Oracle® Communications Performance Intelligence Center

Audit Viewer Administrator's Guide

Release 10.1.5

E56976 Revision 1

August 2015

ORACLE®

Oracle Communications Performance Intelligence Center Audit Viewer Administrator's Guide, Release 10.1.5

Refer to Appendix A for instructions on accessing My Oracle Support.

Table of Contents

List of Figures

List of Tables

Chapter 1: About This Help Text

Overview

The Audit Viewer Tool is part of the NSP Toolbox Configuration Library. It is an application that monitors the activities of logged-in users and displays records of those activities. Only users with roles NSP Network Administrator and the NSP Monitoring Manager have have access to this application.

Scope and Audience

This manual provides information about the Audit Viewer's graphic interface (GUI) and is designed around performing common tasks to efficiently and effectively monitor application and user's activities as well as alarm status. Take a few minutes to browse through these tasks and become acquainted with the layout of this guide to become familiar with the headings and subheadings that allow you to find the information you need.

About the Performance Intelligence Center

The Performance Intelligence Center (PIC) is a monitoring and data gathering system that provides network performance, service quality and customer experience - across various networks, technologies, protocols, etc. Beyond monitoring performance and gathering data, the solution also provides analytics, actionable intelligence and potentially an intelligent feedback mechanism. It allows Service Providers to simultaneously look across the Data Link, Network, Transport and Application layer traffic to better correlate and identify the impact of network problems on revenue generating applications and services.

PIC functionality is based on the following general flow. The Integrated Message Feeder (IMF) is used to capture SS7 and SigTran traffic. The Probed Message Feeder (PMF) is used to capture both SS7 and IP traffic. Both products forward Probe Data Units (PDUs) to the Integrated xDR Platform (IXP). The IXP stores this traffic data and correlates the data into detailed records (CDRs, IPDRs, TDRs, etc.). The IXP then stores the data on the system for future analysis. The Network Software Platform (NSP) provides applications that mine the detailed records to provide value-added services such as network performance analysis, call tracing and reporting.

PIC centralized configuration tasks fall into one of two categories:

- Data Acquisition and Processing - the configuration of the probes, routing of PDUs to the xDR builder setup, KPI generation, data feeds, etc.
- PIC System Administration - the configuration of monitoring sites, configuring PIC servers, setting up permissions, etc.

Note: For more information see Centralized Configuration Manager Administrator's Guide. This is a graphic overview of the PIC system.

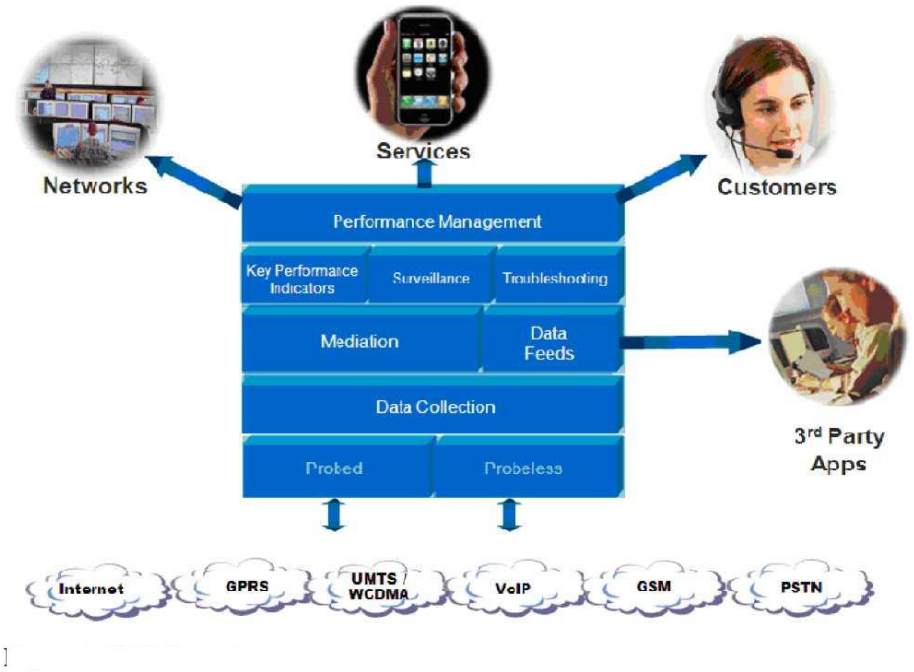


Figure 1 : PIC Overview

Setting User Preferences

Users can set User Preferences that apply across all the NSP applications. These include

- Time specifications (date format, time zone, etc.)
- Directory names (for exporting, uploading, and downloading)
- Enumeration values (numerals vs. text)
- Point code specifications
- CIC specifications
- Default alarm colors
- Default object privacy privileges

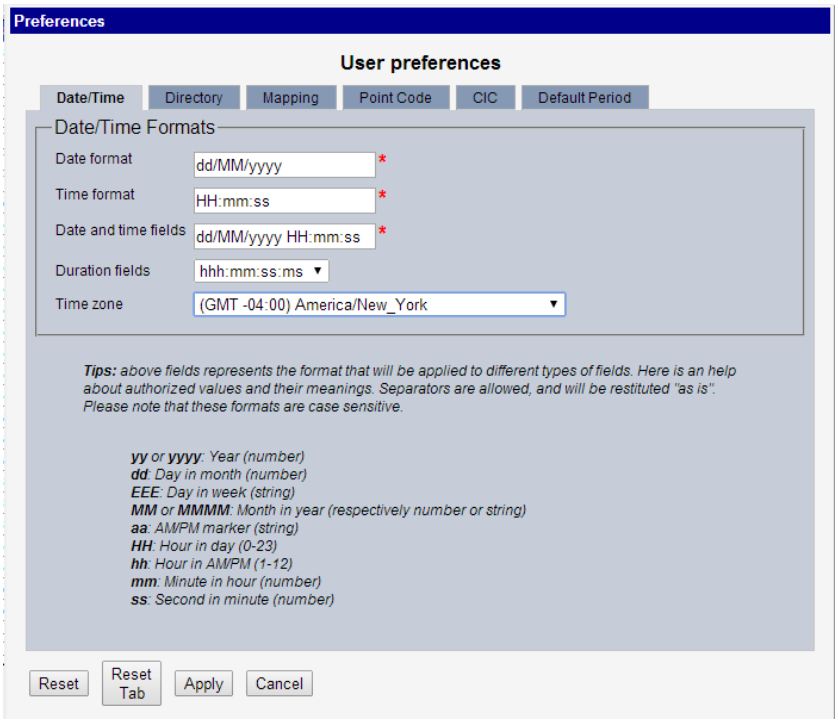
Setting Time Format

Follow these steps to set the time format:

1. Click **User Preferences** on the Application board. The User Preferences page is displayed.
2. Click the **Time** tab.
   The Time page is displayed. The red asterisk denotes a required field.

   Note: Use the tips on the page to help you configure the time format.

Figure 2 : Time Formatting Page



3. Enter the format for these time-related displays.

   - **Date format**
   - **Time format**
   - **Date and time fields**

4. Select the formats for these time-related displays by using the drop-down arrow.

   - **Duration fields**
   - **Time zone**

     Note: You must choose your time zone to get local time.

5. If you want to reset the time-related displays to default settings, click **Reset for Time.** (The bottom **Reset** button resets all the tabbed pages to default settings.)
6. Click **Apply** to save settings.

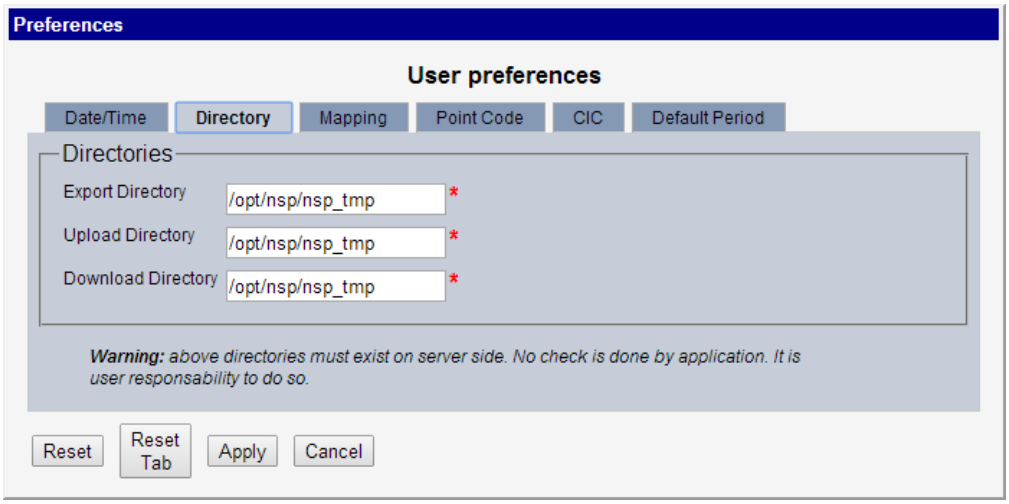
Setting Directory Preferences

Use the User Preferences feature to set the Export, Upload and Download directory paths for your system. These paths define where xDR's, dictionary files and other elements are stored.

Follow these steps to set the directory preferences.

1. Click *User Preferences* on the Application board. The User Preferences page is displayed**.**
2. Click the directory tab**.**
   The directory page is displayed. The red asterix denotes field

Figure 3: Directory Page



3. Type in the following:

- *Export directory*
- *Upload directory*
- *Download directory*

4. If you want to reset the directories to default settings, click "*Reset for Directory".* (The bottom *Reset* button resets all the tabbed pages to default settings.)
5. Click *Apply* to save your settings.

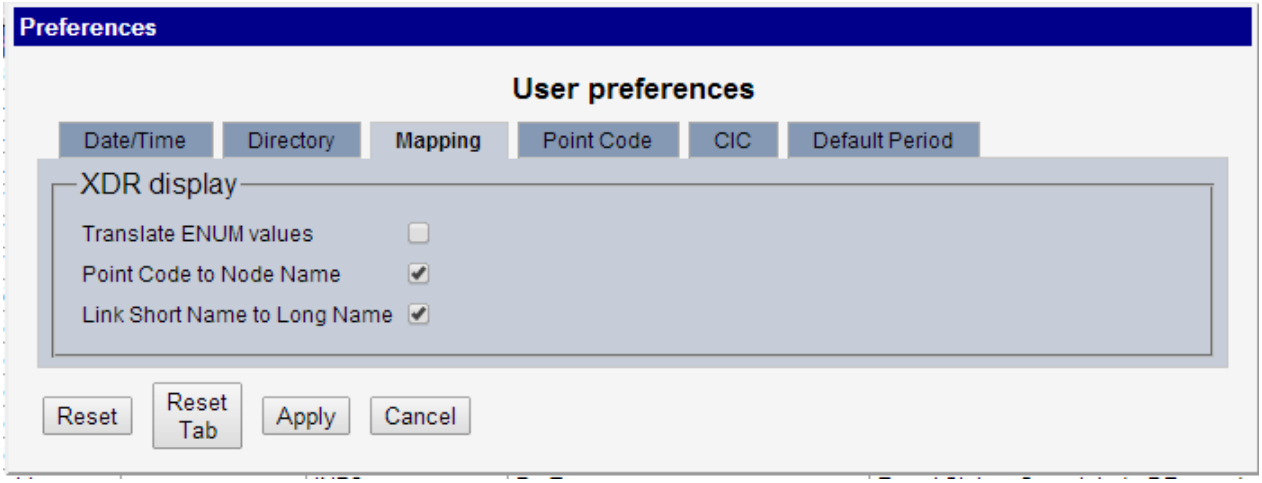
Setting Mapping Preferences

You can set the Mapping settings using the User Preferences feature.
Follow these steps to set Mapping preferences.

1. Click *User Preferences* in the Application board. The User Preferences page is displayed.

2. Click the *Mapping* tab. The Mapping page is displayed.

Figure 4: Mapping Page



3. Check Translate ENUM v***alues*** to display text instead of numerals.

4. Enumeration is used by xDRs to display text values instead of numeric. (For example, rather than showing the numeral for Alarm Severity, the user interface will show the actual word, such as "Major" or "Critical.")

5. Check ***Point Code to Node Name*** to display the custom (user-defined) name of the node. Otherwise, the Point Code value is displayed.

6. Check ***Link Short Name to Long Name*** to display the custom (user-defined) link name or the Eagle link name. Otherwise, the short name is displayed, which is the name that begins with an asterisk(*).

7. To reset the Mapping values to the default, click ***Reset for Enumeration.*** (The bottom ***Reset*** button resets all the tabbed pages to default settings.)

6. Click ***Apply*** to save the changes**.**

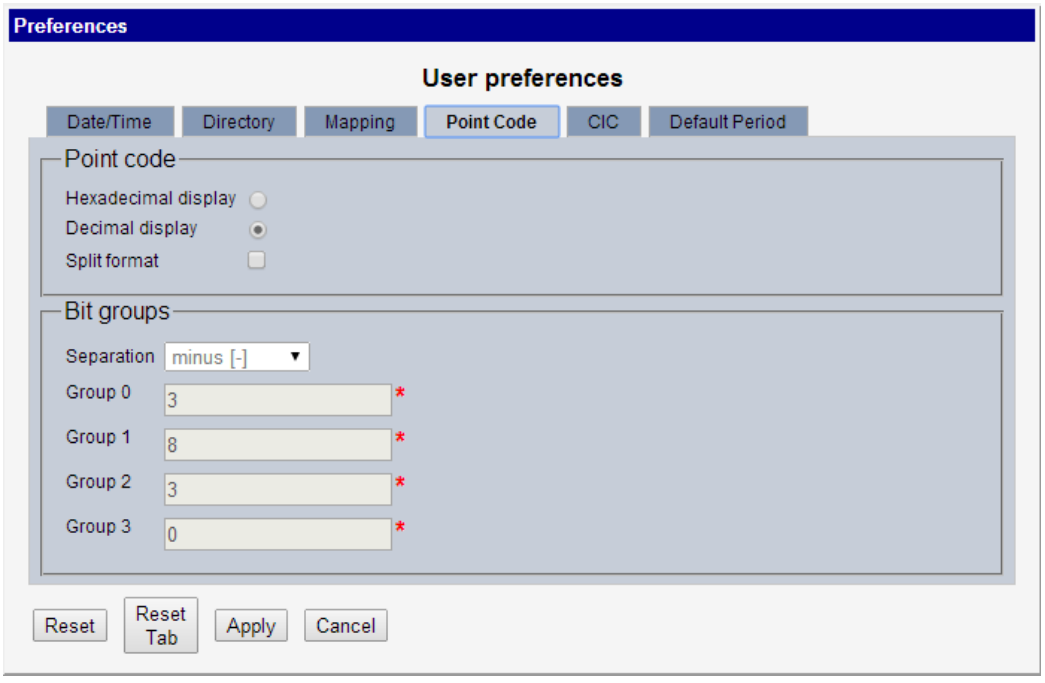
Setting Point Code Preferences

The User Preferences feature enables you to set the Point Code preferences for your system. A Point Code is a unique address for a node (Signaling Point), used to identify the destination of a message signal unit (MSU).
Follow these steps to set the Point Code preferences.

1. Click ***User Preferences*** in the Application board. The User Preferences page is displayed.

2. Click the ***Point Code*** tab.The Point Code page is displayed. The red asterisk denotes a required field.

Figure 5: Point Code Tab



3. Select either *Hexadecimal display* or *Decimal display.*
4. Select or de-select *Split format.*
   If *Split format* is checked, the Bit groups settings in the box below are active. If *Split format* is not checked, Bit groups settings are not applicable.
5. If you selected Split format above, go to the next step. If you did not select Split format, go to 13.

6. In the Bit groups panel, use the drop-down box to select the *Separation* type .
7. Type in values for *Groups 0-3.*
8. To reset the point code preferences to default settings, click *Reset for Point code.* (The bottom *Reset* button resets all the tabbed pages to default settings.)
9. Click *Apply* to save your settings.

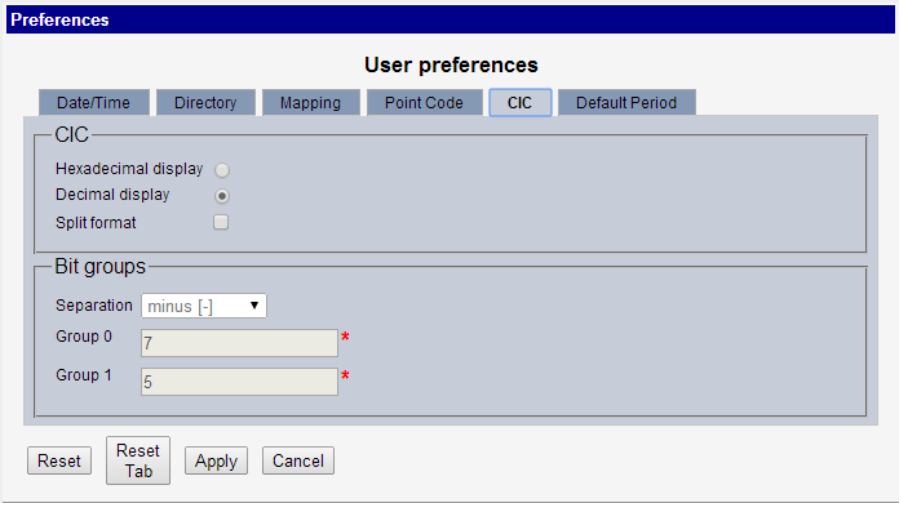
Setting CIC Preferences

The Circuit Identification Code (CIC) provides a way to identify which circuit is used by the Message Signaling Unit (MSU). This is important in ProTrace applications. Use the User Preferences feature to set the CIC settings for your system.

Complete these steps to set the CIC preferences:

1. Click *User Preferences* in the Application board. The User preferences page is displayed.
2. Click the *CIC* tab. The CIC page is displayed. The red asterisk denotes a

Figure 6: CIC Tab



3. Select either *Hexadecimal display* or *Decimal display.*
4. Select or de-select *Split format.*
   If *Split format* is checked, the Bit groups settings in the box below are active. If *Split format* is not checked, Bit groups settings are not applicable.
5. If you selected Split format above, go to the next step. If you did not select Split format, go to *14*.
6. In the Bit groups panel, use the drop-down box to select *Separation* type..
7. Type in values for *Group 0* and *Group 1.*

8. If you want to reset CIC preferences to the default, click *Reset for CIC.* (The bottom *Reset* button resets all the tabbed pages to default settings.)
9. Click *Apply* to save your settings.

PIC Documentation Library

PIC customer documentation and online help are created whenever significant changes are made that affect system operation or configuration. Revised editions of the documentation and online help are distributed and installed on the customer system. Consult your NSP Installation Manual for details on how to update user documentation. Additionally, all customer documentation is available on the Oracle Technology Network (OTN). Release Notes are available on OTN with each new release of software. The Release Notes list the PRs that have been resolved in the current release and the PRs that are known to exist in the current release.

Listed below is the entire PIC documentation library of User's Guides.

- Security Guide
- NSP Security User's Guide
- Alarm Forwarding Administrator's Guide
- ProAlarm Viewer User's Guide
- ProAlarm Configuration User's Guide
- Centralized Configuration Manager Administrator's Guide
- Customer Care User's Guide
- ProTraq User's Guide
- ProPerf User's Guide
- ProPerf Configuration User's Guide
- System Alarms User's Guide
- ProTrace User's Guide
- Data Feed Export User's Guide
- Audit Viewer Administrator's Guide
- ProDiag User's Guide
- SigTran ProDiag User's Guide
- Reference Data User's Guide
- Exported Files User's Guide
- Scheduler User's Guide
- Quick Start User's Guide

Chapter 2: Introducing Audit Viewer

Topics:

About Audit Viewer - Overview

Audit Viewer is a specific-purpose application which is part of the NSP Toolbox. This system allows the NSP *Monitoring Manager* to view logged user activities. The tool stores user-audit data for the previous four months.

Audit Viewer Functionality

Audit Viewer supports the following functions:

- Listing audit records - The records contain date and time, user login, NSP application, problem severity and message information.
- Exporting audit records - Displayed audit logs are exportable in CSV and other formats.

Chapter 3: Getting Started With Audit Viewer

Topics:

Accessing and logging into NSP

To access and log into NSP, follow these steps:

1. Open your Web browser.
2. In the Address bar, type the following **Uniform Resource Locator (URL)** for NSP: **http://nspserver/nsp** , where the nspserver is the IP address of NSP.

   Note: NSP only supports versions of IE 7.0 or later and Firefox 3.6 or later. Before using NSP, turn off the browser pop up blocker for the NSP site.

   The NSP login screen opens.

   Note: Before you can start NSP, you must first have a userid and password assigned to you by your NSP system administrator.

3. Type your **username** assigned to you in the *Username* field.
4. Type your **password** in the *Password* field.
5. Click **OK.**

   The NSP *Application Board* opens.

6. Click on the *Audit Viewer* icon to open the application.

Opening Audit Viewer

Click on the ***Audit Viewer icon.*** The *Audit Viewer* home page opens with a list of audit records shown below.

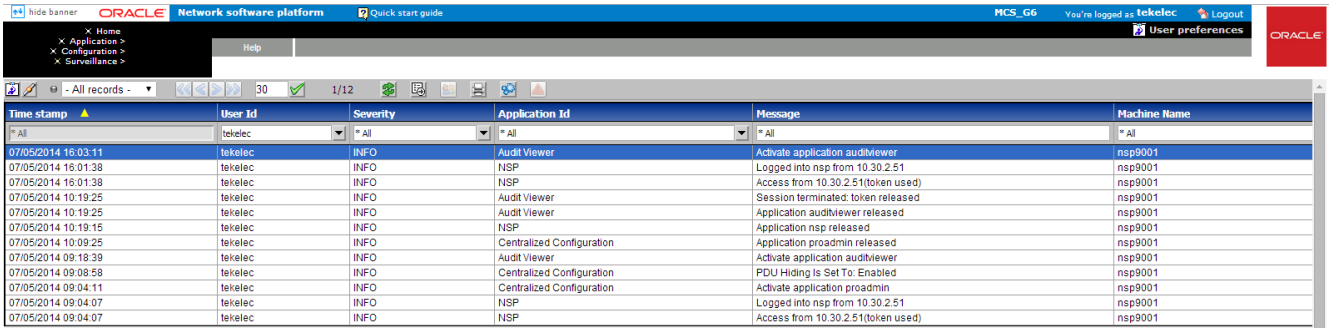


Figure 7: *Audit Viewer* Home Page

The *Audit Viewer* home page shown in Figure 9 consists of two parts, a table of logged user activities and a tool bar. The tool bar contains icons for managing the display of groups of records in the table. The Auditviewer table contains the logged records of last 24 hours of user activity. User can view older records by *Using the Execute Query Dialog to filter Audit Viewer Records.*

Note: Do not use the Function Keys (F1 through F12) when using the NSP. Function keys work in unexpected ways. For example, the F1 key will not open NSP 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.

User Activity Table

The table consists of eight headings:

- Log Time stamp - The time and date the log record was generated by the NSP system.
- User Id - Name of user defined in NSP database
- Log Severity - Relative importance of the log record: Fatal, Error, Warn, Info and Debug.
- Application ID - PIC system component for example NSP
- Message - Log record information line.
- Machine Name - Network ID of the affected server.

The default display order for records is based on *Log Time stamps* from most-recent-to-oldest. Clicking the column heading reverses the sort order. Selecting the column heading again toggles back to the default order. Other columns also can be used as sort criteria. Clicking on a column heading the first time puts the records in alphabetical order. Clicking again toggles to the reverse alphabetical order. In all cases an arrowhead symbol in one of the column headings defines the column which controls the sort and whether the sort is first-to-last or last-to-first.

Tool Bar

The tool bar contains icons used to scroll up and down through lists of records larger than the display can accommodate in a single page, to sort or filter records in the table according to various criteria, and to count records on demand.

Toolbar

The toolbar has the following function buttons:

 Execute Query - enables you to create and execute queries on the data records.

 Export - enables you to export sessions using a variety of formats.

 Refresh -enables you to refresh the current screen to see all recent changes.

 First Page**-** clicking this button opens the first page of logs.

 Previous Page – clicking this button opens the previous page of logs.

 Next Page - clicking this button opens the next page of logs.

 Last Page - clicking this button opens the last page of logs.

 Set Size – use this button to set the session list size from 10-500 per page.

 Message Details – use this button to see the whole message after selecting the row whose message needs to be displayed to user

Chapter 4: Filtering Audit Viewer Records and Viewing Message Details

Topics

Overview

This chapter covers:

- The method for selecting subsets of *Audit Viewer* records using *Quick filters* in the tool bar.
- The method for selecting subsets of *Audit Viewer* records using Filter in the tool bar.

Using Quick filters to select Audit Viewer Records

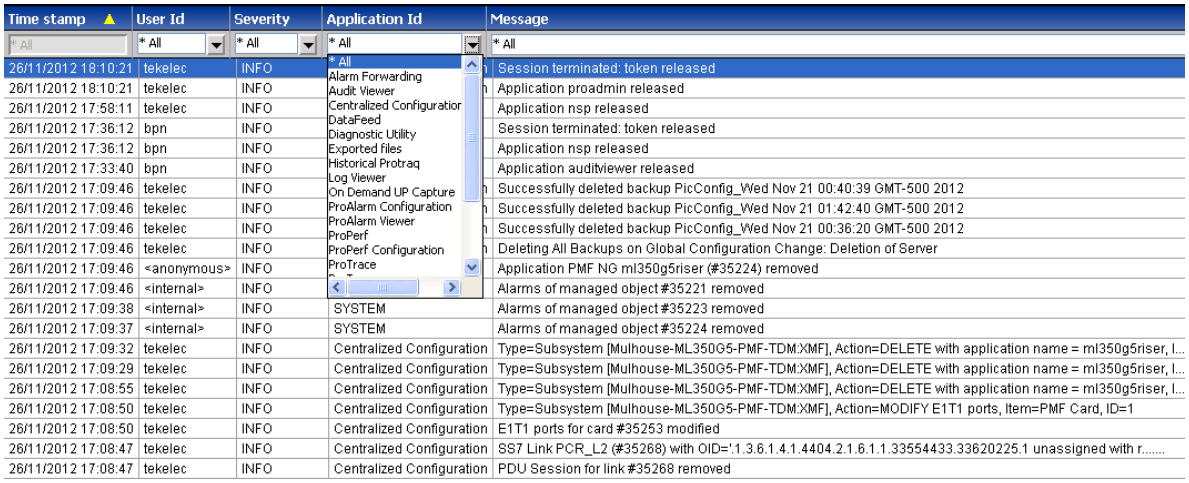
The fastest way to locate and display records is to use the *Quick filters* option in the toolbar. The figure below shows, there are three criteria: User Id, Severity, Application Id. Any criterion or combination of criteria can be used for the search.

Figure 8: Quick Filters Tool Bar Option

1. Select the **application criterion.**

The *Application* window in the tool bar is a pulldown menu for selecting the NSP application whose user activities you want to view. The figure below shows the application choices.

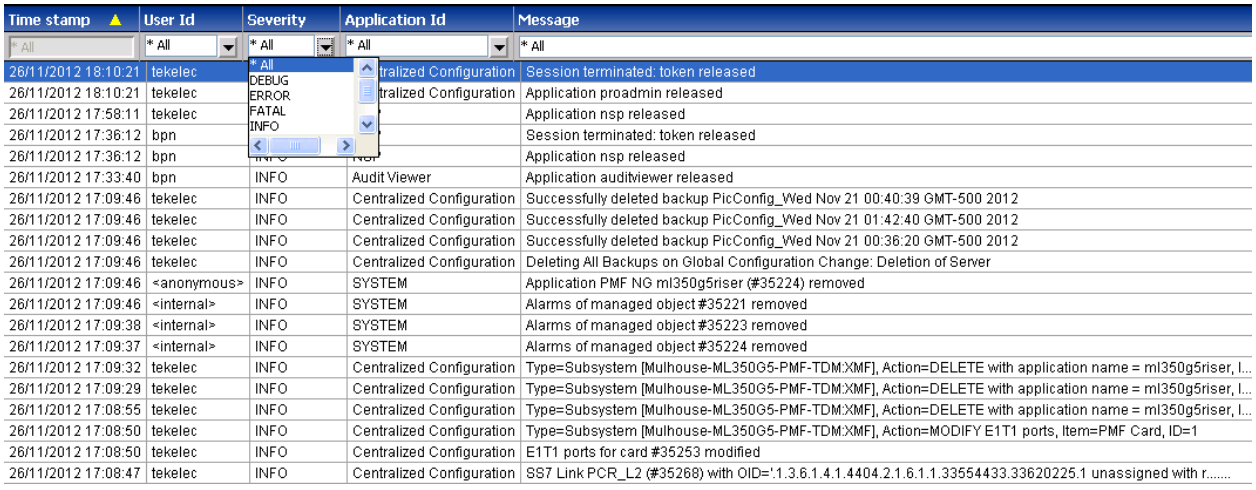
Figure 9: *Application* Window



2. Select **severity criterion.**

The *Severity* window's pulldown menu identifies the priority to use for the search. The figure below shows the options.

Figure 10: Severity Window



The hierarchy of severity is in the following order - top to bottom as follows:

a) Fatal
b) Error
c) Warning

d) Info

e) Debug

3. Select **user criterion.**

The *User* window pulldown menu lists the users eligible to be filtering criteria. The figure below shows an example of user criterion.

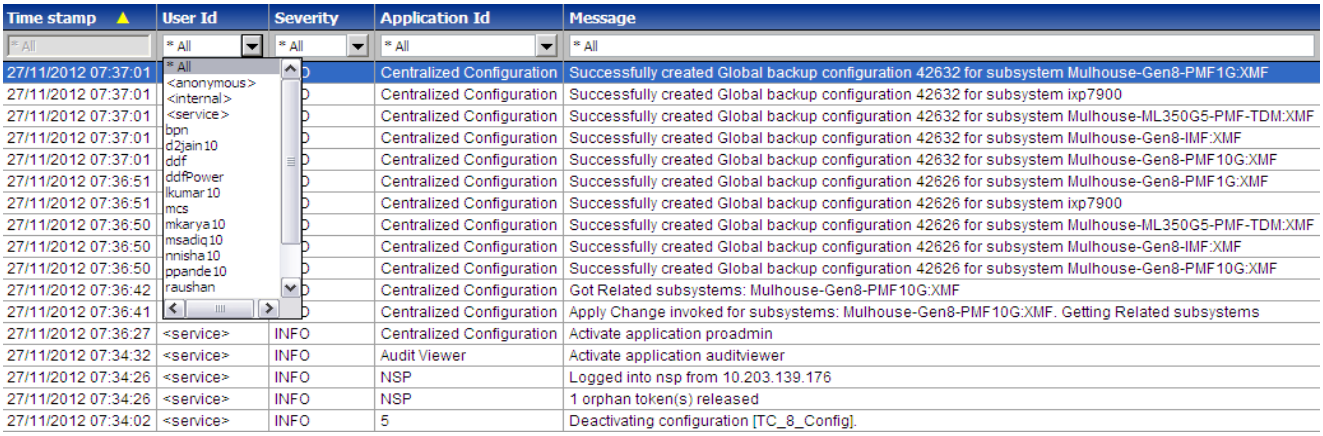


Figure 11: User Window

Note: You can select *any combination of the three* options in each pull down menu and apply filters on the records to be seen in the screen.

The figure below shows a result based on all three criteria. The *green field* in the tool bar indicates that filtering is active. The number of records per screen and the total number of records in the filtered list appear in the upper row of the tool bar.

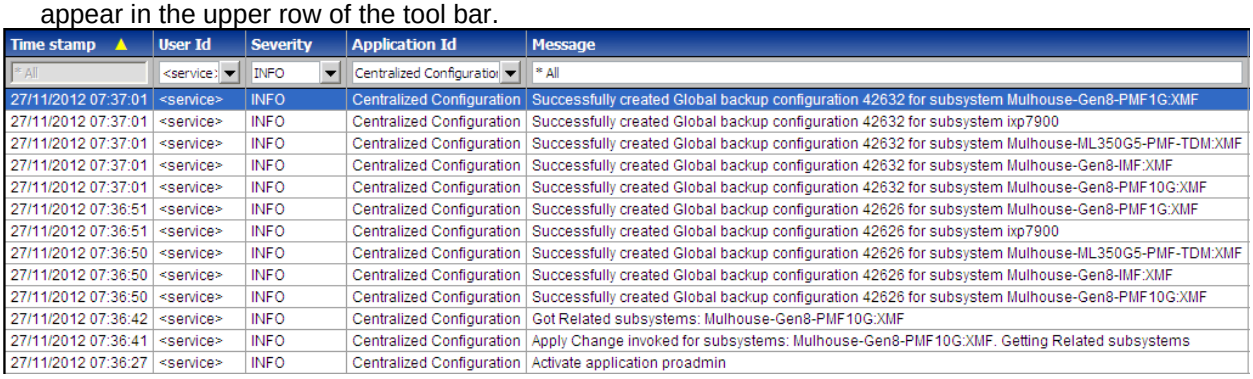


Figure 12: Filtered List Using All Three Criteria

Using the Execute Query Dialog to filter Audit Viewer Records

You can also filter records based on key criteria of timestamp using the execute query functionality. To filter records, perform the following steps:

1. Click the **execute query** button, the query setting dialog opens shown in *Figure 13: Query Setting Dialog Box*.

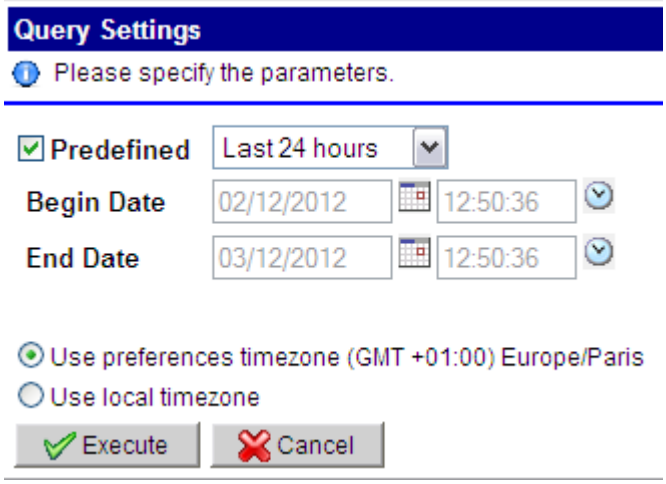


Figure 13: Query Setting Dialog Box

2. If user want to see the records for last few minutes or hours then user can select this option by selecting PREDEFINED checkbox then the dropdown associated to it becomes active.

3. The dropdown contains various items like Last 5 minutes, Last 10 minutes etc. When user select any of this item records which are logged for that time are displayed to user. Last 24 hours is default selected in the dropdown.

While selecting the predefined option, the list which appears in the drop down is shown in *Figure 14: Dropdown present in Query Setting Dialog Box* and

Figure 14: Dropdown present in Query Setting Dialog Box

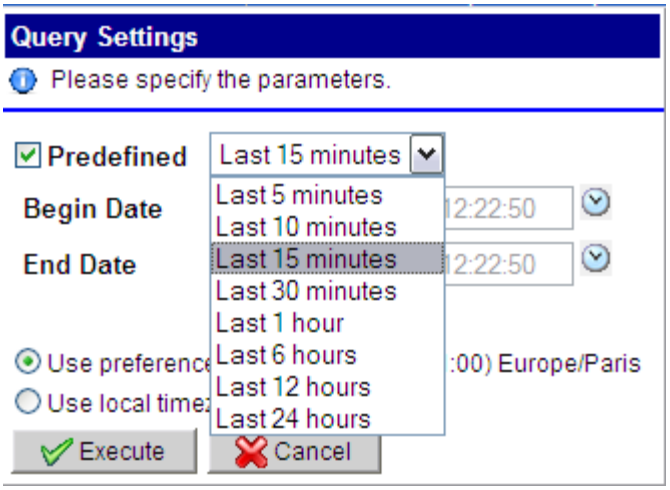
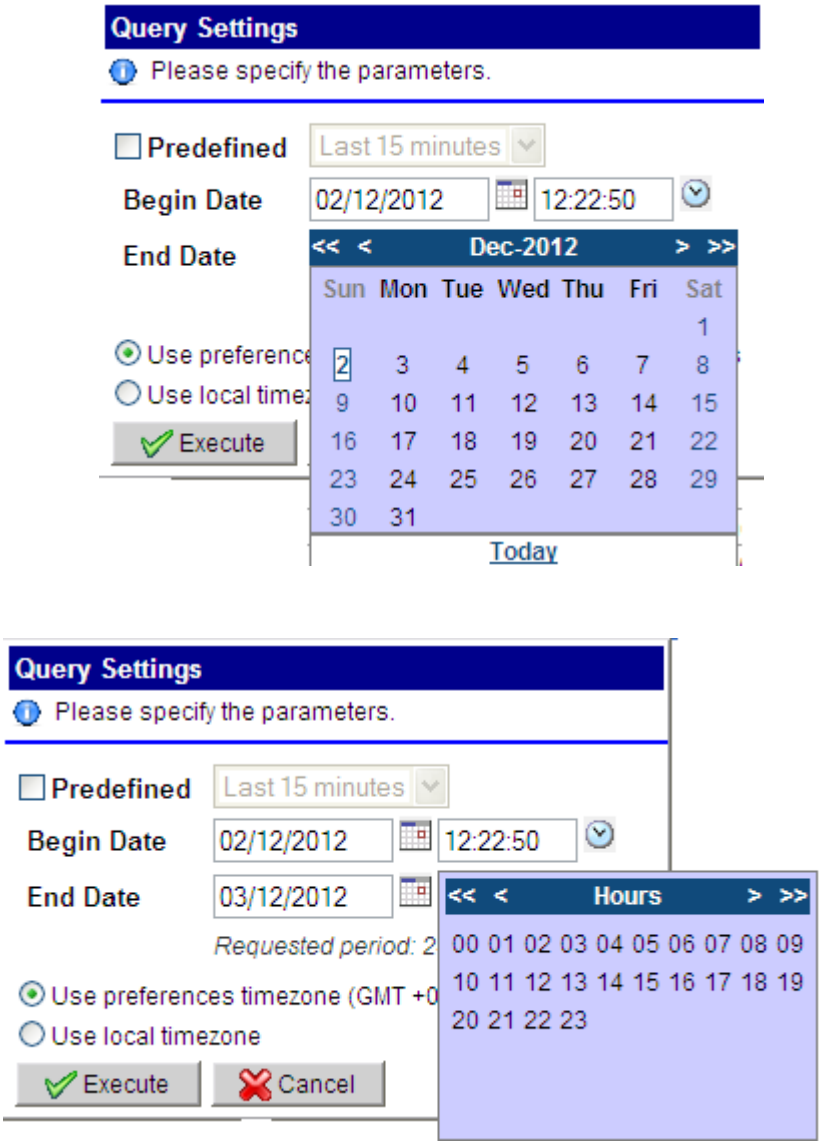


Figure 15: Selecting date and time for Begin or End Date Option in Query Setting Dialog Box



4. User can himself select the begin date and end date from the dialog box. The records logged between this time period is shown on the screen.

5. User can select between the User preferences timezone and local timezone by selecting any of the two radio buttons.

6. When user clicks on the Execute Button the query is executed and list is populated with records as desired by the end user.

Viewing Message Details

In message column of the Auditviewer logs list is the column which depicts the details of the message associated with the log. This message can be very long sometime. Hence long messages are truncated and followed by dots. If user wants to see the details of such messages then he needs to select that row in the table and then click Message Details button.

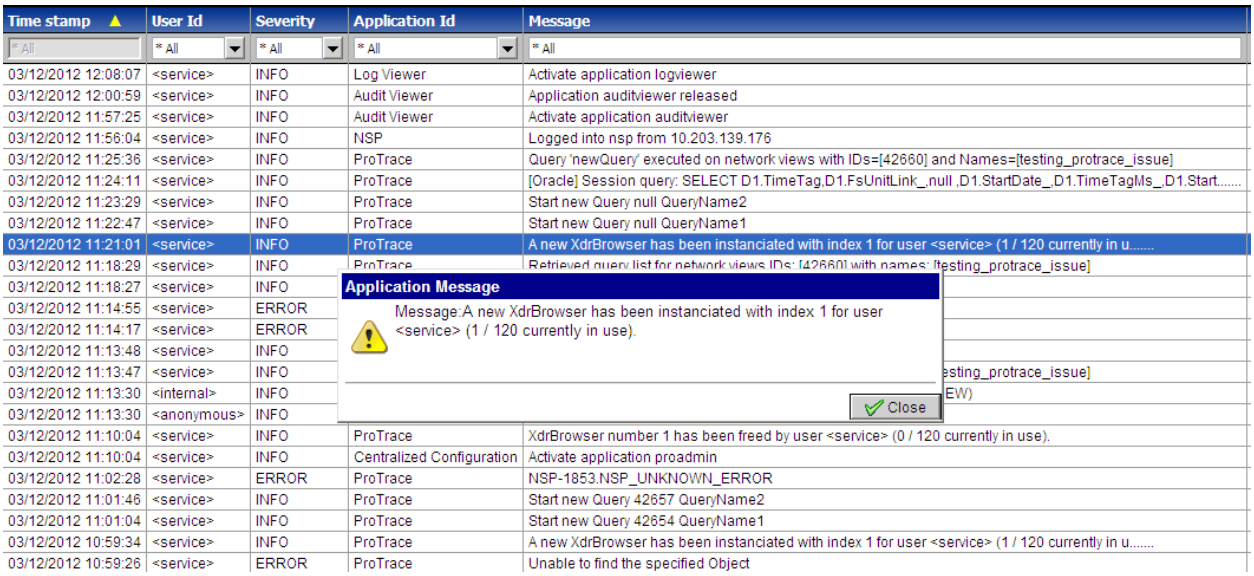


Figure 16: Message Details Dialog

For rows in which complete message is visible in the row, Message Details button remains inactive.

Chapter

5

Chapter 5: Viewing User Activity

Topics:

About tracking user Activities

The following table provides information for tracking user activity using Audit Viewer. The tables show the following information for each message tracked by the user:

- Application
- Component
- Functionality
- Message

Table 1 : User's Activity For Application, Component And Function

Application	Component	Functionality	Message
ProAlarm Viewer	Map	List, Execute	Map # <ID> opened Map # <ID> closed
	Alarm list	Terminate an alarm	Cleared alarmID=<ID>
			Alarm #<ID> acknowledged
			Alarm #<ID>unacknowledged
			Alarm #<ID> commented
			Alarm #<ID> terminated
			Alarms of managed object #<MOD_ID> removed
			Comment #<COMMENT_ID> updated
			Failed to terminate alarms on application server
			Failed to acknowledge alarms on application server
			Failed to comment alarms on application server!
ProTrace	Query List	List	List of queries = Query list retrieved for network viewID = <>
		Create	QueryID=<>, Name=<> created
		Modify	QueryID=<>, Name=<> modified
		Delete	QueryID=<> deleted
	xDR Browsing	Start	<query name> executed on networks views IDs=<> Names=<>
	Trace	Start	Trace started on network views IDs=<> Names=<>
		Export	User exported trace in HTML format
			User exported trace in binary format
		Import	User imported trace
ProDiag	NA	Start	[Table/Chart] monitoring started on [link status/state/...] counts on following elements: []
		Reset	User reset elements with ids: []
		Export	User exported monitoring data inCSV format
			User exported monitoring data in PNG format
		Import	User imported trace

ProDiag	NA	Start	[Table/Chart] monitoring started on [link status/state/...] counts on following elements: []
		Reset	User reset elements with ids: []
		Export	User exported monitoring data inCSV format
			User exported monitoring data in PNG format

Table 2 : User Activity Chart - Centralized Configuration Manager

Application	Component	Functionality	Message
ProAlarm configuration	ProAlarmConfiguration	All	Activate application ALRMapconfig
Alarm Forwarding	Filter	Add, Modify, Remove	Alarm forwarding filtering rules changed
	Destination	Configure	Alarm forwarding destination settings changed
xDR Browser	Schedule	Stop	-XDR EXPORT- : Stops scheduled export : <JOB_NAME> --> output file : <FILENAME>
		Start	-XDR EXPORT- : Starts scheduled export : <JOB_NAME> --> output file : <FILENAME>
		Edit, Add, Delete	Edit the task <JOB_NAME> (<JOB_GROUP>)
ProTraq	StatConfiguration	Create	Configuration <NAME> (#<ID>) created
		Update	Configuration <CONFIG_NAME> (#<CONFIG_ID>) modified (corner filter created)
		Update (corner	Configuration <NAME> (#<ID>) modified (corner filter created)
		filter)	Configuration <NAME> (#<ID>) modified (corner filter updated)
		Update (columns)	Configuration <NAME> (#<ID>) modified (column filter "+_columnName+" created)
			Configuration <NAME> (#<ID>) modified (column filter <COLUMN_NAME> removed)
			Configuration <NAME> (#<ID>) modified (order of column filters)
		Update (lines)	Configuration <NAME> (#<ID>) modified (line filter "+_lineName+" created)
			Configuration <NAME> (#<ID>) modified (line filter "+_lineName+" updated)
			Configuration <NAME> (#<ID>) modified (line filter "+lineName+" removed)
			Configuration <NAME> (#<ID>) modified (order of line filters)
		Update (alarms)	Alarm on configuration <NAME> (#<ID>) for line <LINE_NAME>and column
			<COLUMN_NAME>created
			Alarm on configuration <NAME> (#<ID>) for

			line <LINE_NAME>and column
			<COLUMN_NAME>updated
			Alarm on configuration <NAME> (#<ID>) for line <LINE_NAME>and column
			<COLUMN_NAME>removed
		Delete	Configuration <NAME> (#<ID>) removed
	Configuration	Set	Instance of DSE configuration <NAME> (#<ID>) on session <SESSION_NAME> created
	applying		
		Activate	Instance of DSE configuration <NAME> (#<ID>) on session
			<SESSION_NAME>activated
		Deactivate	Instance of DSE configuration <NAME> (#<ID>) on session
			<SESSION_NAME>deactivated
		Delete	Instance of DSE configuration <NAME> (#<ID>) on session
			<SESSION_NAME>removed
	Schedule	NA	Creating Historical Task
			Getting Historical Task status
			Deleting Historical Task
ProPerf	Dashboard view	List, Execute	Display dashboard <NAME> (#<ID>)
ProPerlConfiguration	Dashboard	Create,	Dashboard <NAME> (#<ID>) created
		Remove,	Dashboard <NAME> (#<ID>) removed
		Update	Dashboard <NAME> (#<ID>) updated
			Panel <NAME> (#<ID>) added to Dashboard #<DASHBOARD_ID>
			Panel <NAME> (#<ID>) updated
			Panel <NAME> (#<ID>) removed
			KPI <NAME> (#<ID>) added to Panel #<PANEL_ID>
			KPI <NAME> (#<ID>) updated
			KPI <NAME> (#<ID>) removed
Datafeed	NA	NA	DataFeed <feedId> created. Name=<feedName>, Session Name=<feedSessionName>, Start Time=<feedStartTime>,Filter Name=<feedFilterName>, Period Length=<feedPeriodLength>
			DataFeed <feedId> modified. Name=<feedName>, Session Name=<feedSessionName>, Start Time=<feedStartTime>,Filter Name=<feedFilterName>, Period Length=<feedPeriodLength>
			DataFeed <feedId> deleted. Name=<feedName>, Session Name=<feedSessionName>, Start Time=<feedStartTime>,Filter

			Name=<feedFilterName>, Period Length=<feedPeriodLength>
			DataFeed <feedId> activated. Name=<feedName>, Session Name=<feedSessionName>, Start Time=<feedStartTime>,Filter Name=<feedFilterName>, Period Length=<feedPeriodLength>
			DataFeed (#<feedId>) deactivated. Name=<feedName>, Session Name=<feedSessionName>, Start Time=<feedStartTime>,Filter Name=<feedFilterName>, Period Length=<feedPeriodLength>
ProAdmin	Network	NA	Node <NAME> (#<ID>) created
			Node <NAME> (#<ID>) updated
			Node #<ID> removed
			LegacySS7 SP <NAME> (#<ID>) with OID=<OID>
			LegacySS7 SP <NAME> (#<ID>) with OID=<OID>
			AssociateSS7 SP to new node <NAME> (noCLLI defined)
			AssociateSS7 SP to already existing node <NAME>
			AssociateSS7 SP to new Eagle node <CLLI>
			Negative Point code <PC>
			AssociateSS7 SP with Subsystem
			SS7 SP <NAME> created
			SS7 SP updated : node discovered name is <NAME>
			SS7 SP <NAME> updated
			NgSS7 SP : node discovered name is <NAME>
			NgSS7 SP <NAME> updated
			SS7 SP #<ID> deleted
			LegacyIMF Linkset <NAME> (#<ID>) with OID :<OID> updated
			Legacy PMF Linkset <NAME> (#<ID>) with
			OID :<OID> updated
			MSW <NAME> (#<ID>) with OID :"
			Linkset <NAME> (#<ID>) removed
			LegacyIMF Linkset <NAME> (#<ID>)
			removed
			Legacy PMF Linkset <NAME> (#<ID>)
			removed
			Linkset <NAME> (#<ID>) removed
			Link <NAME> associated to Site <SITE_NAME>
			Link <NAME>" with discovered name='<DICOVERED>
			Associated the link with application

			subsystem
			Eagle Linkset is already assigned to anIMF for monitoring
			Monitored links exceeds Max number of links allowed
			Eagle card <CARD> and port : <PORT>
			Eagle card #<CARD_ID> removed
			LegacySS7 Link <NAME> (#<ID>) with
			OID=<OID> removed
			LegacySS7 Link <NAME> (#<ID>) with OID=<OID> removed
			Monitored links exceeds Max number of links allowed
			SS7 Link <NAME> updated (discovered
			name=<DISCOVERED>
			SS7 Link <NAME> (#<ID>) removed
			SS7 SP <NAME> (#<ID>) removed
			SS7 Link #<LINK_ID> removed
			GPRSSP <NAME> (#<ID>) with OID=<OID> removed
			GPRSSP <NAME> with OID=<OID> updated
Application	**Component**	**Functionality**	**Message**
		Update (columns)	Configuration <NAME> (#<ID>) modified (column filter "+_columnName+" created)
			Configuration <NAME> (#<ID>) modified (column filter <COLUMN_NAME> removed)
			Configuration <NAME> (#<ID>) modified (order of column filters)
		Update (lines)	Configuration <NAME> (#<ID>) modified (line filter "+_lineName+" created)
			Configuration <NAME> (#<ID>) modified (line filter "+_lineName+" updated)
			Configuration <NAME> (#<ID>) modified (line filter "+lineName+" removed)
			Configuration <NAME> (#<ID>) modified (order of line filters)
		Update (alarms)	Alarm on configuration <NAME> (#<ID>) for line <LINE_NAME>and column <COLUMN_NAME>created
			Alarm on configuration <NAME> (#<ID>) for line <LINE_NAME>and column <COLUMN_NAME>updated
			Alarm on configuration <NAME> (#<ID>) for line <LINE_NAME>and column <COLUMN_NAME>removed
		Delete	Configuration <NAME> (#<ID>) removed
	Configuration applying	Set	Instance of DSE configuration <NAME> (#<ID>) on session <SESSION_NAME>

			created
		Activate	Instance of DSE configuration <NAME> (#<ID>) on session <SESSION_NAME>activated
		Deactivate	Instance of DSE configuration <NAME> (#<ID>) on session <SESSION_NAME>deactivated
		Delete	Instance of DSE configuration <NAME> (#<ID>) on session <SESSION_NAME>removed
	Schedule	NA	Creating Historical Task
			Cancelling Historical Task
			Deleting Historical Task

Application	Component	Functionality	Message
			GPRSSP #<ID> removed
			IP SP <NAME> (#<ID>) with OID=<OID> removed
			IP SP <NAME> with OID=<OID> updated
			IP SP #" + spId + " removed
			GbLink <NAME> (#<ID>) with OID=<OID> removed
			GbLink <NAME> with OID=<OID> updated
			GbLink Assignment forLink <NAME> (#<ID>)
			SS7 Link Assignment for <NAME> (#<ID>)
			SS7 Link <NAME> (#<ID>) with OID=<OID> removed
			SS7 Link <NAME> (#<ID>) with OID=<OID> updated
			GbLink <NAME> (#<ID>) with OID=<OID> removed
			GbLink <NAME> (#<ID>) with OID=<OID> updated
			GbLink #<LINK_ID> removed
			PDU Session #<ID> created
			PDU Session for link #<LINK_ID> removed
			PDU Session for linkset #<LINKSET_ID> and link #<LINK_ID> removed
			SP #<ID> upgraded
			Linkset #<ID> upgraded
			Link #<ID> upgraded
	View	NA	Session Network view <NAME> (#<ID>) created
			Link Network view <NAME> (#<ID>) created
			Network view #" <ID> removed
	Reference Data	Import	Invalid Direction category elements Data.
			Invalid Q850ISUP parameter Data
			Invalid Q708 Area Code parameter Data
			Invalid Q708 Country Code parameter Data

Application	Component	Functionality	Message
			Invalid Q850 parameters Data
			Invalid carrier network elements Data
			Invalid carrier category elements Data
			InvalidNPA Configuration elements Data
	System	NA	Application <TYPE> <NAME> (#<ID>) created
			DB Link <NAME>created
			Connection <NAME>created
			Host <NAME> (#<ID>) created
			Site <NAME> (#<ID>) created
			Application <TYPE> <NAME> (#<ID>) removed
			Host (#<ID>)removed
			Site (#<ID>) removed
			Application <TYPE> <NAME> (#<ID>) updated
			Host (#<ID>) updated
			Site <NAME> (#<ID>) updated
			RID group #<ID> removed
	XMF	NA	[XMF] ComboPDU filter <NAME>(#<ID>) created.
			[XMF] DlciPDU filter <NAME>(#<ID>) created.
			[XMF]GT PDU filter <NAME>(#<ID>) created.
			[XMF]IP PDU filter <NAME>(#<ID>) created.
			[XMF]PC PDU filter <NAME>(#<ID>) created.
			[XMF] Port filter <NAME>(#<ID>) created.
			[XMF] RawPDU filter <NAME>(#<ID>) created.
			[XMF]SSN PDU filter <NAME>(#<ID>) created.
			[XMF] VlanPDU filter<NAME>(#<ID>) created.
			[XMF]PDU Filter <NAME>(#<ID>) removed.

Application	Component	Functionality	Message
			[XMF] ComboPDU filter <NAME>(#<ID>) updated.
			[XMF] DlciPDU filter <NAME>(#<ID>) updated.
			[XMF]IP PDU filter <NAME>(#<ID>) updated.
			[XMF]PC PDU filter <NAME>(#<ID>)
			updated.
			[XMF] PortPDU filter <NAME>(#<ID>) updated.
			[XMF] RawPDU filter <NAME>(#<ID>)
			updated.
			[XMF]SSN PDU filter <NAME>(#<ID>)
			updated.
			[XMF] VlanPDU filter <NAME>(#<ID>)
			updated.
			[XMF] Pmf Card (#<ID>) with application name <NAME> and location <LOCATION> created.
			[XMF] PMF Card (#<ID>) updated with State <STATE>.
			[XMF] PMF Card #<ID> removed.
			[XMF] Port #<ID> and associated links created.
			[XMF] Port #<ID> and associated links removed.
			[XMF] E1T1 Port #<ID> removed.
			[XMF] Q752 counter #<NAME> modified.
			[XMF] EagleOAM Alarm number <NUMBER> disabled.
			[XMF] EagleOAM Alarm number <NUMBER> enabled.
			[XMF] Q752 Alarm <NAME> modified with AutoClear <VALUE>.
			[XMF] Q752 Alarm <NAME> is modified with
			Enable <ENABLE VALUE>.
			[XMF] Parameter (Long) <NAME> saved.
			[XMF] Parameter (String) <NAME> saved.
			[XMF] Parameter (Long) <NAME> removed.

.

Application	Component	Functionality	Message
			[XMF] Parameter (String) <NAME> removed.
			[XMF] Parameter <NAME> created.
			[XMF] Parameter <NAME> modified.
			[XMF] Parameter <NAME> removed.
			E1T1 ports for card #<ID> modified.
			E1T1 ports # <PORT NUMBERS> created.
			E1T1 ports for card #<ID> modified.
			Monitoring group <NAME>(#<ID>) created.
			Monitoring group <NAME> (#<ID>) updated.
			Monitoring group #<ID> removed.
	IXP	Discover	Error during XdrBuilder <NAME> <VERSION> discovery.
			XdrBuilder <NAME> <VERSION> discovered by user <USERNAME> during builder discovery.
			Deleted XDR Builder <NAME>.
			Cannot delete XDR Builder having id <ID>.
		Configure	Error while creating Ixp Config Migration Log forIXP - <SUBSYSTEM NAME>.
			Builder Parameter - Pdu Datasource - <STREAM NAME> is not routed to any xMF.
			NoHost IP found in Pdu DTS stream - <STREAM NAME>

Table 3 : User Activity - Security

Application	Component	Functionality	Message
Security	User	Create	User<USER_ID> created
		Update	User < USER_ID > updated
		Remove	User < USER_ID > removed
		Logout	Tokens invalidated by administrator.
	Role	Create	Role<ROLE_ID> created
		Update	Role < ROLE_ID > updated
		Remove	Role < ROLE_ID > removed
	Profile	Create	Profile <PROFILE_ID> created
		Update	Profile <PROFILE_ID> updated
		Remove	Profile <PROFILE_ID> removed
	Objects	Owner	Change object owner from <OLD_OWNER> to <NEW_OWNER>
			Change owner to <OWNER> for <N> object(s)
	Other actions	Access level	Access level set to<ACCESS_LEVEL>
		Purchased token	Purchased token set to <TOKEN_LIMIT>
		Security notice	Security warning text at login modified
NSP Core	NA	Login	Logged into NSP Access denied : No more available token Access denied : Too many tokens used by this user Access denied : SERVICE access level required Access denied : RESTRICTED access level required Access denied : logout by administrator
		Logout	Logout requested
		Navigate	Activate application <APPLICATION_NAME> Application <APPLICATION_NAME> released

Chapter 6: Exporting Audit Records

Topics :

Overview

This chapter provides a procedure for exporting audit records from the NSP to remote systems in one of five selectable formats: CSV, HTML, XML, TXT, XLS.

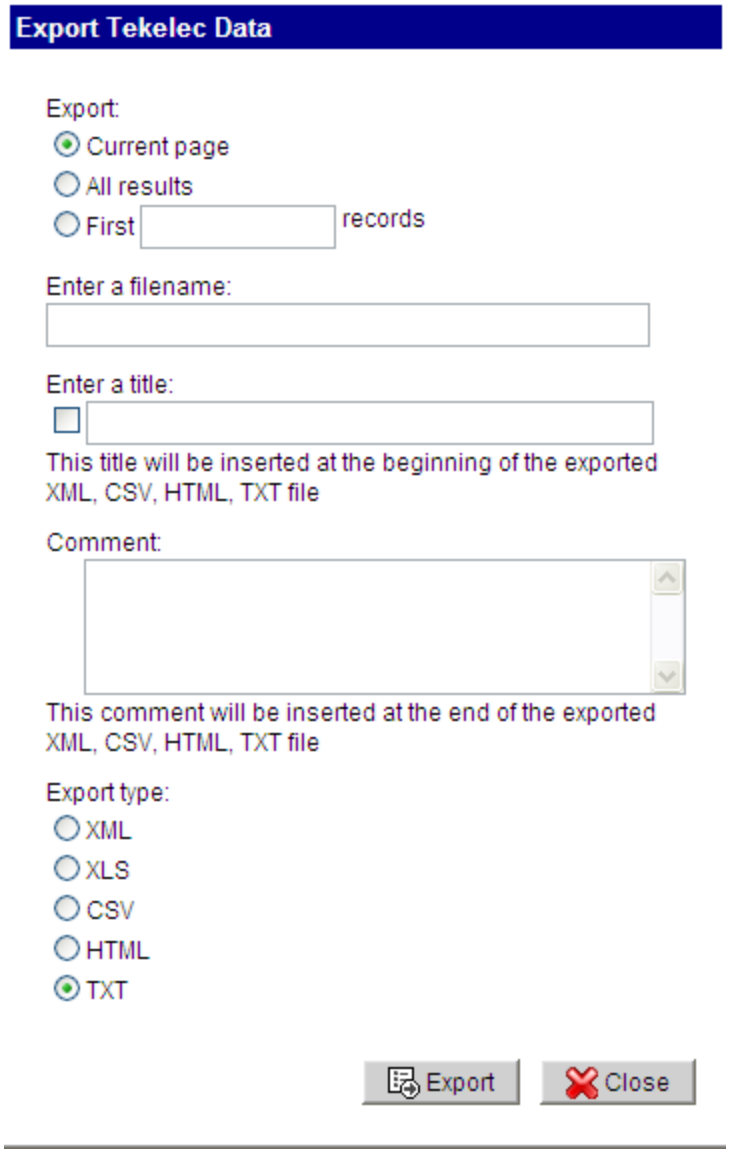
How to export audit Records

This procedure gives you a way to export audit records in comma separated variable (CSV) format or in one of four other standard data formats. The result file contains only visible records; active filters are taken into account.

1. Click **Export.**

The *Export Tekelec data* window opens shown below.

Figure 17 : Export Tekelec Data Window



.

3. Select the **Export** type located in the *Choice of data* section of the screen. You can select:

   a) Current Page
   b) All results
   c) First *blank* records (the number of records you want to export).

4. Enter **file name**
5. (Optional) Enter any **comments** that are related to the export file.
6. Select the **Export type** from the formats

provided. You have the option to select

a) XML format
b) CSV format
c) HTML format
d) TXT (text) format

7. Click **Export** to start the file transfer.

   An export status widget appears at the top of the table on the screen shown below.

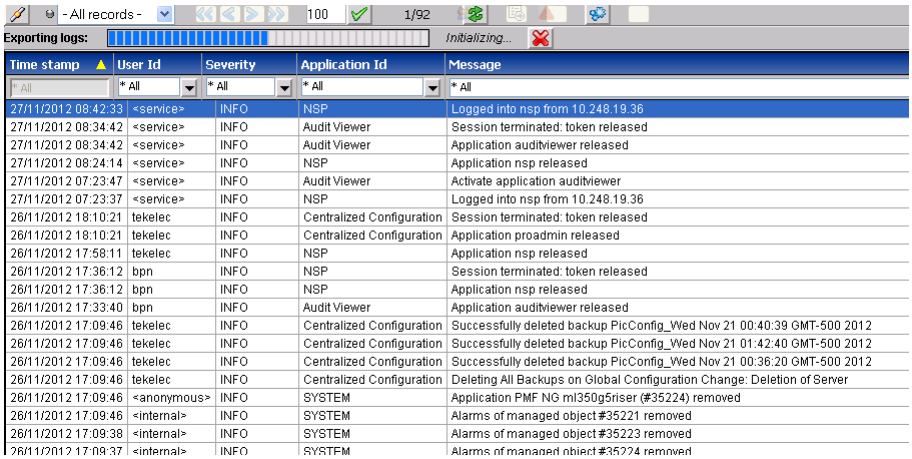


Figure 18 : Export Status formatting page

There is a progress bar showing the percentage of the data exported.

Stopping the export Process

To stop the export process, click **Cancel** button which appears along in export status widget. The export is stopped.

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 customer documentation is available on the web at the Oracle Technology Network (OTN) 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. Log into the Oracle Technology Network site at http://docs.oracle.com.

2. Under Industries, click the link for Oracle Communications documentation.

The Oracle Communications Documentation window opens with Tekelec shown near the top.

3. Click Oracle Communications Documentation for Tekelec Products.

4. Navigate to your Product and then the Release Number, and click the View link (the Download link will retrieve the entire documentation set).

5. To download a file to your location, right-click the PDF link and select Save Target As.