autoAnalyzer™ Consultancy Kit and Remote Management using autoAnalyzer and autoVoIP Probes

Getting Started Guide
INTRODUCTION

- Installation
- Loading
- Toolbox packaging
- Remote Management
- Access Information
- Check lists

APPENDICES

- APPENDIX 1 – GETTING STARTED CHECK LIST covering :-
  - autoAnalyzer Consultancy Kit/Probes
  - Remote Management
- APPENDIX 2 – DEPLOYMENT
- APPENDIX 3 – SYSTEM REQUIREMENTS
- APPENDIX 4 – USEFUL REFERENCE MATERIAL AND HELP LINKS

This document covers issues that are relevant to the successful operation of the autoAnalyzer tool. It also addresses remote management.

autoAnalyzer™ Consultancy Kit

Remote Management using autoAnalyzer and autoVoIP Probes
Installation

Use the following URL to obtain for detailed installation/upgrade instructions and other relevant information.


Loading

Use Start Menu – select programs : Codima, Codima Toolbox

![Codima Toolbox](image)

Toolbox packaging

**autoAnalyzer Consultancy Kit** – The getting started guidance for the autoAnalyzer component of this tool is the same as it would be for a autoAnalyzer Probe. The autoMap component is covered in a separate guide.

Remote Management

This document also covers issues that are relevant to the successful operation of the Remote Management System which makes use of the following Probe types

- autoVoIP Probe
- autoAnalyzer Probe
- Combination of autoAnalyzer and autoVoIP Probes

The remote operation process is the same for all Probe types, any functions that are specific to one type of Probe are highlighted. A separate *Getting Started Guide* is provided for the autoVoIP tool focusing on the specialist autoVoIP requirements and operations. This document covers issues associated with remote management.

The Remote Management facility is included in the autoAnalyzer Consultancy Kit and can be provided as an add on to other tools in the Codima Toolbox.
Expand the autoAnalyzer Branch of the Pane 1 Tree view

- Local Segment
  - Historical Analysis
  - Traffic
  - Map of Segment
  - Capture Frames
  - Review Frames
  - Expert System

The entries in section 4 of APPENDIX 1 provide information on how to access individual autoAnalyzer modules and how to obtain help information.

You can also access modules by using the Toolbar icons at the top of the display, to access the full range you should right click in the empty area at the end of the toolbar list, and select Show All Toolbars from the menu provided.

Display showing default Icon range and menu used to Show All Toolbars

Display showing all Toolbar icons – the grey icons become active when you select the module they apply to

Check list

The following Appendices provide a check list to ensure you have all the necessary components and other information needed to use the autoAnalyzer Consultancy Kit or Probes.
APPENDICES

APPENDIX 1 – GETTING STARTED CHECK LIST covering :-

autoAnalyzer Consultancy Kit/Probes

1. License Files
2. Network Connection
3. Platform IP address
4. End Results – autoAnalyzer Probe and autoAnalyzer component of autoAnalyzer Consultancy Kit:
   - Viewing network/node statistics and monitoring frames
   - Viewing and setting alarm thresholds

5. End Results – autoVoIP Probe: Viewing autoVoIP Reports and accessing other autoVoIP functions

Remote Management:

1. License Files
2. Network Connection
3. Platform IP address
4. Configuration
5. End Results:
   - Probe connected.
   - Check list should you have problems connecting with Probe

APPENDIX 2 – DEPLOYMENT covering :-

1. Connecting AutoAnalyzer Consultancy Kit/Probe to Network
2. Connecting Remote Manager to Network
3. Remote Manager and Probe deployment

APPENDIX 3 – SYSTEM REQUIREMENTS

APPENDIX 4 – USEFUL REFERENCE MATERIAL AND HELP LINKS
Ensure you have the correct license file to operate this tool.

The autoAnalyzer Consultancy Kit/Probes require:

- A Toolbox license (license.txt)

A Trial license file is provided when you download a trial version of the tool from the Codima Web site.

For non trial systems – A Machine locked license file is emailed with installation instructions.

The Toolbox License defines the user Interface, i.e., configures it as a autoAnalyzer Consultancy Kit

Ensure license file is copied to the correct folder.

- Copy Toolbox license file (License.txt) into the "C:\Program Files\CODIMA\Express\neonet\bin\license" folder

Active analysis is needed to run:

- SNMP operations
- Remote operations
- Name discovery
- Ping functions

For detailed information on deployment, see APPENDIX 2

Does the autoAnalyzer Consultancy Kit/Probe platform have a suitable IP Address for the network it is connected too.

Is the autoAnalyzer Consultancy Kit /Probe configured with the correct IP address?, for example if using a autoAnalyzer Consultancy Kit/Probe on a network with DHCP, you may find that the IP address configured on the system is no longer the one allocated to the Network Adapter Card. In such cases undertake the following actions:

1. Close the Codima Toolbox
2. Delete the file Network Interface Settings from the root directory – C:\Program Files\CODIMA\Express
3. Restart the Codima Toolbox, you will immediately have access to the Product Selector - Choose Network Interface dialog box
4. Select the Probe product tab - select the required range of adapters

For detailed information on deployment, see APPENDIX 2
4. End Results

autoAnalyzer Probe (local access) or autoAnalyzer component of the autoAnalyzer Consultancy Kit
- viewing network/node statistics and monitoring frames

Map Module

Following loading the autoAnalyzer Probe/autoAnalyzer Consultancy Kit automatically starts building a real time map of the segment being monitored. The map provides facilities to view:

- **Historical traffic trends for the nodes**: drill down to shows Patterns
- **Alarm Reports**
- **Transmitted Frames**: Node – Filter, this option automatically sets up a frame filter for the selected nodes address and allows the user to activate frame capture.
- **SNMP browse facility** and more

- **Map Module**:
  - Click on Map Icon - select Node and right click
  
  Example showing Map Module interface

  Example showing Right Click Menu

  Example showing SNMP Browse Window

Help Access - <F1> from this screen will provide a screen description and a direct link to instructions covering how to operate the Map module.
This map does NOT use the discovery engine associated with the autoMap tool, its discovery is based on passive analysis of the monitored frames.

**History Module**

The autoAnalyzer also starts gathering a wide range of statistical information for the segment and monitored devices. This information can be viewed by accessing a range of History Charts.

- **History Module**: Click on History Icon
- Use cycle icons to select charts.

**Example showing History Module interface**

- **Menu bars**: Icons
- **Panels 1**: Tree View, Control
- **Panels 2**: History Module selected
- **Panels 3**: Statistics Tab

**Help Access**: <F1> from this screen will provide a screen description and a direct link to instructions covering how to operate the History module.

**The Pane 3 bottom window will only be displayed if you select it:**
The statistical information can be also be viewed in a tabular format by accessing a range of Traffic Profiles.

**Traffic Module**

- Click on Traffic Icon
- Use cycle icons to select profiles

**Example showing Traffic Module interface:**

Help Access - <F1> from this screen will provide a screen description and a direct link to instructions covering how to operate the Traffic module.

The Pane 3 bottom window will only be displayed if you select it.

Note: The system defaults to load a small subset of Toolbar Icons, you can then switch on individual Icon ranges or change the display to show all the available Icons, including the cycle icons mentioned above, see Help entries titled “How to display all the available Toolbar Icons.”
The History Charts and Traffic Views will automatically provide suitable templates for the quick generation of HTML, CSV, TSV reports.
Alarm logs are also automatically populated with reports to:-

- Provide an early warning system
- Log network changes, for example:-
  - New MAC Address monitored
  - New Unit type identified
  - IP address identified
  - Node Names discovered
- Log events associated with network security.
- Log important network and node events such as statistical threshold breaches and automatically send out notifications via email and as SNMP traps.

**Alarm Module**: Click on Alarm Icon - click on Alarm Tab counters to access logs and acknowledge alarm reports

*Example showing Alarm Module interface:*

*Help Access - <F1> from this screen will provide a screen description and a direct link to instructions covering how to operate the Alarm module*

*The Pane 3 bottom window will only be displayed if you select it:*

<table>
<thead>
<tr>
<th>Tools</th>
<th>Pane 3 Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Bar</td>
<td>Pane 3 Bottom Window</td>
</tr>
<tr>
<td>Options</td>
<td>Standard</td>
</tr>
</tbody>
</table>
To view and change the default Alarm Threshold settings for the autoAnalyzer tool access the **Browse Alarm Thresholds** view. This will show the default range of settings provided and will include any new threshold settings you add.

For additional information, see Help entries titled:-

- **How to view Alarm Threshold Settings**
- **How to set Alarm Thresholds**
Frames capture can also be immediately started.

**Capture Module**: Click on Capture Icon - click on icons to start and stop capture

*Example showing Capture Module interface:*

![Capture Module interface](image)

*Help Access* - <F1> from this screen will provide a screen description and a direct link to instructions covering how to operate the Capture module

*The Pane 3 bottom window will only be displayed if you select it:*

![Pane 3 bottom window](image)

**Review Frames Module**

The Capture frames can then be saved to the Review Frame Library and replayed at a later time.

**Review Module**: Click on Save icon to add files to Library

Click on Review Module icon to access Review Module interface, then the Open icon to access the Library of saved frame files, stored in:-
The autoFilters Facility can be accessed post and pre-capture.

**autoFilters**: Click on Post and Pre Capture Filter Icons

*Example showing interface used to set up and control and monitor filter*

Help Access - <F1> from this screen will provide a screen description and a direct link to instructions covering how to operate the Filter module.

---

**Expert System**

The captured frames can also be run through the Expert system. The facility will help you identify anomalies on your network.

**Expert Module**: Click on Expert Icon

Help Access - <F1> from the Expert Log will provide a screen description and a direct link to instructions covering how to operate the Expert system facilities.
Following loading the autoVoIP Probe starts to populate the history databases. The autoVoIP Reports can then be opened, to enable the user to monitor and troubleshoot the VoIP network.

- **autoVoIP**
  - Double Click on Report name in relevant autoVoIP branch of Pane 1 Tree view to open:

  **Examples showing Traffic Police and Troubleshooting Reports**
  
  **Drill down functions**
  
  **Help Access** - <F1> from these screens will provide a screen description and a direct link to instructions covering how to operate that component of the autoVoIP tool.

For detailed information, see autoVoIP Getting Started Guide
Remote Management

1. License Files

The Remote Management facility is included in the autoAnalyzer Consultancy Kit and can be provided as an add on to other tools in the Codima Toolbox. So the only license requirement that is specifically for the Remote Management is to have a Toolbox License that allows access to the Remote manager interface.

2. Network Connection

Ensure that the Host PC for the Remote Manager is connected to Network, and is correctly positioned and configured to undertake both active and passive analysis.

For detailed information on deployment, see APPENDIX 2

3. Platform IP Address

Does the Remote Manager Host PC have a suitable IP Address for the network it is connected too?

Is the Remote Manager Host PC configured with the correct IP address?: For example if using it on a network with DHCP, you may find that the IP address configured on the system is no longer the one allocated to the Network Adapter Card. In such cases undertake the following actions:-

1. Close the Codima Toolbox
2. Delete the file Network Interface Settings from the root directory – C:\Program Files\CODIMA\Express
3. Restart the Remote Codima Toolbox - you will immediately have access to the Product Selector - Choose Network Interface dialog box
4. Select the relevant product tab - select the required range of adapters
4. Configuration

The Remote Manager will require to be configured with information on the Probes it is going to be managing, each probe will extend the managers domain to cover a new network segment.

**Configuration**: Click on the Add New Segment icon.

*Note: This icon is only available if you have a Remote Management Add on.*

Add Segment/Probe name, Probes IP address, Probes password and color selection.

**Segment details dialog box**

This will add the new segment/probe name to the Pane 1 Tree view, e.g.,

and immediately activate a connection with the Probe

*Help Access - <F1> from this screen will provide guidance on adding a new Segment to the Remote Manager*
The Pane 1 Tree view will show a + entry next to the probe name following a successful connection:

![Image of Pane 1 Tree view showing a + entry]

To view what is happening during the connection phase you should open the Remote Log.

**View information from Probe**:

- **To view a Probe**: Double Click on Probe Name
- **Use same access methods as you would to drive the Toolbox locally.**

**Example showing Map Module interface for selected Probe**

![Image of Map Module interface for selected Probe]

See Help entries titled:
- How to view information held on a Probe
- Remote Operations
1. Ensure that the Remote Manager has the address of a Router to use when it has to issue frames to another network. This should be picked up automatically.

   - see Help entry titled *How to set Router Address* if the address is not set automatically.

2. Ensure that any firewalls between the Remote Manager and Probe have been configured to allow the Remote Protocol through - see Help entry titled *About Remote Protocol – CRTP*

   **To initiate a connection with a Probe:**
   Right Click on Probe Name – select to *Initiate a connection*.

   **Pane 1 Tree view display during the connection:**
   - No Connection made with remote link - 🍀
   - Connection set up attempt being made - 🤝 (Connection Set Up Phase)
   - Connection set up attempt being made - 🤝 (Data Transfer Phase)
   - Connection established - ⚽️

   See Help entry titled :: *How to connect with a Probe*

**Troubleshooting**

See Help entries
- *Remote Connection Check List*
- *How to troubleshoot Remote connection attempt*
The software uses standard Network Adapters (NIC)s. This section covers connecting the Network Adapters (NICs) used by the autoAnalyzer Consultancy Kit/Probe to the network.

Active operation is required by the autoAnalyzer Consultancy Kit/Probes for remote operations.

Other issues associated with connection are:

1. Whether or not the connection is running as Full Duplex.
2. Whether or not you are connecting to a Switched Network.
3. Whether or not you are running Dual Port Analysis.

**Diagram 1 - covering connections for half and full duplex monitoring**

**Half Duplex**

- **Option 1 – connecting to Switch**
  - Port 1: Connect to Mirror Port
  - Comms Port: Connect to a Free Switch Port

Note: In this configuration – Port 1 and Comms Port must be separate Network Adapters

- **Option 2 – connecting to Hub**
  - Port 1: Connect to a Free Port on the Hub

Note: In this configuration – Port 1 can also be assigned as the Comms Port

**Full Duplex**

- Port 1
- Port 2
- Tap
- Connect to a Free Switch Port

**KEY**
- Full Duplex link
- 1G/100G/1000Mbps link
2. Connecting Remote Manager to Network

The Remote Management facility is included in the autoAnalyzer Consultancy Kit and provided as a Remote Management Add for other tools in the Codima Toolbox.

The Connection requirements for the Remote Manager are therefore the same as for the autoAnalyzer Consultancy Kit (see Diagrams 1 and 2 above)
3. Remote Manager and Probe deployment

The following diagram provides an overview of the typical Remote Manager and Probe deployment.

Deployment point examples:

1. Attach Manager to a free port on Switch
2. Attach Probes to Span Port on Switches and to free Switch Port - scope subject to port configuration
3. Attach Probes to Half/Full Duplex connection, monitor using TAP and to a free Switch Port

Note: The Probes need a connection to a free switch port to run active functions, which include communication with Manager.

Cables: Use an RJ45/Cat 5 drop cable.
Here are the operating requirements for the PC platform to be used with the autoAnalyzer Consultancy Kit, Probes and Remote Manager.

### IMPORTANT INFORMATION

The information below applies to the minimum specification, Codima strongly recommend when using these tools on medium/large networks that you use the best platform available, for example use PCs with 2Gb of memory, avoid PCs with Celeron chips or slow memory bus speeds. A Pentium Extreme single core CPU would be suitable (dual core processors are not required for this tool).

### DESCRIPTION

<table>
<thead>
<tr>
<th>PC Platform</th>
<th>2 GHz or faster.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory</strong></td>
<td></td>
</tr>
<tr>
<td>512Mb minimum for autoAnalyzer Consultancy Kit/Probe and Remote Manager</td>
<td></td>
</tr>
<tr>
<td>1Gb minimum for autoVoIP Probe</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The memory recommendations apply to the use of the Codima Toolbox applications, if you are running other memory intensive applications on the PC you will need more memory.

<table>
<thead>
<tr>
<th>Graphics Card</th>
<th>Minimum 16Mb</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating System</strong></td>
<td>Microsoft® XP® Microsoft® Windows® 2003 Server Microsoft® Vista</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software Versions</th>
<th>Microsoft® Internet Explorer Version 6 or above.</th>
</tr>
</thead>
</table>

| Disk space | Database Files: Subject to size allocated to Database Files, e.g., 10Mb files = 150Mb |
|           | Other Files : 200 Mb |
|           | Windows Swap File : 200 Mb. |
|           | Free disk space for creation of new user files : 300Mb |

Recommended 30 Gb for a live system.

<table>
<thead>
<tr>
<th>Monitor Resolution</th>
<th>1024 x 768 (minimum) for autoAnalyzer Consultancy Kit/Probes and Remote Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1280X1024 recommended if using Remote Manager with autoVoIP Probe.</td>
</tr>
</tbody>
</table>

| CD Rom Drive | A CD Rom Drive will be required to install the Codima Toolbox Software, if you do not download it. |

---

APPENDIX 3 – SYSTEM REQUIREMENTS
APPENDIX 4 – USEFUL REFERENCE MATERIAL AND HELP LINKS

Reference Material

Access the Codima Web site Support page:-

http://www.codimatech.com/support.php

This will provide access to the Customer Support section, where a comprehensive FAQ document is available covering a wide range of questions on the Codima Toolbox.

Help facility

Pressing <F1> will provide access to the Codima Help facility.

The following help entries will assist you in using the autoAnalyzer Consultancy Kit, Probes and Remote Management Add on.

<table>
<thead>
<tr>
<th>Help Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Codima Toolbox</td>
<td>Provides a detailed overview of the tools in the Codima Toolbox.</td>
</tr>
<tr>
<td>How to use Codima Toolbox</td>
<td>Provides a link to the Help entries that cover all the Codima Toolbox operations</td>
</tr>
<tr>
<td>Readme</td>
<td>List of useful help entries</td>
</tr>
<tr>
<td>How to troubleshoot tools in the Codima Toolbox</td>
<td>Help entry covering troubleshooting the operation of the tools in the Codima Toolbox.</td>
</tr>
<tr>
<td>About Remote Facilities</td>
<td>Help entry describing the remote facilities</td>
</tr>
</tbody>
</table>