Oracle® Communications Performance Intelligence Center

Quick Start User Guide

Release 9.0

February 2014

Oracle Communications Performance Intelligence Center Quick Start User Guide, Release 9.0

Table of Contents

Chapter 1 About This Help Text 7

Scope and Audience.. 8

About the Performance Intelligence Center 8

Java Runtime settings 9

Setting User Preferences.. 9

Customer Care Center 17

PIC Documentation Library.. 19

Locate Product Documentation on the Customer Support Site.. 20

Chapter 2 Setting Up a Basic System 21

Basic Workflow.. 22

Creating a Site.. 23

Virtual IP Address Assignment 23

Adding an IMF Subsystem to a Site.. 24

About Monitoring Groups (IMF) 26

About Associations (IMF) 28

About PDU Dataflows.. 29

Adding a PMF Subsystem to a Site.. 33

Adding an E1/T1 (SPAN) Card (PMF) 36

About Traffic Classifications (PMF).. 38

Adding a GPRS Gb Dataflow 40

Adding an IXP Subsystem to a Site 40

Monitoring xDRs and PDUs with ProTrace 46

Opensource notice 47

List of Figures

Figure 1: PIC Overview 7
Figure 2: Time Formatting Page 8
Figure 3: Directory Page 9
Figure 4: Mapping Page 10
Figure 5: Point Code Tab 11
Figure 6: CIC Page 12
Figure 7: Alarms Page 13
Figure 8: Privacy Page 14
Figure 9: Verification Screen - Done Button Not Shown 22
Figure 10: Results Summary Screen - Host Tab 23
Figure 11: Results Summary Screen - Application Tab 23
Figure 12: Results Summary Screen - Network Element Discovery 23
Figure 13: SS7 Dataflow List Screen 27
Figure 14: Direction, Service Indicator, Filter & Truncation Details Screen 27
Figure 15: Monitored Linkset Details Screen 29
Figure 16: SS7 Linkset Selector Filter Screen 29
Figure 17: IP Dataflow List Screen 30
Figure 18: IP Data Flow Add Screen 30
Figure 19: IP Dataflow Associations Selector Screen 30
Figure 20: PMF Results Summary Screen 32
Figure 21: Discovery Summary Screen - Hosts Tab 32
Figure 22: Discovery Summary Screen - Application Tab 32
Figure 23: Discovery Summary Screen - PMF Card Discovery 33
Figure 24: Add Card Screen 33
Figure 25: Span Card Screen with Unconfigured Ports 34
Figure 26: Span Card Configure Screen with Channel Link Mapping Section 34
Figure 27: Span Card Configure Screen with Channel Link Mapping Add Screen 35
Figure 28: Span Card Configure Screen with Channel Link Mapping Add Screen 35
Figure 29: Subsystem Results Summary Screen 39
Figure 30: Results Summary Screen With Error Symbol 39
Figure 31: Object Tree Showing Added Subsystem With Results Screen 40
Figure 32: xDR Dataflow Assistant Initial Screen-PDU Sources 41
Figure 33: Dataflow Assistant xDR Builder Selection 41
Figure 34: xDR Assistant - Enrichment Selection 42
Figure 35: xDR Assistant - Configuring Sessions Screen 42

List of Tables

Table 1: xMF Subsystem Add Screen Field Descriptions 21
Table 3: Direction, Service Indicator, Filter & Truncation Details of SS7 Dataflow Screen Fields 28
Table 4: xMF Subsystem Add Screen Field Descriptions 31
Table 5: IXP Subsystem Add Screen Field Descriptions 38

Chapter 1

About This Help Text

Topics:

Scope and Audience 6

About the Performance Intelligence Center 6

Customer Care Center 14

PIC Documentation Library 16

Locate Product Documentation on the Customer Support Site 17

Scope and Audience

This guide is designed to assist those users (individuals with roles NSPConfigManager, NSPAdministrator) to set up a basic system configuration using Centralized Configuration Manager (CCM) and be able to monitor traffic (xDRs and PDUs) using ProTrace. All basic procedures are described in this guide along with key concepts about using CCM to configure a system.

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 Administration Guide. This is a graphic overview of the PIC system.

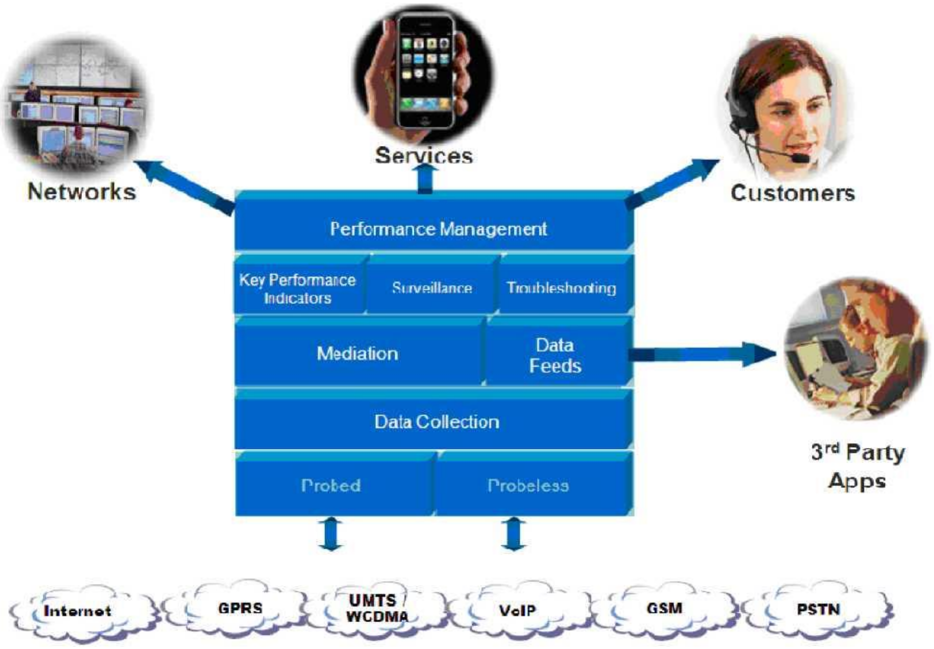


Figure 1: PIC Overview

Java Runtime settings

User has to Configure workstation Java plug-in for ProAlarm:

- Update to the latest JRE (**version 7 update 51 or later**)
- Configure Runtime parameters
  a) Go to **Start Menu ➤ Control Panel ➤ Java**
  b) Select the **Java tab** and click on **View** button
  c) Here, you will find Java Runtime parametersremove any memory parameter (-Xmx or –Xms)
- As security rules have been enforced in order to run applets (ProAlarm config), configure Exception Site List in Security parameters
  a) Go to **Start Menu ➤ Control Panel ➤ Java**
  b) Select the **Security tab**
  c) Click on **Edit Site List ➤ Add**
  d) Enter NSP URL like *https://<NSP_IP*>

To apply new settings close the Browser and start it again in case application is already running

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

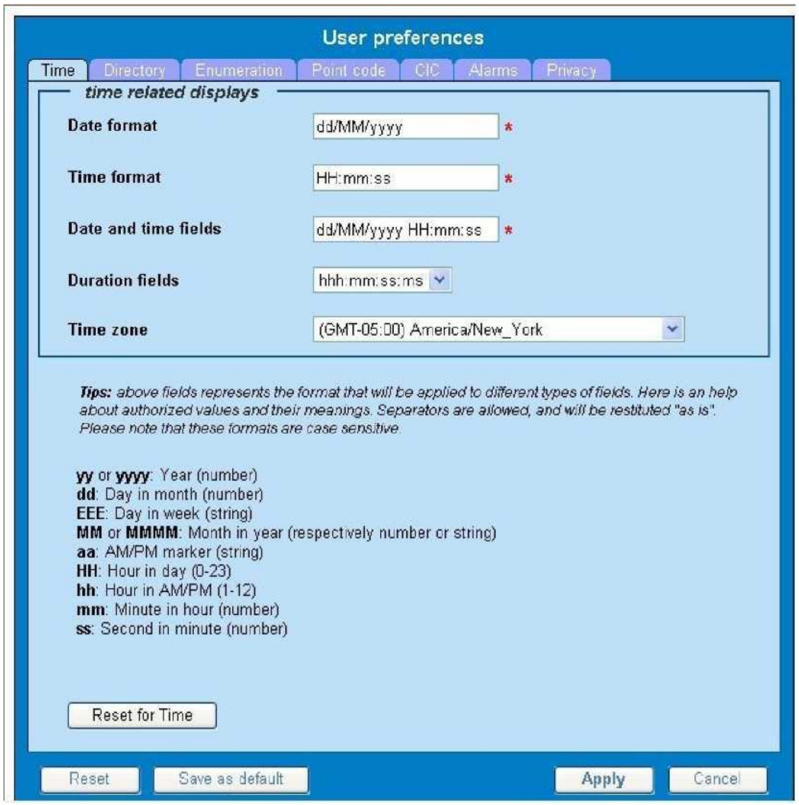
Follow these steps to set the time format:

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

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.



Date format: dd/MM/yyyy *

Time format: HH:mm:ss *

Date and time fields: dd/MM/yyyy HH:mm:ss *

Duration fields: hhh:mm:ss:ms

Time zone: (GMT-05:00) America/New_York

Tips: *above fields represents the format that will be applied to different types of fields. Here is an help about authorized values and their meanings. Separators are allowed, and will be restituted "as is". Please note that these formats are case sensitive.*

yy or **yyyy**: Year (number)
dd: Day in month (number)
EEE: Day in week (string)
MM or **MMMM**: Month in year (respectively number or string)
aa: AM/PM marker (string)
HH: Hour in day (0-23)
hh: Hour in AM/PM (1-12)
mm: Minute in hour (number)
ss: Second in minute (number)

Figure 2: Time Formatting Page

Enter the format for these time-related displays.

Date format

Time format

Date and time fields

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.

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.)

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.

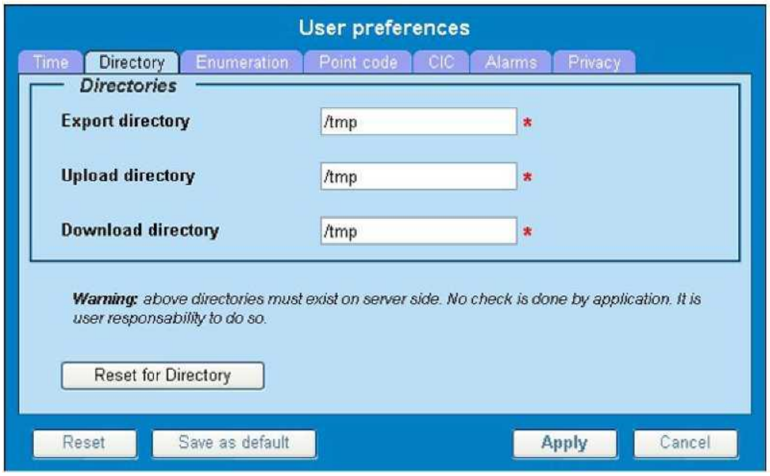
Follow these steps to set the directory preferences.

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 asterisk denotes a required field.



Export directory /tmp *

Upload directory /tmp *

Download directory /tmp *

Warning: above directories must exist on server side. No check is done by application. It is user responsability to do so.

Figure 3: Directory Page

Type in the following:

Export directory
Upload directory
Download directory

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.)

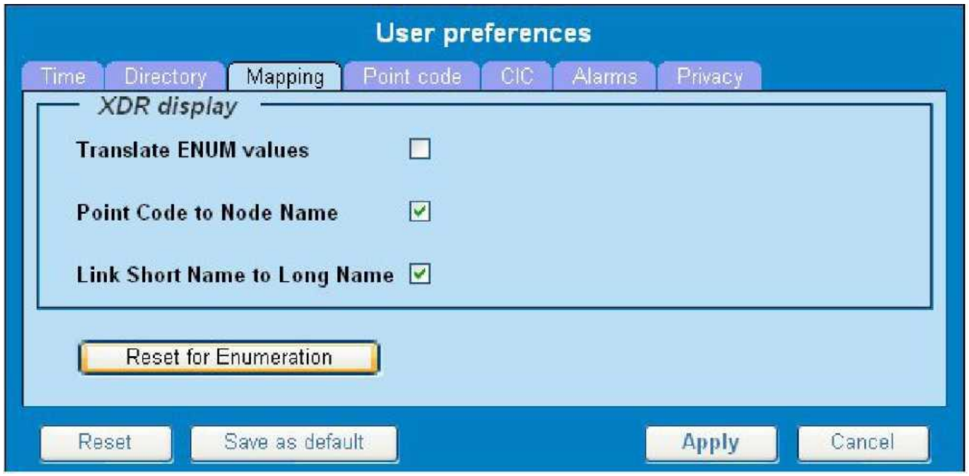
Click **Apply** to save your settings.

Setting Mapping Preferences

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

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

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



XDR display

Translate ENUM values □

Point Code to Node Name ☑

Link Short Name to Long Name ☑

Figure 4: Mapping Page

Check **Translate ENUM values** to display text instead of numerals.

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.")

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

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 (*).

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

Click **Apply** to save the changes.

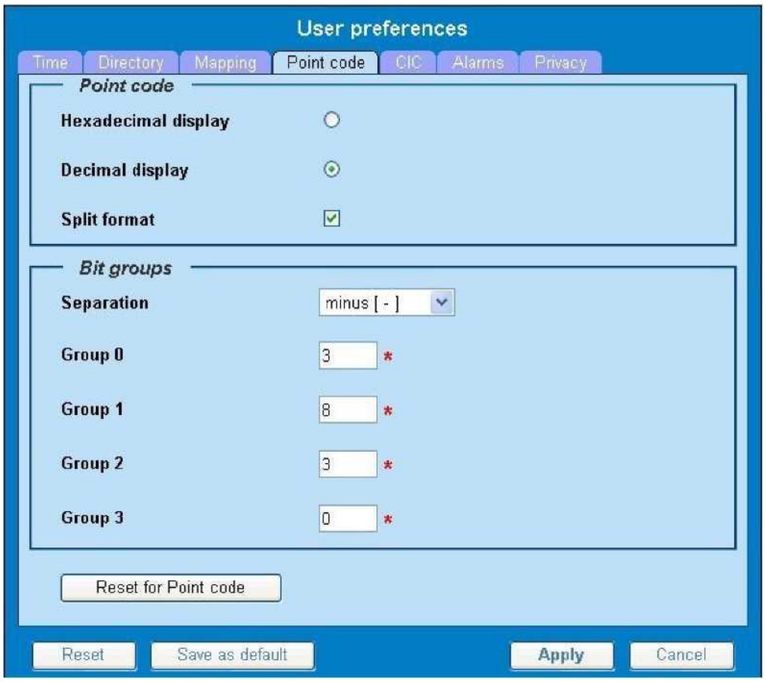
Setting Point Code Preferences

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.

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

Click the **Point Code** tab.

The Point Code page is displayed. The red asterisk denotes a required field.



Point code

Hexadecimal display ○

Decimal display ●

Split format ☑

Bit groups

Separation: minus [-]

Group 0: 3 *

Group 1: 8 *

Group 2: 3 *

Group 3: 0 *

Figure 5: Point Code Tab

Select either **Hexadecimal display** or **Decimal display.**

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.

If you selected Split format above, go to the next step. If you did not select Split format, go to step *Step 8*.

In the Bit groups panel, use the drop-down box to select the **Separation** type .

Type in values for **Groups 0-3.**

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.)

Click **Apply** to save your settings.

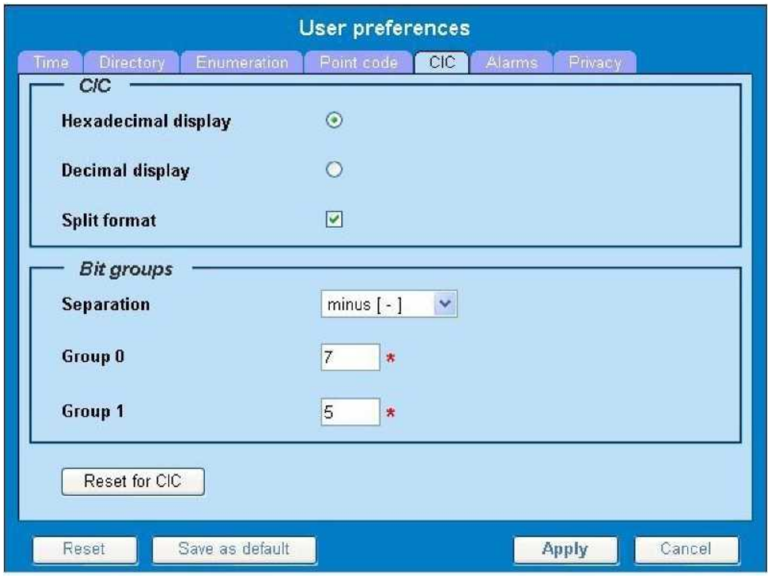
Setting CIC Preferences

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:

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

Click the **CIC** tab. The CIC page is displayed. The red asterisk denotes a required field.



User preferences

CIC

Hexadecimal display ●

Decimal display ○

Split format ☑

Bit groups

Separation: minus [-]

Group 0: 7 *

Group 1: 5 *

Figure 6: CIC Page

Select either **Hexadecimal display** or **Decimal display.**

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.

If you selected Split format above, go to the next step. If you did not select Split format, go to step *Step 8*.

In the Bit groups panel, use the drop-down box to select **Separation** type..

Type in values for **Group 0** and **Group 1.**

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.)

Click **Apply** to save your settings.

Setting Alarms Preferences

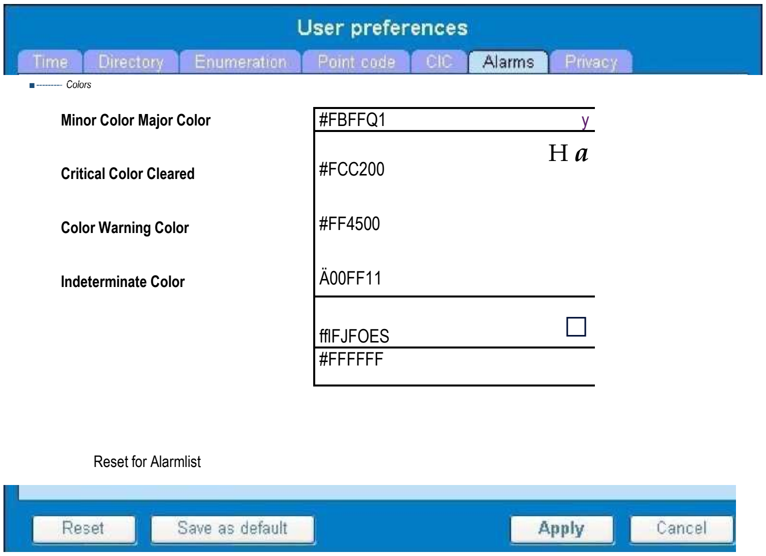
Use the Alarms tab in User Preferences to define the default colors that indicate alarm severity. The colors are displayed in the Perceived Severity column of alarms tables and on object icons in maps.

Follow these steps to modify alarm status colors.

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

Click the **Alarms** tab.

The Alarms page is displayed. The red asterisk denotes a required field.



Minor Color Major Color #FBFFQ1

Critical Color Cleared #FCC200

Color Warning Color #FF4500

Indeterminate Color Ä00FF11

ffIFJFOES

#FFFFFF

Reset for Alarmlist

Figure 7: Alarms Page

Click the color palette (icon on the right side of the screen) associated with the alarm status color(s) you want to modify.

A pop-up palette window is displayed.

Click the color you want for the type of alarm.

The color palette pop-up is closed and the color box for the alarm displays the selected color. The number for the color is also displayed.

If you want to reset the Alarm preferences to the default, click **Reset for Alarmlist.** (The bottom **Reset** button resets all the tabbed pages to default settings.)

Click **Apply** .

The changes do not take effect until you log out of and in again to NSP.

Setting Default Object Privacy

All NSP users can set default access privileges for Objects (data) they create in NSP applications. An owner has full rights to modify or delete the object . Other users are assigned to a Profile and have access to these Objects through that Profile's associated Privacy Roles.

To enter the default Object Privacy (data) settings, follow these steps:

Click **User preferences** in the Application board menu.

The User Preferences window is displayed. The **Time** tab is active by default.

Click the **Privacy** tab .

The Privacy page is displayed.

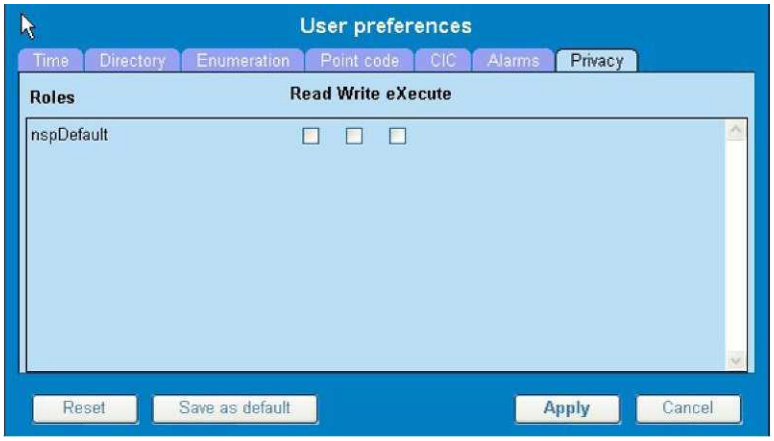


Figure 8: Privacy Page

Click the appropriate box to select **Read, Write,** or **eXecute.** If you want the role to have no access to the selected object(s), ensure that no box is checked.

Click **Save as default.**

To reset all the tabbed pages to default settings, click **Reset.**

Click **Apply.**

The settings are saved.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations: **Tekelec - Global**

Email (All Regions): support@tekelec.com • **USA and Canada** Phone:
1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

1-919-460-2150 (outside continental USA and Canada) TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays • **Caribbean and Latin America (CALA)** Phone:

USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free) TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

Argentina Phone:
0-800-555-5246 (toll-free)

Brazil
Phone:
800-891-4341 (toll-free)
TAC Regional Support Office Hours:
8:30 a.m. through 6:30 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

Chile Phone:
1230-020-555-5468

Colombia
Phone:
800-912-0537

Dominican Republic
Phone:
1-888-367-8552

Mexico
Phone:
001-888-367-8552

Peru
Phone:
0800-53-087

Puerto Rico
Phone:
1-888-367-8552 (1-888-FOR-TKLC)

Venezuela

Phone:

0800-176-6497

Europe, Middle East, and Africa

Regional Office Hours:

8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

Signaling Phone:

+44 1784 467 804 (within UK)

Software Solutions

Phone:

+33 3 89 33 54 00

Asia

India

Phone:

+91 124 436 8552 or +91 124 436 8553 TAC Regional Support Office Hours:

10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

Singapore

Phone:

+65 6796 2288

TAC Regional Support Office Hours:

9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

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, a Release Notice is distributed on the Tekelec Customer Support site along with each new release of software. A Release Notice lists the PRs that have been resolved in the current release and the PRs that are known to exist in the current release.

Listed is the entire PIC documentation library of user guides.

- Security User Guide
- Alarms User Guide

- ProAlarm Viewer User Guide
- ProAlarm Configuration User Guide
- Centralized Configuration Manager Administration Guide
- Customer Care User Guide
- Alarm Forwarding Administration Guide
- Diagnostic Utility Administration Guide
- ProTraq User Guide
- ProPerf User Guide
- ProPerf Configuration User Guide
- System Alarms User Guide
- ProTrace User Guide
- Data Feed Export User Guide
- Audit Viewer Administration Guide
- ProDiag User Guide
- SigTran ProDiag User Guide
- Report Server Platform User Guide
- Reference Data User Guide
- Exported Files User Guide
- Scheduler User Guide
- Quick Start User Guide

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

Log into the *Tekelec Customer Support* site.

Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

Click the **Product Support** tab.

Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.

Click a subject folder to browse through a list of related files.

To download a file to your location, right-click the file name and select **Save Target As.**

Chapter 2

Setting Up a Basic System

Topics:

- *Basic Workflow........... 19*

Basic Workflow

This outline represents the main steps in configuring a basic PIC system with traffic. For more detail on configuring a PIC system, refer to the Centralized Configuration Manager (CCM) online help.

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.

1. Using the Security application, set up a user with NSPAdministrator privileges. (See Security online help for setting up users, groups and privileges.)

   Note: If setting up time format, directory and mapping preferences, point code format, CIC and alarm preferences is needed, see *Setting User Preferences*.

   Note: In a typical initial PIC deployment, it is advisable to start the configuration effort by implementing the security scheme first. The reason is based on object manageability. As the configuration progresses more and more objects are created. A large system may eventually have over 12,000 objects. Each object has an owner and a privacy/privilege assignment. If changes have to be made at a later date on a large system, it is a considerable task to change owners or privacy settings on such a large number of objects.
2. Create a site and add subsystems. (Equipment Registry Perspective in CCM) *Creating a Site*

   Note: After a site is created, subsystems with their components are either discovered, as with IMF and IXP, or manually added as with PMF. Perform the following procedures if needed.

   Discover Legacy subsystems and create destinations if traffic needs to be routed to them.

Add IMF or PMF subsystem for the site. *Adding an IMF Subsystem to a Site* or *Adding a PMF Subsystem to a Site*

Note: Each site can only have one IMF or one PMF subsystem.

Configure xMF subsystems (IMF or PMF). (Acquisition Perspective in CCM)

Create Monitoring Groups and add Associations. *About Monitoring Groups (IMF)* and *Adding a Monitoring Group (IMF)* and *Adding an Association (IMF)*

Create PDU Dataflows. *About PDU Dataflows* and *Adding an SS7 Dataflow* and *Adding an IP Dataflow Using IMF FastCopy*

(Optional) Add and configure an E1/T1 Span Card. *Adding an E1/T1 (SPAN) Card (PMF)* and *Configuring E1/T1 Cards (PMF)*

Add a Traffic Classification *Adding a Traffic Classification (PMF)*

Add a GPRS Dataflow *Adding a GPRS Gb Dataflow*

Add an IXP subsystem(s). (Mediation Perspective in CCM) *Adding an IXP Subsystem to a Site*

Create Dataflow Processings. *Configuring Dataflow Processings*

Open ProTrace to begin tracing xDRs and PDUs (see ProTrace online help for more information on creating queries).

Note: At this point the system is ready to use PIC applications. For more information on the application and its features, please refer to the online help for each application. (See *PIC Documentation Library* for a complete list of PIC applications.)

Note: Some PIC applications may not be available. Contact your Tekelec representative on application availability.

Creating a Site

A site consists of different kinds of subsystems with each subsystem having one or more hosts. Upon installation, CCM, by default, creates two sites (colored blue to denote that they are default sites):

Legacy - has four categories - MSW and XMF-LEGACY. For legacy systems your only have the capability to create subsystems and add hosts to the CCM system. Discovery of application, network elements and sessions happens automatically on creating the subsystem and adding hosts to the subsystem. No further configuration is possible with the legacy systems.

NOC - gives information of the servers that make up the CCM. For all servers you do not need to change/add anything under the NOC site. You do not need to change/add anything under the NOC site. Apart from these two default sites, you can add any number of sites. The number of sites depends on the logical grouping of the monitored location. Once you create a site four categories of subsystems are automatically created under the site.

Manually add and configure the following sites as needed.

DWH - Data Warehouse

IXP - Integrated xDR Processor (Mediation Perspective)

xMF - Integrated Message Feeder (IMF) or Probe Message Feeder (PMF) (Acquisition Perspective)

EFS - Exported Filer Server

This procedure must be followed by users who are setting up the PIC system for the first time, adding new PIC servers or adding new applications on an existing server.

Complete these steps to create a site.

Select **Equipment Registry > Sites.**

Click **Add** from the tool bar.

Note: You can also right-click on the sites icon and select **Add** from the menu.

Type in a site **Name.**

(Optional) Type in a **Description** of the site that gives useful information about the site.

Click **Add** to add the site to the system.

After the site is created, subsystems can be discovered, or in the case of PMF, added and configured.

Virtual IP Address Assignment

To assign a Virtual IP Address (VIP address) the following criteria need to be met.

The VIP must be in the same subnet for the subsystem (IXP or xMF) and not being used for a host.

In addition, it is recommended to take the last available IP from the subnet since the IP is always assigned from the small number to the big number starting with server "1a."

Note: To find out the last available IP address, run `ifconfig` from one of the servers (or `platcfg` for the user) to get the broadcast address.

Here is an example of using the `ifconfig` for finding the last available IP address.

```
[root@ixp03 01-1c ~]# ifconfig
eth01  Link encap:Ethernet    HWaddr 00:24:81:FB:CB:78
inet addr:10.240.9.102    Bcast:10.240.9.127 Mask:255.255.255.192
UP BROADCAST RUNNING MULTICAST    MTU:1500 Metric:1
RX packets:100220031 errors:0 dropped:0 overruns:0 frame:0
TX packets:103153021 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100 0
RX bytes:1700925078   (1.5 GiB)     TX bytes:3351841865   (3.1 GiB) Interrupt:185
Memory:f8000000-f8011100
lo     Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING    MTU:16 43 6 Metric:1
RX packets:10626760 errors:0 dropped:0 overruns:0 frame:0 TX packets:10626760 errors:0
dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0
RX bytes:1952272307   (1.8 GiB)     TX bytes:19522 72 3 0 7   (1.8 GiB)
```

In this examplethe Bcast 10.240.9.127 is one plus the last IP in the subnet, so 10.240.9.126 is the best candidate for the VIP.

Adding an IMF Subsystem to a Site

After you have created a site, complete these steps to add an IMF subsystem. **Note:** A site can only have one IMF subsystem.

Note: When an IMF subsystem is added all network elements are automatically discovered.
Select **Equipment Registry > Site > xMF.**
Click **Add** on the xMF subsystem tool bar.
Note: The right-click menu on the xMF folder can be also used. Select **Add** from the menu options.

Table 1: xMF Subsystem Add Screen Field Descriptions

Field	**Description**
Subsystem Name	Name is identical to site name since only one xMF subsystem can exist on a site.
VIP Address	This is the Virtual IP address of the server where the xMF subsystem resides. **Note:** The VIP is established by the xMF subsystem when it is installed and integrated into the customer network. The assignment of the VIP address can be the default of the broadcast address for the subnet or it can be manually assigned to an address in the subnet. See *Virtual IP Address Assignment*.
IP Address	The IP address of IMF subsystem.
Add button	Adds the IP address to the list (you can have more than one IP address for a subsystem).

Field	Description
Delete button	Deletes the subsystem parameters from the list.
Reset button	Resets all settings to default.
Cancel button	Cancels the current process and returns back to original screen.
Create button	Adds the subsystem to the site.

Enter the **VIP Address.** (See *Virtual IP Address Assignment* for more information on using VIPs.)

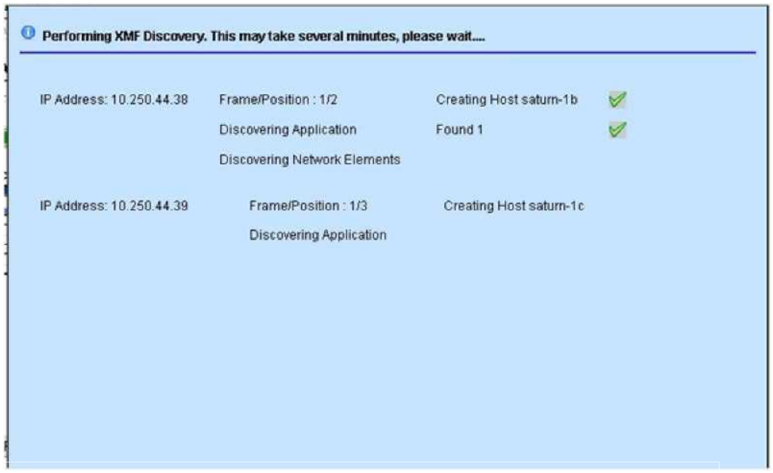
Enter the **IP Address** for the IMF host.

Note: This address is established when the IMF subsystem is installed and integrated into the customer network.

Click **Add.**

Click **Create.**

The *Verification* screen opens to show the discovery process.



Performing XMF Discovery. This may take several minutes, please wait....

IP Address: 10.250.44.38 Frame/Position : 1/2 Creating Host saturn-1b ✓

Discovering Application Found 1 ✓

Discovering Network Elements

IP Address: 10.250.44.39 Frame/Position : 1/3 Creating Host saturn-1c

Discovering Application

Figure 9: Verification Screen - Done Button Not Shown 7. Click

Done.

The *Results* screen opens showing the following information:

Note: The Results Summary screen only opens when the discovery process has finished.

Host tab - showing the IP addresses of the discovered hosts and the result

Application - showing the applications that were discovered

Network Element Discovery - showing the links belonging to the hosts that has the following five tabs:

Added - shows any elements that have been added to the host since the last discovery process

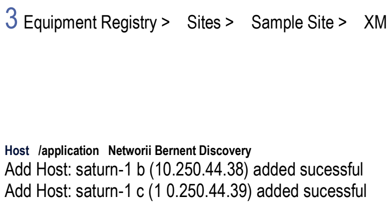
Removed - shows any elements that have been removed since the last discovery process

Modified - shows any elements that have been modified since the last discovery process

No change - shows the elements that have not changed since the last discovery process

Error - shows any errors that occurred in the discovery process

Note: If this is the first discovery process, all the tabs will be empty except for Added and Error. The other tabs are only populated when changes have been made to an existing IMF subsystem and the *Synchronize* function is used and the discovery process is repeated (see how to modify hosts).

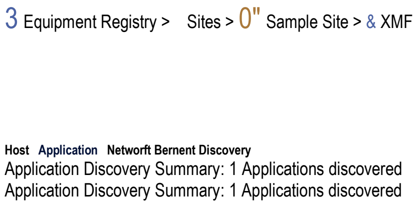


3 Equipment Registry > Sites > Sample Site > XMF > ^ Add

Host /application Networii Bernent Discovery

Add Host: saturn-1 b (10.250.44.38) added sucessful
Add Host: saturn-1 c (1 0.250.44.39) added sucessful

Figure 10: Results Summary Screen - Host Tab

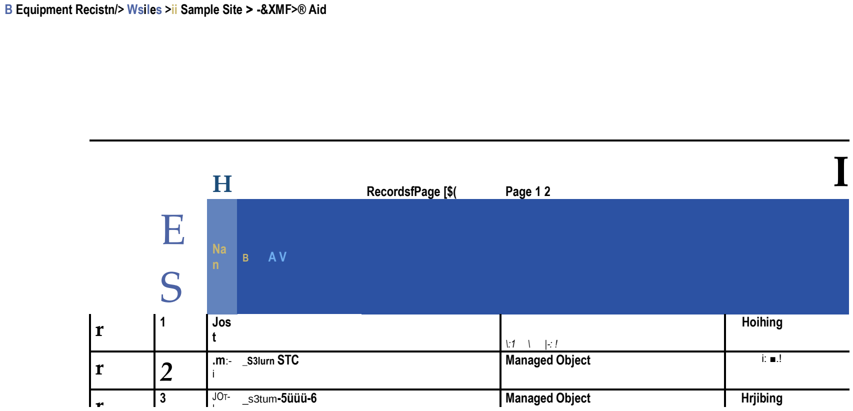


3 Equipment Registry > Sites > 0" Sample Site > & XMF > ^ Add

Host Application Networft Bernent Discovery

Application Discovery Summary: 1 Applications discovered
Application Discovery Summary: 1 Applications discovered

Figure 11: Results Summary Screen - Application Tab



B Equipment Recistn/> Wsiles >ii Sample Site > -&XMF>® Aid

RecordsfPage [$(Page 1 2

r	1	Jos t	\:1 \ |-: !	Hoihing
r	2	.m:- i _S3lurn STC	Managed Object	i: ■.!
r	3	JOT- _s3tum-5üüü-6	Managed Object	Hrjibing

Figure 12: Results Summary Screen - Network Element Discovery

8. Select the **subsystem** again to see the newly created hosts and applications.

About Monitoring Groups (IMF)

A Monitoring Group is used to configure a IMF to monitor specific Linksets and/or Associations. Once a Linkset/Association is part of a Monitoring Group, the IMF instructs the Eagle to send MSUs/PDUs to the IMF for capturing. When Linksets and/or Associations are monitored by the IMF, the IMF captures the MSUs/PDUs received from Eagle and forwards these to the IXP for processing/storage based on PDU Data Flows Configurations on IMF and Dataflow Processing Configurations on IXP.

Monitoring Groups support Associations for *SigTran Fast Copy* capability. This capability provides efficient configuration and maintenance of the IMF subsystem by integrating it with the Eagle without impacting the internal *Eagle IMT* bus. In addition, the SigTran data is monitored in real time, similar to the port mirroring with PMF, again with no internal impact to the IMT bus. For more information on supporting and configuring Fast Copy, refer the documentation for Eagle.

Note: Since monitoring groups must be associated with a linkset, you must have existing linksets before you can assign a monitoring group.

Note: Linksets that have not been associated with any monitoring group will not be monitored. It is recommended that when creating an association, you also monitor the other links in the linkset(s).

The monitoring group list page has five columns:

Groups listed for a site - shows the record number of the monitoring group

Group Name - shows the name of the monitoring group

Description - shows a short description of the group (optional).

Number Links - shows the number of monitored linksets

Number Associations - shows the number of monitored associations

Automatic Failover Capability

IMF has an automatic failover capability to reduce PDU loss in case of server hardware failure. Whenever an IMF server fails, the IMF subsystem automatically shifts all the linksets/links monitored by the failed server to an available spare server within the subsystem. In order to support this feature, there needs to be one IMF server (spare) that does not have a monitoring group assigned to it.

The maximum number of monitoring groups you can configure *is equal to the number of servers available in the subsystem.* You can assign linksets to each monitoring group. A linkset can be assigned to only one monitoring group. You can also configure *n-1 monitoring groups* (n is the number of servers), to guarantee one server being available for failover.

Adding a Monitoring Group (IMF)

Complete these steps to add a monitoring group to an IMF subsystem.

Select **Acquisition > Sites > Host > xMF (IMF) subsystem > Server > Monitoring Group.**

The monitoring groups list screen opens.

Click **Add** from the toolbar. The Monitoring Group Add screen opens.

Note: There must be monitored links and associations present for the monitoring group to be created. If no linksets or associations are present, they must be added and then the changes applied to the IMF subsystem.

Field	**Description**
Group Name	Provides the name of the monitoring group that is being added.
(Optional) Description	Provides some useful information about the monitoring group.

Field	Description
Linksets and Associations Notation	Shows the number of linksets and associations that belong to the IMF subsystem.
Linksets Tab	Shows un-monitored and monitored linksets on the IMF server.
Associations Tab	Shows un-monitored and monitored associations on the IMF server.
Cards Tab	Shows un-monitored and monitored cards on the IMF server.
Reset Button	Resets the screen back to its default status.
Cancel Button	Cancels any changes in progress.
Add Button	Adds the monitoring group to the IMF server.

Enter the **Group Name.**
(Optional) Enter a **Description.**
Select the **Un-monitored Linksets** that will belong to the monitoring group.
Note: Each linkset is listed by name and how many STC links and associations it has. The notation is:
`linksetname (STC=<n>,ASSOC=<n>)` For example,
`s1cssg-lsto12551 (STC=2,ASSOC=0)`
Click the **right arrow** to move the linkset(s) to the monitored linksets field.
Click the **Associations Tab** and select the un-monitored association(s).
Click the **right arrow** to move the selected association(s) to the monitored field.
Click the **Card Tab** and select the un-monitored card(s).
Click the **right arrow** to move the selected card(s) to the monitored field.
Click **Add.**
The monitoring group is added to the list.
Note: For the changes to take effect, right-click on the IMF subsystem and select **Apply Changes** from the menu.
Note: You can assign both linksets and associations to a monitoring group when you are monitoring more than just SS7 linksets such as SigTran Links.

About Associations (IMF)

Associations refer to SCTP associations within a SIGTRAN (SS7 over IP) network. An association provides the transport mechanism for the delivery of SCCP-User protocol data units and SUA layer peer messages. Associations are similar to a TCP connection, because they support multiple IP addresses at either or both ends (multi-homing). In addition, associations support multiple logical streams (multi-streaming) as well as provide sequenced delivery for user datagrams within a single input stream.

Adding an Association (IMF)

Complete these steps to add an association to a monitoring group.

Select **Acquisition > Sites >xMF (IMF) subsystem > Server > Monitoring Group** to open the Monitoring Group screen.

Click **Add** from the tool bar.

Alternative procedure: Select Acquisition > Sites > xMF (IMF) subsystem. Right-click on Monitoring Group and select **Add.**

Enter the **Group Name.**

(Optional) Type a **Description.**

Click the **Associations** tab.

The Associations screen opens showing all un-monitored associations.

Select one or more **un-monitored associations**

Click the **right arrow** to place the *Un-monitored associations* to the *Monitored Associations* field.

Note: The bottom field (Un-monitored Linksets and Associations) shows those elements that are un-monitored but are part of the monitored linkset/association. This list appears when a linkset is monitored but the association is not (and visa versa). It is recommended that these related elements be monitored together so as to keep all linksets and associations in the same group.

Select the **Cards** tab.

Select one or more **cards** from the Un-monitored Cards section.

Click the **right arrow** to place the Un-monitored Cards to the Monitored Cards field.

Click **Add.**

The monitoring group with associations is added to the list.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

About PDU Dataflows

PDU Data Flows are used to group Linksets and/or Associations that are being captured on the IMF/PMF and deliver them to the IXP for protocol analysis and storage. The MSUs/PDUs are packaged and shipped to the IXP over an input stream (IP Stream). Once configured, the PDU Data Flows can be used by the IXP for processing xDR storage.

PDU dataflows are created for each specific xMF (IMF or PMF) subsystem to route both filtered and unfiltered data to IXP for xDR creation. The PDU dataflows contain linksets which can belong to different servers across a subsystem or all together different subsystems. There are different categories of PDU dataflows defined to route different types of data.

CCM provides the capability to configure PDU Dataflows for each xMF subsystem. The capability allows for greater flexibility and quicker search capabilities when creating dataflows.

The following PDU dataflows can be configured in a subsystem:

- GPRS dataflows (for PMF only)

SS7 MSU dataflows (Including BICC monitoring over SigTran and L2 LSSU) IP dataflows Q.752 dataflows

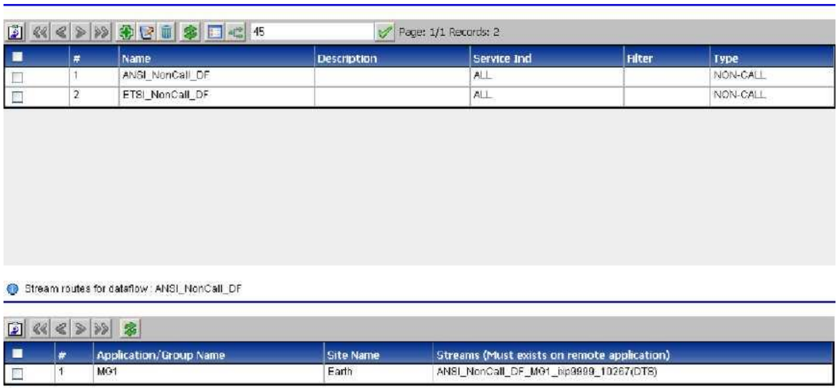
Note: In an IMF subsystem there is a hard-coded limit of 20 input streams a dataflow can be routed per server.

Adding an SS7 Dataflow

Complete these steps to create a SS7 PDU dataflow.

1. Select **Acquisition > Site > Subsystem > PDU Data Flows > SS7** .

The Add SS7 dataflow list screen opens.



45 Page: 1/1 Records: 2

■	#	Name	Description	Service Ind	Filter	Type
□	1	ANSI_NonCall_DF		ALL		NON-CALL
□	2	ETSI_NonCall_DF		ALL		NON-CALL

Stream routes for dataflow : ANSI_NonCall_DF

■	#	Application/Group Name	Site Name	Streams (Must exists on remote application)
□	1	MG1	Earth	ANSI_NonCall_DF_MG1_iip9999_10267(DTS)

Figure 13: SS7 Dataflow List Screen

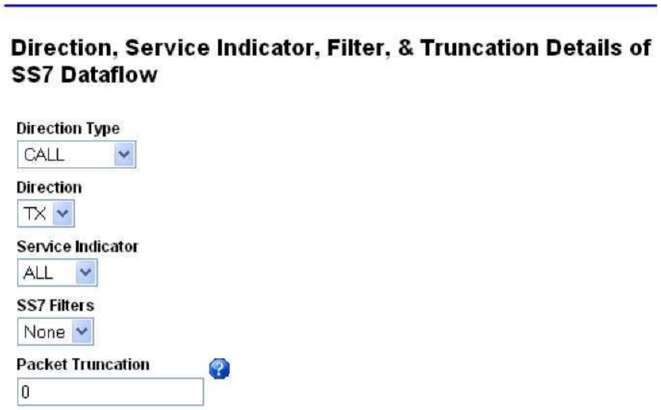
Click **Add** on the tool bar.

Type in the **Name** of the SS7 dataflow.

(Optional) Type in a **Description** of the dataflow record.

Click **Next.**

The *Direction,* Service *Indicator and* Filter *Details* screen opens



Direction, Service Indicator, Filter, & Truncation Details of SS7 Dataflow

Direction Type: CALL

Direction: TX

Service Indicator: ALL

SS7 Filters: None

Packet Truncation: 0

Figure 14: Direction, Service Indicator, Filter & Truncation Details Screen

The table describes the default fields on this screen.

The table describes the default fields on this screen.

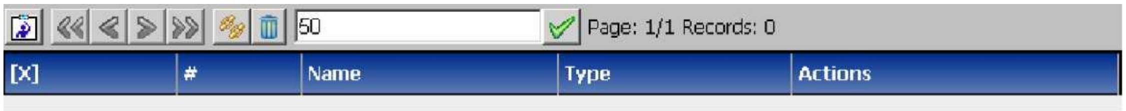
Note: For LSSU support (selecting the Non-Call), the screen has only three fields with the following choices:

Direction Type - Non-Call
Direction - TX, RX or BOTH
Service Indicator - ALL

Table 2: Direction, Service Indicator, Filter & Truncation Details of SS7 Dataflow Screen Fields

Field	Description
Direction Type	Drop-down menu has the following options: • CALL or MSUCALL: For certain SCCP, TUP, or ISUP Service Indicator Message Types. Direction for this Direction Type can be only either RX or TX. • MSU: All other MSU data types including BICC over SigTran. Call direction can be RX, TX or Both • Non_Call: (For LSSU support.) The Direction for this message type can be RX, TX or Both. The service indicator will always be "ALL"
Direction	What is the source of the dataflow Either RX, TX, or Both (MSU and LSSU)
Service Indicator	• Drop-down menu of supported SS7 types **Note:** For LSSU support ALL is the only selection
SS7 Filters	Select the filters to be associated with the dataflow.
Packet Truncation	Enter an integer for the maximum length, in bytes, for each PDU. The range is between 0-4000.
Cancel / Previous /Next	Click on one of the following: • Cancel: Information is not saved. • Previous: Returns you to the SS7 Dataflow Information screen. • Next: The Monitored Linksets Details screen opens.

Select the **Direction Type.** (MSU, Call, or NON_CALL).
Select the **Direction.** (Both, Rx, Tx)
Select the **Service Indicator.** (For Non_Call only ALL is available).
Select a **SS7 Filter.**
Enter the length of the PDU in the **Packet Truncation** field. (Integer between 0-4000)
Click **Next.**
The Monitored Linkset Details screen opens.



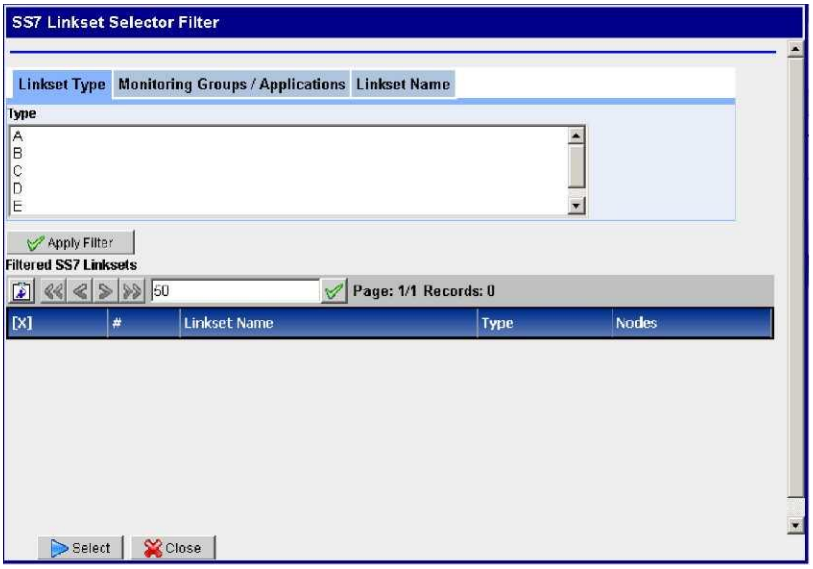
50 Page: 1/1 Records: 0

[X]	#	Name	Type	Actions

Figure 15: Monitored Linkset Details Screen

Click the **Linksets** icon to show the existing linksets. You can also create linksets if you need to.
Click **Add** to add the record to the database. SS7 Linkset Selector Filter opens.

Select the **Linkset Type** (A-F) from the Linkset Type tab.
(Optional) Select an option from the **Monitoring Group/Applications** tab .
Select the **Linkset Name** tab and enter a **Linkset Name.**



SS7 Linkset Selector Filter

Type
A
B
C
D
E

Filtered SS7 Linksets

50 Page: 1/1 Records: 0

[X]	#	Linkset Name	Type	Nodes

Figure 16: SS7 Linkset Selector Filter Screen

Click **Apply Filter** to apply the filter you created.
Select a **Filtered Linkset** from the list at the bottom table.
Select the **Monitored Linkset.**
Click **Add.**
Note: For the changes to take effect, right-click on the IMF subsystem and select **Apply Changes** from the menu.

Adding an IP Dataflow Using IMF FastCopy

Complete these steps to create an IP dataflow using IMF FastCopy.

1. Select **Acquisition >IMF Site > PDU Data Flows > IP.**

The IP Dataflow list screen opens.

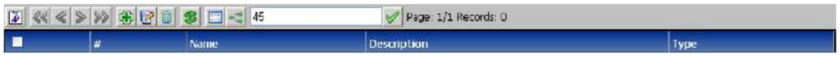


Figure 17: IP Dataflow List Screen

2. Click **Add.**
The Add screen opens.

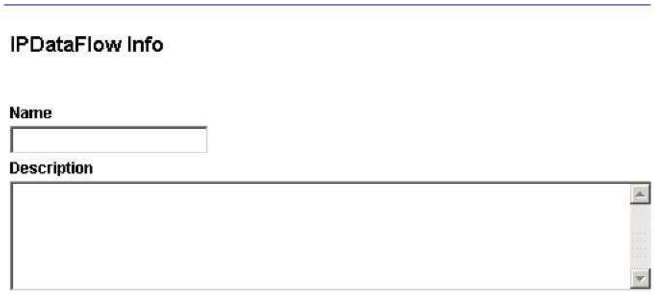


Figure 18: IP Data Flow Add Screen

Type in the **Name** of the IP dataflow
(Optional) Type in a **Description** of the dataflow record.
Click **Next.**
The IP Dataflow Associations Selector screen opens.

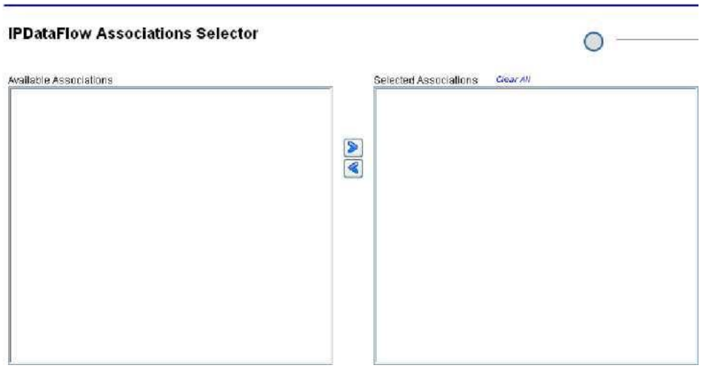


Figure 19: IP Dataflow Associations Selector Screen

Select one or more **Available Associations.**
Click the **right arrow** to place them into the Selected Associations field.
Click **Add.**
Note: For the changes to take effect, right-click on the IMF subsystem and select **Apply Changes** from the menu.

Adding a PMF Subsystem to a Site

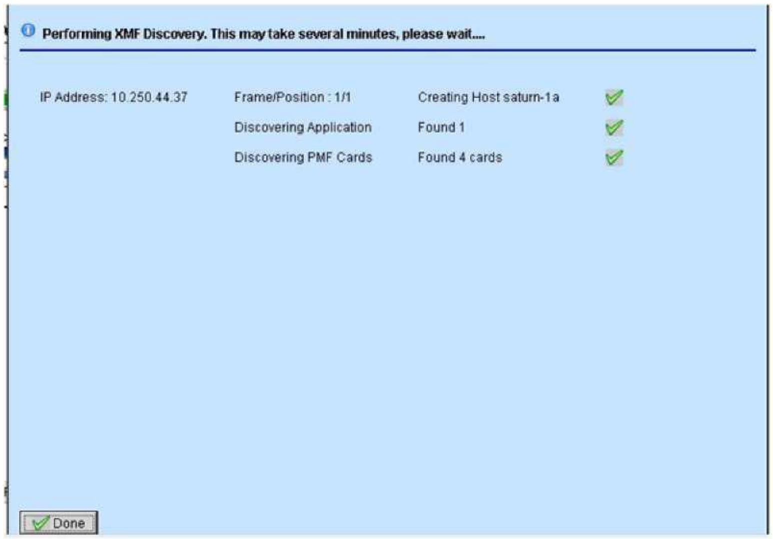
After you have created a site, complete these steps to add a PMF subsystem to a site. **Note:** Each site can only have one PMF subsystem.

Select **Equipment Registry > Site > xMF.**
From the xMF subsystem right-click menu select **Add.**

Table 3: xMF Subsystem Add Screen Field Descriptions

Field	Description
Subsystem Name	Name is identical to site name since only one xMF subsystem can exist on a site.
VIP Address	This is the Virtual IP address of the server where the PMF subsystem resides. **Note:** The VIP address is established when the PMF subsystem is initially installed and integrated into the customer network. The assignment of the VIP address can be the default of the broadcast address (broadcast-1) for the subnet, or it can be manually assigned to an address in the subnet. See *Virtual IP Address Assignment*.
IP Address	The IP address of xMF server where the PMF subsystem resides.
Add button	Adds the IP address, to the list (you can have more than one IP address for a subsystem).
Delete button	Deletes the subsystem parameters from the list.
Reset button	Resets all settings to default.
Cancel button	Cancels the current process and returns back to original screen.
Create button	Adds the subsystem to the site.

Enter the **VIP Address.**
Enter an **IP Address** for the PMF host.
Click **Add.**
Click **Create.**
The system discovers the hosts and cards that belong to the PMF subsystem. All successful discoveries are shown with a check mark beside it. See the figure below.
Note: If there is an error, a red x will appear beside the host or application that could not be discovered.
Note: E1/T1 Span cards are not auto-discovered, they are manually added to the PMF subsystem. See *Adding an E1/T1 (SPAN) Card (PMF)* for more information.

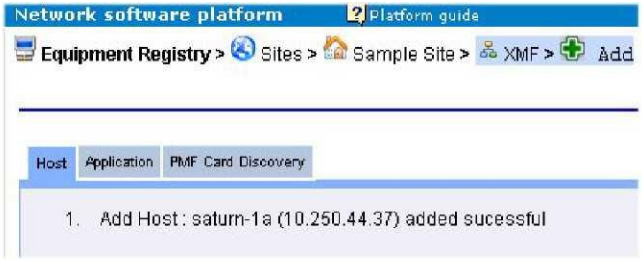


Performing XMF Discovery. This may take several minutes, please wait....

IP Address: 10.250.44.37	Frame/Position : 1/1	Creating Host saturn-1a	✓
	Discovering Application	Found 1	✓
	Discovering PMF Cards	Found 4 cards	✓

Figure 20: PMF Results Summary Screen

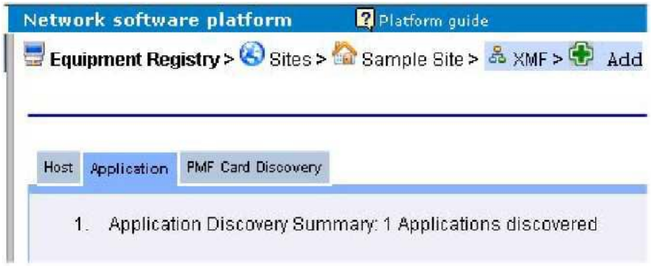
7. Click **Done** to close the Results Summary screen and view the discovery summary. The screen has the following tab information shown in the figure shown here:
Host tab - showing the IP addresses of the discovered hosts and the result
Application - showing the applications that were discovered
PMF Card Discovery - showing the cards installed on the host



Network software platform
Platform guide
Equipment Registry > Sites > Sample Site > XMF > Add
Host
Application
PMF Card Discovery

1. Add Host : saturn-1a (10.250.44.37) added sucessful

Figure 21: Discovery Summary Screen - Hosts Tab

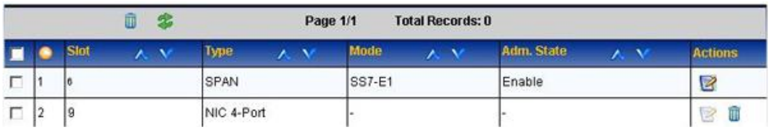


Network software platform
Platform guide
Equipment Registry > Sites > Sample Site > XMF > Add
Host
Application
PMF Card Discovery

1. Application Discovery Summary: 1 Applications discovered

Figure 22: Discovery Summary Screen - Application Tab

Note: The Results screen only opens when the discovery process has been completed.
Note: If this is the first discovery process, all the tabs will be empty except for Added and Error. The other tabs are only populated when the discovery process is repeated after there has been some modification to the host (see how to modify hosts.).



Page 1/1 Total Records: 0

☐	●	Slot	Type	Mode	Adm. State	Actions
☐	1	6	SPAN	SS7-E1	Enable	
☐	2	9	NIC 4-Port	-	-	

Figure 23: Discovery Summary Screen - PMF Card Discovery

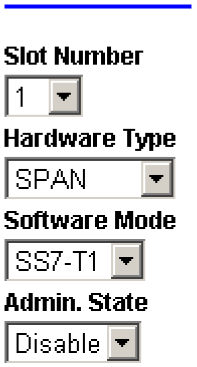
8. Select the **subsystem** again to see the newly created hosts and applications.
If there is an E1/T1 card for the PMF, open the Acquisition perspective to configure the card.
Note: Network cards and NGP cards are automatically discovered and do not have to be manually added.

Adding an E1/T1 (SPAN) Card (PMF)

If E1/T1 cards are being used for a PMF system, these cards have to be manually added and configured. These procedures are performed from the Acquisition perspective. Complete these steps to add an E1/T1 SPAN card to a PMF subsystem.

Select **Acquisition > Site (with PMF subsystem) > subsystem > Server > Cards.**

Select **Add** from the pop-up menu. The Add Card screen appears.



Slot Number: 1
Hardware Type: SPAN
Software Mode: SS7-T1
Admin. State: Disable

Figure 24: Add Card Screen

3. Select the **Slot Number**.
4. Select the **Hardware Type** to SPAN.
5. Select the **Software Mode** .

- SS7-T1
- SS7-E1
- GB-E1
- GB-T1

6. Modify the various **parameters** in the port.
7. Select the **Admin. State** (enable/disable).
8. Click **Create** for the Linkset.

The card is created.

Note: For the changes to take effect, right-click PMF subsystem that has the card and select **Apply Changes** from the menu.

Configuring El/Tl Cards (PMF)

After you have created a PMF subsystem and discovered its applications, you can configure the PMF applications. Complete these steps to configure a PMF application (E1/T1 Span Card).

Select **Acquisition > Site (with PMF subsystem) > PMF Subsystem > Server > Cards** .

Select the appropriate **Card.**

Note: E1/T1 Cards will be labeled in numerical order with name of SPAN, for example 1: SPAN.

Right-click on the **Card.**

Click **Modify.**

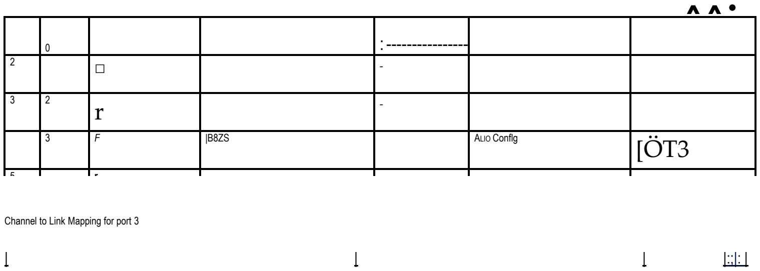
The Card screen opens showing the cards ports.

Figure 25: Span Card Screen with Unconfigured Ports

5. Select the port you want to configure by clicking the check box in the **Configured** column.
id

The screen changes to show configurable parameters such as Zero Suppression, Framing, Access Mode and Bit Inversion along with the Channel Link Mapping screen for that port.

Figure 26: Span Card Configure Screen with Channel Link Mapping Section



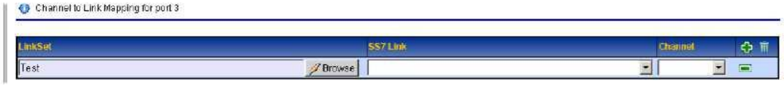
	0			:---------------		
2		□		-		
3	2	r		-		
	3	*F*	|B8ZS		AUO Config	[ÖT3

Channel to Link Mapping for port 3

Modify the various **parameters** in the port.

Click the **Add** icon on the tool bar in the Channel to Link Mapping section. **Note:** Only unmonitored links (SS7 and Gb) are shown.

Note: Other PMF configurations such as site configuration, discovery, network elements (linkset and link), traffic classifications and PDU data flows remain unchanged and remain consistent across the PMF subsystem.



Channel to Link Mapping for port 3

LinkSet	SS7 Link	Channel
Test		

Figure 27: Span Card Configure Screen with Channel Link Mapping Add Screen

8. Click **Browse** for the Linkset.

Note: You can also use the "auto complete" text box to search the linksets or Gb links quickly if you know the name.

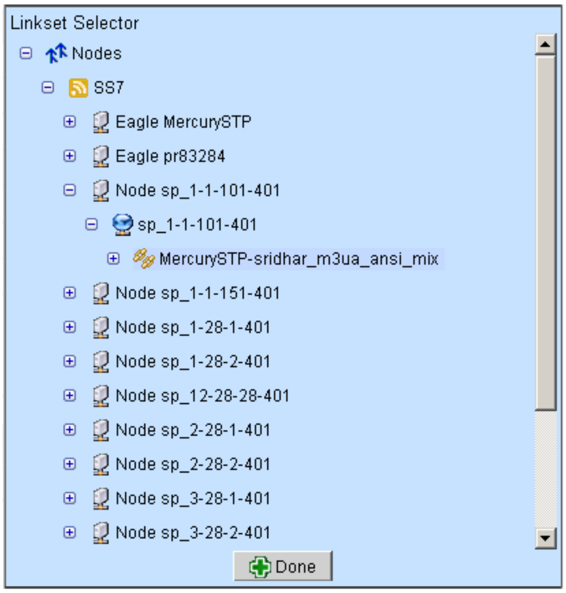


Figure 28: Span Card Configure Screen with Channel Link Mapping Add Screen

When you have selected the linkset, click **Done.**

Select the **Link** associated with the linkset.

Select the **Port** associated with the linkset.

Click **Modify.**

The card port is configured.

Make sure to apply the changes to the subsystem when you have finished using the subsystem right-click menu.

About Traffic Classifications (PMF)

A Traffic Classification on PMF is similar to a Monitoring Group on an IMF because the settings made for a Traffic Classification are used by the PMF to process the captured MSUs/PDUs received from the network. These captured MSUs/PDUs are forwarded to the IXP for processing/storage. The forwarding is based on PDU Data Flow Configurations, filters on the PMF and Dataflow Processing Configurations on IXP.

A Traffic Classification on PMF is similar to a Monitoring Group on an IMF in that a Traffic Classification is used by the PMF to process the captured MSUs/PDUs received from the IP probe. A Traffic Classification is a filter-like construct that is applied on an IP probe (NIC). Each input stream (IP stream) selects a part of the traffic from one or more IP probes. The basic idea is that each IP stream splits the traffic into manageable partitions that are used by downstream applications hence the term "traffic classifications". These captured MSUs/PDUs are forwarded to the IXP for processing/storage. The forwarding is based on PDU Data Flow Configurations, filters on the PMF and Dataflow Processing Configurations on IXP.

PIC filters IP traffic on the protocols.

TCP

UDP

ICMP

SCTP

RTP

Note: All Traffic Classification counts are reset in Diagnostic Utility. For more information, see the Diagnostic Utility Administration Guide.

Adding a Traffic Classification (PMF)

Complete these steps to add a traffic classification (IP stream).

Select **Acquisition > Sites > PMF subsystem > Servers > Application > Traffic Classifications.**

The List screen opens.

Click **Add** on the tool bar to open the wizard.

Enter the **Name** of the traffic classification.

(Optional) Enter a **Description.**

Select an **Internet Protocol** from the pull-down list.

Note: If ICMP is selected, no transport or application layers are utilized. Proceed to step 8.)

Select a **Transport Protocol** from the pull-down menu.

Note: If SCTP is selected, then all application layers are also selected by default (see step 7).

Select an **Application Layer** from the pull-down list.

Select a **Filter.**

Note: The list of filters presented is dependent upon the Transport Protocol selected.

Select the **Forwarding** method.

Note: If SCTP is selected as transport protocol, then the chunks or packets can be sent.

If chunk is selected as the forwarding mechanism, then only matched chunks are sent (as well as the IP and SCTP header).

If packet (IP Raw) is selected as the forwarding mechanism, then the whole IP packet is sent when at least one chunk in the packet matches the filter.

Select an **Association** to be associated with the TC.

If SCTP is selected, click **Association Selector** from the Association Selector tool bar.

Select one or more **Associations** from the Association Selector pop-up screen.

Click **Select** to add the associations to the traffic classification.

Click **Next** to open the probe assignment screen.

Select one or more **probes** from the available options field.

Click the **right arrow (>)** to move them to the selected options field.
Click **Next** to open the Annotation screen.
Enter an **Annotation.**
(Optional) Click **Add To List.**
The annotation is added to the *Selected Annotations* list.
Note: You can also select existing annotations by typing the first letter and select from the list that appears.
Note: To remove an annotation, select the annotation and click **Remove From List.**
Click **Create.**
The traffic classification is added to the list .
Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Adding a GPRS Gb Dataflow

Complete these steps to add an GPRS data flow for a PMF subsytem.
Select **Acquisition > Sites > Subsystem >PDU Data Flows > GPRS > Add.**
Type in the **Name** of the *Gb dataflow.*
(Optional) Type in a **description** of the dataflow record.
Click **Next.**
Select a **Gb Filter** from the drop-down menu.
Enter the **number** for packet truncation.
Click **Next.**
Click the **Gb link** icon.
Enter the **Gb Link Name.**
Click **Apply Filter.**
Select **Gb Link Record** from the list.
Click **Select.**
Click **Close.**
Click **Add.**
The GPRS dataflow is added to the system.
Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Adding an IXP Subsystem to a Site

Note: You can have an unlimited number of IXP subsystems per site. Complete these steps to add an IXP subsystem to a site and discover its elements.

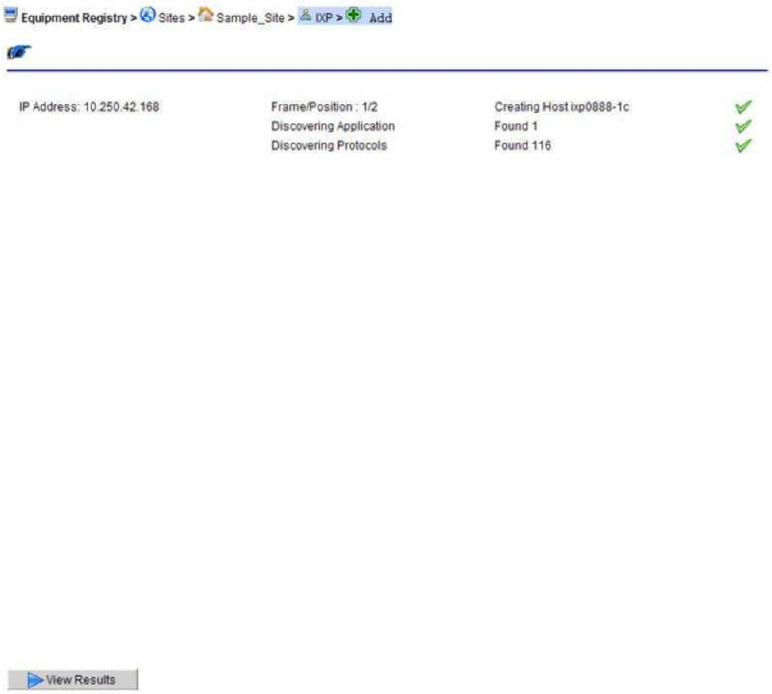
1. Select **Equipment Registry > Site** that has the IXP subsystem.

2. Right-click on the site **IXP.**
3. Select **Add.**

Table 4: IXP Subsystem Add Screen Field Descriptions

Field	Description
Subsystem Name	The name of the IXP subsystem (required).
VIP Address	This is the Virtual IP address of the server where the IXP subsystem resides. **Note:** The VIP address is established when the IXP subsystem is initially installed and integrated into the customer network. The assignment of the VIP address can be the default of the broadcast address (broadcast-1) for the subnet, or it can be manually assigned to an address in the subnet. See *Virtual IP Address Assignment*.
IP Address	The IP address of IXP server where the IXP subsystem resides.
Add button	Adds the IP address to the list (you can have more than one IP address for a subsystem).
Delete button	Deletes the subsystem parameters from the list.
Reset button	Resets all settings to default.
Cancel button	Cancels the current process and returns back to original screen.
Create button	Adds the subsystem to the site.

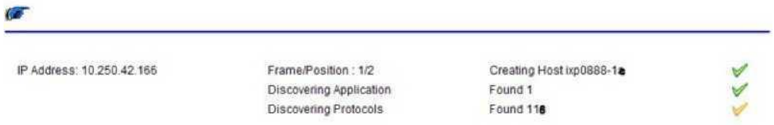
Enter the **Name** of the IXP subsystem.
Enter the **VIP Address** of the subsystem.
Enter the **IP Address** of the subsystem.
Click **Add** to add the subsystem to the list.
Note: Repeat steps 4-7 to add each additional subsystem.
Click **Create.**
A progress bar appears as the system searches out the IP address, applications and protocols. When the discovery process is completed a Results Summary screen opens.
Note: Some systems use a large number of protocols and the time span for the discovery process can take several minutes.
Note: Use the *Modify* function to add a host(s) to an IXP subsystem.



IP Address: 10.250.42.168 Frame/Position : 1/2 Creating Host ixp0888-1c ✓
Discovering Application Found 1 ✓
Discovering Protocols Found 116 ✓

Note: If there is a problem with the position, application or protocols, the color of the check mark will be yellow.

Figure 29: Subsystem Results Summary Screen



IP Address: 10.250.42.166 Frame/Position : 1/2 Creating Host ixp0888-1a ✓
Discovering Application Found 1 ✓
Discovering Protocols Found 116 ✓

Figure 30: Results Summary Screen With Error Symbol

9. Click **View Results.**

The Results screen opens.

The screen has four tabs with five subtabs:

Host - Shows the host parameters and status (added successfully or not)

Application - Shows a summary of the number of applications discovered

xDR Builders - Opens another screen with five tabs that lists the following parameters:

Note: xDR Builders are discovered and are the same for the entire subsystem.

Added - shows the xDR Builders that added to the subsystem from the last synchronization

Removed - shows the number of xDR Builders removed from the system from the last synchronization

Modified - shows any xDR Builders that have been modified from the last synchronization

No Change - shows any xDR Builders that have not been changed from the last synchronization

- Errors - shows a list of any errors that occurred during the discovery process or synchronization

d) Synchronize IXP - shows if the synchronization was successful or not.

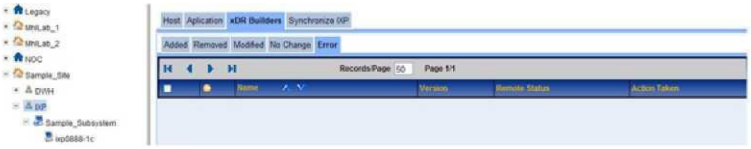


Figure 31: Object Tree Showing Added Subsystem With Results Screen

At this stage, legacy subsystems can be added or additional IXP subsystems can be manually added.

10. Right click on the **IXP subsystem** and select **Apply Changes** for the changes to take effect.

About Dataflow Processings

Dataflow Processing is the receiving end from a PDU Stream or PDU Dataflow as configured on the IMF/PMF. The Dataflow Processing configuration is used to build a xDR for storage on the IXP. The configuration is required based on the protocol and type of post-processing prior to storage on the IXP. Once a Dataflow Processing has been configured, the IXP will start receiving MSUs/PDUs from the IMF/PMF over the input stream that was created for the IMF/PDU PDU Data Flows.

Configuring Dataflow Processings

The most important aspect of IXP configuration is the creation of xDR Dataflows. An xDR Dataflow is made of interconnected processes referred to as dataflow processings. Dataflow processings are categorized into three types listed in the order that they should be created:

Building - this dataflow processing creates or builds xDRs

Operation - this dataflow processing generates statistics and applies filters for data enrichment

Storage - this dataflow processing stores information on the system

Note: If you do not have licenses to use specific xDR builders, the builder selection screen will not show them.

Configure dataflow processings using the xDR Dataflow Assistant.

Select **IXP subsystem > Subsystem** that needs the configured dataflow processings.

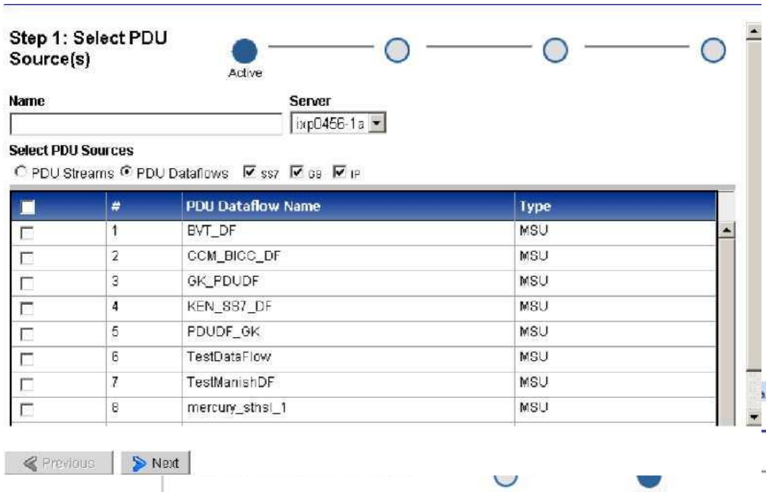
Right-click on the **Subsystem.**

The pop-up menu opens.

3. Right-click on **Dataflow Processings.**

4. Select **xDR Dataflow Assistant** from the pop-up menu.

The first screen of the wizard opens in the *Table* section shown here.



Step 1: Select PDU Source(s)

Name:

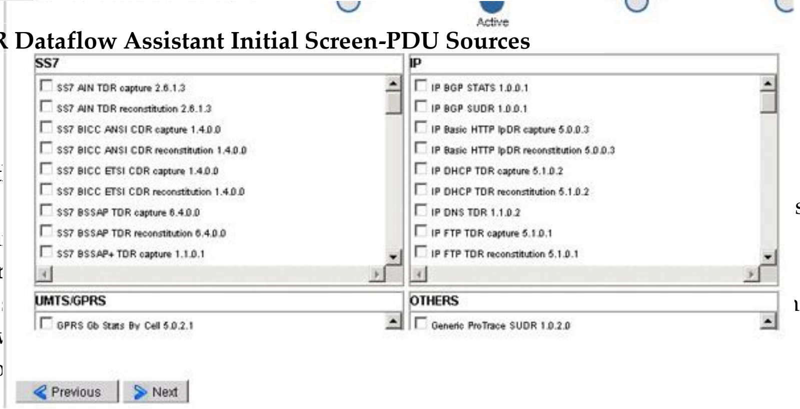
Server: ixp0456-1a

Select PDU Sources

○ PDU Streams ● PDU Dataflows ☑ SS7 ☑ GB ☑ IP

□	#	PDU Dataflow Name	Type
□	1	BVT_DF	MSU
□	2	CCM_BICC_DF	MSU
□	3	GK_PDUDF	MSU
□	4	KEN_SS7_DF	MSU
□	5	PDUDF_GK	MSU
□	6	TestDataFlow	MSU
□	7	TestManishDF	MSU
□	8	mercury_sthsl_1	MSU

Figure 32: xDR Dataflow Assistant Initial Screen-PDU Sources



SS7
- □ SS7 AIN TDR capture 2.6.1.3
- □ SS7 AIN TDR reconstitution 2.6.1.3
- □ SS7 BICC ANSI CDR capture 1.4.0.0
- □ SS7 BICC ANSI CDR reconstitution 1.4.0.0
- □ SS7 BICC ETSI CDR capture 1.4.0.0
- □ SS7 BICC ETSI CDR reconstitution 1.4.0.0
- □ SS7 BSSAP TDR capture 6.4.0.0
- □ SS7 BSSAP TDR reconstitution 6.4.0.0
- □ SS7 BSSAP+ TDR capture 1.1.0.1

IP
- □ IP BGP STATS 1.0.0.1
- □ IP BGP SUDR 1.0.0.1
- □ IP Basic HTTP IpDR capture 5.0.0.3
- □ IP Basic HTTP IpDR reconstitution 5.0.0.3
- □ IP DHCP TDR capture 5.1.0.2
- □ IP DHCP TDR reconstitution 5.1.0.2
- □ IP DNS TDR 1.1.0.2
- □ IP FTP TDR capture 5.1.0.1
- □ IP FTP TDR reconstitution 5.1.0.1

UMTS/GPRS
- □ GPRS Gb Stats By Cell 5.0.2.1

OTHERS
- □ Generic ProTrace SUDR 1.0.2.0

Type in the **Name**

Select the **server.**

Note: Do not use t

Note: If multiple server be used to

facilitate load bala

Select a **PDU Sour**

You can filter by ıer the source is a

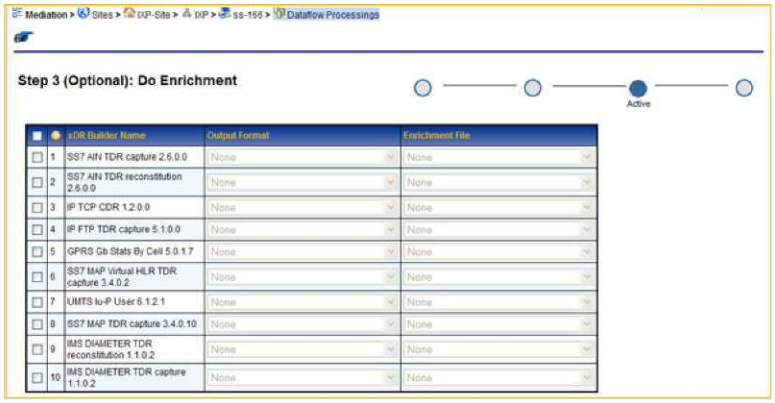
Stream or Dataflov

Click **Next** to choo

Figure 33: Dataflow Assistant xDR Builder Selection

9. Select one or more **xDR Builders** from the four categories (SS7, IP, UMTS/GPRS or Others). **Note:** You can select multiple builders from one or more of the categories.

10. Click **Next** to open the optional *Enrichment* screen.



Mediation > Sites > IXP-Site > IXP > ss-166 > Dataflow Processings

Step 3 (Optional): Do Enrichment

□	●	xDR Builder Name	Output Format	Enrichment File
□	1	SS7 AIN TDR capture 2.6.0.0	None	None
□	2	SS7 AIN TDR reconstitution 2.6.0.0	None	None
□	3	IP TCP CDR 1.2.0.0	None	None
□	4	IP FTP TDR capture 5.1.0.0	None	None
□	5	GPRS Gb Stats By Cell 5.0.1.7	None	None
□	6	SS7 MAP Virtual HLR TDR capture 3.4.0.2	None	None
□	7	UMTS Iu-P User 6.1.2.1	None	None
□	8	SS7 MAP TDR capture 3.4.0.10	None	None
□	9	IMS DIAMETER TDR reconstitution 1.1.0.2	None	None
□	10	IMS DIAMETER TDR capture 1.1.0.2	None	None

Figure 34: xDR Assistant - Enrichment Selection

(Optional) The *Enrichment* screen enables you to select specific output format and files to be included into the dataflow processing that is to be used in data feed exporting.

To create an enrichment complete these steps.

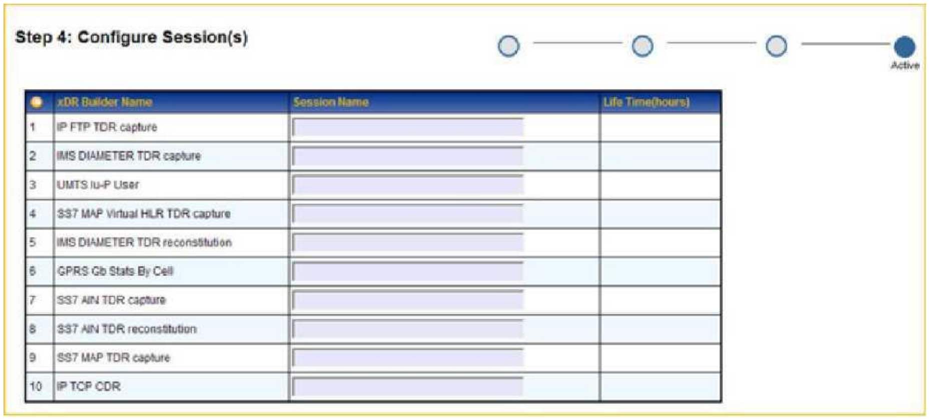
Select an **xDR Builder.** The row is highlighted.

From the *Output Format* column select **upload a new format** or select **none** from the pull-down list.

From the *Enrichment* column select to **upload a new file** or select **none** from the pull-down list.

Repeat **steps a-c** for each builder.

Click **Next** to configure xDR sessions.



Step 4: Configure Session(s)

●	xDR Builder Name	Session Name	Life Time(hours)
1	IP FTP TDR capture		
2	IMS DIAMETER TDR capture		
3	UMTS Iu-P User		
4	SS7 MAP Virtual HLR TDR capture		
5	IMS DIAMETER TDR reconstitution		
6	GPRS Gb Stats By Cell		
7	SS7 AIN TDR capture		
8	SS7 AIN TDR reconstitution		
9	SS7 MAP TDR capture		
10	IP TCP CDR		

Figure 35: xDR Assistant - Configuring Sessions Screen

Type in the **session name.**

Type in the **Life Time** (in hours the default is 72 hours).

Note: The Life Time defines how long an xDR is stored. It is a tuning parameter used as a safeguard to conserve disk space and is an important factor in managing your system. After the set amount of time, the xDRs are deleted from the disk. The longer the life time, the longer that disk space is used by the xDRs. It is important to know how much storage you have on your system when setting the Life Time parameter. If the parameter is set too high, then more disk space will be required than is available on the IXP server. Disk space used per xDR will vary from session to session depending upon the number of columns and enrichment settings.

Repeat **steps 11-14** for each builder session.

Click **Done.**

For changes to take effect, click right-click on the IXP subsystem that has changed, then select **Apply Changes** from the menu.

Monitoring xDRs and PDUs with ProTrace

Once the basic steps of creating a site, discovering subsystems, and routing traffic have been completed in CCM, use ProTrace to monitor the xDRs and PDUs. For more information on using ProTrace see the ProTrace online help.

Opensource notice

Tekelec Global, Inc. ("Tekelec") distributes certain open source software licensed under various open source licenses in association with certain Tekelec products. Below is a listing of open source software distributed by Tekelec identified by the associated Tekelec product.

PIC

The following files are licensed under the GNU General Public License v. 2.0:

(1) chkconfig v. 1.3.49.3
Copyright © Red Hat
(2) ctcs v. 1.3.0
Copyright © Jason T. Collins <jcollins@valinux.com> for VA Linux Systems
(3) drbd v. 8.3.7
Copyright © Philipp Reisner <philipp.reisner@linbit.com> & Lars Ellenberg <lars.ellenberg@linbit.com>
(4) e2fsprogs-libs v. 1.39
Copyright © Theodore Ts'o
(5) gdbm v. 1.8.0
Copyright © Philip A. Nelson, Jason Downs, Sergey Poznyakoff
(6) hp-be2iscsi v. 4.0.480.0
Copyright © ServerEngines Corporation
(7) hp-be2net v. 4.1.450.7
Copyright © Emulex Corporation
(8) hp-e1000 v. 8.0.25
Copyright © Intel Corporation
(9) hp-igb v. 3.2.10
Copyright © Intel Corporation
(10) hp-netxtreme2 v. 7.2.55
Copyright © Broadcom Corporation
(11) hp-netxtreme2-iscsi v. 7.0.39
Copyright © Broadcom Corporation
(12) hp-tg3 v. 3.122q
Copyright © Broadcom Corporation
(13) i2c-tools v. 3.0.0
Copyright © Frodo Looijaard, Mark D. Studebaker and Jean Delvare
(14) initscripts v. 9.03.31
Copyright © Canonical Ltd.
(15) iptables v. 1.4.7
Copyright © Rusty Russell
(16) kernel v. 2.6.32
Copyright © Linus Torvalds
(17) lm_sensors v. 3.1.1
Copyright © Frodo Looijaard, Merlin Hughes, Bob Schlaermann, Mark M. Hoffman, Jean Delvare
(18) lzma v. 4.32.7

Copyright © Igor Pavlov, Ville Koskinen and Lasse Collin

(19) module-init-tools v. 3.9
Copyright © Jon Masters <jcm@jonmasters.org>

(20) net-tools v. 1.6
Copyright © 1988-1994 MicroWalt Corporation, Copyright © 1995-1996 Bernd Eckenfels, Copyright © 1997-2000 Andi Kleen, Copyright © 1997-2000 Donald Becker

(21) qla2xxx v. 8.03.07.13.06.0
Copyright © QLogic Corporation

(22) rhpl v. 0.221
Copyright © Red Hat

(23) rinetd v. 0.62
Copyright © Thomas Boutell

(24) rpm v. 4.8.0
Copyright © Erik Troan and Marc Ewing

(25) udev v. 147
Copyright © Greg Kroah-Hartman

(26) Wireshark v. 0.9
Copyright © 1988, 1992, 1993 The Regents of the University of California, Copyright © 2003 Markus Friedl, Copyright © 2003 Endace Technology Ltd, Hamilton, New Zealand, Copyright © 1995, 1996, 1997 and 1998 WIDE Project, Copyright © 1997, 1999 Hellmuth Michaelis

Each of these programs is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

Each of these programs is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with these programs; if not, see <http://www.gnu.org/licenses/> or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The following files are licensed under the GNU General Public License v. 3.0:

(1) readline v. 6
Copyright © Chet Ramey

(2) selinux-policy v. 3.7.19
Copyright © Tresys Technology

(3) setools v. 3.3.7
Copyright © Tresys Technology

Each of these programs is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version.

The following files are licensed under the GNU Lesser General Public License v. 2.1:

(1) Glib v. 1.231
Copyright © 2003-2005 by the gtk2-perl team
(2) gobject-introspection v. 0.10.8
Copyright © Colin Walters <walters@verbum.org>, Johan Dahlin <johan@gnome.org>, Matthias Clasen <mclasen@redhat.com> and <j@bitron.ch>
(3) kiratool v. 1.5.15
Copyright © Raritan, Inc.
(4) lksctp-tools v. 1.0.11
Copyright © 2002 La Monte H. P. Yarroll; Copyright © 2002, 2004 IBM Corp.; Copyright © 2010, 2013 Red Hat
(5) mysql++ v. 3.0.8
Copyright © Kevin Atkinson
(6) open-vm-tools v. 0.0.0.217847
Copyright © VMware Guest Components Team
(7) perl-Glib-Object-Introspection v. 0.001.20110920git
Copyright © Emmanuele Bassi, muppet, Torsten Schöfeld
(8) perl-Net-XMPP v. 1.02_04
Copyright © Ryan Eatmon
(9) perl-XML-Stream v. 1.23_06
Copyright © Darian Anthony Patrick, Ryan Eatmon, Thomas Charron, Jeremie
(10) teng v. 2.0.4
Copyright © Seznam.cz, a.s., Jan Nemec
(11) Adobe BlazeDs v. 3.2
Copyright © Adobe
(12) xhtmlrenderer v. 4
Copyright © xhtmlrenderer
(13) AntXtras v. 2.0.1, 3.0.0, 3.5.0b2
Copyright © iDare Media, Inc.
(14) DBUnit+C93 v. 2.1
Copyright © DbUnit.org
(15) Crystal Project Icons
Copyright © Everaldo Coelho
(16) joeSNMP v. 0.3.4
Copyright © 2002-2003 Blast Internet Services, Inc., Copyright © 1999-2001 Oculan Corp.

(17) GWT Component Library
Copyright © Google

Each of these programs is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

Each of these programs is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with these programs; if not, see <http://www.gnu.org/licenses/> or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The following files are licensed under the GNU Lesser General Public License v. 3:

(1) Ext JS - JavaScript Library v. 2
Copyright © Ext JS, LLC
(2) JFreeChart v. 1.0.12
Copyright © JFreeChart

Each of these programs is free software: you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

Each of these programs is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with these programs; if not, see <http://www.gnu.org/licenses/> or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The following files are licensed under the MPL License v. 1.1:

(1) nss v. 3.13.5
Copyright © The Regents of the University of California, The Open Group, Network Computing Devices, Inc., X Consortium, Sun Microsystems, Inc., Massachusetts Institute of Technology, Jean-loup Gailly, Mark Adler, Red Hat, Inc, RSA Security Inc., Netscape Communications Corporation, Michael J. Fromberger, Mark Adler
(2) nss-softokn v. 3.12.9
Copyright © The Regents of the University of California, The Open Group, Network Computing Devices, Inc., X Consortium, Sun Microsystems Inc., Netscape Communications Corporation, Michael J.

Fromberger
(3) nss-util v. 3.13.5
Copyright © The Regents of the University of California, The Open Group, Network Computing Devices, Inc., X Consortium, Network Computing Devices, Inc., RSA Security Inc., Sun Microsystems Inc.

The contents of each of these files are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use these files except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/.

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The following files are licensed under the MPL License v. 2.0:

(1) nspr v. 4.9.1
Copyright © Netscape Communications Corporation, Lucent Technologies, Student Information Processing Board of the Massachusetts Institute of Technology, The Regents of the University of California, Digital Equipment Corporation, Internet Systems Consortium, Inc.

The Source Code Form of this file is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, you can obtain one at http://mozilla.org/MPL/2.0/. A copy of the Source Code Form of each of these files can be located as http://support.tekelec.com
.

The following files are licensed under the Apache License v. 1.1.

log4cplus-1.0.2-6.0.0_80.8.0.x86_64.rpm
Copyright © Tad E. Smith tcsmith@users.sourceforge.net

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-1.1 (the "License").

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The following files are licensed under the DOC Software License:

ace-6.0.1-6.0.0_80.8.0.x86_64.rpm
Douglas C. Schmidt
Ace-6.0.1-6.0.0_80.1.0
Douglas C. Schmidt

You may obtain a copy of the License at http://www.cs.wustl.edu/~schmidt/ACE-copying.html.

The following files are licensed under the Creative Commons Attribution License v. 2.5: