s) by selecting the marker and clicking delete.

11.2. Adding static markers to maps

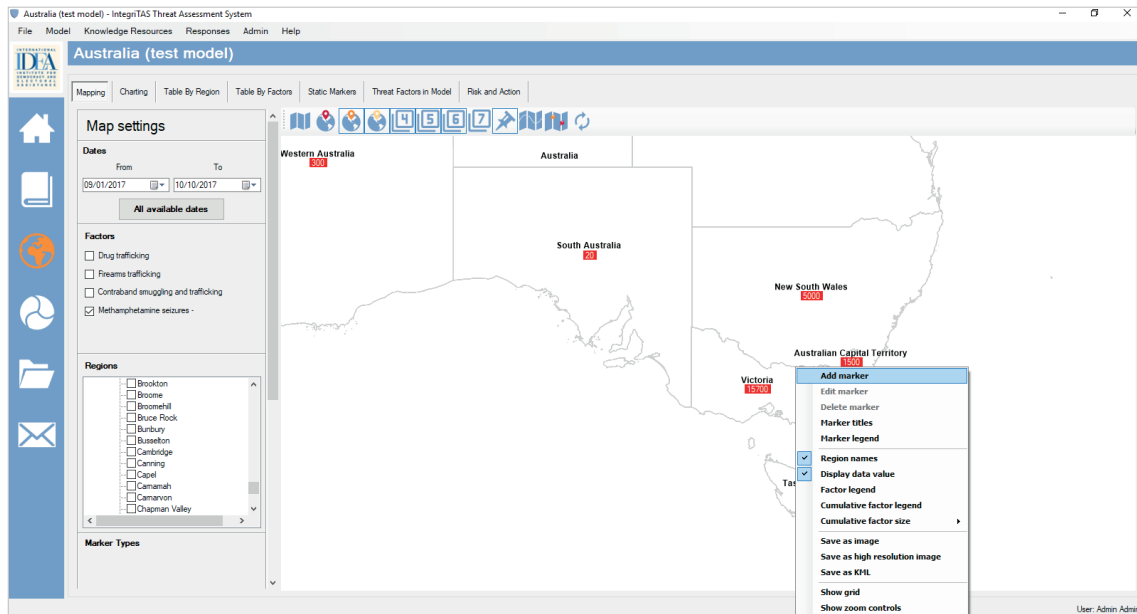
Once created, static markers can be added to the map.

Step 1

In Analytical Instruments, right click on the area where the marker will be added.

A menu appears, as shown in Figure 11.6. Select 'Add Marker'.

Figure 11.6. Add marker popup menu



Step 2

A window as shown in Figure 11.7 appears.

Figure 11.7. Marker popup window

 The screenshot shows a 'Marker' popup window. It has a 'Title' field with a 'Title Color' selector (currently black). Below is a 'Text' field with a scrollable area. Underneath is a 'Select Marker Type' dropdown menu currently set to 'Gender issues'. At the bottom, there are date pickers for 'From' (09/10/2017) and 'To' (09/10/2017), and input fields for 'Latitude' (-37.25075989743) and 'Longitude' (146.1331726031). 'Save' and 'Cancel' buttons are at the bottom.

Enter the required information, as shown in Figure 11.8.

- Add the 'Title' for the marker.
- Change the title colour by clicking the colour.
- Add the description in 'Text Field'.
- Select the marker type.
- Select the date. This allows the marker to be viewed during the specified period.
- Latitude and Longitude are already added. However, more specific values can be added if required.

Figure 11.8. Marker information in popup window

Step 3

Click 'Save' to add the marker to the map.

Step 4

To view the marker in the map, the marker toggle button must be enabled.

To do this, click on the Marker Toggle button (the pin image) as shown in Figure 11.9.

Figure 11.9. Marker toggle button



Step 5

To resize the marker, click on 'Marker Types' in 'Map settings', as shown in Figure 11.10.

Figure 11.10. Resize marker functionality in marker types popup window

The screenshot shows the 'Map settings' window with the following sections:

- Dates:** Includes 'From' and 'To' date pickers set to 02/02/2016 and 16/02/2016, and a button labeled 'All available dates'.
- Factors:** A list of checkboxes:
 - ☐ Contested electoral law
 - ☐ Inadequate electoral administrative rules
 - ☐ Inadequate funding, financing and
 - ☒ Complaints - Cumulative
- Regions:** A hierarchical tree view showing a selection of regions in Nepal:
 - ☒ Nepal
 - ☒ Central
 - ☒ Bagmati
 - ☒ Bhaktapur
 - ☒ Dhading
 - ☒ Kathmandu
 - ☒ KavrePalanchok
 - ☒ Lalitpur
 - ☒ Nuwakot
 - ☒ Rasuwa
 - ☒ Sindhupalchok
 - ☒ Janakpur
 - ☒ Dhanusa
- Marker Types:**
 - ☒ Dispute
- Resize markers:** A slider control with a blue handle positioned towards the right end.

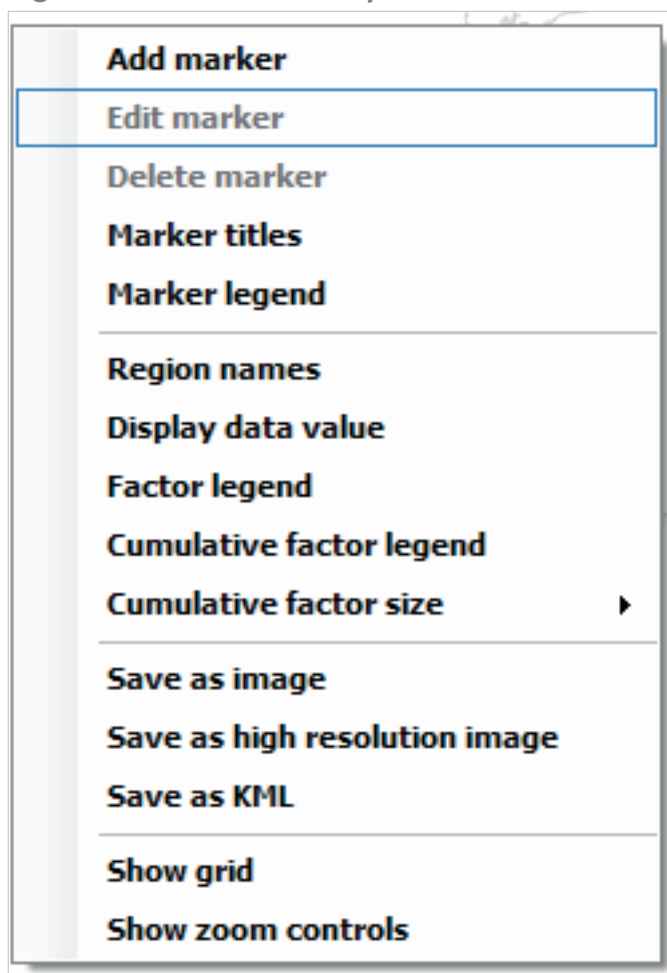
11.3. Editing markers

You can also edit markers if required.

Step 1

Right click on the marker – select ‘Edit marker’, as shown in Figure 11.11.

Figure 11.11. Edit marker option



Step 2

A window as shown in Figure 11.12 appears.

Edit title, title colour, text, marker type, date, and latitude and longitude as required.

Click 'Save' to save changes.

Figure 11.12. Edit marker information

The screenshot shows a 'Marker' dialog box with the following elements:

- Title:** A text box containing 'Dispute'.
- Title Color:** A black color swatch.
- Text:** A text area containing 'There was a dispute between two parties'.
- Select Marker Type:** A dropdown menu showing 'Dispute' with a warning triangle icon to its right.
- From:** A date picker showing '16/02/2016'.
- To:** A date picker showing '16/02/2016'.
- Latitude:** A text box containing '28.49535863'.
- Longitude:** A text box containing '83.98367248'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

Further functionality includes:

- To view the legend(s), right click and select 'Marker Legend'.
- To view the title of the marker within the map, right click and select 'Marker Title'.
- To see the description (if any), hover over a marker.
- You can view all the markers, add new ones or edit markers from the 'Static Markers' tab on the 'Tab Bar', and can also export to or copy from an Excel file.

12. Charting

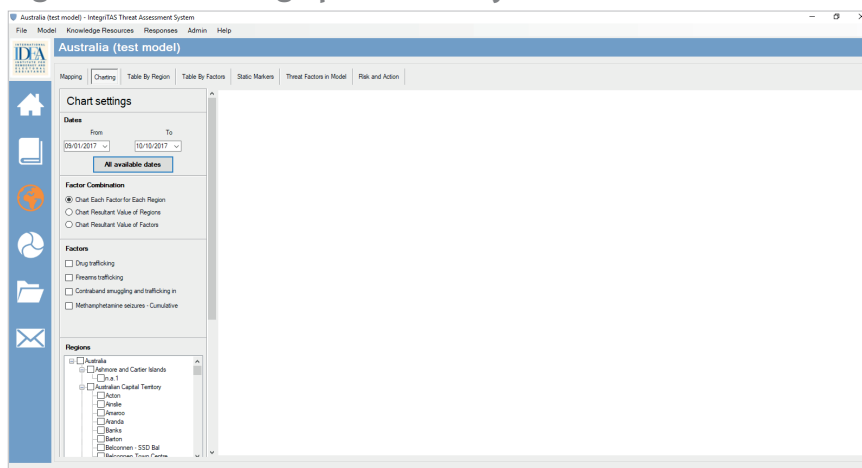
Threat maps by themselves tend to be static, but combined with charts they are more dynamic. Trend analysis allows you to see factor changes over time, for example during and between elections. There are three ways to view charting in the tool:

- ‘Resultant value of factor’, which shows all data using one simple graph. You can deselect geographical regions to view, for example, the resultant value of a factor for a specific region.
- ‘Resultant value of region’ plots a graph for a particular region, taking into account several factors.
- ‘Chart resultant value of region’ plots a graph for a particular region, taking into account several factors. This feature is only useful when data have been collected for two or more factors. You can create five types of charts: line, fast line, spline, spline area and column.

Step 1

On the Analytical Instrument module, go to ‘Charting Tab’ from the Tab menu. A screen appears, as shown in Figure 12.1.

Figure 12.1. Charting option in analytical instruments module

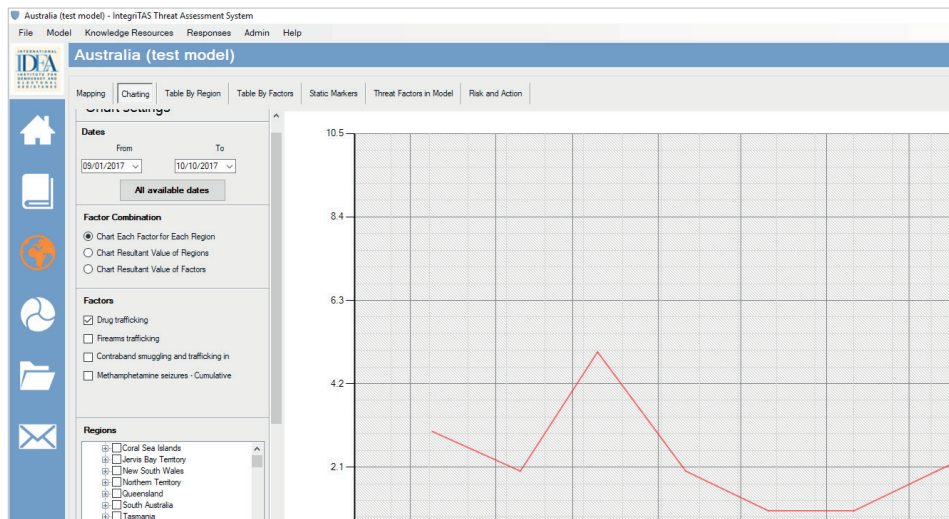


Step 2

Select and enter the date, 'Factor combination', 'Factors', 'Regions' and 'Chart Type' (Fast Line, Line, Spline, Spline Area or Column).

In the example shown in Figure 12.2, data have been entered for three dates, the factor combination is 'Chart Each Factor' for 'Each Region', the factor selected is 'Drug trafficking', and Victoria has been selected as the region and Spline as the chart type.

Figure 12.2. Example of charting

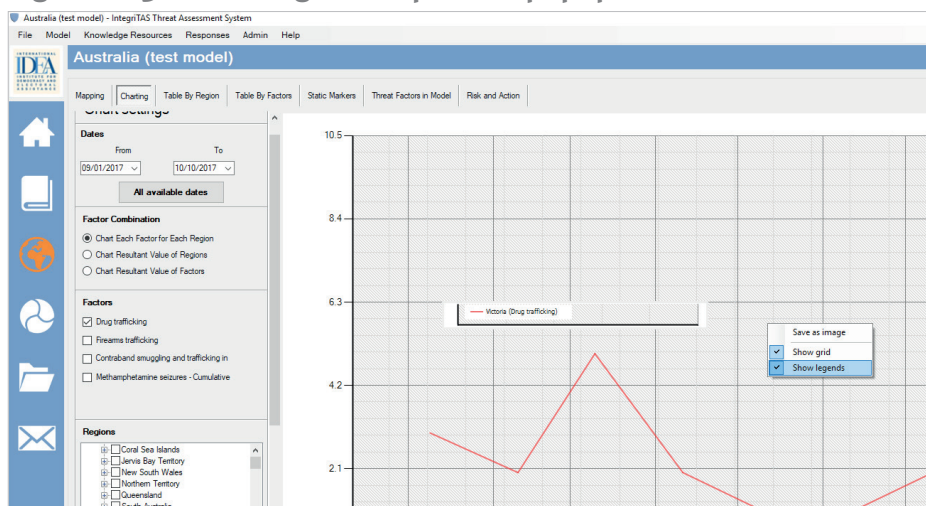


Step 3

The legend(s) of different types of factor combinations can be viewed.

Right click on the chart and click 'Show legends' in the menu that appears, as shown in Figure 12.3.

Figure 12.3. 'Show legends' option in popup menu



Step 4

Save the chart as an image.

Right click on the chart and select 'Save as image'. A dialogue box will appear to guide you where to save the image on your computer.

13. Keyhole mark-up language and Google Earth

Colour-coded maps and static markers can be saved in the KML and uploaded onto Google Earth, which must be installed beforehand. You can display IntegriTAS maps on Google Earth, which is great for presentation purposes.

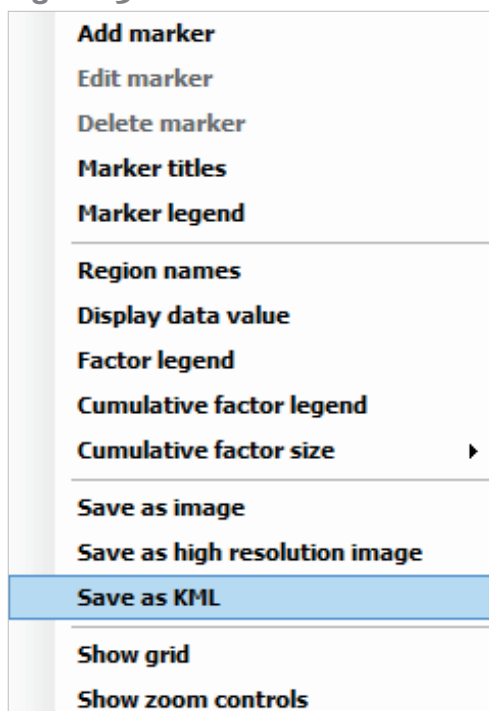
Step 1

Right click on the map and select 'Save as KML', as shown in Figure 13.1.

A dialogue box appears, as shown in Figure 13.1. Select the location and click 'Save' to save the KML.

For this demonstration, the example of Nepal has been used.

Figure 13.1. 'Save as KML' function in dialogue box popup window



Step 2

After the KML has been saved, double click to open the file (in the example in Figure 13.2, Nepal_Test).

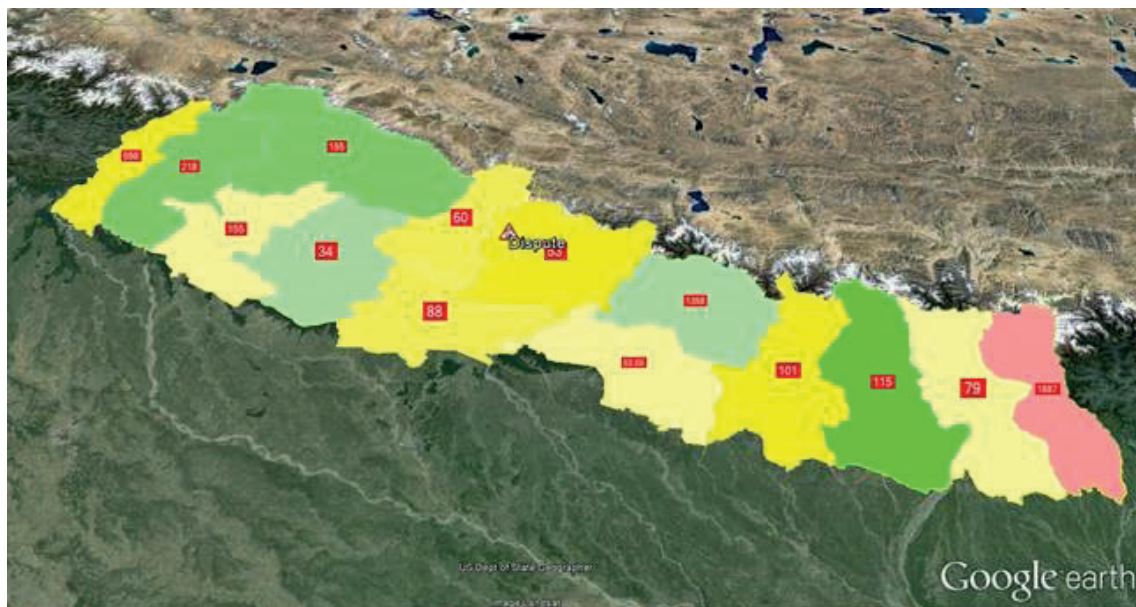
Figure 13.2. Example of saved KML: Nepal_Test

Name	Date modified	Type	Size
Images	17-Feb-16 10:52 AM	File folder	
Nepal_Test	17-Feb-16 11:02 AM	KML	581 KB

Step 3

Google Earth opens the file. A screen will appear showing the territory embedded in Google Earth, as seen in Figure 13.3.

Figure 13.3. Example of territory embedded in Google Earth



By default, the model name is used to save the KML file, but you can insert an alternative file name.

Google Earth shows the exact map as seen in IntegrITAS. Therefore, if you have enabled region names, static markers or other features, it also shows these.

14. Threat and Action Register (TAR)

The Threat and Action Register (TAR) is the institutional depository for the threat alerts created. It enables you to save the information used during the creation of the threat alerts. There are two types of TAR: i) Model-specific TAR and ii) Master TAR. Model-specific TAR is used to store a single model of threat alerts. Master TAR is the collection of all model-specific TARs.

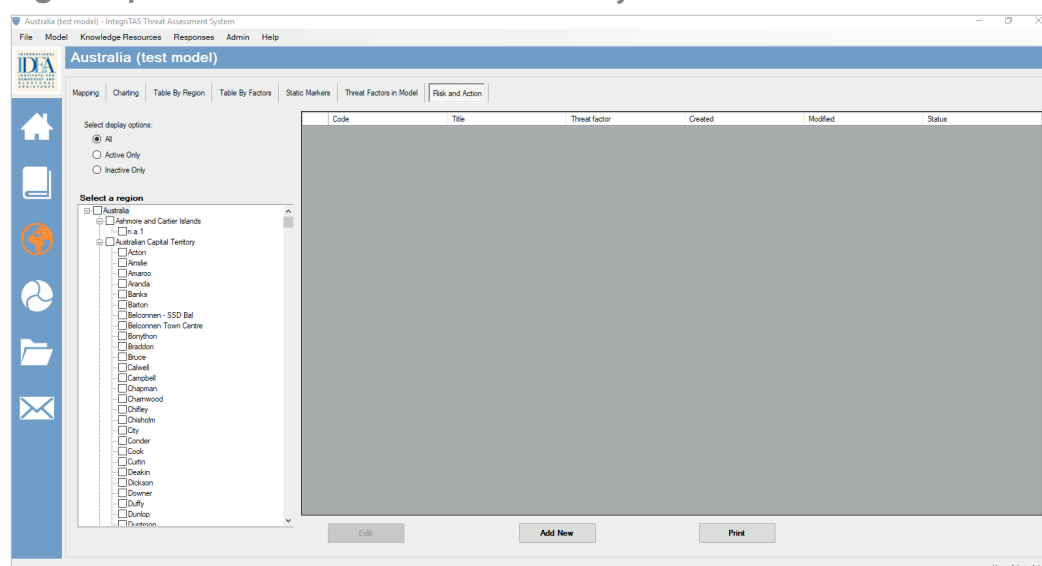
Threat alerts are created and saved in the Analytical Instrument module using the ‘Threat and Action’ tab. These features allow you to systematically document threat alerts issued, actions taken and outcomes of actions.

14.1. Creating a threat alert

Step 1

Go to the ‘Risk and Action’ tab from the Tab Bar in the Analytical Instruments module. The screen as shown in Figure 14.1 appears.

Figure 14.1. ‘Risk and Action’ tab in the analytical instruments module



Step 2

Create a new Threat register. Click 'Add New'.

A new window pops up within the tool as shown in Figure 14.2.

Figure 14.2. Risk and action popup window

Complete the following information:

- 'Region': From the list on the left, select at least one region for the alert.
- 'Code': Use any code for the alert. If you do not want to use a particular code, then leave the field empty. It is automatically populated with a number assigned by the application.
- 'Title': The title of the alert.
- 'Date from and to': The date range.
- 'Electoral Phase': Click on 'Add' text, and a list of electoral phases is displayed. You must select at least one.
- 'Analysis': This allows you to add documents to the alert. You cannot add documents until you save the alert for the first time. Then you can edit the alert and add documents to it.
- 'Threat Description': Written analysis as seen in the threat alert.
- 'Action': Suggested action of electoral management bodies, security sector agencies and civil society organizations.
- 'Result': Actions taken are recorded here.
- 'Status': Active when the result is not achieved, and inactive when the result has been achieved.

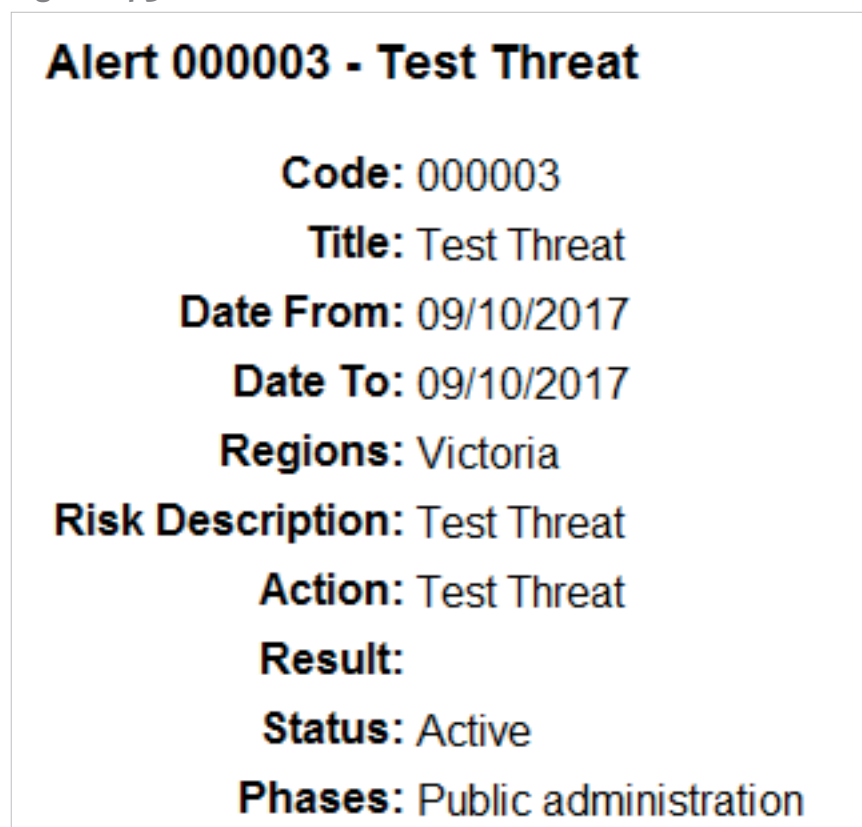
Step 3

After all fields are completed, click 'Save'.

Step 4

View the 'Threat alert' by clicking 'View'. The information will appear as in Figure 14.3.

Figure 14.3. Information in threat alert

**14.2. Master Threat and Action Register (TAR)**

The Master TAR is the depository of all TAR entries from all models in the tool. You can view the code, model, title, electoral phase, TAR created date, TAR modified date and status of the TAR entry.

Step 1

Access the Master TAR.

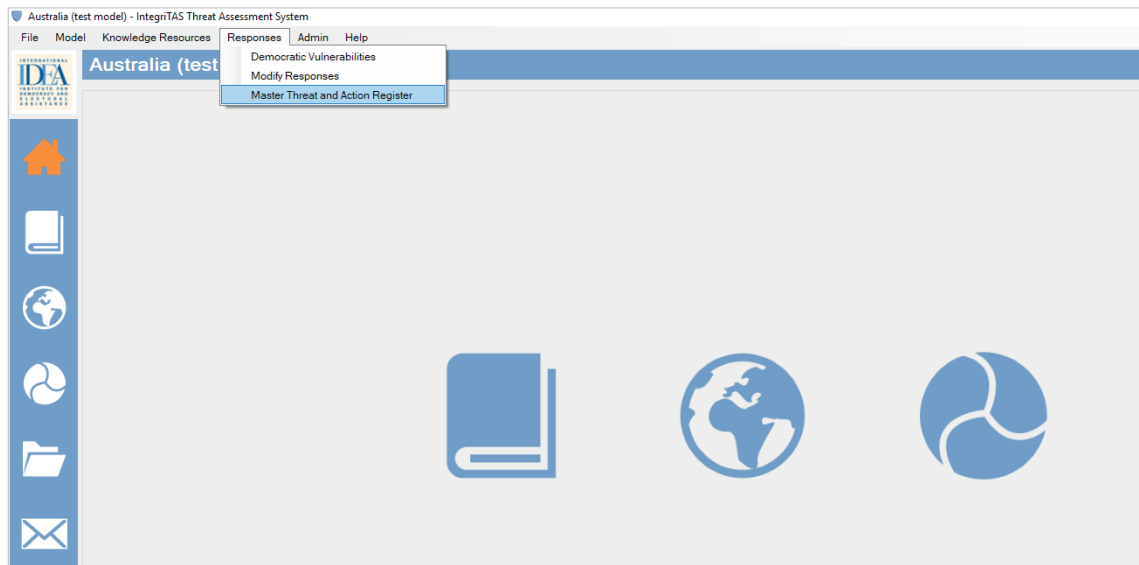
Go to 'Response Menu' → 'Master TAR'.

OR

Click on the folder icon on 'Side bar'.

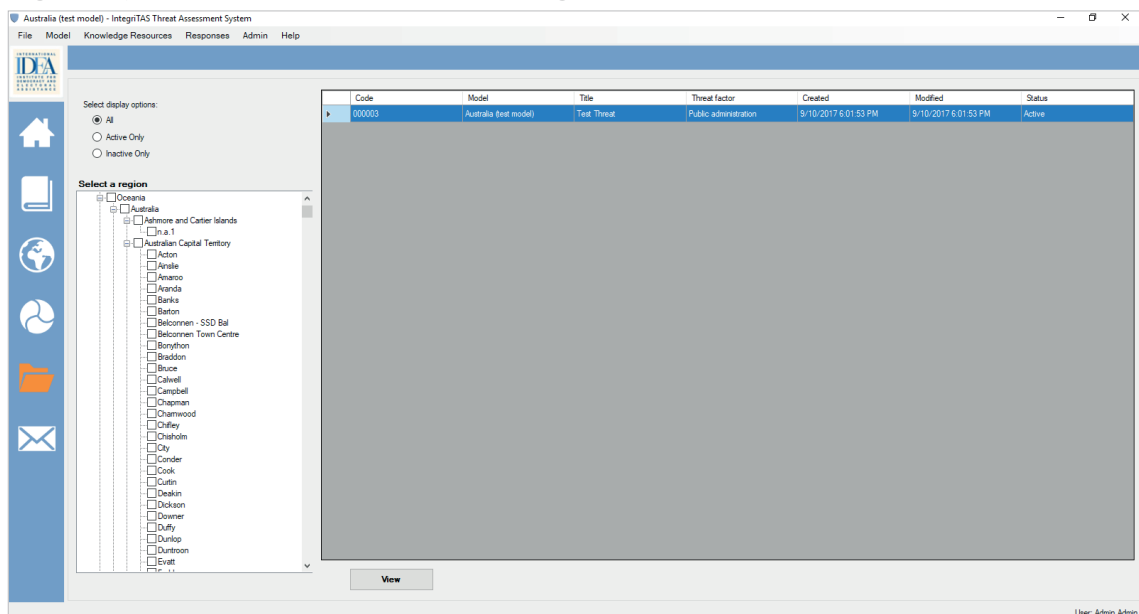
Both options are shown in Figure 14.4 below.

Figure 14.4. Master threat and action register in ‘Response’ dropdown menu and folder icon



The screen as shown in Figure 14.5 appears.

Figure 14.5. Master threat and action register



Step 2

Click the TAR and click ‘View’.

OR

Double click to view the TAR entry.

You can filter the TAR entry based on regions or status (‘active’ or ‘inactive’).

15. Prevention and Mitigation Module

The Prevention and Mitigation Module allows you to access a specific phase of the electoral cycle and learn about possible measures to prevent and mitigate the threats of organized crime on democratic politics. Comparative action points presented in this module are developed, implemented and perfected by electoral management bodies, security sector agencies, and other state and non-state actors around the world. The cases and action points aim to inspire you to design prevention and mitigation strategies that are sensitive to your specific national and electoral context.

Action points in the prevention and mitigation module or the support document IntegriTAS Strategies for Prevention and Mitigation Guide (which mirrors the information presented in the module) may be useful recommendations that can be included in the action box of the threat and action register. The results depend on which action was implemented and the result of that action. Several action points can be recommended depending on the threat and threat level, and these recommendations can be included in the threat alert.

The IntegriTAS Action Guide draws on cross-country research and national experiences to provide insights on strategies to prevent and mitigate the nexus between illicit actors and political processes and institutions. Recognizing the multi-faceted nature of these challenges, the Action Guide combines measures to identify and correct institutional vulnerabilities with steps to protect and empower anti-corruption reformers.

The module includes 30 comparative action points to address the influence of organized crime on democratic political systems. Action points present possible approaches, based on empirical cases, which can be taken to prevent and mitigate the influence of organized crime on 'political entry points', presented here in the framework of 'democratic vulnerabilities'.

These democratic vulnerabilities are:

1. Foundational democratic vulnerabilities
 - Socio-economic conditions
 - Political transition processes
 - Geostrategic conditions

2. Institutional democratic vulnerabilities

- Rule of law and access to justice
- Political parties
- Legislature
- Public administration
- Electoral system

3. Associated democratic vulnerabilities

- Media and civil society watchdogs
- Financial system

You can modify or remove the tool's presentation and mitigation measures. As part of the customization process, you can easily modify or remove responses, or add new responses.

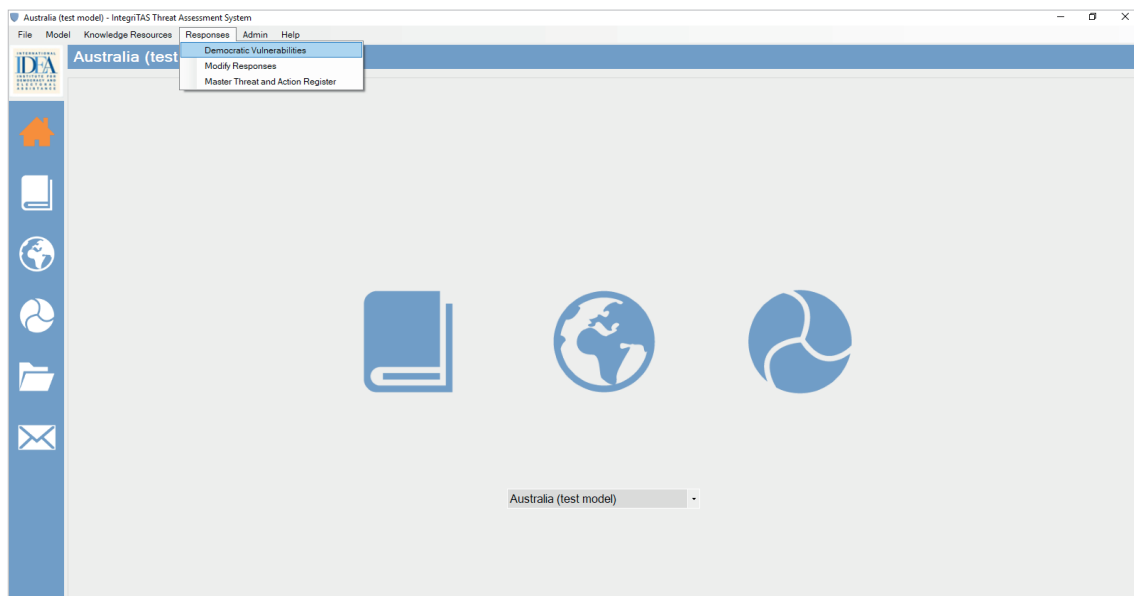
15.1. Accessing the Prevention and Mitigation Mode

Step 1

There are three ways to access 'Prevention and mitigation'. All three are highlighted in Figure 15.1 below.

- Responses Menu – 'Democratic Vulnerabilities'
- Side Bar
- Module Selection Bar

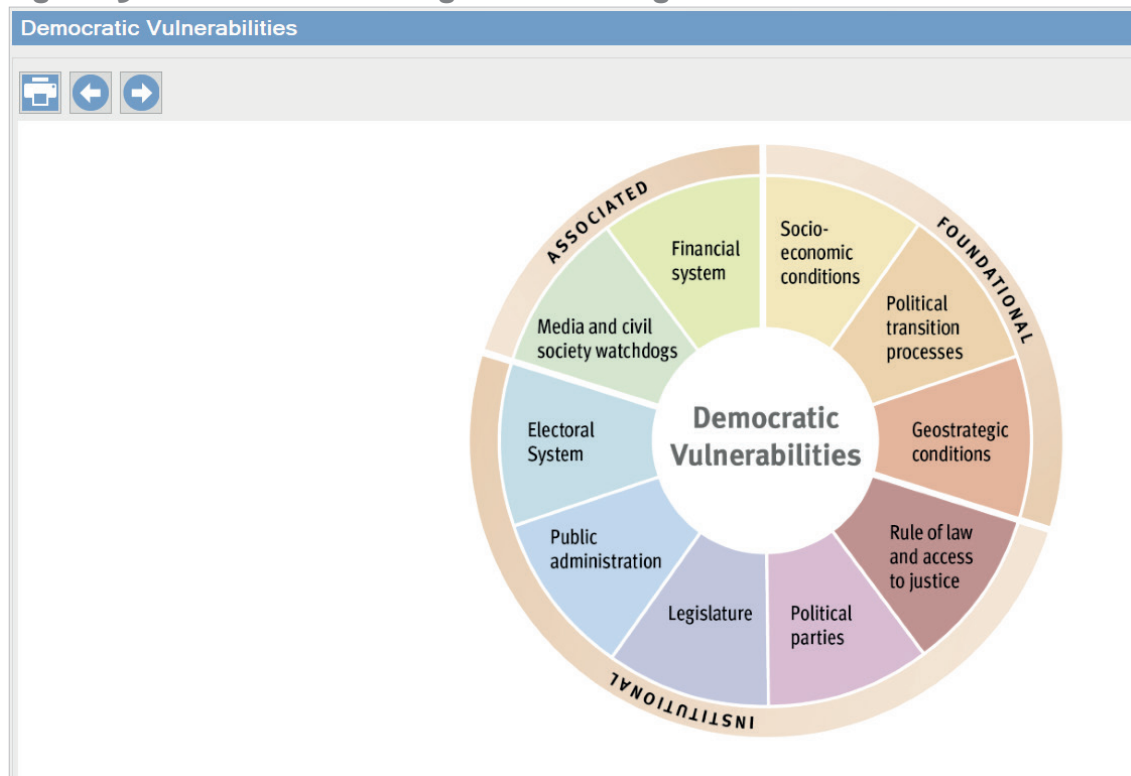
Figure 15.1. Prevention in mitigation access



Step 2

After clicking any of the three menus, a screen appears, as shown in Figure 15.2, displaying all the Democratic Vulnerabilities.

Figure 15.2 Prevention and mitigation according to democratic vulnerabilities



15.2. Managing responses

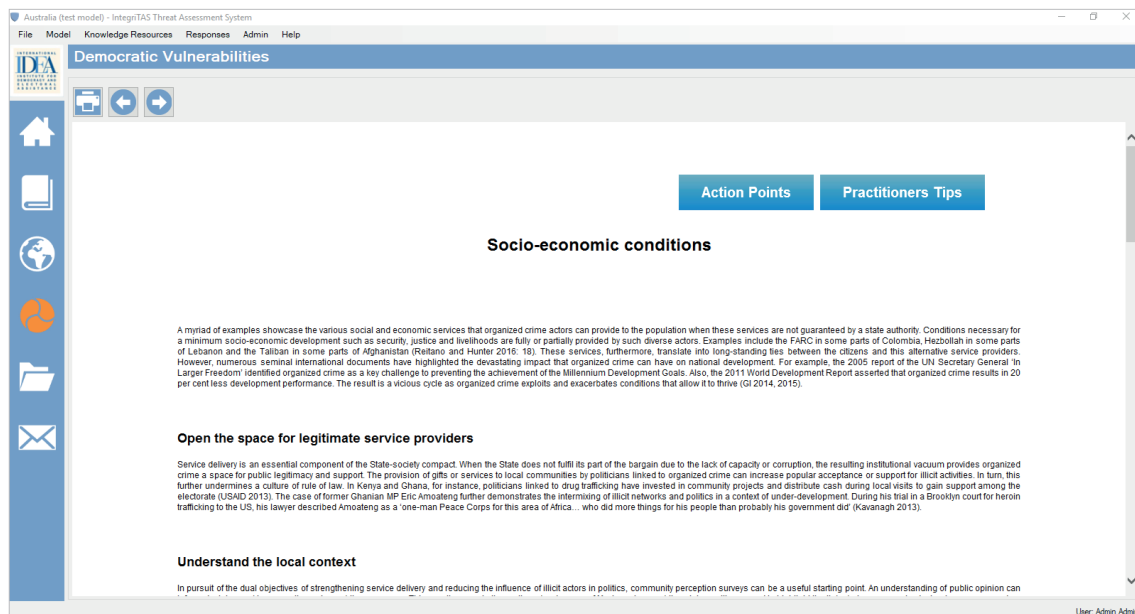
You can use the prevention and mitigation measures provided in the tool or refer to the *IntegriTAS Action Guide*. The threat factors and corresponding response strategies have been divided into three clusters of democratic vulnerabilities (Foundational, Institutional and Associated).

Step 1

Begin with the wheel of the Democratic Vulnerabilities accessed in Section 15.1 (Figure 15.2). Click on any of the threat factors to open the prevention and mitigation measures for that vulnerability.

This example uses 'Socio-economic conditions'. The full text and description with some examples and best practices appears, as shown in Figure 15.3.

Figure 15.3. Example of description of prevention and mitigation strategies: Socio-economic conditions



Step 2

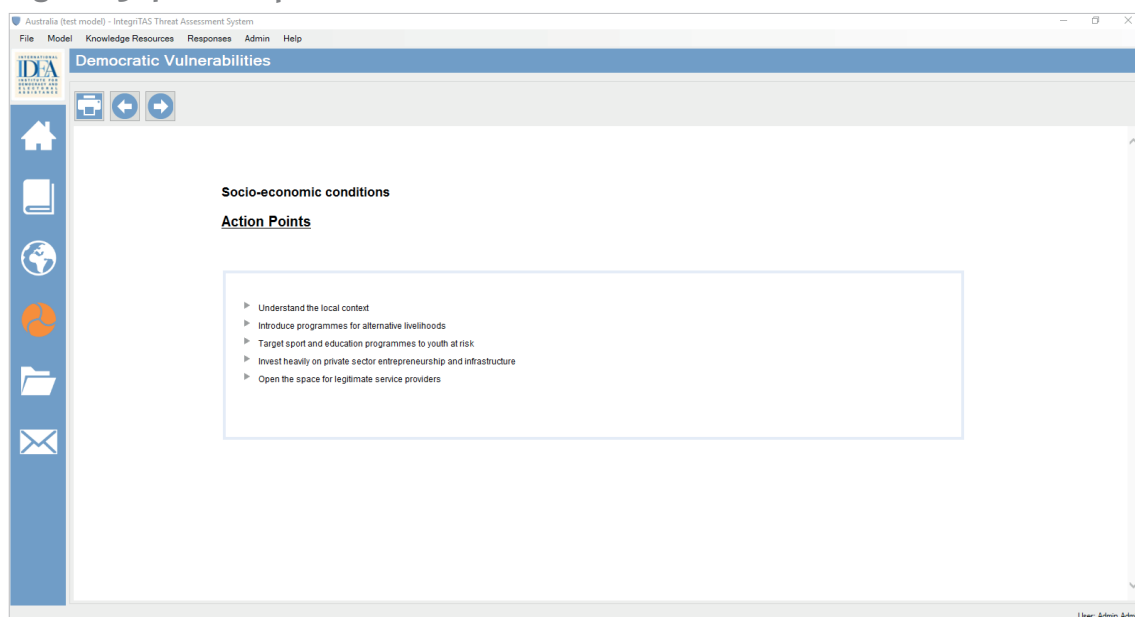
Select the required mitigation measures for any threat.

You can copy this to the TAR mentioned in Section 14.2, or to any threat alert reports.

Step 3

To view the summarized Action Points of that cluster, click 'Action Points'. A new window appears, as shown in Figure 15.4.

Figure 15.4. Action points



- Click on the 'Navigation' button to navigate forward and back.
- Click the 'Print' button to print the currently viewed page.
- Copy and paste the relevant action point into the TAR entry.

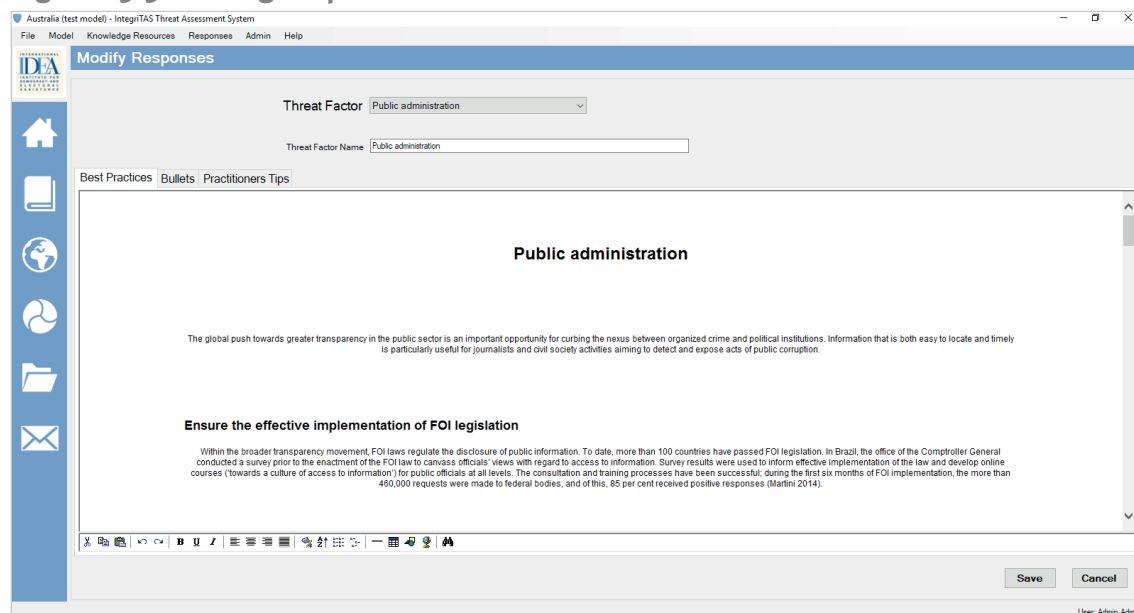
15.3. Adding responses

Step 1

Go to 'Responses' → 'Modify Responses'.

A new window appears, as shown in Figure 15.5.

Figure 15.5. Adding responses



Step 2

Select the specific threat factor from the dropdown menu.

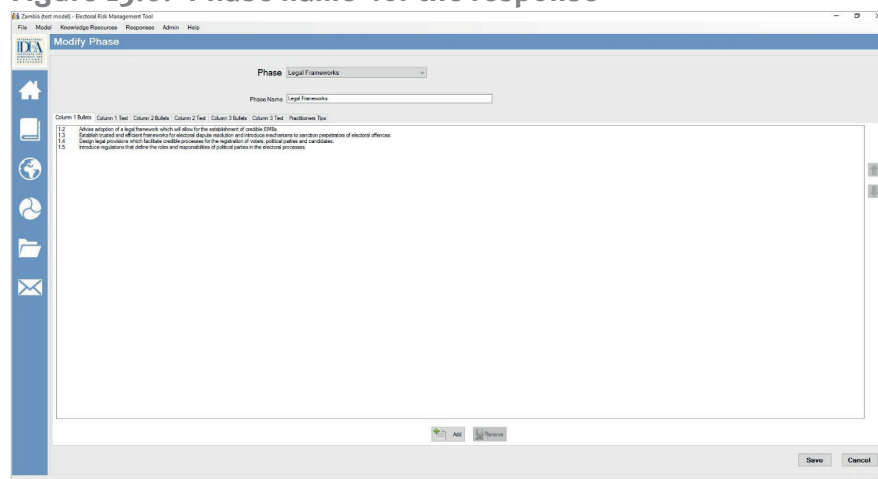
Step 3

Select the specific 'Phase name' for the response, as shown in Figure 15.6.

The following functionalities are available:

- 'Best Practices' demonstrates the mitigation strategies for anti-corruption reformers.
- 'Bullets' summarizes the mitigation strategies that you can modify.
- 'Practitioner Tips' allows you to add your own notes or research on the topic.

Figure 15.6. 'Phase name' for the response



15.4. Action points

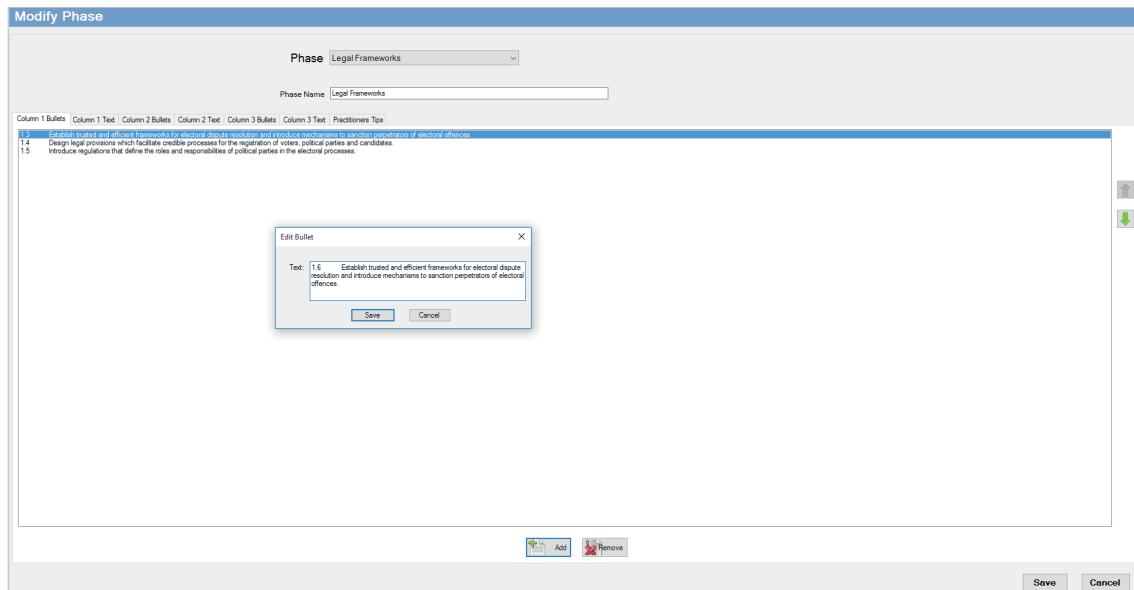
Step 1

Add new action ‘bullet’ points.

Click ‘Add’, and enter your action points.

Click ‘Save’, as shown in Figure 15.7.

Figure 15.7. ‘Save’ function for adding a new action point



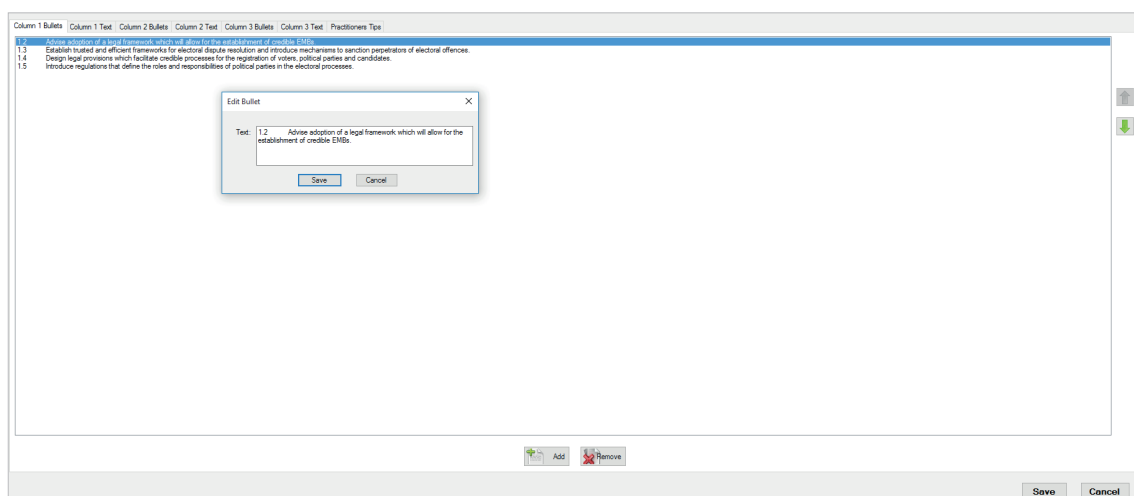
Step 2

Edit any action ‘bullet’ point.

Double click on the particular action point. A window appears, as shown in Figure 15.8.

Enter your changes and click ‘Save’.

Figure 15.8. Popup window when selecting an action point and save function



Step 3

To change the description of any action points, go to the column text and double click and edit the description as required.

Click 'Save' to save the changes.

Step 4

To remove action points, select the action point that you want to delete or remove.

Click 'Remove'. A dialogue window appears. Click 'Confirm' to confirm the action.

Step 5

To delete the description, go to the column text relevant to the action point.

Locate and select the description. Click the 'Delete' button on your computer keyboard.

Step 6

Click 'Save' before exiting the Modify Responses menu, as highlighted in Figure 15.8.

About IntegriTAS

Transnational organized crime threatens democracy. Supporting the capacity of national and local institutions to prevent and mitigate the nexus between organized crime and democratic politics is an important part of fighting against these threats. The *IntegriTAS Threat Assessment System* is a multipurpose data-driven software application that helps national and local institutions identify the threats that organized crime poses to politics. Focusing on the threat—instead of seeking to establish the existence of links between organized crime and politics, or their impact—allows users to map and focus on the factors that contribute to corruption, and to identify strategies to prevent or mitigate the threat.

Modules

IntegriTAS is structured around three interactive modules: (a) a virtual library providing a list of factors which increase the threat that organized crime will distort democratic politics; (b) a software application that helps users easily map, geo-reference, present and visualize different types of democratic vulnerabilities and organized crime activities to build a country-specific model; and (c) a framework that equips users with global good practices and lessons learned for preventing and mitigating organized crime influence on democratic politics.

Documentation

The IntegriTAS software is accompanied by three Guides. The IntegriTAS Process Guide describes the process of implementing IntegriTAS. It includes a description of the system's structure and its implementation stages. The IntegriTAS Factors Guide provides basic definitions of the threat factors used in IntegriTAS. It includes an Annex which provides a more comprehensive list of potential indicators that can be used to observe each factor. The IntegriTAS Prevention and Mitigation Guide discusses the various prevention and mitigation strategies that can be applied to reduce the undue influence of organized crime on democratic processes. The software is also accompanied by a User Manual and a help file.

Download

Access the IntegriTAS software and supporting documentation online:

<<https://www.idea.int/data-tools/tools/integritas-threat-assessment-system>>.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with the mission to advance democracy worldwide, as a universal human aspiration and enabler of sustainable development. We do this by supporting the building, strengthening and safeguarding of democratic political institutions and processes at all levels. Our vision is a world in which democratic processes, actors and institutions are inclusive and accountable and deliver sustainable development to all.

What do we do?

In our work we focus on three main impact areas: electoral processes; constitution-building processes; and political participation and representation. The themes of gender and inclusion, conflict sensitivity and sustainable development are mainstreamed across all our areas of work.

International IDEA provides analyses of global and regional democratic trends; produces comparative knowledge on good international democratic practices; offers technical assistance and capacity-building on democratic reform to actors engaged in democratic processes; and convenes dialogue on issues relevant to the public debate on democracy and democracy building.

Where do we work?

Our headquarters is located in Stockholm, and we have regional and country offices in Africa, the Asia-Pacific, Europe and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

<<http://www.idea.int>>

Transnational organized crime threatens democracy. Supporting the capacity of national and local institutions to prevent and mitigate the nexus between organized crime and democratic politics is an important part of fighting against these threats.

The *IntegriTAS Threat Assessment System* is a multipurpose data-driven software application that helps national and local institutions identify the threats that organized crime poses to politics. Focusing on the threat—instead of seeking to establish the existence of links between organized crime and politics, or their impact—allows users to map and focus on the factors that contribute to corruption, and to identify strategies to prevent or mitigate the threat.

This User Manual provides advice for users of the *IntegriTAS Threat Assessment System*. It presents the steps required to get the system up and running, including system requirements, installation and user administration.

International IDEA
Strömsborg
SE-103 34 Stockholm
Sweden
Tel + 46 8 698 37 00
Email: info@idea.int
Website: <http://www.idea.int>