Oracle® Communications Performance Intelligence Center

Sigtran Surveillance Guide

Release 10.2

E66875 **Revision 1**

February 2016

ORACLE®

Oracle Communications Performance Intelligence Center Sigtran Surveillance Guide, Release 10.2

CAUTION: Use only the guide downloaded from Oracle Help Center (OHC) (http://www.oracle.com/technetwork/indexes/documentation/oracle-comms-tekelec-2136003.html).
Refer to Appendix section for instructions on accessing My Oracle Support.

Table of Contents

List of Figures

List of Tables

Chapter 1: About this Help Text

Scope and Audience

This guide is designed to assist users assigned the roles of nspUser, nspPowerUser and nspManager in working with Sigtran Surveillance. This application is designed to enable the user to view the operational state, (status and state), of a monitored network using SigTran regardless of whether any monitored element (association, linkset, link, cards and application server) is in an alarm state or not.

Note: In order to get the most from this user guide, the user should have a good working knowledge of SS7, SigTran and other telecom-related protocols. For more information on Eagle SigTran, refer to the Tekelec Eagle 5 SigTran User Guide.

General Information

You can find general information about OCPIC, such as product overview, list of other guides, workstation requirements, login and logout procedures, user preference settings, in the Quick Start Guide. This document is available from the Portal menu or can be downloaded from Oracle Help Center (OHC).

Chapter 2: Getting Started With Sigtran Surveillance

Introduction to Sigtran Surveillance

Sigtran Surveillance is an application developed to gather and display information pertaining to SS7 links and associations when the underlying transport mechanism is SigTran. Functioning as a near real-time application, Sigtran Surveillance indicates state and status of links, linksets, associations, cards and application server(s) that make up a network. The Sigtran Surveillance application is integrated into the Management Application Platform and functions on a network view context. Sigtran Surveillance provides the capability to view overall status of elements, as well as to drill down to individual links and associations.

When Integrated Acquisition based, only traffic from IPSG and IPGW cards is supported and the SigTran mechanism must be used to send data to the Integrated Acquisition.

Logging into Sigtran Surveillance

Complete these steps to open the Sigtran Surveillance application.

Note: Reference Data is an application that runs on Management Application, it must be opened from the Management Application portal.

1. Using a Web browser, type in the IP address of the Management Application Server.

Note: 1.Management Application only supports versions of IE 11.0 or later and Firefox 3.6 or later. Before using Management Application, turn off the browser pop up blocker for the Management Application site.

2. Contact your system administrator to obtain the IP address for the Management Application Server.

3. Reference Data runs on a Web interface and uses an IP address to access the Management Application platform. The URL can be saved in the Favorites list on your browser.

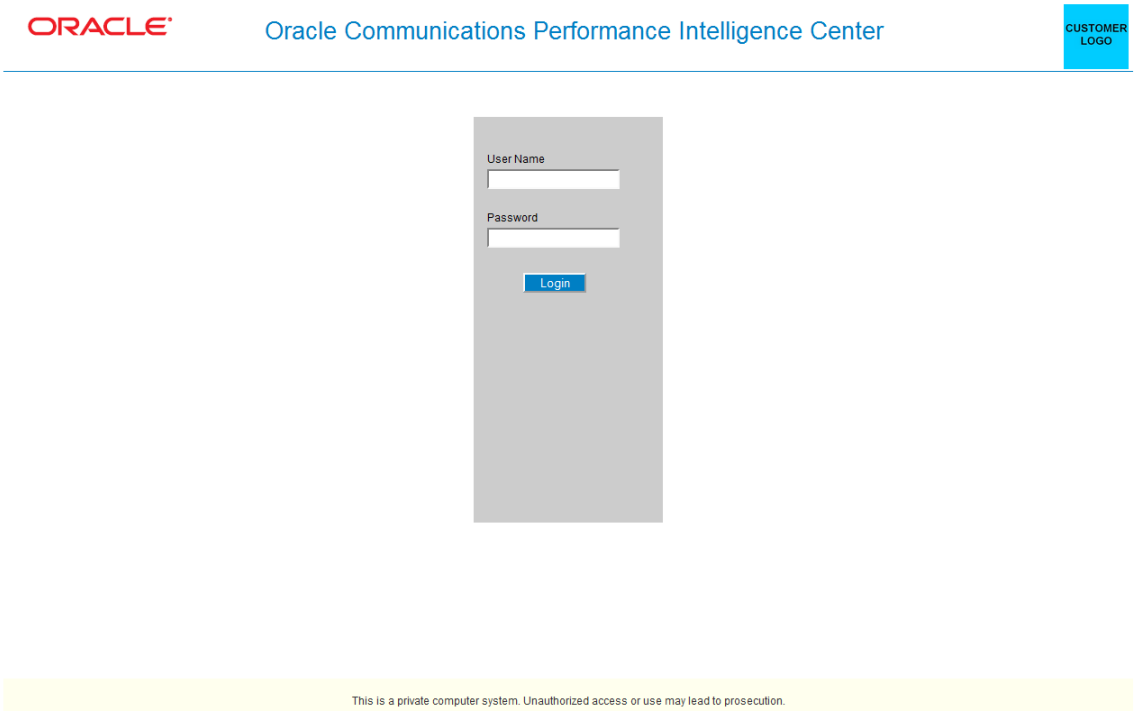

Figure 1: Login Screen

2. Log into Management Application by typing:
- Your Userid
- Your Password

Note: Check with your system administrator for your userid and password.

3. Click the **Sigtran Surveillance** icon in the application section of the portal to open the Sigtran Surveillance main page.

Sigtran Surveillance Main Screen

The Sigtran Surveillance application monitors the state and status of the Eagle elements (application servers, application server processes, associations, linksets, links and cards), that reside on Integrated Acquisition. It also can monitor the state and status of Probed Acquisition elements when Probed Acquisition is using SigTran.

Note: For proper monitoring and viewing, the correct version and configuration of Adobe Flash Player Plug-in and Internet Explorer must be loaded on the system. (The system must have IE 7 and Flash Player 10 or later.) Please check with your Authorized representative.

Note: Network Elements associated with Integrated Acquisition must be synchronized through the Centralized Configuration. For more information about Centralized Configuration, see the Centralized Configuration Guide or contact your system administrator.

Note: Unconfigured elements, (not configured in Centralized Configuration), associated with Probed Acquisition are also displayed in Sigtran Surveillance in black (see *Status / State Color Interpretations* for more information).

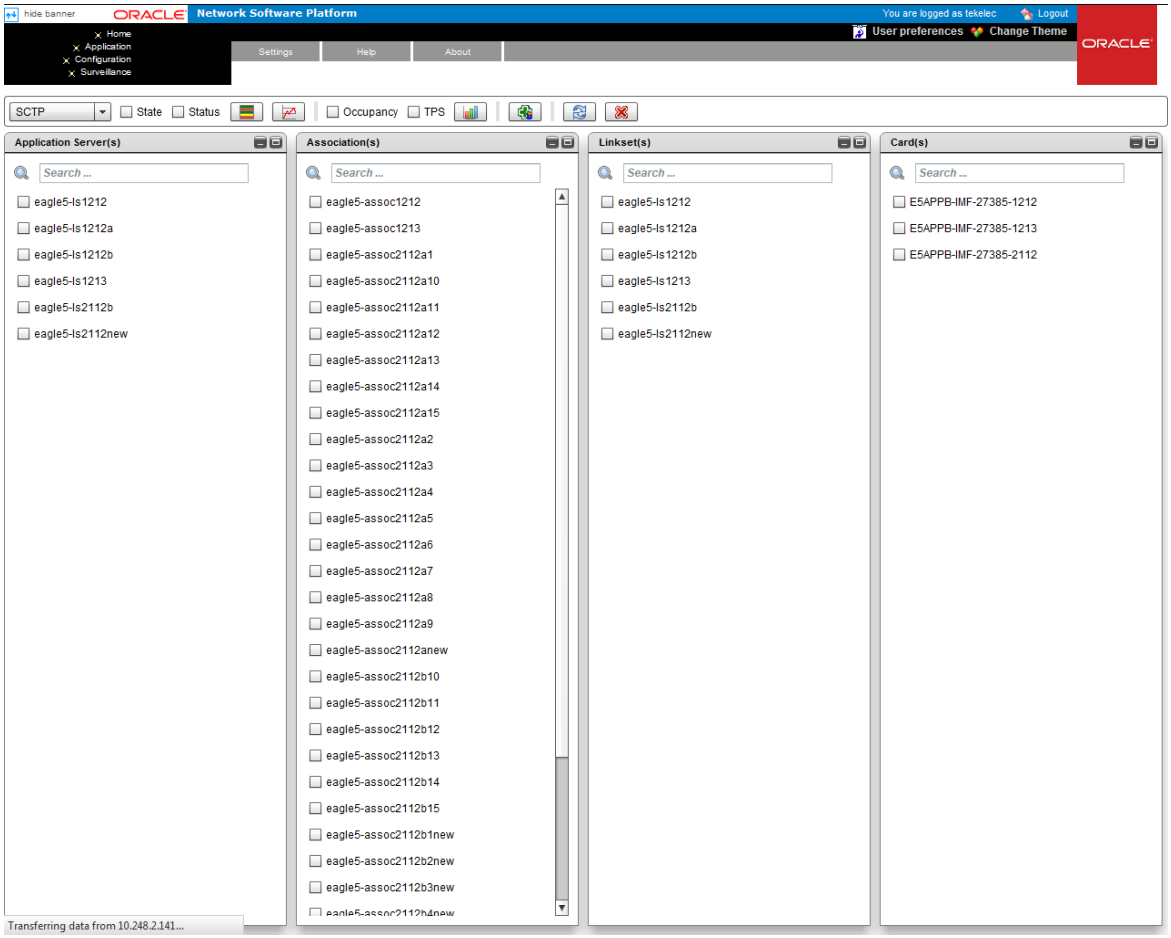

Figure 2: Sigtran Surveillance Main Screen

The Sigtran Surveillance main screen has the following sections.

- Menu - this section has the following menus.
  - Settings - has the Monitoring Settings option, (see *Sigtran Surveillance Monitoring Settings*).
  - Help - opens online help system
  - About - shows the version of Sigtran Surveillance that is opened.
  - Tool bar - provides function buttons for working with Sigtran Surveillance. (See *Sigtran Surveillance Toolbar*.)
  - Workspace - divided into columns that represent the elements monitored in Sigtran Surveillance. (See *Workspace*)

Note: All screens are configurable and allow for different table layouts (column layout button). Tables can be minimized or maximized so that the desired table can always be viewed. Record columns can to be re-arranged (by drag and drop) and sort order (ascending or descending) is changed by clicking on the column heading.

Note: Do not use the Function Keys (F1 through F12) when using the Management Application. Function keys work in unexpected ways. For example, the F1 key will not open Management Application help but will open help for the browser in use. The F5 key will not refresh a specific screen, but will refresh the entire session and will result in a loss of any entered information.

Sigtran Surveillance Toolbar

The Sigtran Surveillance tool bar.

Figure 3: Sigtran Surveillance Toolbar

The toolbar is divided into different functional groups: monitoring protocol state and status, monitoring occupancy and transactions per second as well as monitoring TOP "N" associations, saving and loading favorites, application utilities such as refreshing and resetting counts.

Monitoring Protocol State and Status

Protocol selection - a drop-down menu that shows the available protocols to monitor

- State - a check box, when selected, monitors the state of the elements selected
- Status - a check box, when selected, monitors the status of the elements selected
- Status/State Tabular Monitoring - launches a new window and displays the monitored element(s) in tabular format

Note: Both State and Status can be opened together

- Status/State Graphical Monitoring - launches a new window that displays monitored elements in graph format

Monitoring Occupancy, Transactions per Second and TOP "N"

- Occupancy - a check box, when selected, monitors the list of the associations sorted by occupancy when the TOP 'N' Monitoring function is activated
- TPS (Transactions Per Second) - a check box, when selected, monitors the list of the associations sorted by TPS when the TOP 'N' Monitoring function is activated
- Launch TOP 'N' Monitoring - function button that launches the TOP 'N' Monitoring window that shows a panel for TPS and/or Occupancy (the associations are ordered by TPS or Occupancy), the range for the number of associations is 0-100 and set in the Monitoring Settings option

Note: Both TPS and Occupancy can be opened together

Note: The associations that are listed are dependent upon user role/privilege

Application Utilities

- Save and Load Favorite - saves and loads selected element as a "favorite" stored in the system
- Refresh - reloads all lists again and clears all old lists, for example, if changes have been made in Centralized Configuration, click refresh and all lists are reloaded with changes without having to restart the application
- Reset Selected Counts - resets all cumulative state monitoring counts (only functional to users with role nspManager)

Workspace

The Sigtran Surveillance application workspace is divided into columns that show the elements and sub-elements that belong to a protocol. Each column is inter-dependent so that by selecting one element, all the other elements related to the selected element are highlighted.

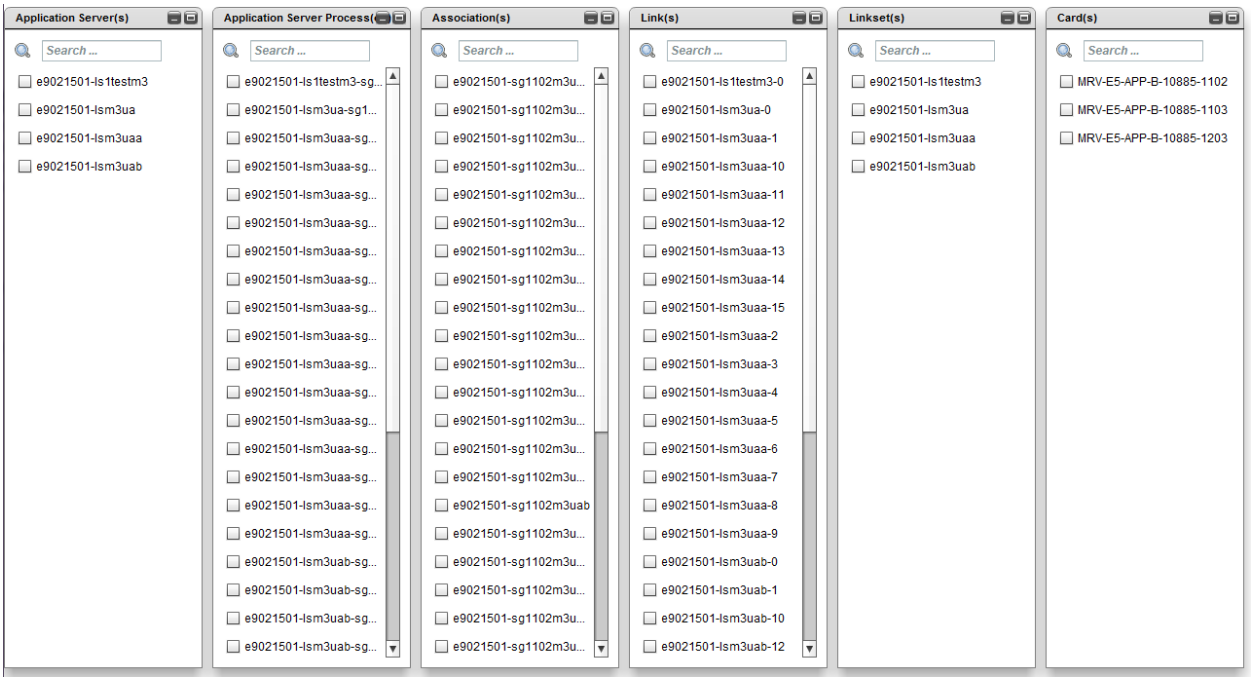

Figure 4: Sigtran Surveillance Workspace - Server Element Selected

The number of columns shown on the screen is dependent on the configured elements of the selected protocol. For example, if no links are configured for the system, the link column will not appear on the screen.

The Work area table is divided into columns (columns are dependent upon the elements configured for the particular protocol). A fully configured system can have up to six columns if using all possible protocols. The possible columns are:

- Application Server(s) - provides a check box for selecting specific server(s) to monitor.
- Application Server Processes (ASPs) - provides a check box for selecting specific ASPs to monitor.
- Association(s) - provides a check box for selecting specific association(s) to monitor.
- Link(s) - provides a check box for selecting specific link(s) to monitor.
- Linkset(s) - provides a check box for selecting specific linkset(s) to monitor.
- Card(s) - provides a check box for selecting specific card(s) to monitor.

The screen also has "drag and drop" capability. Clicking on a column and dragging it to another position on the screen automatically re-organizes the screen to show the new configuration.

Sigtran Surveillance Monitoring Settings

Sigtran Surveillance has a Monitoring Settings menu option that enables the user to customize the following settings:

- Hierarchy Root Switch - enables the user to select the root element of the displayed hierarchies.

Note: The default hierarchy is either Linkset or Application Server (AS). The other available option for hierarchy root is Card.

- Top N Count Value - creates an upper limit to the associations displayed in the TOP N monitoring screen.

Note: Range is 0 to 100 with default value 10.

Note: The associations are listed in order of activity. The most active association first to the least active.

- Top N Association Exclusion - enables you to exclude specific associations from being displayed in the TOP N monitoring screen.

Note: Only configured associations are excluded. Unconfigured associations while visible cannot be managed in any form until they are configured in Centralized Configuration.

Each screen has the following button options:

- Reset - resets all screens to default value
- Reset Tab - resets the default values for the particular tab
- Apply - applies the changes to the system
- Cancel - cancels any actions and exits the screen

Hierarchy Root Switch tab

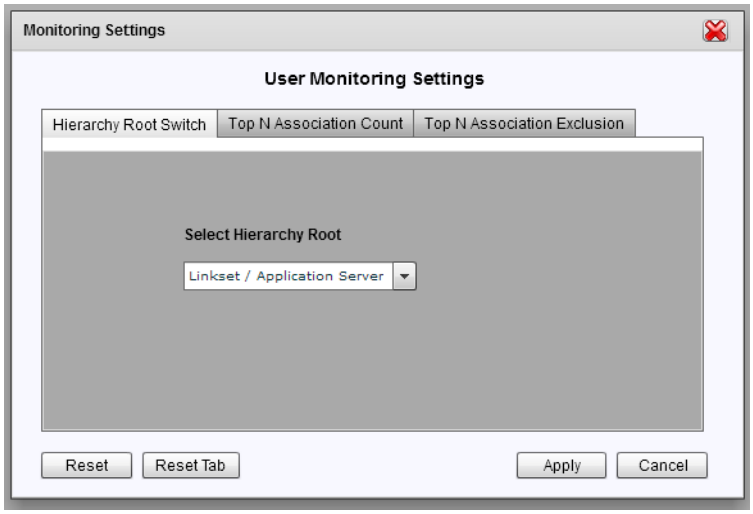

Figure 5: Hierarchy Root Switch Tab

Select the **Hierarchy Root Switch** tab to set the default hierarchy root element, (Linkset/AS or Card), used by Sigtran Surveillance.

Field	Description
Select Hierarchy Root	Drop-down list that allows the selection and configuration of a default root element in the selected hierarchy. **Note:** The default hierarchy is either Linkset or Application Server (AS). The other available option for hierarchy root is Card.

Table 1: Hierarchy Root Switch Tab Screen

Top N Association Count Tab

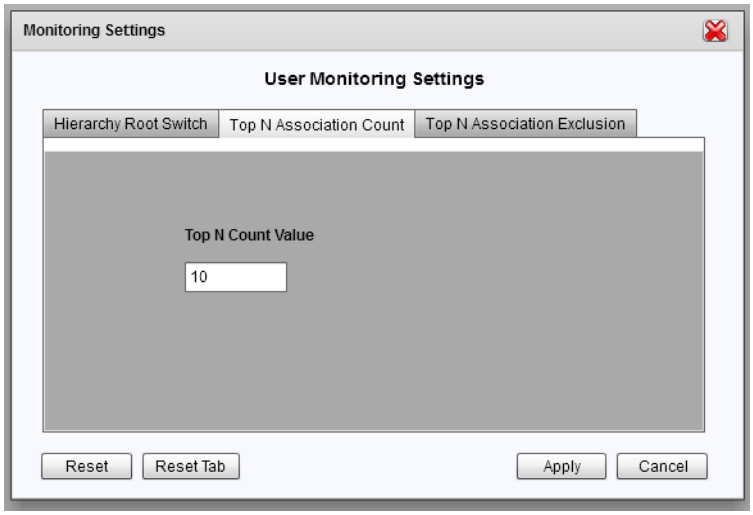

Figure 6: TOP N Association Count Tab

Select the **Top N Association Count** tab to set the number of associations to be viewed.

Field	Description
Top N Count Value	A numeric field that shows the top limit of the associations displayed in the TOP N monitoring screen. **Note:** The minimum value is 0, the maximum value is 100, default is 10.

Table 2 : Top N Count Tab

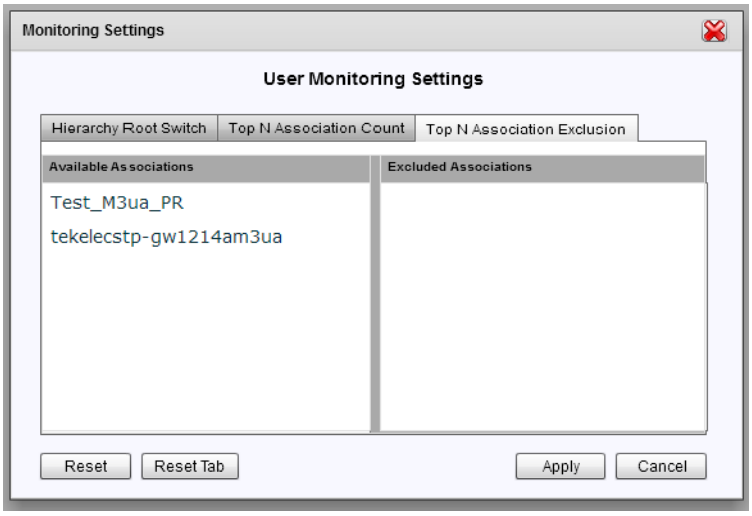

Figure 7: Top N Association Exclusion Tab

Select the **Top N Association Exclusion** tab to select specific associations that will not be displayed.

Field	Description
Available Associations	Selection list of available associations displayed in the TOP N screen.
Excluded Associations	This shows the specific associations that are excluded from display in the TOP N screen. **Note:** Only configured associations are excluded. Unconfigured associations, while visible on the state/status screen, cannot be managed in any form until they are configured in Centralized Configuration.

Table 3: Association Exclusion Tab Filed Description

- To select associations to be excluded from the display, drag each association from the Available Associations column to the Excluded Associations column.
- Click Apply. The associations are excluded.
- To re-instate an association(s), drag the associations from the Excluded Associations column to the Available Associations column.
- Click Apply. The changes are saved to the system.

Chapter 3: Working in Sigtran Surveillance

Overview of Sigtran Surveillance Functionality

Sigtran Surveillance supports SigTran by Integrated Acquisition integrated with both Eagle IPGW as well as IPSG cards.

In addition, since Probed Acquisition connects directly to an IP network carrying the SigTran traffic, reference data must be supplied by the customer in order for Sigtran Surveillance to accurately monitor Probed Acquisition carrying SigTran traffic. This reference data is used to "instruct" the OCPIC system on relationships between linksets, links, associations and application servers. The reference data required also specifies the capacity and threshold for the defined element.

Sigtran Surveillance performs the following functions:

- Allow monitoring of multiple cards, Probed Acquisition s, linksets, links, associations, application servers and application processes
- Allows searching for specific elements utilizing a search field
- Saving Favorite List
- Monitor status and state of an element(s)
- Show missing Probed Acquisition reference data for an element
- Monitor element(s) in either table or graph format
- Monitor TOP N Associations by TPS or Occupancy
- Reset capability for state counts to zero
- Choose a specific color scheme using the themes option

Card Functional Specifications

Sigtran Surveillance supports SigTran by Integrated Acquisition integrated with both Eagle IPGW as well as IPSG cards. This table shows the functional expectations on a per card basis.

Application	Hardware	GPL	Protocols	ANSI/ITU	Monitoring Type
SS7IPGW	SSEDCM	SS7IPGW	M3UA	ANSI	STC-STYLE
SS7IPGW	E5-ENET	IPGHC	SUA / M3UA	ANSI	STC-STYLE or SigTran
IPGWI	SSEDCM	IPGWI	M3UA	ITU	STC-STYLE
IPGWI	E5-ENET	IPGHC	SUA / M3UA	ITU	STC-STYLE or SigTran
IPSG	E5-ENET	IPSG	M2PA / M3UA	ANSI+ITU	STC-STYLE or SigTran

Table 4: Functional Expectations per Card Basis

Network Elements in Sigtran Surveillance

Network elements refer to customer network elements monitored by the OCPIC system such as:

- Application Servers
- Application Server Processes
- Associations
- Linksets
- Links
- Cards (IPSG, IPGW for Integrated Acquisition and third-party cards for Probed Acquisition)

Selecting Elements in Sigtran Surveillance

All elements belonging to a protocol are viewed from the workspace section on the main screen. In addition, when one or more elements are selected, any other element/sub-element related to the selected element(s) is highlighted. This feature allows for more refined and quicker searches and selections.

Complete these steps to select elements to be monitored.

1. Select parent **protocol** from the drop-down list.

Note: If you have selected an element(s) and change protocols, a prompt appears stating, "If you choose to change the protocol, all your selections will be lost. Do you wish to continue?" Click **yes** if you want to continue in changing protocols.

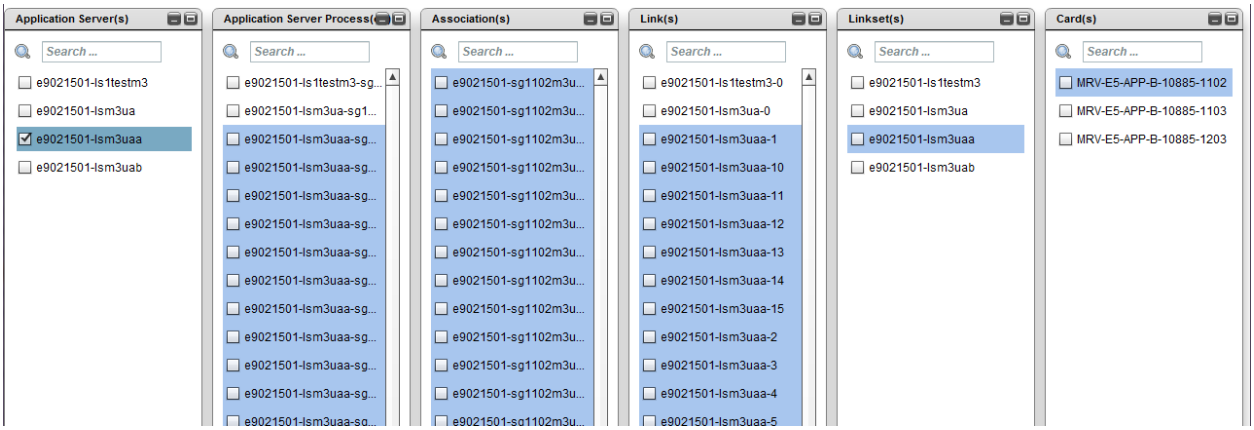

Figure 8: Selected Element and Related Sub-elements

2. Select one or more **element(s)** using the selection boxes next to the element.
3. Select either **State** or **Status** from the tool bar.
4. Click, (depending on what format is needed), either the **State/Status Tabular Monitoring** or **State/Status Graphical Monitoring** button on the tool bar.
   The monitoring screen opens showing the elements being monitored in hierarchical format.

Searching for Elements

In large systems, one or more elements can be found by using the search operation. The search field is located at the top of each column. To search for an element(s) complete these steps.

1. Select parent protocol from the drop-down list.
2. Enter the element name in the search field. This activates the search function. Using wild card in searches

To use the wild card operation, type in the name of the element followed by "*" symbol. Those elements that meet the search criteria will appear in the appropriate column.

How to Create Favorites

If you work with specific elements (application servers, application server processes, associations, linksets, links or cards) you can save them as Favorites.

Note: Up to 25 Favorites can be saved.

Complete these steps to save specific groups of SigTran Elements as Favorites.

1. Select the **Element(s)** from the work space that is to be saved.
2. Click **Save as favorites** from the tool bar.
3. Enter the **Name** for the favorite in the bottom field.
4. Click **Save.**

   A message appears at the top of the page stating the list was saved. How to Load

Saved Favorites

Complete these steps to open a list of elements saved in the favorites list.

1. Click **Save/Load favorites** from the tool bar.
2. Select a **Favorite** from the list in the top field.
3. Click **Load.**

The work space opens showing the element list with the selections present.

How to Modify Favorites

Complete these steps to modify an existing favorite.

1. Click **Save/Load favorites** from the tool bar.
2. Select a **Favorite** from the list.
3. Click **Load.**
4. Add or delete an **element(s)** from the screen.
5. Click **Save/Load Favorites** from the tool bar.
6. Select the **List** that was modified.
7. Click **Save.**
8. Click OK at the prompt.

   The modified list is saved.

How to Delete Favorites

Complete these steps to delete a saved favorite.

Note: It is possible to delete multiple favorites at one time.

1. Click **Save/Load Favorites** from the tool bar.
2. Select the **favorite** to be deleted.
3. Click **Delete.**
4. Click **OK** at the prompt.

   The favorite is deleted.

Selecting Themes

The Sigtran Surveillance application Change Theme function, allows for different screen color patterns. Complete the following steps to select a theme.

1. In the main screen, click **Change Theme** at the top right-hand corner of the screen.
2. Select one of the six **themes** on the pop-up side bar.
3. Click **Save.**

Status and State Protocol Hierarchy Structures

Each protocol can have up to two hierarchy structures depending if the card is the root or the application server/linkset is the root. Listed here are each of the protocol hierarchies that would appear in either the state or status monitoring screen when an element(s) is selected in the main screen.

Note: Wherever the element of the type defined by a particular level of hierarchy between the related elements of the selected element is not defined in Centralized Configuration, the hierarchy level will be skipped in the current hierarchy. For example, using a hierarchy with the structure of **Card > Linkset > Association.** If the association A1 in the hierarchy has no linkset defined, and has only the related card C1 defined in the hierarchy, then the hierarchy shown in the monitoring screen will just be **Card > Association.**

Hierarchy structure(s) according to protocol

Integrated Acquisition-based protocols

IPSG SCTP (Status and State)

Card > Association

IPSG M2PA (Status and State)

Linkset > Card > Association (Link) Card > Linkset > Association (Link)

Note: Where Association and Link have 1:1 mapping, the Association and Link rows will only be one row since the counts are identical.

IPSG M3UA (Status and State)

Linkset > Association > Link Association > Link

IPGW SCTP (Status and State)

Linkset > Application Server > Association Card > Application Server > Association

IPGW M3UA (Status and State)

Linkset > Application Server > Association > Application Server Process Card > Application Server > Association > Application Server Process

IPGW SUA (Status only)

Linkset > Application Server > Association > Application Server Process Card > Application Server > Association > Application Server Process

Probed Acquisition-based protocols

SCTP (Status and State)

Application Server > Association

Third Party Card > Application Server > Association

M2PA (Status and State)

Linkset > Association (Link)

Third Party Card > Association (Link)

M3UA (Status and State)

Application Server > Association > Application Server Process

Third Party Card > Application Server > Association > Application Server Process

SUA Status

Application Server > Association > Application Server Process

Card > Application Server > Association > Application Server Process

Status and State Protocol Hierarchy Constraints
General guidelines for hierarchies
When viewing hierarchies in tabular format, the following guidelines are used:

- The selected element is always displayed in the table.
- The direct parents, grand parents, etc. (to the root), if they exist, are also displayed in the table.
- The display of children elements is filtered through the parent elements.

Additional guidelines when viewing hierarchies

- If there is no related element for some level of hierarchy, the level is skipped.
- Hierarchies can be mixed together; there can be more than one type of hierarchy shown in a table. In addition, for M3UA protocol one element can be related to multiple hierarchies. For example, a linkset, having links to both IPSG and IPGW cards, will appear in the monitoring table like this:

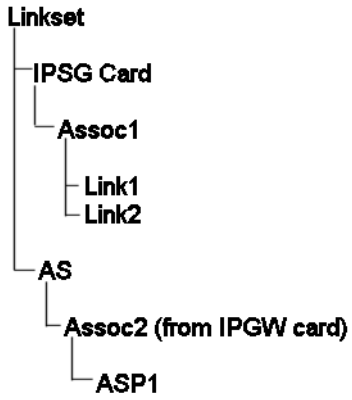

Figure 9: Linkset with IPSG and IPGW Card Links

- Any unconfigured associations for a given protocol are displayed, in italics, as the last elements in the table.

Note: All unconfigured elements are shown as having no children.

There are some exceptions for partially-configured associations on Probed Acquisition and Network management counts on Integrated Acquisition (the display is the same and both are only for M3UA and SUA protocols). They are:

- If traffic exists for an association that is not configured for any ASP belonging to it, then there is a new child shown under the association that shows the counts for the unconfigured traffic - the name of this element is in italics and uses the same name as the association.
- If the association in the hierarchy has no AS or Linkset, the new child is shown in the hierarchy. Conversely, if the association has an Application Server of Linkset in the hierarchy, the new child is shown in the bottom table only (it is filtered out because the unconfigured traffic is not a part of that AS or Linkset) and the association with this child is repeated on the same level as the AS or Linkset and the child is visible alone in the top table. Both association name and the new child name will be in italics. For example, there is Assoc1 on M3UA that has ASP1 and ASP2 with an AS as its parent. In this example, Assoc1 has unconfigured traffic. The hierarchy will appear like this in the tabular monitoring screen:

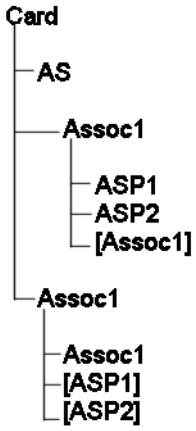

Figure 10: Hierarchy with Unconfigured Traffic

Note: the new child, (Assoc 1), will be visible in the top table and will only appear in the bottom table when the Assoc1 is selected.
Note: Brackets signify that the element is visible only in the bottom table.

Monitoring M2PA and M3UA Guidelines
When monitoring the status or state of an element using these protocols the following network configuration guidelines should be considered:

- For Integrated Acquisition or Probed Acquisition using IPGW, the card can only support one link.
- For Integrated Acquisition or Probed Acquisition using IPSG, the card can support up to 16 links.
- When using the M2PA protocol use a 1:1 ratio of Associations to Links.
- When using the M3UA protocol one association can have multiple links.

Filtered Elements
The filtering function in Sigtran Surveillance filters out elements that are not related to the root of the hierarchy being monitored. These unrelated elements are not visible in the top table of the monitoring screen, but are visible in the bottom table of the tabular monitoring screen when the related element is selected in the top table.
For example, in a hierarchy that has the linkset selected as the root of the hierarchy, the following can occur:
Linkset1 has two associations: A1 and A2 that has the following relationships: A1 is related to the Card 1 A2 is related to the Card 2
Card1 also has A3 and A3 is not related to the Linkset1
In this example the hierarchy: Linkset > Card > Association will be seen in the monitoring table screen.

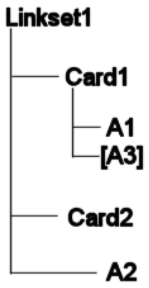

Figure 11: Example 1 of Filtered Elements

Note: Brackets [ ] signify that an element will not be visible in the top table and only visible in the bottom table when the parent is highlighted. In this example, A3, because it is not related to Linkset1, does not show up on the top panel of the table, but will show up in the bottom panel when Card1 is highlighted in the top panel.

Shown in this next example is the SCTP protocol where one linkset has been selected as the root. The filtered monitoring screens show the discrepancies between the top and bottom tables.

Note: Brackets [ ] signify that an element will not be visible in the top table and only visible in the bottom table when the parent is highlighted. In this example, A3, because it is not related to Linkset1, does not show up on the top panel of the table, but will show up in the bottom panel when Card1 is highlighted in the top panel.

Shown in this next example is the SCTP protocol where one linkset has been selected as the root. The filtered monitoring screens show the discrepancies between the top and bottom tables.

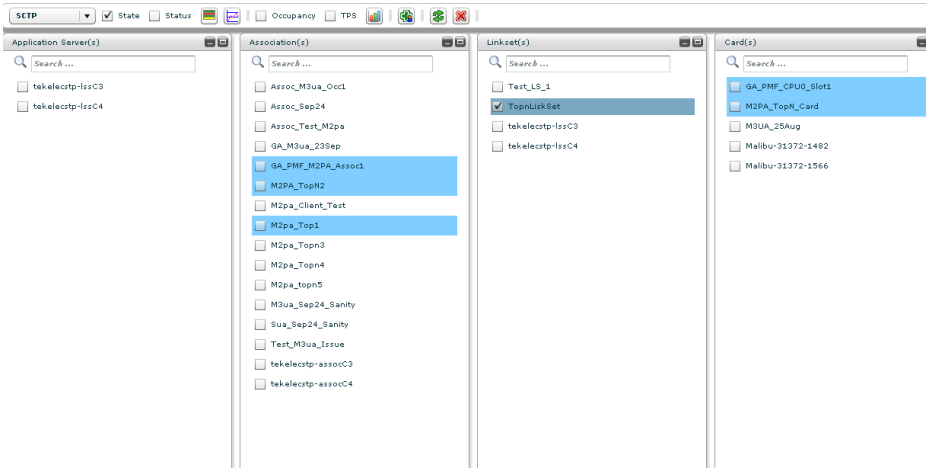

Figure 12: Linkset Selected as Root in Element Selection Screen

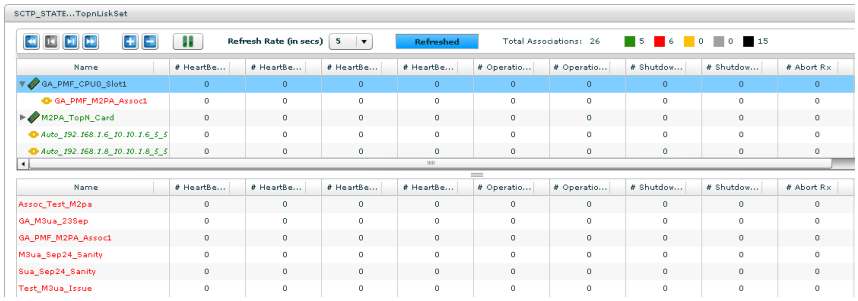

Figure 13: State Monitoring Screen Showing First Card Selected

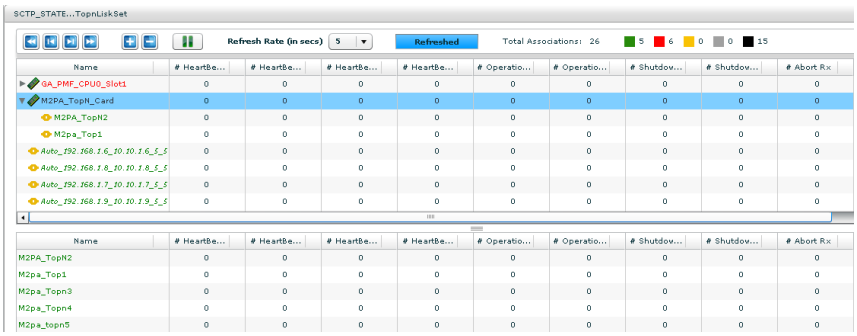

Figure 14: State Monitoring Screen Showing Second Card Selected

A second example shows the hierarchy is only Card > Association, (with the same relationships as in example 1).

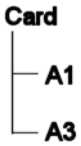

Figure 15: Example 2 of Filtered Elements

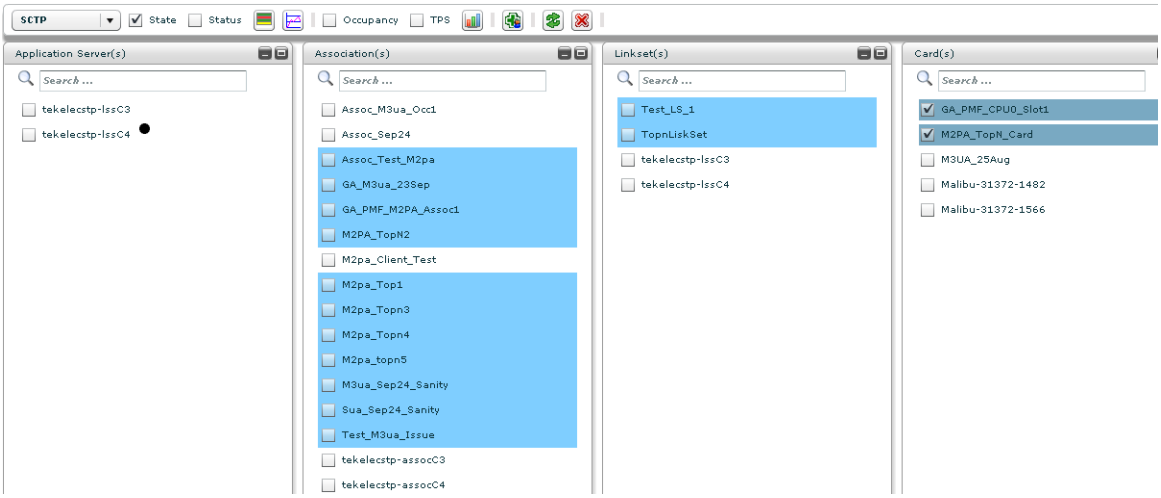

Figure 16: Cards Selected as Root in Element Selection Screen

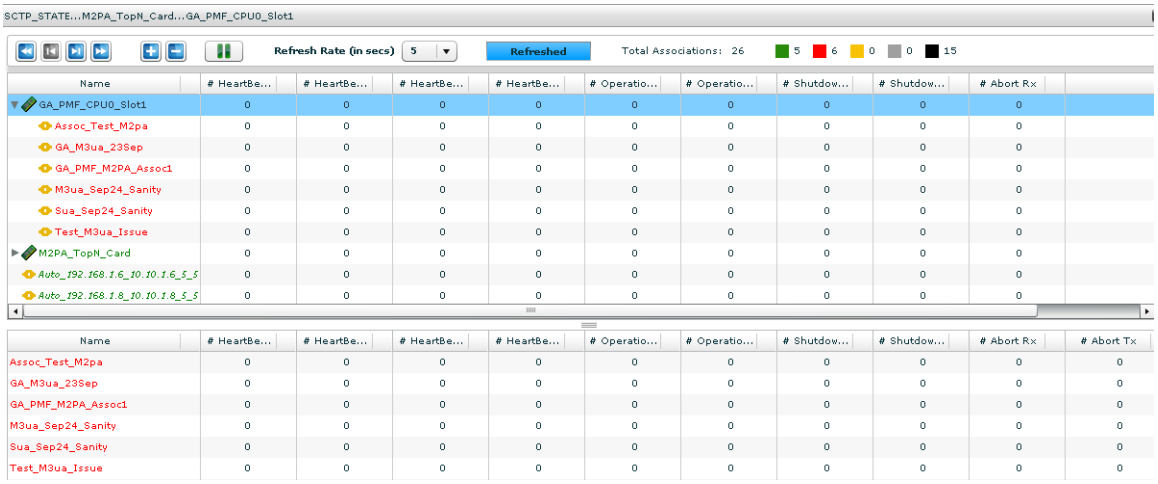

Figure 17: State Monitoring Screen Showing First Card Selected

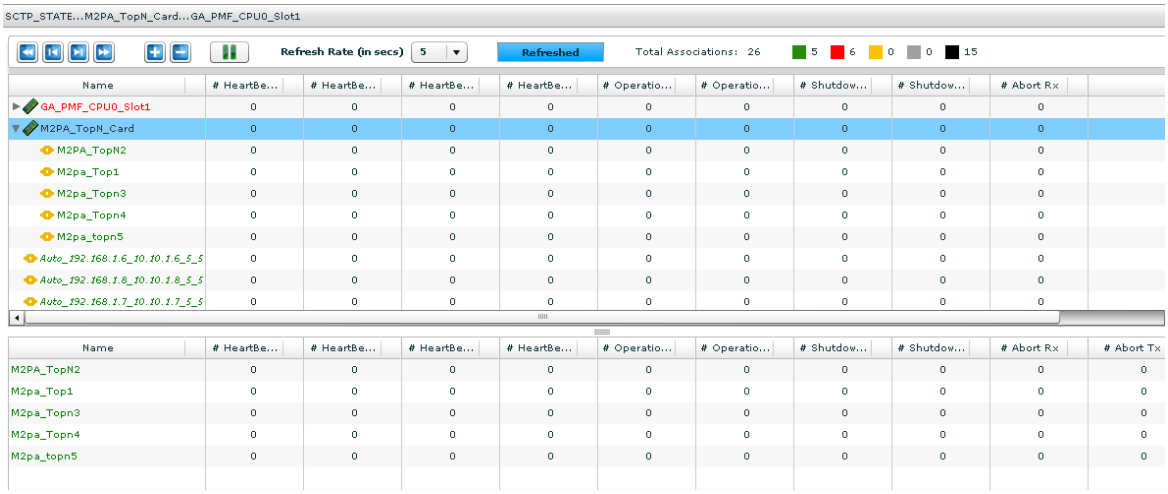

Figure 18: State Monitoring Screen Showing Second Card Selected

Sigtran Surveillance Monitoring Counts Capability

Sigtran Surveillance Monitoring Counts feature displays both cumulative (for State counters only) and current status (for status counts for measurements such as current throughput, current occupancy, etc). Sigtran Surveillance will monitor counts in the following intervals:

- Status monitoring intervals - every 1, 3 or 5 seconds
- State monitoring intervals - every 5, 10 or 15 seconds
- Chart monitoring intervals for either state or status - 5, 10, 15, 20, 30 or 60 seconds

Sigtran Surveliance Count Reset Capability

Sigtran Surveillance Monitoring Counts feature allows for counts to be reset manually or automatically. When invoking the reset function, the date and time of the reset will be logged and visible in the Audit Viewer application (see Audit Viewer Administrator's Guide for more information).

Note: The manual count re-set is restricted to those users with role nspManager.

Note: Integrated Acquisition or Probed Acquisition automatically resets counters once they have reached the value of 2 to the 32 power (approx 4,300,000,000).

Element Status Values

Status values for elements can differ depending upon their context. Absolute status values, such as TPS or Heartbeat counts, are the same regardless of what hierarchy is selected. In contrast, status values can differ depending upon the status of the child elements in the hierarchy. This difference is due to the parent element status not reflecting the its own status but reflecting the status of all the children below. The status of the children can vary depending on what hierarchy is currently displayed.

(See Table 7 : Status/State Color and Parent Element Status Value and Color Interpretations for more information).

Status and coloring have different meanings for base elements versus parent elements. A base element either works or does not work, that is, it is either green (working) or red (not working). These colors represent the true status of that element. The colors and status of parent elements is an indicative status of its children. It does not really reflect a true status for that parent. It simply means that one or more of its "children" in the hierarchy has a problem. The user then can deeper into the area where the issue exists. Thus an issue somewhere in the hierarchy is not missed because a card can never be green if an application server (AS) connected to it has a problem. What is important to note is that if that card is red, it does not mean that the problem is with the card. It indicates that all related elements have a problem.

For example, if AS1 had a problem and was red, then Card1 would be yellow, even though the card itself is functioning normally, because one of the children elements related to it had a problem.

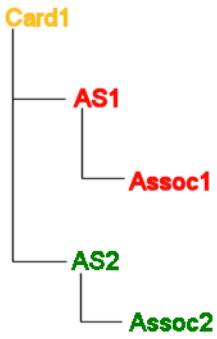

Figure 19: Example

Element State and Status

The Sigtran Surveillance application allows for the viewing of both element state and status in either tabular or graph layout. Both state and status are displayed in a separate screen that opens when either function is launched.

Note: Both state and status can be selected at the same time when monitoring in either the tabular or graph format.

The tabular monitoring screen has two sections. The top section displays monitoring counts for the state or status in hierarchical format and the bottom section is a drilldown of what is selected from the top section.

Note: The drill-down function in the tabular monitoring screen is in hierarchical form and is based on the relevance of the protocol status or state counters for the particular element.

Note: In the tabular monitoring screen, element hierarchies depend on the protocol and acquisition mode (Integrated Acquisition or Probed Acquisition) as well as the card type if Integrated Acquisition is being monitored.

Monitoring State and Status of Elements Using Tabular Monitoring Function

Sigtran Surveillance enables the monitoring of the state and status of an element(s) using the tabular monitoring function. Complete these steps to use the table function to monitor the state of an element(s).

- Select the network element(s) to be monitored

Note: To view elements that have not been configured in Centralized Configuration, launch the tabular monitoring window without selecting any elements.

- Select either or both monitoring options (State/Status) from the tool bar.
- Click Start Tabular Monitoring button on the tool bar.
  The Monitoring page opens.

Field/Element	Description

Show/Hide Column Button	Clicking this button opens a drop-down list showing all the counter columns. The screen can be customized to show only desired columns using this function.
Navigation Buttons	There are four buttons on the monitoring page. The buttons are: Move First - moves to the first element in the list of elements. Move Previous - moves to the previous element on the list. Move Next - moves to the next element on the list. Move Last - moves to the very last element on the list.
Expand All	Button with plus (+) sign - expands all the elements on the list.
Collapse All	Button with negative (-) sign - collapses all the elements on the list.
Pause Button/ Continue Monitoring	Pauses the monitoring process. When pause button is activated, the button changes to Continue Monitoring. To continue monitoring, click the button and the Pause button re-appears.
Refresh Rate	Provides the interval when the screen is refreshed Status - 1, 3 or 5 seconds State - 5, 10 or 15 sec intervals Chart (status or state) - 5, 10, 15, 20, 30 or 60 seconds.
Total Associations	Shows the total number of associations connected with the selected elements.
Association Legend	Shows the number of associations that are in a particular state (see color/state designations).
Top Table	Shows list of elements in hierarchical order filtered by parent elements.
Bottom Table	Shows list of all elements with no filtering.

Table 5: Tabular Monitoring Page Tool Bar

Elements in italics
All elements that are in italics are not configured in Centralized Configuration (black square on monitoring window tool bar that shows the number of unconfigured elements). The elements can be in any status, but they must be configured in Centralized Configuration before they are represented without italics.

Upper Table
The upper table represents the monitored element in a hierarchy(ies) related to the selected protocol.

Lower Table
The lower table represents the elements that reside under an element that has been selected in the upper table.

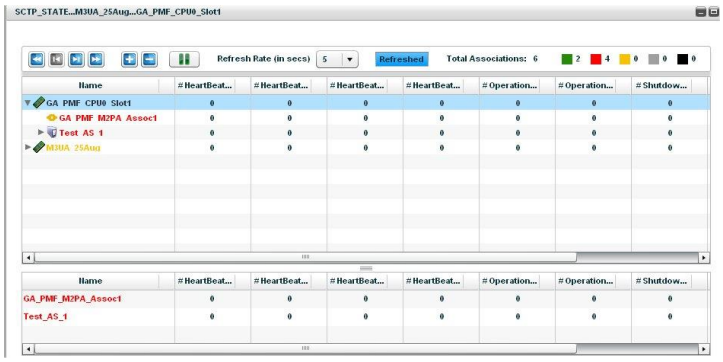

Figure 20: Tabular Monitoring Screen

- Set the screen Refresh Rate from the pull-down list.
  (Default is 5 seconds.)
- Select Element from the list to view the children of that element.
- When monitoring is finished close the screen by clicking the "x" on the top right-hand corner of the screen (as if closing a regular window).

Monitoring State and Status of Elements Using Graph Function

Sigtran Surveillance enables you to monitor the state and status of an element(s) using the chart monitoring function. Complete these steps to use the graph function to monitor the state and status of an element(s).

- Select the network element(s) to be monitored.

Note: A maximum of eight graph windows can be displayed at one time.
Note: Depending on what functions are selected you can select from two to a maximum of eight elements to monitor. See the table for examples.

Protocol(s)	State	Status	Max # of elements
SCTP	x		8
SCTP	x	x	4
M2PA+SCTP	x	x	2

- Select the monitoring state from the tool bar (either state, status or both can be selected).
- Click Start Graph Monitoring button on the tool bar. The Monitoring page opens.

Field/Element	Description
Pause Button	Pauses the monitoring process.
Refresh Rate	Provides the interval when the screen is refreshed.
Time Range	Shown in the x-axis. It provides the length of time previous to the current time and can run for more than the previous 24-hours.

Count Value	Shown in the y-axis. It provides the number of counts for a given time span. Note: If percent counts are available, then two Y-axis are viewed. The percentage graph has a thicker border.
Select Line Color	Enables you to choose the colors or hide the line for each of the elements being monitored. (See How to Configure Line Colors.)
Threshold Min	Sets a minimum threshold to graph. Provides a visual aid during the monitoring. The threshold appears as a red line.
Threshold Max	Sets the maximum threshold to graph. Provides a visual aid during the monitoring. The maximum threshold appears as a red line.
Set Button	Sets the threshold level which appears in the screen as red lines.

Table 6: Start State Graph Screen Tool Bar

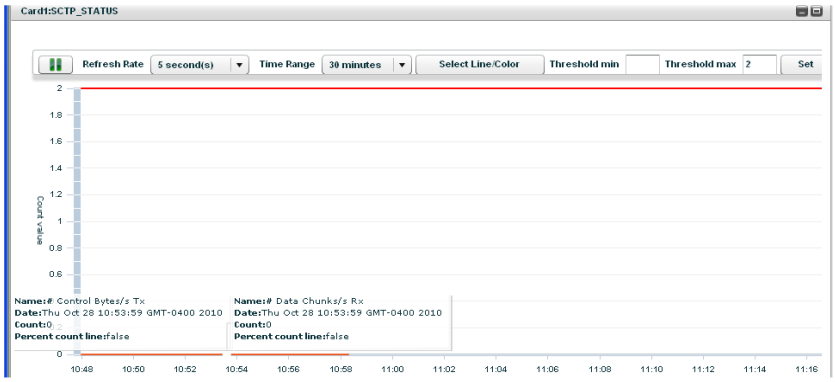

Figure 21: Graph Monitoring Screen with Rollover Feature

Note: The element graphs can be minimized. The remaining graph(s) on the screen automatically adjust in size.

- Set the screen Refresh Rate from the pull-down list. Default is 5 seconds.)

Note: If there are two Y-axis, then the axis that shows percentage is on the right and the axis that shows the number of counts is on the left.

- Set the Time Range from the pull-down list.

The range is 15 minutes to 24 hours. (Default is 15 minutes.)

- Select the Line Color of the elements.
- Select the Minimum Threshold.
- Select the Maximum Threshold.

Note: The threshold line will not show if the threshold is set to zero.

- When monitoring is finished, close the screen by clicking the "x" on the top right-hand corner of the screen (as if closing a regular window).

How to Configure Line Colors in Graphs

Sigtran Surveillance has the capability to change the colors used for the counter lines used in the graph mode. Follow these steps to change the color of a counter graph line.

1. From the Table or Chart monitoring page, click Select Line/Color.

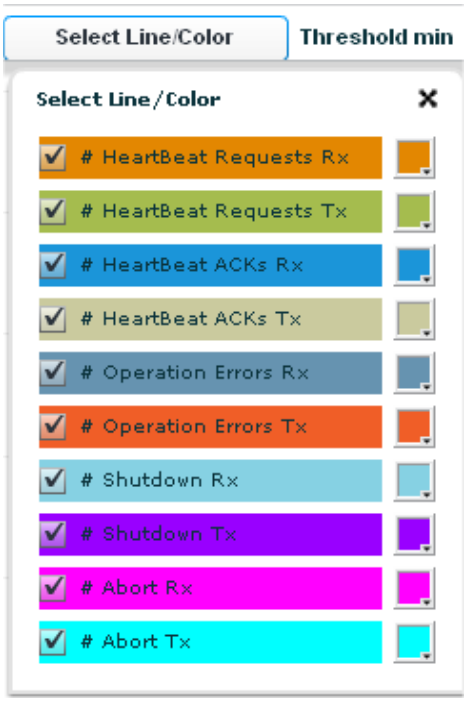

Figure 22: Line Color Settings Screen

2. Select the counter that needs a color change.
3. Select the color from the selection.
4. Click on Palette beside counter.
   - Select the color from the selection.
   - Repeat steps 2-3 to change other counter colors.
5. Close the Color Selection window.

Note: If you choose a color that is already being used, you prompted that that you must choose another color.

Hiding or Showing Counter Lines

Sigtran Surveillance has the capability to hide or show counter lines in the graph screen. Complete these steps to hide or show columns.

Note: The default is to show all counter lines.

1. Select an element.
2. Click Monitor State or Status from the tool bar.
3. Select the Monitor Graph from the tool bar.
4. Click Select Line/Color.
5. Un-select or select the check box by the counter name to hide or view the line.
6. Close the box.
   The changes are saved.

State Counters

The state monitoring screen for Integrated Acquisition and Probed Acquisition is displayed either in tabular or graph format depending on which format is chosen. This is a list of all counters for the SigTran protocols monitored.

SCTP

- Heartbeat requests Rx/Tx
- Heartbeat ACKS Rx/Tx
- Operation Errors Rx/Tx
- Shutdown Rx/Tx
- Abort Rx/Tx

M2PA

- Alignment Rx/Tx
- Proving Normal Rx/Tx
- Emergency Rx/Tx
- Out of Service Rx/Tx
- Processor Outage Rx/Tx
- Busy Rx/Tx

M3UA

- Management Messages Rx/Tx
- SSNM Messages Rx/Tx
- ASPSM Messages Rx/Tx
- ASPTM Messages Rx/Tx
- RKM Messages Rx/Tx
- Destination Unavailable Rx/Tx
- Signaling congestion Rx/Tx

Status Counters

The status monitoring screen for Integrated Acquisition and Probed Acquisition is displayed either in table or chart format depending on which format is chosen. This is a list of all counters for the SigTran protocols monitored.

SCTP

1. # Control Chunks Rx/Tx
2. # Data Chunks Rx/Tx
3. # Control Bytes Rx/Tx
4. # Data Bytes Rx/Tx
5. Total Packets Rx/Tx
6. Total Bytes Rx/Tx

M2PA

- # UDMs Rx/Tx

- # UDM Bytes Rx/Tx
- SS7 SCCP Messages Rx/Tx
- SS7 ISUP Messages Rx/Tx
- SS7 Management Messages Rx/Tx
- SS7 Message Bytes Rx/Tx
- Total Messages Rx/Tx
- Current TPS Rx/Tx
- Occupancy % (TPS) Rx/Tx
- Reserved Occupancy % Rx/Tx

M3UA

- Non-data Messages Rx/Tx
- Non-data Message Bytes Rx/Tx
- Data Messages Rx/Tx
- Data Message Bytes Rx/Tx
- Current TPS Rx/Tx
- SCCP Message Rx/Tx
- ISUP Message Rx/Tx
- Total Messages Rx/Tx
- % Total Occupancy (TPS) Rx/Tx
- Reserved Occupancy % (TPS) Rx/Tx (Available only for links)

SUA

- Management Messages Rx/Tx
- Management Message Bytes Rx/Tx
- Data Messages (CLDT + CLDR) Rx/Tx
- Data Messages (CLDT + CLDR) Bytes Rx/Tx
- Total Messages Rx/Tx
- Total Messages Bytes Rx/Tx
- Current TPS Rx/Tx
- Total Occupancy % Rx/Tx

Status / State Color Interpretations

In the tabular monitoring screen the status or state of each element within a hierarchy is represented by a color. This table provides the interpretation of each status/state color.

Color	Interpretation
Green	Network element is up and running. It is the normal functioning state when none of the elements in the hierarchy is red.
Red	Network element is down. Action has to be taken as the element is not connected and/or traffic is not being captured.
Yellow	At least one child network element is in red state. For example, when an M3UA association is YELLOW, it means that at least one of its links is down (in red).

Gray	Associations are present but data is not available
Black	Associations are not configured in Centralized Configuration

Table 7: Status / State Color

Parent Element Status Value and Color Interpretations

The status of a parent element depends on the status of its children. In other words, the status of the parent reflects the status of its children for the whole sub tree.

Note: The term children mean all children, not only ones that are visible in the hierarchy. Rules governing parent status value are:

- If the status of all children is the same, then the parent status is the same.
- If the status of the children differs, then the parent status is of the form *[...] where all statuses of the children are listed.

Note: Only part of the list can be visible if the cell is too narrow. The table shows the parent element color and its status value interpretation:

Parent Element Color	**Interpretation**
Gray	All children belonging to parent have N/A (not available) status
Green	All children of parent element have green status
Red	All children of parent element have red status
Yellow	If one or more (but not all) children have status other than green

Table 8: Parent element Color

Status / State Color Interpretations for SCTP Protocol

The status display colors for the network elements using the SCTP protocol are the following:

Color	**Displayed Value**	**Interpretation**
Red	Closed	Closed
Red	Init	Initialed
Green	Established	Established
Red	Shutdown	Shutdown

Table 9: SCTP Protocol Color

Status / State Color Interpretations for M2PA Protocol

The status display colors for base network elements using the M2PA protocol are the following:

Color	Displayed Value	Interpretation
Red	OS	Link/ASP is Out of Service
Red	N	Link/ASP has entered Normal Alignment proving period
Red	E	Link/ASP has entered Emergency Alignment proving period
Green	A	Link/ASP is in Service
Red	PO	Link/ASP is reporting Processor Outage
Red	B	Link/ASP is reporting Busy

Table 10: M2PA Protocol Color

Note: Base element is Link for IPSG and Application Server Process (ASP) for IPGW

Status/State Color Interpretations for M3UA and SUA Protocols

The status display colors for network elements the M3PA and SUA protocols are the following:

Color	Displayed Value	Interpretation
Red	ASPDN	ASP is down
Green	ASPAC	ASP is active
Red	ASPIA	ASP is inactive

Table 11: M3UA and SUA Protocol Color

Note: Base element is Link for IPSG and Application Server Process (ASP) for IPGW

TOP "N" Associations Capability

The Sigtran Surveillance application has a Top "N" capability. This capability allows for the monitoring of the most active associations in terms of TPS, (Transactions per Second), or Occupancy, (up to 100%), in order of activity. The number of associations is configured in the "Monitoring Settings" option on the Sigtran Surveillance menu. (For information on configuring TOP "N", see *Sigtran Surveillance Monitoring Settings*.

Monitoring Using Occupancy and TPS Functions

Sigtran Surveillance has the capability to monitor the occupancy and transactions per second (TPS) in both table and graph views. Complete these steps to monitor either occupancy and/or TPS in table and/or graph format.

- Select the **network element(s)** to be monitored.
- Select either the **Occupancy** or **TPS** (or both) from the tool bar.
  Note: TPS shows actual number of transactions where Occupancy shows a percentage of TPS. Therefore, depending on the capacity, the ranking of the associations may differ. For example if the capacity of an element is 1000 and a TPS of 100, then the occupancy is 10%. If another element has a capacity of 100 and a TPS of 50, then the occupancy is 50%. In this example, the element that has 50 TPS would be ranked higher in occupancy graph but lower on the TPS graph.
- Click **TOP "N" Monitoring** button on the tool bar.

- The Monitoring page opens.

Field/Element	Description
Pause Button	Pauses the monitoring process.
Refresh Rate	Provides the interval when the screen is refreshed (5, 10 or 15 second intervals with 5 seconds as default).
Refresh Status	Shows if the screen is being refreshed at the specified rate.
Column Chart/Bar Chart button	Clicking this button switches between either a column graph (horizontal-default) or bar graph (vertical).
Chart	Selecting this box (selected by default) the chart view is active. De-selecting shows only the table format.
Table	Selecting this box (selected by default) the table view is active. De-selecting shows only the chart format.
Color Palette	Clicking on this icon opens the color selection box for selecting column/bar chart colors.

Table 12: Top N Monitoring Page

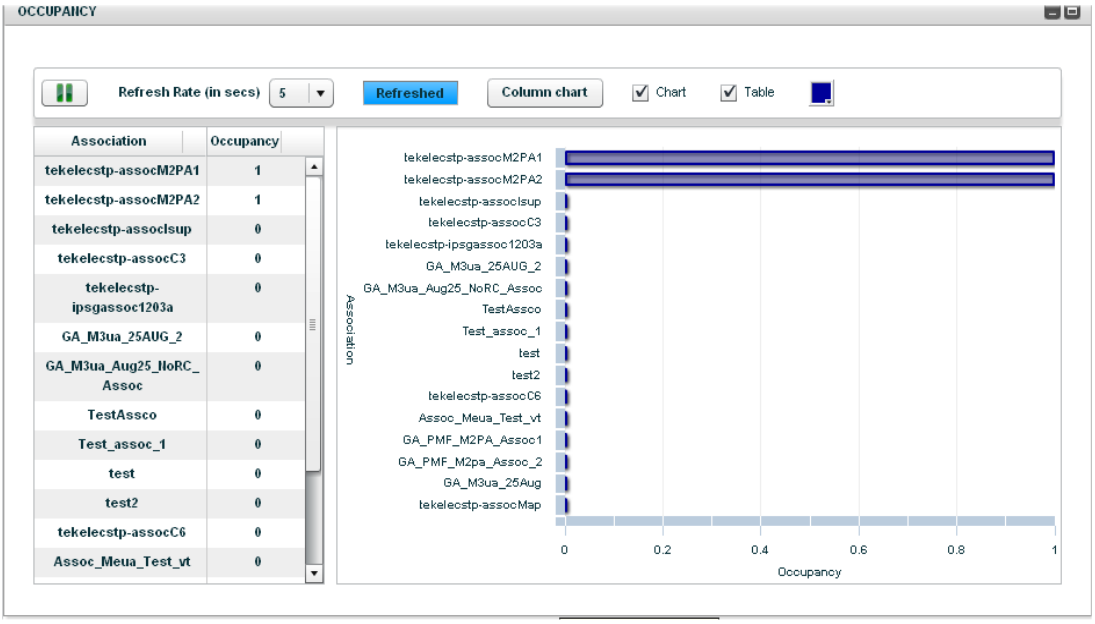

Figure 23: Occupancy Default Monitoring Page - Column Graph

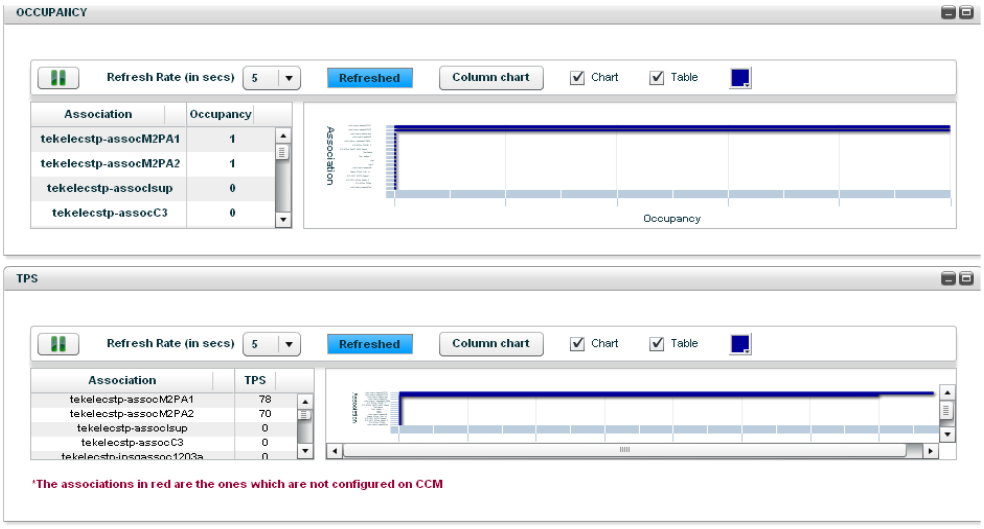

Figure 24: Combination Occupancy/TPS Monitoring Page - Column Graph

- Set the screen Refresh Rate from the pull-down list. Default is 5 seconds.)
- Select the type of view Chart or Table.
- (Optional) Select the color of the column or bar graph.
- Note: If there are associations present that are not configured in Centralized Configuration, they are marked in red. (Also shown by note at bottom of screen.)
- When monitoring is finished close the screen by clicking the "x" on the top right-hand corner of the screen (as if closing a regular window)

Appendix A: My Oracle Support (MOS)

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request

2. Select 3 for Hardware, Networking and Solaris Operating System Support

3. Select 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Appendix B: Locate Product Documentation on the Oracle Technology Network Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click **Industries** icon.
3. Under the **Oracle Communications** heading, click the **Oracle Communications documentation** link.The Communications Documentation page appears. Go to the **Network Visibility and Resource Management** section.
4. Click on **Performance Intelligence Center** and then the release number. A list of the entire documentation set for the selected release appears.
5. To download a file to your location, right-click the **PDF** link and select Save Target As (or similar command based on your browser), and save to a local folder.

Note: As long as the documentation site has not been significantly refactored, you can use this link as a shortcut to step 4:
http://docs.oracle.com/en/industries/communications/performance-intelligence-center/index.html