DIH 1.2

DIH Quick Start User Guide

910-6517-001 Revision A

August 2012

Table of Contents

List of Figures

List of Tables

Chapter 1

About This Help Text

Topics:

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 Diameter Intelligence Hub (DIH)

The Diameter Intelligent Hub (DIH) is used to monitor a LTE network. DIH also creates a small hardware "footprint" for customers who administer 3G and 4G diameter networks. The DIH:

- Is a single blade server and storage blade collocated within a single or dual Diameter Signaling Router (DSR) enclosure(s).
- Provides filtering, data feed, tracing, decoding, and SNMP functions.
- Enables the selective collection and storage of diameter traffic within one or more instances of PMF and IXP.
- Provides nodal diameter troubleshooting.
- Provides data export for diameter messages.
- Supports both IPv4 and IPv6 traffic simultaneously.
- Provides KPI tracking using ProTrace application as well as viewing KPIs in graphic format using ProPerf dashboard configured at installation.
- Provides filtering for alarms using ProTraq Cell filter (see system alarms online help).
- Uses diameter protocol exclusively.

  Note: The DIH system can use other protocols if the Diameter mode has not been selected and system is in Standard mode. (Default setting is Standard mode. For more information on selecting Diameter mode, see Centralized Configuration Manager Administration online help, "Setting System to Diameter Mode."

The Diameter Protocol

The diameter protocol has evolved from the Radius protocol and enables diameter applications to extend the base protocol by adding new commands and/or attributes, such as those for use of the Extensible Authentication Protocol (EAP).

The diameter protocol provides for an Authentication, Authorization, and Accounting (AAA) framework that overcomes the limitations of RADIUS, (a protocol that handles AAA and EAP), which cannot effectively deal well with remote access, IP mobility and policy control. The Diameter protocol defines a policy protocol used by clients to perform Policy, AAA and Resource Control. This allows a single server to handle policies for many services.

As mentioned above, Diameter protocol provides AAA functionality, but in addition it is made more reliable by using TCP and SCTP instead of UDP. The Diameter protocol is further enhanced by the development of the 3rd Generation Partnership Project (3GPP) IP Multimedia Subsystem (IMS). Through the use of extensions, the protocol was designed to be extensible to support Proxies, Brokers, Strong Security, Mobile-IP, Network Access Servers (NASREQ), Accounting and Resource Management.

Setting User Preferences

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

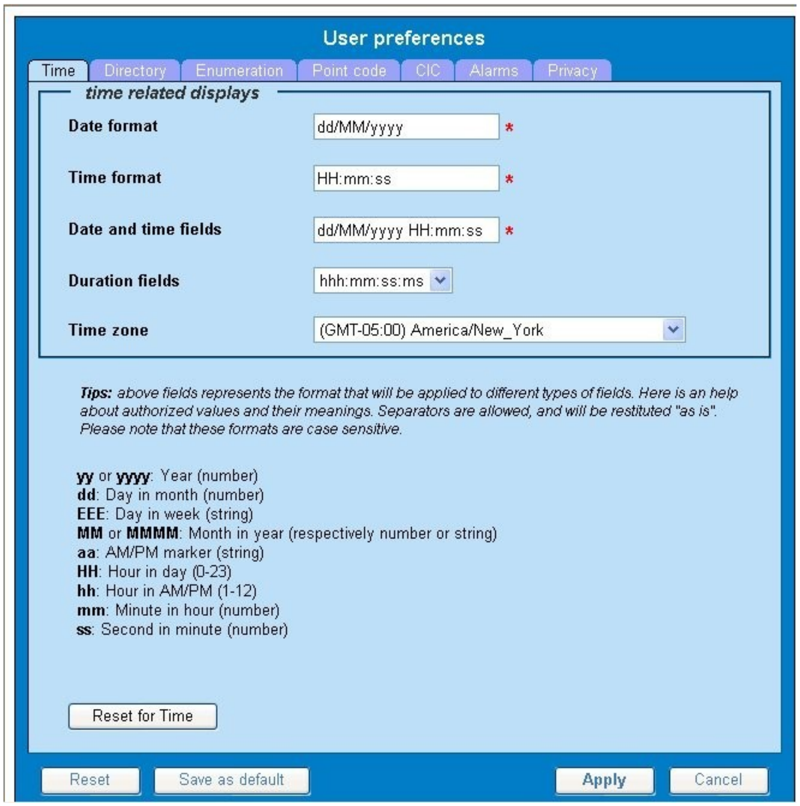
- Time specifications (date format, time zone, etc.)
- Directory names (for exporting, uploading, and downloading)
- Enumeration values (numerals vs. text)
- Point code specifications
- CIC specifications
- Default alarm colors
- Default object privacy privileges

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.



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 1: 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.

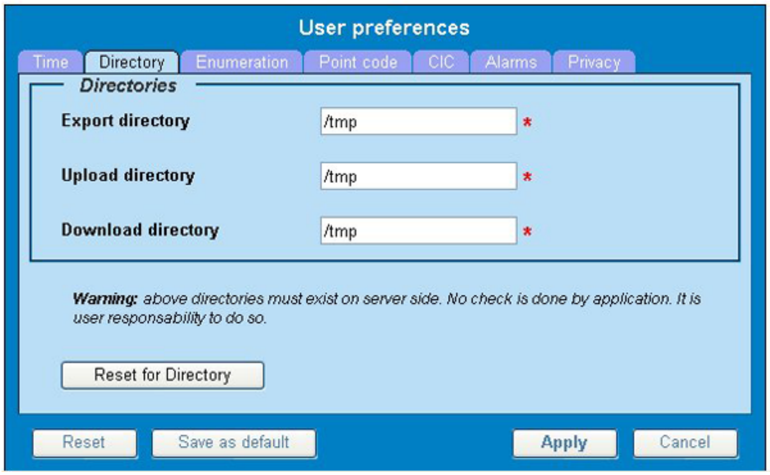
Setting Directory Preferences

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 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 2: Directory Page

3. Type in the following:
   - **Export directory**
   - **Upload directory**
   - **Download directory**

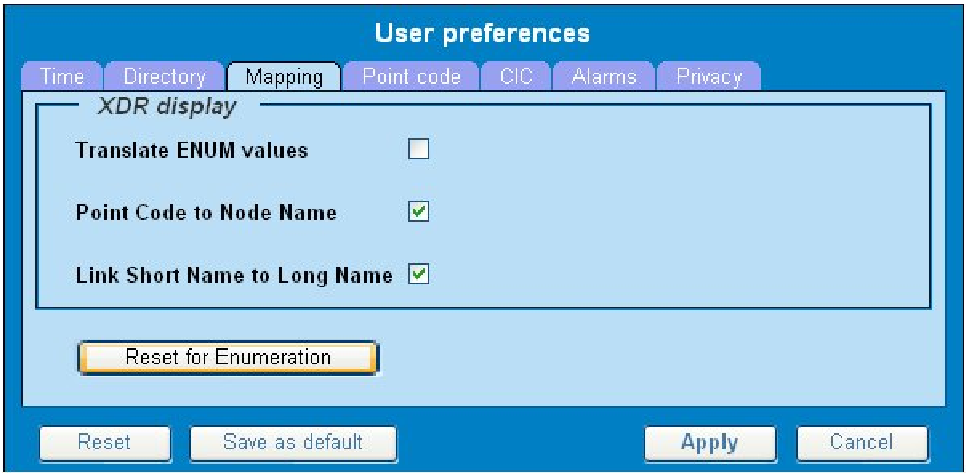
4. If you want to reset the directories to default settings, click **Reset for Directory.** (The bottom **Reset** button resets all the tabbed pages to default settings.)
5. Click **Apply** to save your settings.

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.



Translate ENUM values □

Point Code to Node Name ☑

Link Short Name to Long Name ☑

Figure 3: Mapping Page

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

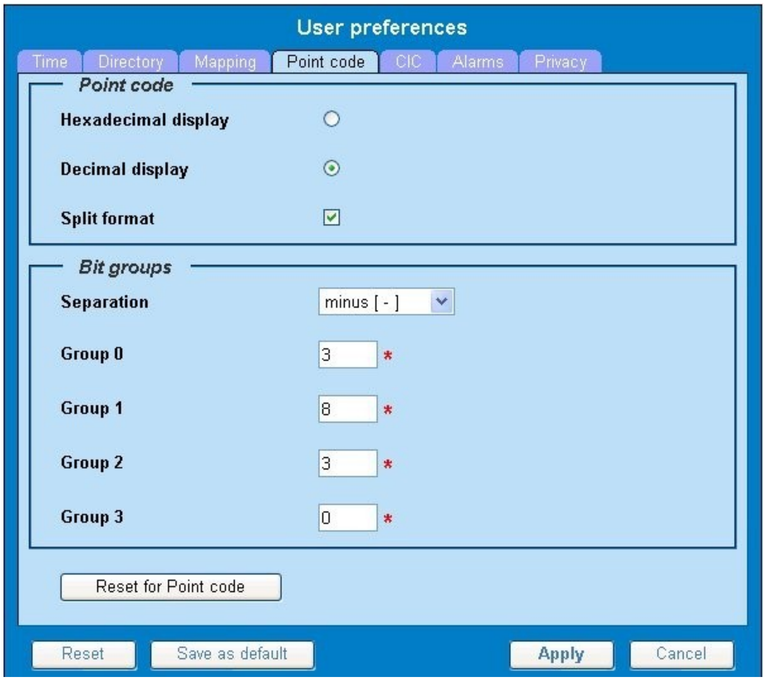
   Enumeration is used by xDRs to display text values instead of numeric. (For example, rather than showing the numeral for Alarm Severity, the user interface will show the actual word, such as "Major" or "Critical.")
4. Check **Point Code to Node Name** to display the custom (user-defined) name of the node. Otherwise, the Point Code value is displayed.
5. 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 (*).
6. To reset the Mapping values to the default, click **Reset for Enumeration**. (The bottom **Reset** button resets all the tabbed pages to default settings.)
7. 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.



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 4: Point Code Tab

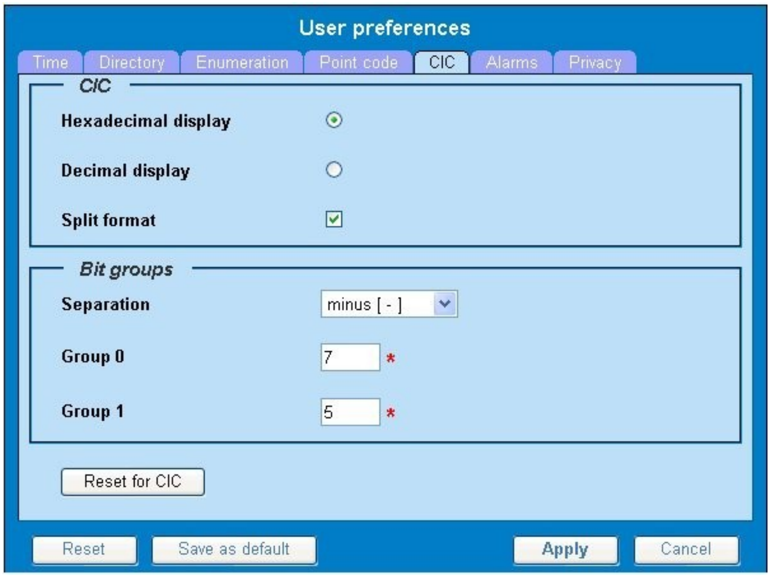
3. Select either **Hexadecimal display** or **Decimal display**.
4. Select or de-select **Split format**.
   If **Split format** is checked, the Bit groups settings in the box below are active. If **Split format** is not checked, Bit groups settings are not applicable.
5. If you selected Split format above, go to the next step. If you did not select Split format, go to step *Step 8*.
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 required field.



CIC

Hexadecimal display ●

Decimal display ○

Split format ☑

Bit groups

Separation minus [-]

Group 0 7 *

Group 1 5 *

Figure 5: CIC Page

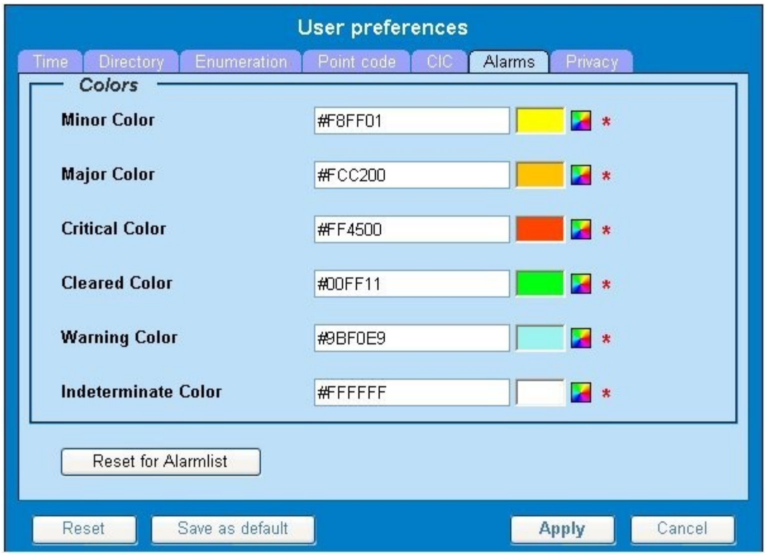
3. Select either **Hexadecimal display** or **Decimal display**.
4. Select or de-select **Split format**.
   If **Split format** is checked, the Bit groups settings in the box below are active. If **Split format** is not checked, Bit groups settings are not applicable.
5. If you selected Split format above, go to the next step. If you did not select Split format, go to step *Step 8*.
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.

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.

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



Minor Color #F8FF01 *

Major Color #FCC200 *

Critical Color #FF4500 *

Cleared Color #00FF11 *

Warning Color #9BF0E9 *

Indeterminate Color #FFFFFF *

Figure 6: Alarms Page

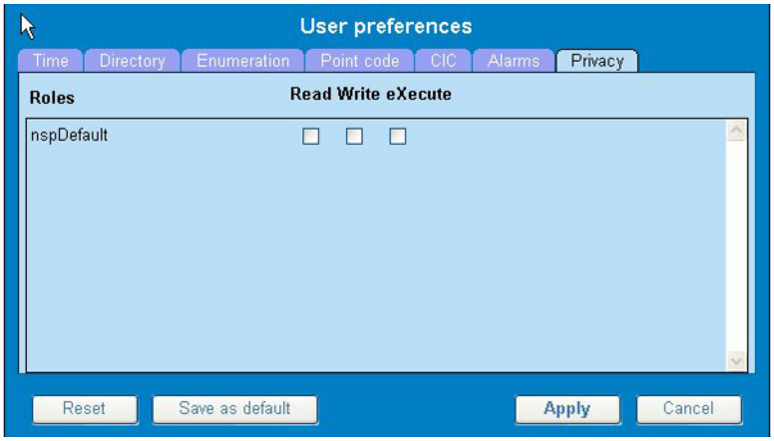
3. Click the color palette (icon on the right side of the screen) associated with the alarm status color(s) you want to modify.
   A pop-up palette window is displayed.
4. Click the color you want for the type of alarm.
   The color palette pop-up is closed and the color box for the alarm displays the selected color. The number for the color is also displayed.
5. 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.)
6. 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:

1. Click **User preferences** in the Application board menu.
   The User Preferences window is displayed. The **Time** tab is active by default.
2. Click the **Privacy** tab .
   The Privacy page is displayed.



Roles	Read	Write	eXecute
nspDefault	□	□	□

Figure 7: Privacy Page

3. 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.
4. Click **Save as default**.
5. To reset all the tabbed pages to default settings, click **Reset**.
6. 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:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **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

DIH Documentation Library

DIH 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 DIH documentation library of online help.

- Centralized Configuration Manager Administration Online Help
- Alarm Forwarding Administration Online Help

- Diagnostic Utility Administration Online Help
- ProTrace Online Help
- System Alarms Online Help
- ProPerf Online Help
- ProTraq Configuration Online Help
- Data Feed Export Online Help
- System Alarms Online Help

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.

1. 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.

2. Click the **Product Support** tab.
3. 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.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Diameter Intelligent Hub (DIH) - Copyright, Notice, Trademarks, and Patents

Notice

Information in this documentation is subject to change without notice. Unauthorized use, copying, or translation of this documentation can result in civil or criminal penalties.

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced, translated, or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec's WEEE program, contact your sales representative.

Trademarks

TEKELEC, EAGLE, G-Flex, G-Port, and CAMIANT are registered trademarks of Tekelec. The Tekelec logo, A-Port, EAGLE 5, EAGLE 5 ISS, IP7, IP7 Secure Gateway, V-Flex, ngHLR, BLUESLICE, and Subscriber Data Server (SDS) are trademarks of Tekelec. All other trademarks are the property of their respective owners.

Patents

This product may be covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:

6,456,845; 6,765,990; 6,968,048; 7,043,001; 7,155,512; 7,206,394; 7,215,748; 7,231,024; 7,286,516; 7,286,647; 7,401,360; 7,706,343; 7,844,033; 7,860,799;

Foreign Patent Numbers:

None.

Chapter 2

Setting Up a Basic System

Topics:

Basic Workflow

This outline represents the main steps in configuring a basic DIH system with traffic. For more detail on configuring a DIH 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 an PMF subsystem for the site.

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

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

   - Create and configure PDU Dataflows. *About Dataflow Processings* and *Configuring Dataflow Processings*
   - (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*

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

   - Create Dataflow Processings. *Configuring Dataflow Processings*

5. 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 the DIH application ProPerf (if activated). For more information on the ProPerf application, see ProPerf online help.

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.

1. Select **Equipment Registry > Sites**.
2. Click **Add** from the tool bar.

   Note: You can also right-click on the sites icon and select **Add** from the menu.
3. Type in a site **Name**.
4. (Optional) Type in a **Description** of the site that gives useful information about the site.
5. 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 PMF) 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@ixp0301-1c ~]# 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:1000
          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:16436  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:1952272307 (1.8 GiB)
```

In this example the B-cast 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 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.

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

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 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.
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.

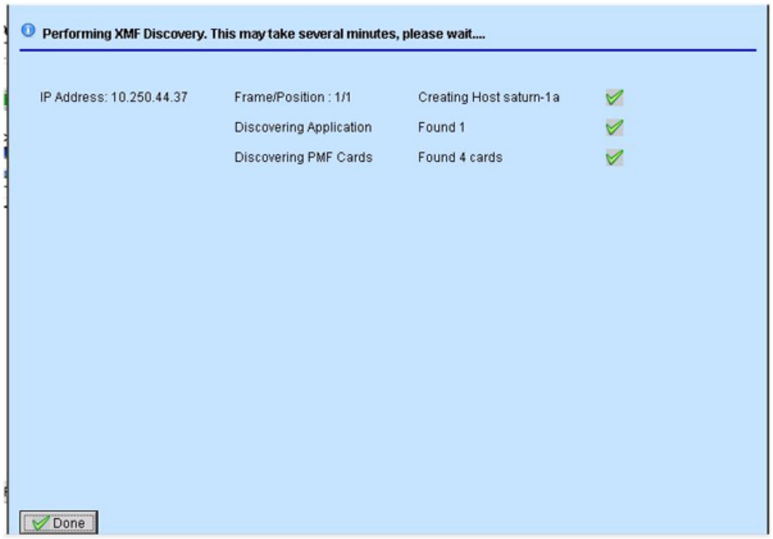
3. Enter the **VIP Address**.

4. Enter an **IP Address** for the PMF host.
5. Click **Add**.
6. 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.



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 ✓

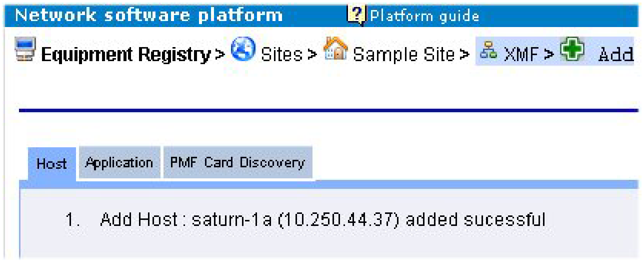
Discovering PMF Cards Found 4 cards ✓

Figure 8: 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:

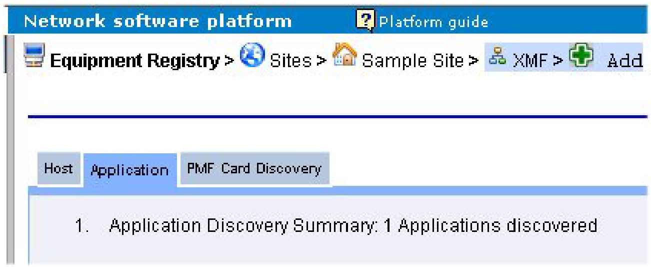
   a) Host tab - showing the IP addresses of the discovered hosts and the result
   b) Application - showing the applications that were discovered
   c) PMF Card Discovery - showing the cards installed on the host



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 9: Discovery Summary Screen - Hosts Tab

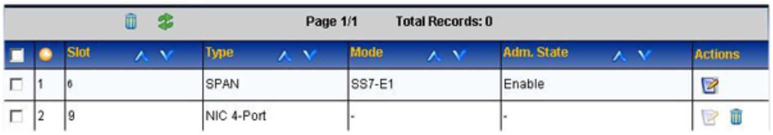

Network software platform
Platform guide
Equipment Registry > Sites > Sample Site > XMF > Add
Host
Application
PMF Card Discovery

1. Application Discovery Summary: 1 Applications discovered

Figure 10: 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.).



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

Figure 11: 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.

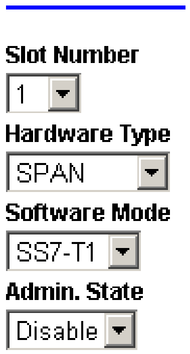
   Note: Network cards and NGP cards are automatically discovered and do not have to be manually added.

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.

1. Select **Acquisition > Site (with PMF subsystem) > subsystem > Server > Cards**.
2. 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 12: 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 E1/T1 Cards (PMF)

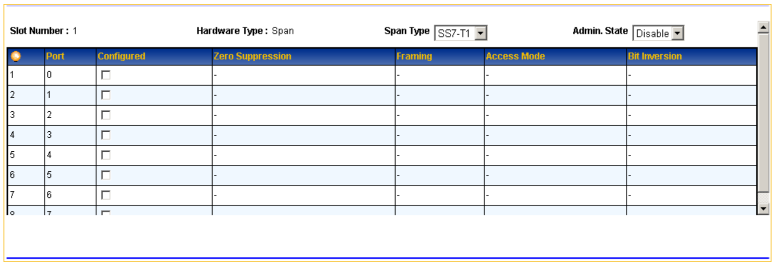
After you have created a PMF subsystem and discovered its applications, you can configure the PMF applications. Complete these steps to configure a PMF application (E1/T1 Span Card).

1. Select **Acquisition > Site (with PMF subsystem) > PMF Subsystem > Server > Cards** .
2. Select the appropriate **Card**.

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

3. Right-click on the **Card**.
4. Click **Modify**.

   The Card screen opens showing the cards ports.



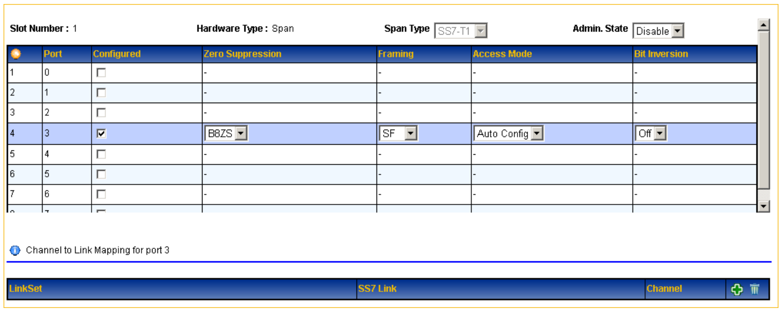
Slot Number : 1 Hardware Type : Span Span Type SS7-T1 Admin. State Disable

●	Port	Configured	Zero Suppression	Framing	Access Mode	Bit Inversion
1	0	□	-	-	-	-
2	1	□	-	-	-	-
3	2	□	-	-	-	-
4	3	□	-	-	-	-
5	4	□	-	-	-	-
6	5	□	-	-	-	-
7	6	□	-	-	-	-

Figure 13: Span Card Screen with Unconfigured Ports

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

   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.



Slot Number : 1 Hardware Type : Span Span Type SS7-T1 Admin. State Disable

●	Port	Configured	Zero Suppression	Framing	Access Mode	Bit Inversion
1	0	□	-	-	-	-
2	1	□	-	-	-	-
3	2	□	-	-	-	-
4	3	☑	B8ZS	SF	Auto Config	Off
5	4	□	-	-	-	-
6	5	□	-	-	-	-
7	6	□	-	-	-	-

Channel to Link Mapping for port 3

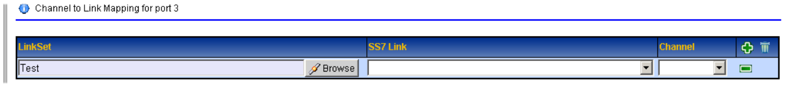
LinkSet	SS7 Link	Channel

Figure 14: Span Card Configure Screen with Channel Link Mapping Section

6. Modify the various **parameters** in the port.
7. 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 15: 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.

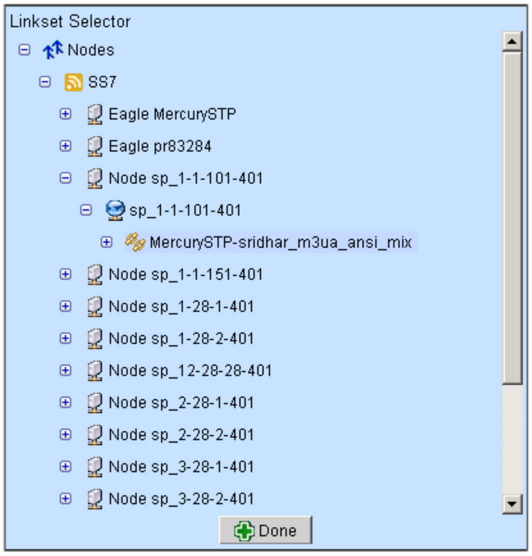


Figure 16: Span Card Configure Screen with Channel Link Mapping Add Screen

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

9. Select the **Link** associated with the linkset.
10. Select the **Port** associated with the linkset.
11. 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.

Setting System to Diameter Mode

Complete these steps to select Diameter mode for a system.

Note: The default setting is "standard" for a system where mode where a variety of traffic classifications (TCs) are created and filters are chosen for those TCs. In Diameter mode there are predefined traffic classifications and filters are chosen just for those pre-defined TCs.

1. Select **Acquisition** > **Sites** > **PMF Site** > **Servers** > **xMF Server** > **Traffic Classifications** from the object menu.

   The Traffic Classifications (TC) list screen opens.
2. From the tool bar, select **Diameter Mode** from the drop-down list at the right-hand side of the tool bar.
3. Click **OK** at the prompt to deactivate TCs in standard mode.
   The three Diameter Traffic Classifications are listed in table format shown in this table.

Column Heading	Description
Selection	This column is for selecting specific TCs.
Record #	This shows the numerical order of the TC in the table.

Column Heading	Description
Traffic Classification Name	Provides the Name of the TC. For Diameter Setting there are only three TCs. They are: • Diameter_Exception • Diameter_Frag • Diameter_Trace **Note:** None of the TCs can be deleted. The only TC that can be modified is Diameter_Trace
Description	(Optional) This column shows any description of the TC.
Internet Protocol	Shows the Internet protocol used (default is ALL).
Transport Protocol	Shows the transport protocol used (default is ALL).
Application Layer	Shows the application layer (ID) used (default is ALL).
Forwarding	Shows the forwarding medium (default is Packets).
Policy	Shows the policy used for the TC.
Annotation	Shows any annotation used for the TC.
Status	Shows the status (shows green for active or red for inactive)
Owner	Shows the name of the user that created the TC.

Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

About Diameter Protocol Filters

Diameter PDU filters are used only when the Traffic Classification for a specific server is set to Diameter. (See "Setting System to Diameter Mode" for more information.)

Multiple Diameter filters can be created but only one filter can be used at a time. The specificity of the filter is based on a combination of any or all of the four components listed at the end of this topic.

Note: When adding a Diameter PDU filter, if the system recognizes Application, Command Code and Host (AND/OR logic) or Realm (OR logic), then the filter will pass the packet to IXP for correlation and storage.

Note: Diameter PDU filters can also be used when creating Combination Filters. (See About IP Combination Filters for more information.)

- Application

- Command Code
- Host
- Realm

Adding a Diameter PDU Filter

Note: When adding a Diameter PDU filter, if the system recognizes any of four components (OR logic filtering), then the filter will pass the packet to IXP for correlation and storage. The four components are represented in the following fields: Enter ApplicationID, Enter Command Code, Enter Host, Enter Realm.

Note: Diameter PDU filters can also be used when creating Combination Filters. (For more information, see "About IP Combination Filters."

Complete these steps to add a Diameter PDU filter.

1. In CCM, select **Acquisition > PDU Filters** from the object menu.

   The PDU Filters list screen opens.
2. Click **Add** on the tool bar (green **+** sign).

   PDU Filter Family screen opens.
3. Select **Diameter - protocol**
4. Click **Next**.

   The Diameter Filters screen opens.

   The table describes the fields on this screen.

Table 2: Diameter Filter Screen Fields

Field	Description
Filter Name	Alphanumeric field providing name of the filter
Description	(Optional) Alphanumeric field for short description of the filter
Enter ApplicationID	Provides the numeric ID for the Application for the diameter filter Numeric field with range of 0- 4294967295
Enter Command Code	Numeric field that provides numeric ID for the 24-bit command code Numeric field with range of 0- 16777215
Enter Host To match Origin-Host or Destination-Host	Provides the Host ID for either the Origin or the Destination An alphanumeric field with no constraints **Note:** The name must be a Fully Qualified Domain Name (FQDN) For exa 123.xyz.com (where 123 = HSS or MME and xyz = domain)
Enter Realm To match Origin-Realm or Destination-Realm	Provides the Host ID for either the Origin or the Destination An alphanumeric field with no constraints **Note:** Just a Domain Name (DN) For example: xyz.com

Field	Description
Add button	Adds the a value of the parameter to the list **Note:** There can be multiple values of each parameter
Remove	Removes the value from the parameter list

Note: Any combination of the fields, ApplicationID, Command Code, Host and Realm can be used.

Note: The fields ApplicationID, Command Code and Host utilize both AND/OR functionality in order to make a filter more specific. The Realm field uses only OR functionality for inclusion.

For example, a simple filter with Command Code (C1) and Host (H1) would filter out all other possibilities that do not contain both of those fields `(C1 AND H1)`. The same filter could include Realm (R1) along with Command Code and Host since the Realm field uses the OR functionality `(C1 AND H1) OR (R1)`. If there are multiple entities for a field (for example Command Code such as C1, C2), then the filter equation would be `((C1 or C2) and (H1)) or (R1)`

5. Enter the **Filter Name**.
6. (Optional) Enter a **Description** of the Diameter filter.
7. Enter the **Application ID** (if one is used).
8. Click **Add** to add it to the Application list.
9. Enter a **Command Code** (if one is used).
10. Click **Add** to add it to the Command Code list.
11. Enter the **Host** (if one is used).
12. Click **Add** to add it to the Host (Origin or Destination) list.
13. Enter the **Realm** (if one is used).
14. Click **Add** to add it to the Command Code list.
15. Click **Finish**.

    The filter appears in the PDU filter list.

    Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

Modifying a Diameter PDU Filter

Complete these steps to modify a Diameter PDU filter.

1. Select the **Diameter filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.

    Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

Deleting a Diameter PDU Filter

Complete these steps to delete a Diameter PDU filter.

1. Select the **Diameter filter** to be deleted.
2. Select **delete** from the tool bar.
3. Click **OK** at the prompt.

   Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

About PMF Traffic Classifications

A Traffic Classification on PMF is used by 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 also used to process the captured MSUs/PDUs received from the IP probe.

Note: Only when CCM has been set to DIH mode, can traffic classifications capture both IPv4 and IPv6 traffic using specific filters and protocols. See topics about configuring traffic classifications to capture IPv6 and IPv4 traffic

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.

DIH when monitoring DSR, filters IP traffic on the Diameter protocol.

DIH filters IP traffic on these protocols.

- FTP
- SFTP

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

Adding a Traffic Classification (PMF)

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

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

   The List screen opens.
2. Click **Add** on the tool bar to open the wizard.
3. Enter the **Name** of the traffic classification.
4. (Optional) Enter a **Description**.
5. Select an **Internet Protocol** from the pull-down list.

   Note: When IPv6 is selected both transport protocol and filters options are disabled.
6. 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).

7. Select an **Application Layer** from the pull-down list.
8. Select a **Filter**.

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

9. 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.

10. Select an **Association** to be associated with the TC.
    a) If SCTP is selected, click **Association Selector** from the Association Selector tool bar.
    b) Select one or more **Associations** from the Association Selector pop-up screen.
    c) Click **Select** to add the associations to the traffic classification.
11. Click **Next** to open the probe assignment screen.
12. Select one or more **probes** from the available options field.
13. Click the **right arrow (>)** to move them to the selected options field.
14. Click **Next** to open the Annotation screen.
15. Enter an **Annotation**.
16. (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**.

17. 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.

1. Select **Acquisition > Sites > Subsystem >PDU Data Flows > GPRS > Add**.
2. Type in the **Name** of the *Gb dataflow*.
3. (Optional) Type in a **description** of the dataflow record.
4. Click **Next**.
5. Select a **Gb Filter** from the drop-down menu.
6. Enter the **number** for packet truncation.
7. Click **Next**.
8. Click the **Gb link** icon.

9. Enter the **Gb Link Name**.
10. Click **Apply Filter**.
11. Select **Gb Link Record** from the list.
12. Click **Select**.
13. Click **Close**.
14. 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 3: 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. (For more information 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.

4. Enter the **Name** of the IXP subsystem.
5. Enter the **VIP Address** of the subsystem.

6. Enter the **IP Address** of the subsystem.
7. Click **Add** to add the subsystem to the list.

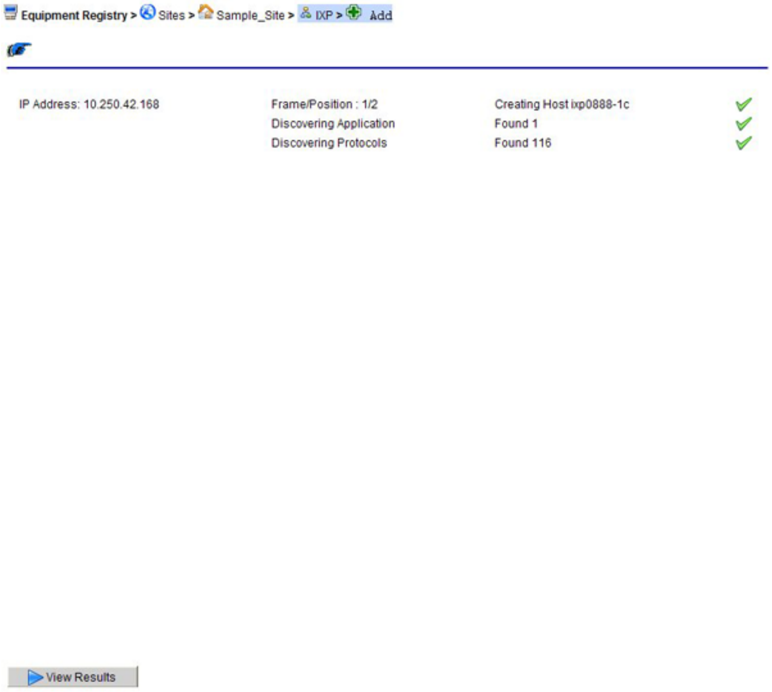
   Note: Repeat steps 4-7 to add each additional subsystem.

8. 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.

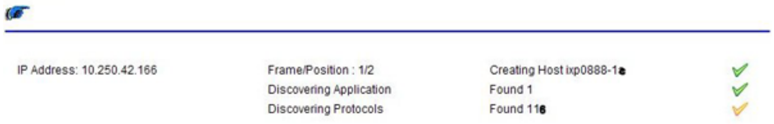
   Note: Use the *Modify* function to add a host(s) to an IXP subsystem.



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 17: 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 18: Results Summary Screen With Error Symbol

9. Click **View Results**.

   The Results screen opens.

   The screen has four tabs with five subtabs:

a) Host - Shows the host parameters and status (added successfully or not)
b) Application - Shows a summary of the number of applications discovered
c) 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.

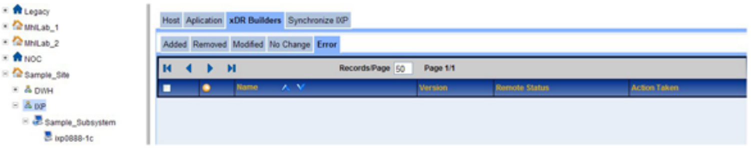


Figure 19: Object Tree Showing Added Subsystem With Results Screen

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 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 PMF over the input stream that was created for the PMF 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.

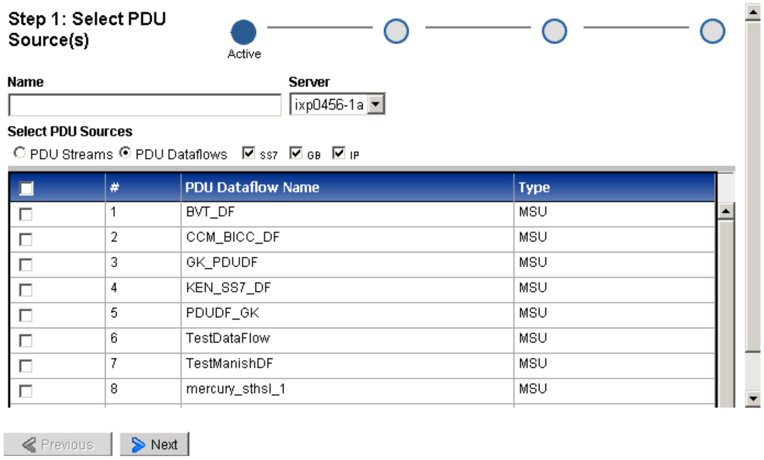
Configure dataflow processings using the xDR Dataflow Assistant.

1. Select **IXP subsystem > Subsystem** that needs the configured dataflow processings.
2. 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 20: xDR Dataflow Assistant Initial Screen-PDU Sources

5. Type in the **Name** of the Dataflow Process.
6. Select the **server**.

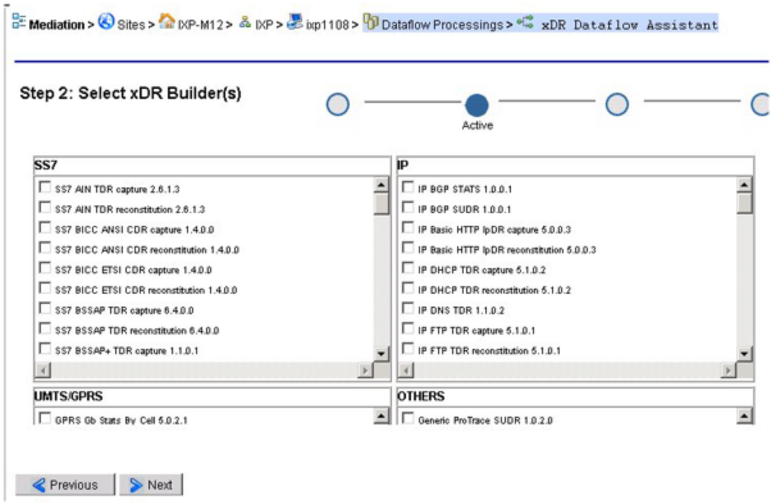
   Note: Do not use the DWH as the server for the Dataflow Process.

   Note: If multiple dataflow processes are created, it is recommenced that more than one server be used to facilitate load balancing.

7. Select a **PDU Source** from the table.

   You can filter by selecting what type of source you want to view/use. For example, whether the source is a Stream or Dataflow and what category (SS7, Gb, IP) it is.

8. Click **Next** to choose an xDR Builder.



Mediation > Sites > IXP-M12 > IXP > ixp1108 > Dataflow Processings > xDR Dataflow Assistant

Step 2: Select xDR Builder(s)

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

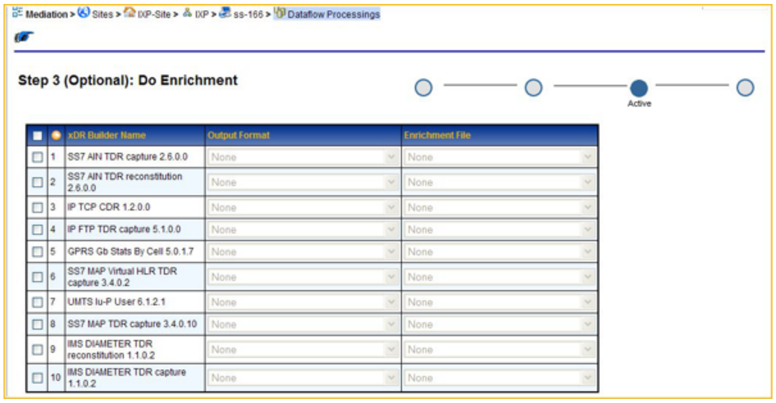
- ☐ Generic ProTrace SUDR 1.0.2.0

Figure 21: 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 22: xDR Assistant - Enrichment Selection

11. (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.

    a) Select an **xDR Builder**.

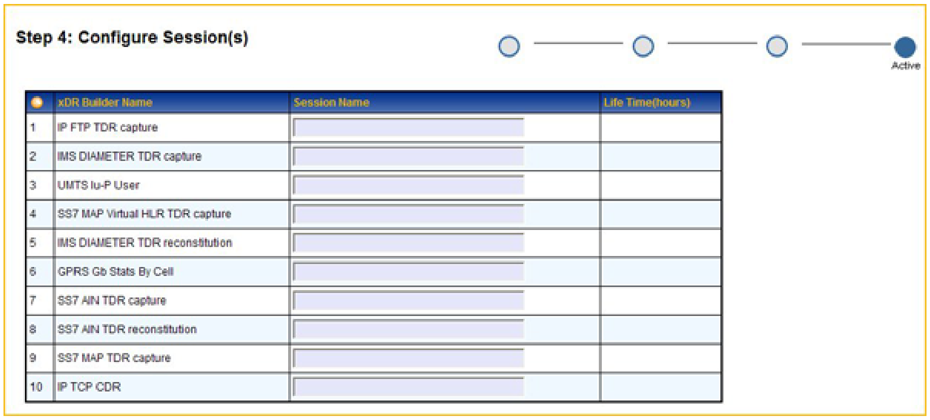
       The row is highlighted.

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

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

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

12. 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 23: xDR Assistant - Configuring Sessions Screen

13. Type in the **session name**.
14. 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.

15. Repeat **steps 11-14** for each builder session.
16. 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.