Oracle® Communications Performance Intelligence Center

SIGTRAN Surveillance Guide

Release 10.4.0

F26331-01

November 2020

ORACLE®

Oracle® Communications Performance Intelligence Center SIGTRAN Surveillance Guide, Release 10.4.0

CAUTION: Use only the guide downloaded from Oracle Help Center.

Table of Contents

List of Figures

List of Tables

1. Chapter 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 Oracle® Communications Performance Intelligence Center, 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).

2. Chapter 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.

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. SIGTRAN Surveillance 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.

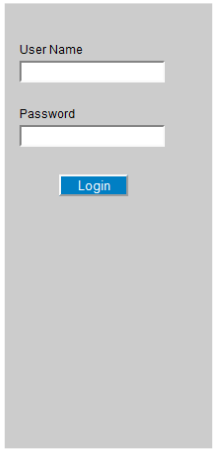

Figure 1: Login Screen

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.

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: 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).

If the user is opening the application first time (meaning no Panel is saved from previous use) then there will be no panels in the page body. If saved panel configurations exist for the user, then those will be

loaded on login and start in refresh active mode, in their last size and order (see **configuration auto-backup**)

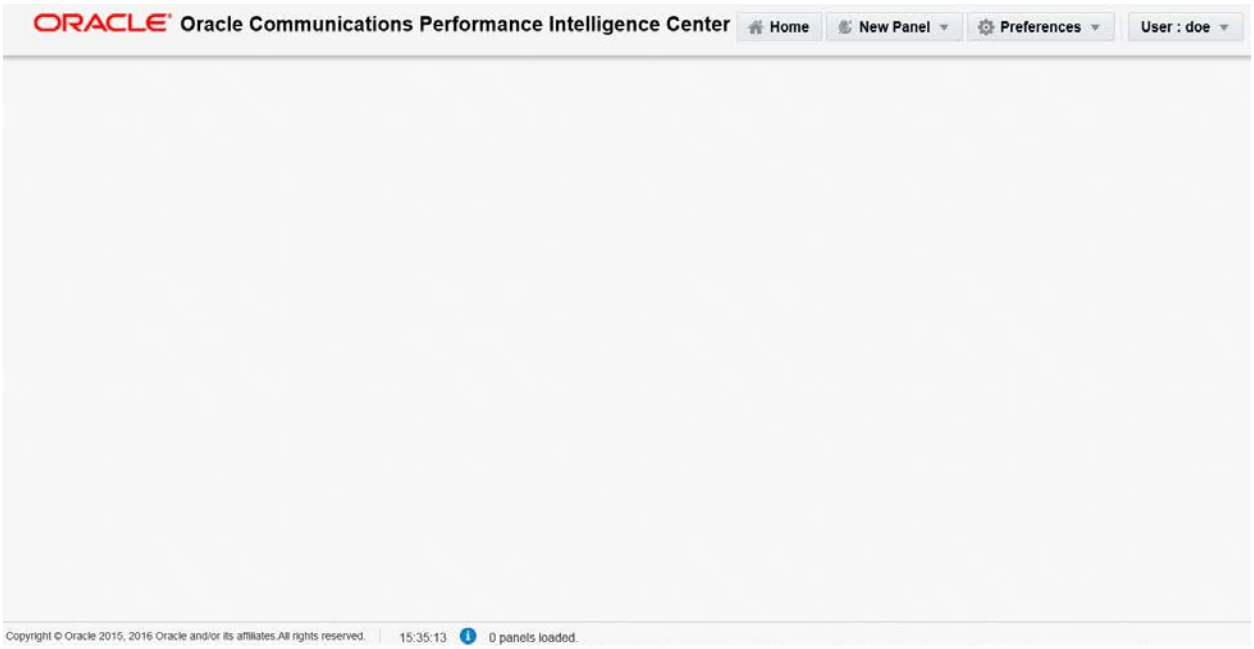

Figure 2: SIGTRAN Surveillance first login for a user

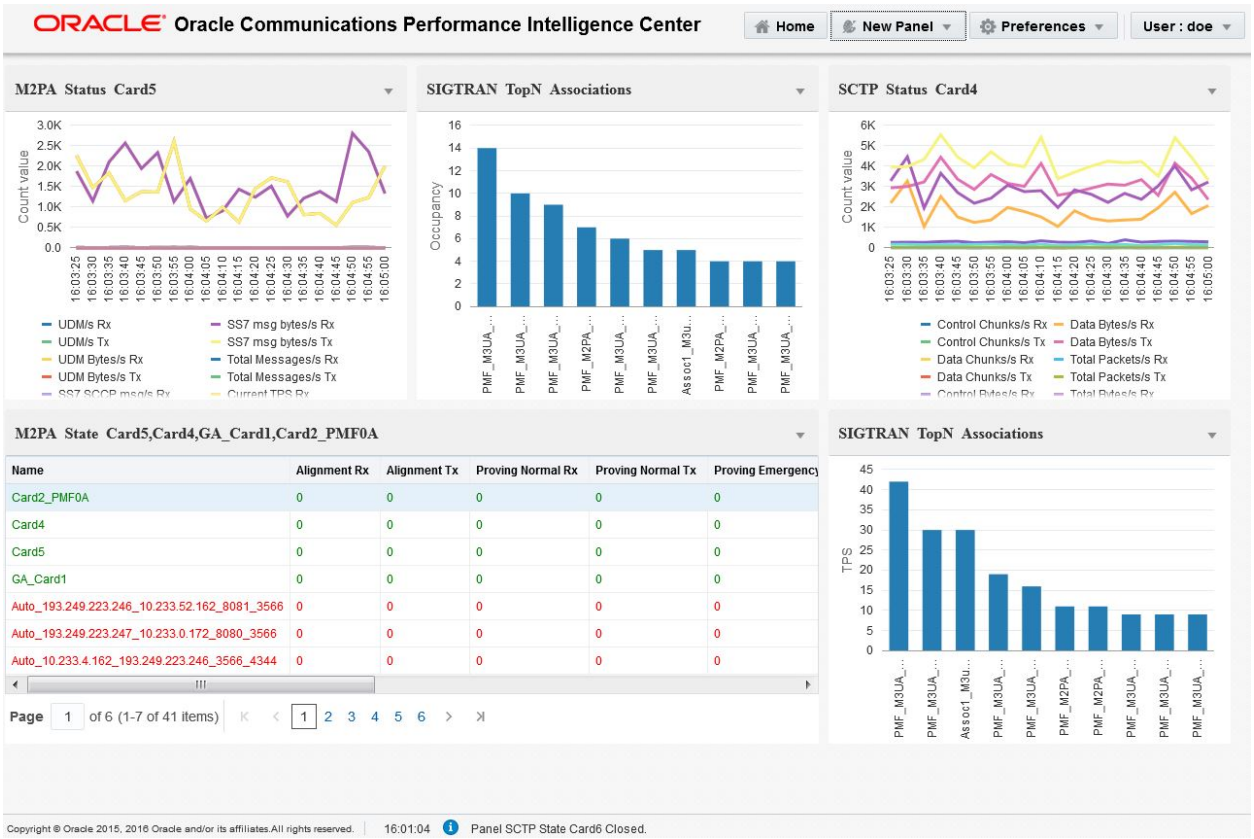

Figure 3: SIGTRAN Surveillance with saved panels

The Sigtran Surveillance main screen has the following sections:

Banner

It is single line component to provide application menus.

Figure 4: Banner

Home

This menu button will take user back to portal screen.

New Panel

It will appear as drop down menu and will provide an option "SIGTRAN Surveillance" to create a panel. On click, a dialogue box shall be launched to collect parameters about panel configuration.

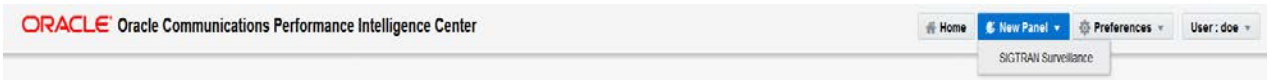

Figure 5: New Paneel

Preferences

This menu option shall provide application specific preferences. In this version it shall provide an option "Reset SIGTRAN Counters", which will reset globally all the counters.

Figure 6: Preferences

Panel Area

This area shall hold all the panels that have been created by the user.

Figure 7: Panel Area

Communication Center

This is present at the bottom and this will inform user about client messages and will be user to perform user interactions.

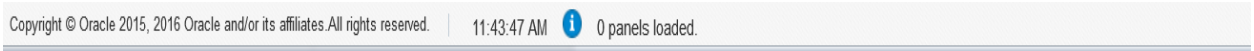

Figure 8: CommCenter

3. Chapter Working with 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 Performance Intelligence Center 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.

Table 1: Functional Expectations 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

NETWORK ELEMENTS IN SIGTRAN SURVEILLANCE

Network elements refer to customer network elements monitored by the Performance Intelligence Center system such as:

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

Panel Creation in SIGTRAN Surveillance

A panel for Table, TopN and Graph monitoring can be created using "New Panel" menu from the banner. A user can select "SIGTRAN Surveillance" option from "New Panel" menu, on click a dialogue box shall be launched to provide configuration information for desired panel.

Following parameters are required for the panel creation:

- Refresh Rate: User can select refresh rate from 5sec, 15sec, 30sec and 1min. Default is 5sec. The data in panel will refresh after selected interval.
- Report: User can select Table, TopN and Graph as monitoring type. The selection for the remaining parameters depend on "Report" type.
- Protocol: User can select "SCTP", "M2PA", "M3UA", "SUA" as protocol. The selection for the remaining parameters depend on the "Protocol".
- Root Hierarchy: User can select "Card" or "ApplicationServer/Linkset". Default is "ApplicationServer/Linkset".
- Counters: User can select State or Status as counters type.
- Include By: This filed denotes the type of network element that can be selected from the drop down list. This list will depend on the "Protocol" selected.
- Element: This is a combo box and user shall select the actual network element in this field. This will depend on the "Include By" field.
- Criteria: user can select "Occupancy" or "TPS". This is applicable only for TopN Association monitoring.
- Excluded Associations: This is a combo box and user can select the associations to be excluded from the TopN monitoring.
- Select By: User can select the type of network element on the basis of which Element can be selected for chart monitoring.

Table Monitoring in SIGTRAN Surveillance

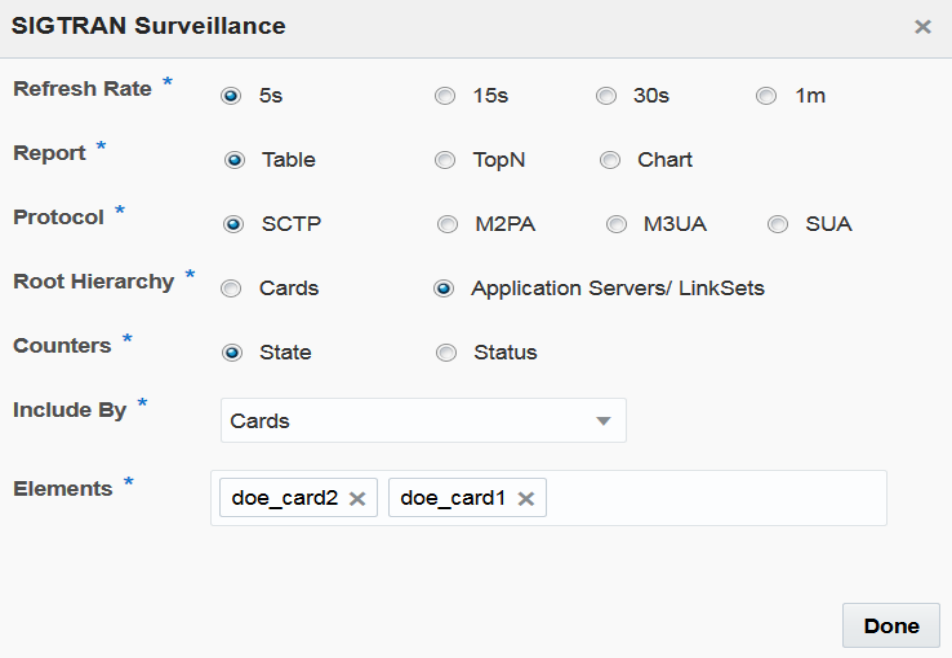

Figure 9: Dialogue Box for Table Monitoring Panel

Complete these steps to create table monitoring panel

1. Click on "New Panel" and select "SIGTRAN Surveillance" option from drop down.
2. Select **"Refresh Rate", "Report as Table", "Protocol", "Root Hierarchy", "Counters", "Include By" and "Elements".**
3. Click on "**Done**" to create the panel.

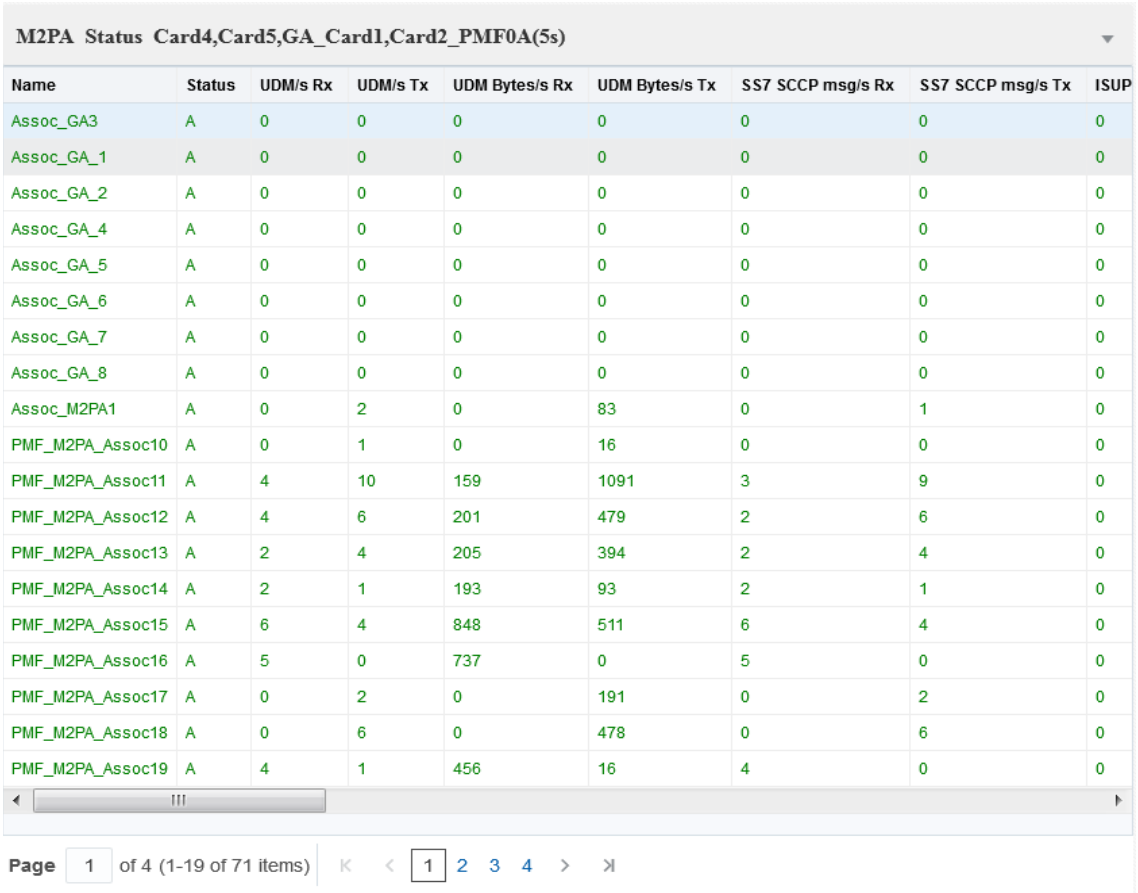

Figure 10: Table Monitoring Panel

The title of the panel should indicate the user selection during panel creation. The refresh rate shall be indicated at the end of panel's title.

TopN Association Monitoring in SIGTRAN Surveillance

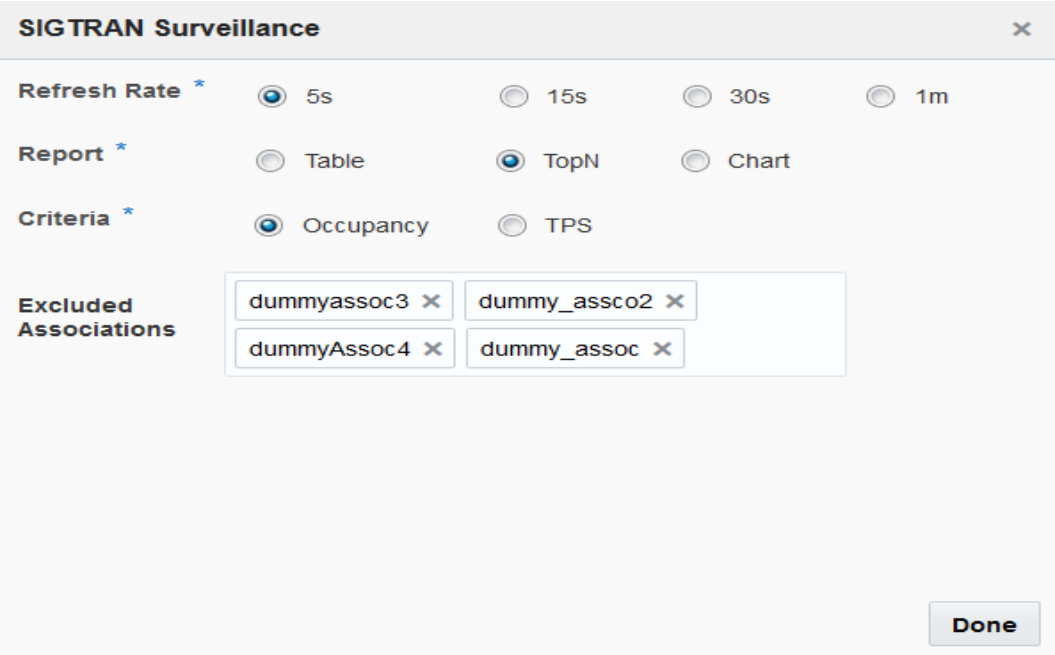

Figure 11: Dialogue Box for TopN Monitoring

Complete these steps to create TopN Association monitoring panel

1. Click on "New Panel" and select "SIGTRAN Surveillance" option from drop down.
2. Select **"Refresh Rate", "Report as TopN", "Criteria" "Exclude Associations".**
3. Click on "**Done**" to create the panel.

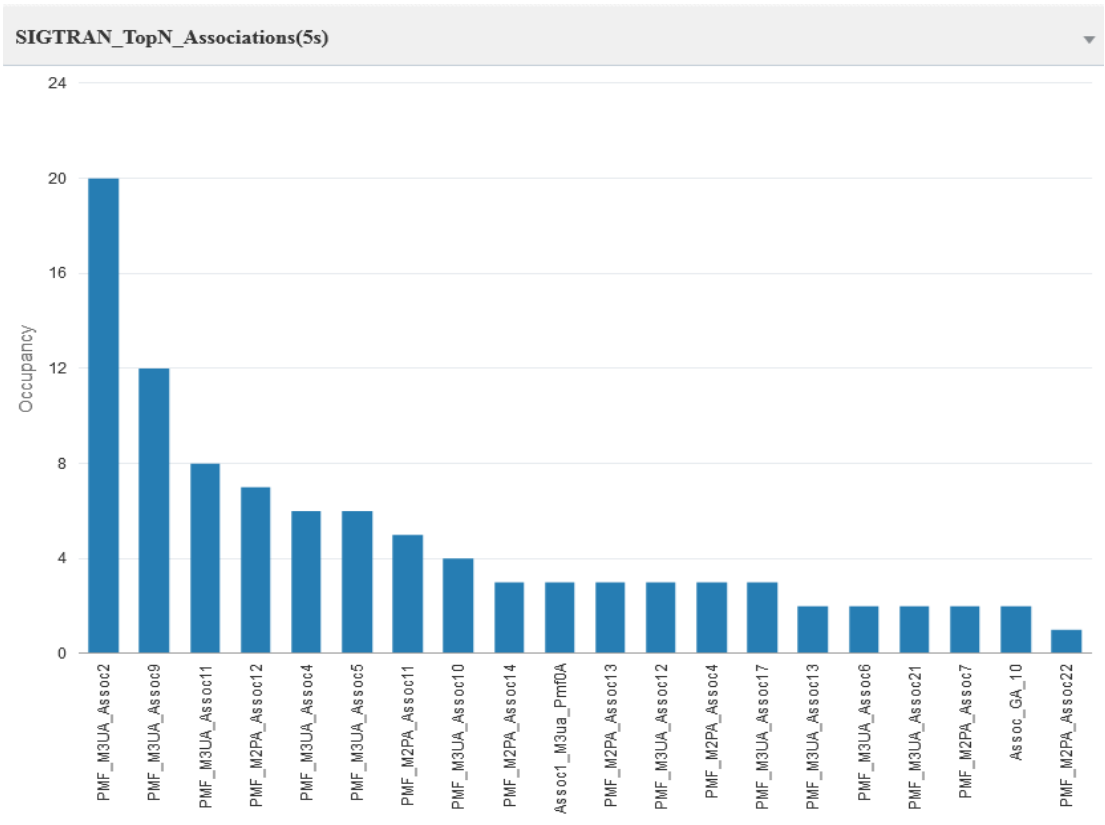

Figure 12: Panel for TopN Monitoring

Graph Monitoring in SIGTRAN Surveillance

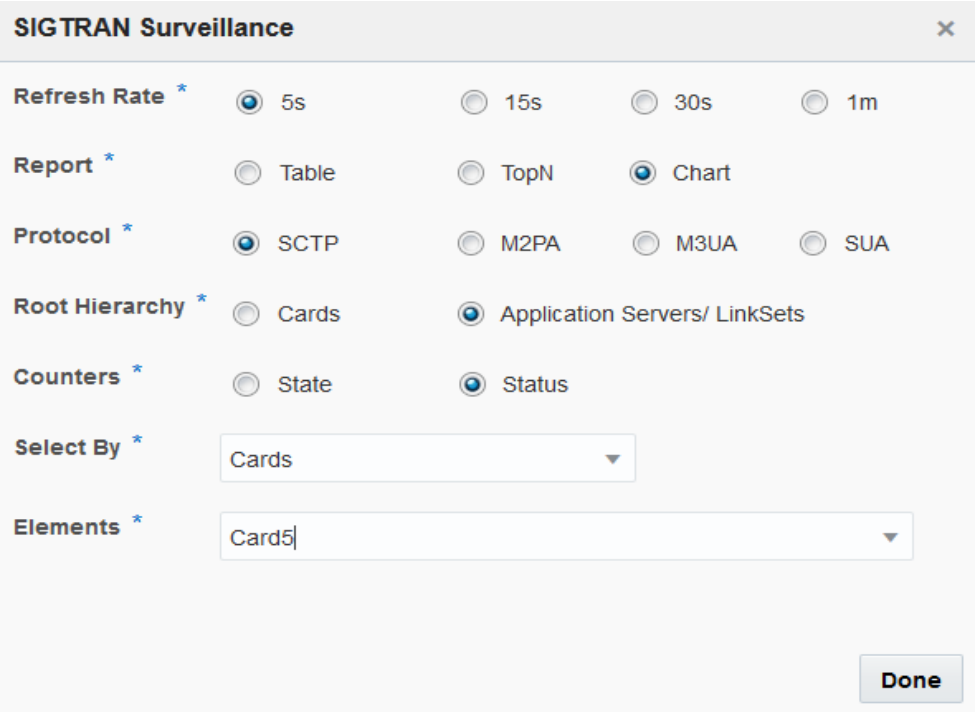

Figure 13: Dialogue Box for Chart Monitoring

Complete these steps to create Chart monitoring panel

1. Click on "New Panel" and select "SIGTRAN Surveillance" option from drop down.
2. Select **"Refresh Rate", "Report as Chart", "Protocol", "Threshold—min and max", "Root Hierarchy", "Counters", "Select By" and "Elements".**
3. Click on "**Done**" to create the panel.

Note: Only one network element can be selected for the chart monitoring.

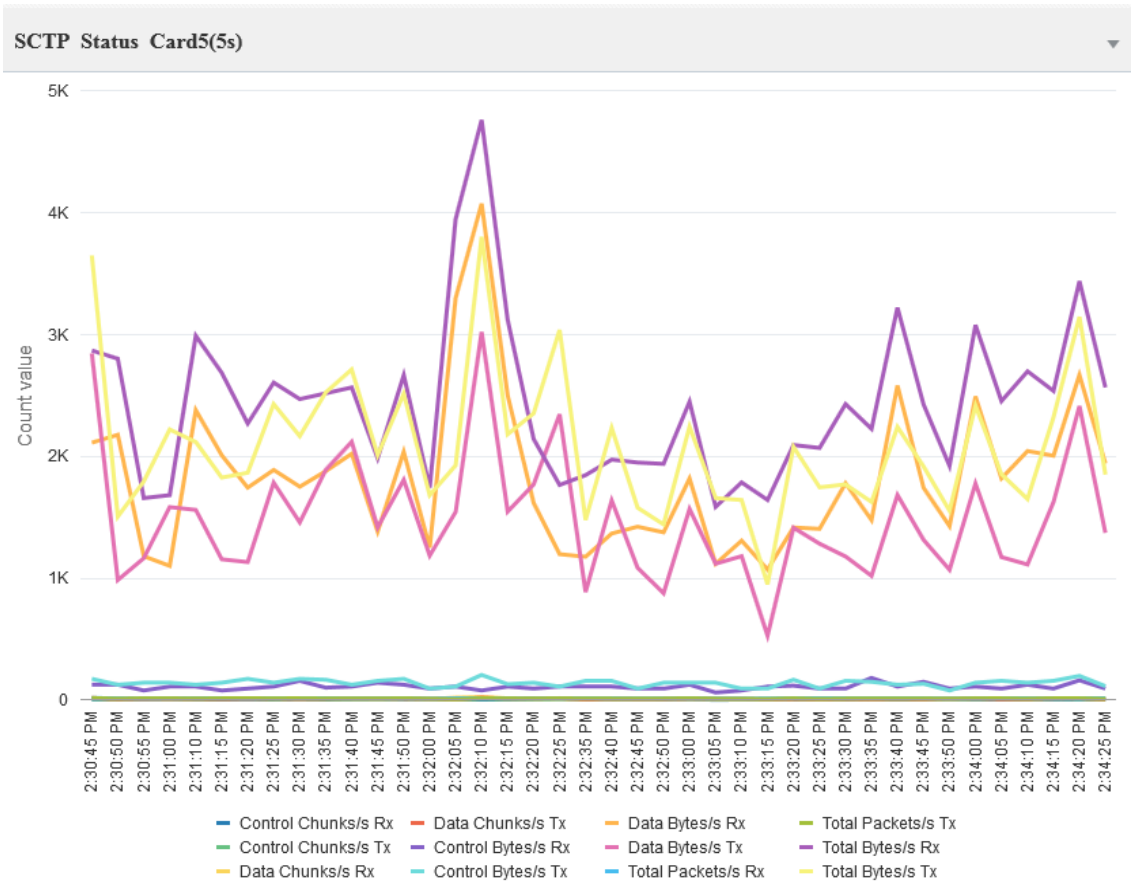

Figure 14: Panel for Chart Monitoring

Dynamic Parametrs for Panel

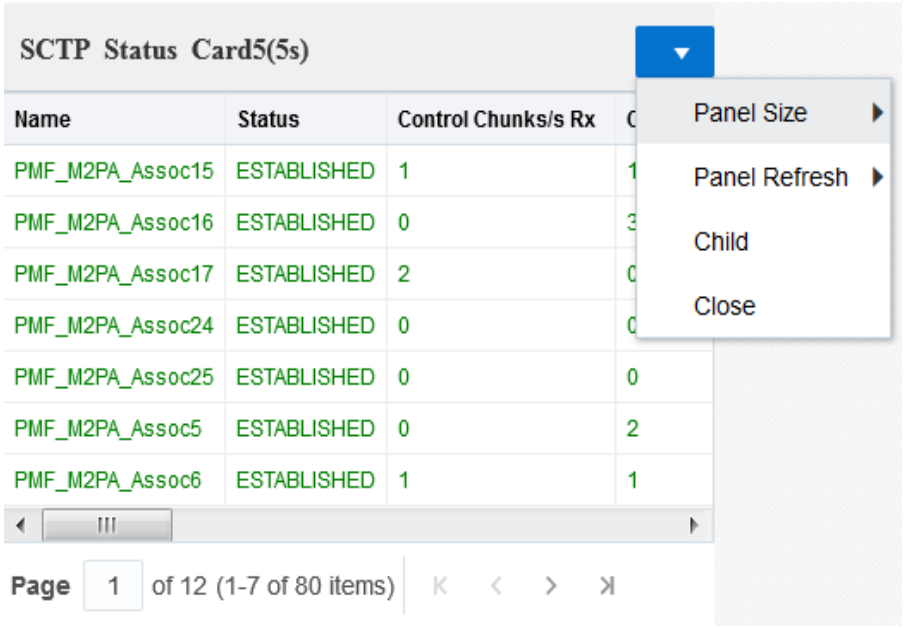

Figure 15: Panel Dynamic Parameters

There are four dynamic parametrs that can be modified/selected after the panel has been created.

Panel Size

User can select the panel size from 1x1, 2x1, 3x1, 2x2, 3x2 options

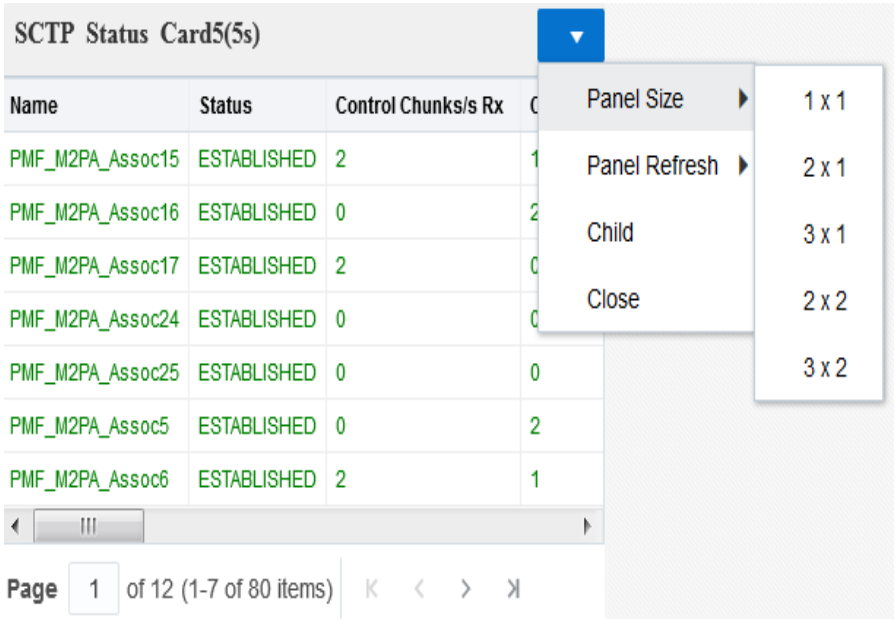

Figure 16: Panel Size

Panel Refresh

User can activate or pause the panel, using Panel Refresh parameter. Active panel will refresh at the rate selected during panel creation. Pause option shall stop the panel data refresh.

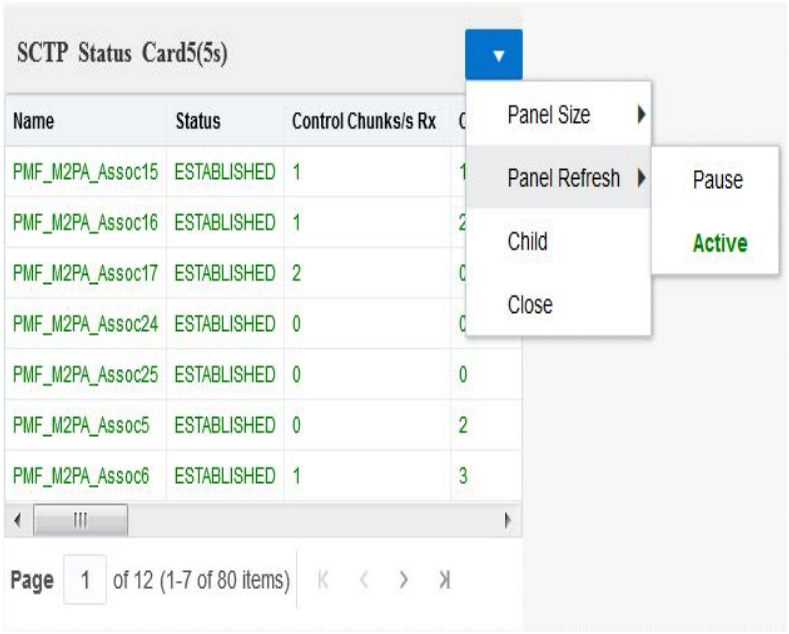

Figure 17: Panel Refresh Parameter

Child

User can open and view the child as a separate panel using this option. In the hierarchy based relation ship e.g. Card->Association, Parent Panel shall display the card and Child panel shall display the Associations. This option is only applicable for the Table Monitoring.

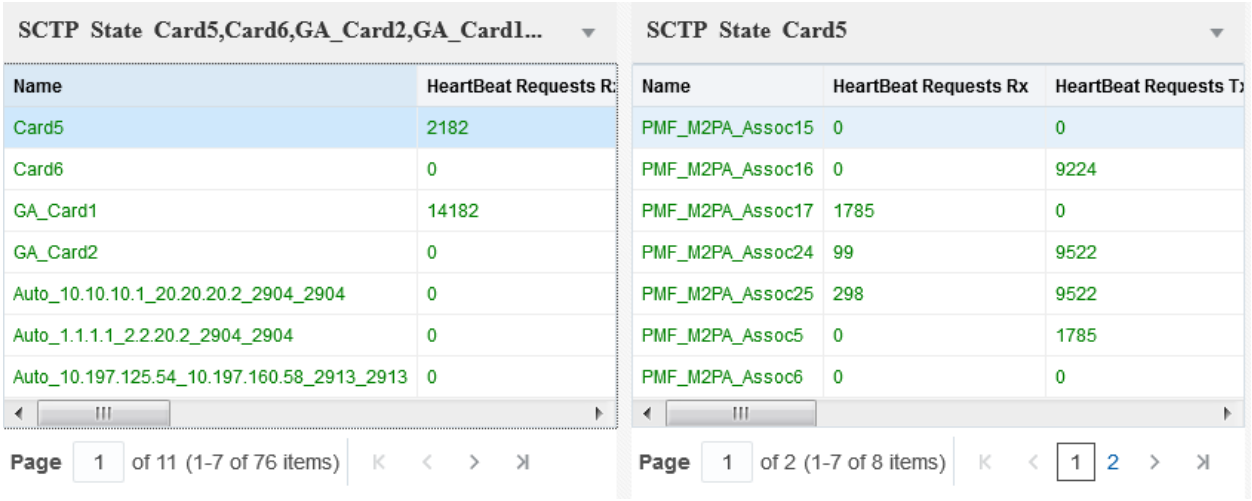

Figure 18: Child Panel

In the above figure, 1st Panel "SCTP State Card5,Card6,GA_Card2,GA_Card1(5s)" is displaying the Cards, the second panel "SCTP State Card5" is the child panel and is displaying all the associations under selected "Card5" in the first panel.

Close

User can use "Close" option to close the panel. On Close, the user shall be asked for the confirmation in the CommCenter.

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 >Card> Association > Link

Card>LinkSet>Association > Link

IPGW SCTP (Status and State)

Linkset > Association

Card > 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)

Third Party Card > 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:

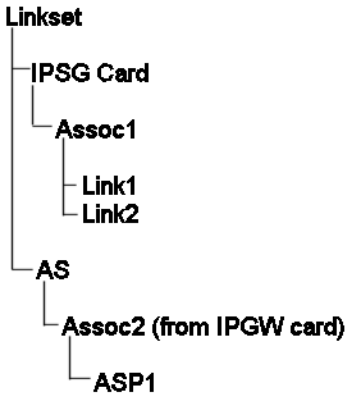

Figure 19: Linkset with IPSG and IPGW Card Links

- 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:

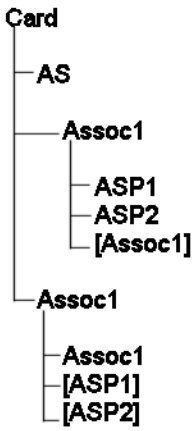

Figure 20: Hierarchy with Unconfigured Traffic

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.

Auto-Backup of Panel Settings

Parameters for all panels (size, pause, contents, title, rank) shall be automatically saved without user additional action. To avoid an overhead of client to server communication in case of multiple changes, this shall be deferred with a timer set on a period of 10 seconds.

The effect of this algorithm is that all changes are tracked in client side only first.After a quiet period of 10 seconds, those changes are sent as one general backup (only settings, no counter values, not the cache). CommCenter will notify the user in case of backup is done with message **"Configuration Saved for <n> panels".**

The effect of the rule above is to have something seamless as long as each user has only one active page (recommended way to use Oracle® Communications Performance Intelligence Center on OJET) but allow predictable behavior in case the user wants to display more (he will not be blocked on changing panels order and content but this will not be persistent).

Normal use of the OJET feature is that each user has his set of 12 most needed panels handy. If a supervision picture wall is needed to service a group, we recommend creating a dedicated account for the group and mnage the supervision panels on this account. Example:

- Joe, Phil, Sam get each a private space that works with up to 12 panels saved automatically,
- As a team they can create a "TeamJPS" account to configure a shared supervision dashboard for their big screen

Appendix A: My Oracle Support

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.