# Table of Contents

Chapter 1: Introduction.........................................................................................7
  Revision History..................................................................................................8
  Overview................................................................................................................8
  Scope and Audience..............................................................................................8
  Manual Organization............................................................................................8
  Documentation Admonishments..........................................................................8
  Related Specifications..........................................................................................9
  Locate Product Documentation on the Oracle Help Center Site.......................9
  Customer Training..............................................................................................10
  My Oracle Support (MOS)..................................................................................10
  Emergency Response..........................................................................................10

Chapter 2: Introduction to Alarm Forwarding.................................................12
  Overview................................................................................................................13
    Setting User Preferences on IDIH Dashboard...................................................13
  Alarm Forwarding Key Features.........................................................................14
  Alarm Forwarding Architecture..........................................................................14

Chapter 3: Working in Alarm Forwarding........................................................21
  Accessing Alarm Forwarding...............................................................................17
  Alarm Forwarding Toolbar....................................................................................17
  Alarm Status Indicator........................................................................................17
  Using Alarm Forwarding......................................................................................19
    Creating a Filter..................................................................................................19
    Editing a Filter....................................................................................................19
  Alarm Forwarding Test Connection....................................................................21
    Test Connection for SMTP................................................................................21
    Test Connection for SNMP...............................................................................22

Chapter 4: SNMP Agent.....................................................................................23
  SNMP Overview..................................................................................................24
  Alarm Forwarding MIB.......................................................................................24
List of Figures

Figure 1: Alarm Forwarding Toolbar............................................................................................................17
Figure 2: Alarm Status Indicator....................................................................................................................18
Figure 3: Alarm List.........................................................................................................................................19
Figure 4: Filter Creation Dialog......................................................................................................................20
Figure 5: Connection Test Dialog...................................................................................................................21
List of Tables

Table 1: Admonishments.................................................................................................................................. 9

Table 2: Alarm Forwarding Toolbar Icons................................................................................................... 17
Chapter 1

Introduction

This section contains an overview of the available information for the Integrated Diameter Intelligence Hub.

The contents include sections on the organization, scope, and audience of the documentation, as well how to receive customer support assistance.

Topics:

- Revision History.....8
- Overview.....8
- Scope and Audience.....8
- Manual Organization.....8
- Documentation Admonishments.....8
- Related Specifications.....9
- Locate Product Documentation on the Oracle Help Center Site.....9
- Customer Training.....10
- My Oracle Support (MOS).....10
- Emergency Response.....10
Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2011</td>
<td>Initial Release</td>
</tr>
<tr>
<td>June 2016</td>
<td>Updated to include accessibility changes</td>
</tr>
</tbody>
</table>

Overview

This documentation provides information about the functions of the Alarm Forwarding application of the Integrated Diameter Intelligence Hub (IDIH).

**Note:** The Alarm Forwarding application is only available to users logging into IDIH as `idihadmin`.

Scope and Audience

This user’s guide provides information about the Alarm Forwarding application. This guide provides definitions and instructions to help the user efficiently and effectively define conditions and destinations for forwarding Alarms.

Manual Organization

*Introduction* contains general information about this document, how to contact *My Oracle Support (MOS)*, and *Locate Product Documentation on the Oracle Help Center Site.*

*Introduction to Alarm Forwarding* provides an introduction to the Alarm Forwarding application.

*Working in Alarm Forwarding* contains information about procedures used while using the Alarm Forwarding application.

*SNMP Agent* contains information about the SNMP Agent of the Alarm Forwarding application.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.
Table 1: Admonishments

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="DANGER" /></td>
<td>Danger: (This icon and text indicate the possibility of personal injury.)</td>
</tr>
<tr>
<td><img src="image" alt="WARNING" /></td>
<td>Warning: (This icon and text indicate the possibility of equipment damage.)</td>
</tr>
<tr>
<td><img src="image" alt="CAUTION" /></td>
<td>Caution: (This icon and text indicate the possibility of service interruption.)</td>
</tr>
<tr>
<td><img src="image" alt="TOPPLE" /></td>
<td>Topple: (This icon and text indicate the possibility of personal injury and equipment damage.)</td>
</tr>
</tbody>
</table>

Related Specifications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

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

2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings “Network Session Delivery and Control Infrastructure” or “Platforms.”
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select **Save target as** (or similar command based on your browser), and save to a local folder.

**Customer Training**

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

*http://education.oracle.com/communication*

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

*www.oracle.com/education/contacts*

**My Oracle Support (MOS)**

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

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

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

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

**Emergency Response**

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:
• A total system failure that results in loss of all transaction processing capability
• Significant reduction in system capacity or traffic handling capability
• Loss of the system’s ability to perform automatic system reconfiguration
• Inability to restart a processor or the system
• Corruption of system databases that requires service affecting corrective actions
• Loss of access for maintenance or recovery operations
• Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.
This chapter provides basic information about the Alarm Forwarding application.

Topics:

- Overview.....13
- Alarm Forwarding Key Features.....14
- Alarm Forwarding Architecture.....14
Overview

Alarm Forwarding enables the user to forward alarms to specified destinations. The user can create alarm forwarding rules using Filters.

This application handles several types of alarms, including those pertaining to:
- Traffic supervision
- Quality of service
- System errors

Setting User Preferences on IDIH Dashboard

Once inside IDIH, a user can set User Preferences. These include:
- Time specifications (such as date format, time zone)
- Enumeration values (numerals vs. text)
- Default alarm colors

Setting Time Format

Follow these steps to set the time format:

1. Click User Preferences on the Application board.
   The User Preferences screen is displayed.

2. Click the Date/Time tab.
   The Date/Time screen is displayed. The red asterisk denotes a required field.
   **Note:** Use the tips on the screen to help configure the time format.

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 - how the hours, minutes, seconds, and milliseconds of the Time format is displayed
   - Time zone
   **Note:** The local time zone must be chosen to get local time.

5. To reset the time-related displays to default settings, click **Reset**.
6. Click **Apply** to save settings.

Setting Mapping Preferences

The user 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 screen is displayed.
2. Click the **Mapping** tab.
   The Mapping screen is displayed.
3. Check **Translate ENUM values** to display text instead of numerals.
   Enumeration is used by TDRs to display text values instead of numeric. Rather than showing the numeral for Alarm Severity, the user interface will show the actual word, such as Major or Critical.
4. Check **IP Address to Node Name** to translate an IP Address to a textual Node Name.
5. To reset the Mapping values to the default, click **Reset**.
6. Click **Apply** to save the changes.

**Alarm Forwarding Key Features**

The key features of Alarm Forwarding include

- A Simple Network Management Protocol (SNMP) agent compliant with ITU x721, X733
- Acknowledge / Terminate capability from SNMP
- For an alarm event, only one email is sent to a selective list of email addresses. Alarm Forwarding allows a list of email addresses to be attached to a filter. It is possible to send a particular type of alarm to a list of email addresses and another type of alarm to a different list of email addresses. These multiple email address are set when Creating a Filter and Editing a Filter.

Each alarm is evaluated against each filter. The same alarm can pass different filter conditions and be sent to different destinations. If the same alarm passes different filters and is forwarded using SNMP in each of those filters, the alarm is sent only once since Alarm Forwarding detects this condition and SNMP has only one destination.

Refer to **Alarm Forwarding MIB** for additional information.

**Alarm Forwarding Architecture**

Alarm Forwarding supports the forwarding of alarms to applications in an external system. It supports two protocols for alarm forwarding:

- Traps (SNMP)
- Mails (SMTP)

Alarm Forwarding supports the use of Filters. You can create, edit, and delete a Filter and a forwarding destination. A Filter List provides information for a Filter:

- Rec No - record number; a number given for indexing alarms in the Filter alarm list
- Rule - unique system-generated number that identifies the Filter
- Filter Name - name of the Filter
- Description - description of the Filter
• Destination Name - destination of the filtered alarm. It can be SNMP or SMTP or both.

You can set the forwarding criteria based on the Filters defined for fields such as:

• Ack State
• Alarm Cleared User
• Alarm ID
• Alarm Type
• Managed Object Class
• Managed Object ID
• Perceived Severity ID
• Probable Cause
• Specific Problem
• User Name

With Alarm Forwarding, parameters can be configured such as:

• Mail server name
• Return address, the “From” address in the mail
• SNMP agent (trap sender)
• Rules for alarm forwarding

Note: Destination configuration is part of platform configuration. These steps (SMTP server, SNMP version, and target IP) are described in IDIH Installation Document.
This chapter provides information about procedures used when working in the Alarm Forwarding application.

Topics:

- Accessing Alarm Forwarding.....17
- Alarm Forwarding Toolbar.....17
- Alarm Status Indicator.....17
- Using Alarm Forwarding.....19
- Alarm Forwarding Test Connection.....21
Accessing Alarm Forwarding

To open Alarm Forwarding, follow these steps:

1. Log in to IDIH.
   The IDIH Application board is displayed.
2. Click Alarm Forwarding.
   The Alarm Forwarding home page is displayed.

Alarm Forwarding Toolbar

![Alarm Forwarding Toolbar](image)

Table 2: Alarm Forwarding Toolbar Icons

<table>
<thead>
<tr>
<th>Button</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Columns</td>
<td>Allows the user to select which columns are displayed</td>
</tr>
<tr>
<td>Navigation Arrows</td>
<td>Moves back and forth among the records.</td>
</tr>
<tr>
<td>Filters</td>
<td>Number of records to display on a page</td>
</tr>
<tr>
<td>Set Size</td>
<td>Sets the number of records to display per page</td>
</tr>
<tr>
<td>Refresh</td>
<td>Resets display to include the most current data</td>
</tr>
<tr>
<td>Add Filter</td>
<td>Adds a Filter, defining the types of alarms to be forwarded and their destination</td>
</tr>
<tr>
<td>Modify Filter</td>
<td>Edits an existing filter’s definition</td>
</tr>
<tr>
<td>Delete Filter</td>
<td>Deletes a selected filter</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Sends a test message to the destination SNMP and/or SMTP</td>
</tr>
</tbody>
</table>

Alarm Status Indicator

When logged in to IDIH, either directly or from DSR launch, the portal header displays a count of current alarms, as shown in Figure 2: Alarm Status Indicator. The alarm status indicator is a count of the highest severity of all open alarms and the alarm status indicator (circle) is the color (user defined, idihadmin) of the highest severity. For example, if there are zero critical, two major, one minor, and three warnings, then the alarm status indicator contains 2+ and the color is the user-defined color for major severity. The + is used to indicate that there are additional alarms at a lesser severity. The + does not appear if, for example, there are zero critical, two major, zero minor, and zero warnings.
Initially, the alarm status is empty (non-visible). Then, after a short interval, the system queries for open alarms and updates the alarm status indicator. After the first update, the system updates the alarm status indicator every 30 seconds.

Figure 2: Alarm Status Indicator

Selecting the alarm status indicator shows a brief description of the open alarms. The system displays the list of open alarms in tabular form, as shown in Figure 3: Alarm List. This list can be dismissed by pressing the Close on the Open Alarm dialog window.

Note: Only open alarms may be viewed. No other actions are provided such as clear or acknowledge.
Using Alarm Forwarding

This section explains how to set conditions and destinations for forwarding alarms.

Creating a Filter

Filters define the types of alarms to be forwarded and their destination. Filters return True or False results depending upon whether the alarm should be forwarded or not. Each Filter that returns True is forwarded to its specified destination.
Figure 4: Filter Creation Dialog

To create a Filter,

1. Click the **Add Filter** icon on the toolbar.
   The Create New Filter dialog is displayed.
2. Type in a **Filter Name** and **Description**.
3. Select Filter and click the **Add** icon.
4. Select a Field, Operator, and Value from the drop-down menus.
5. Enter an Expression.
6. Select **Next** to advance to the Destination display.
7. Select SNMP and/or SMTP.
8. Enter Email list (addresses) information.
   **Note:** Email list is only used when SMTP is selected.
9. To advance to the Filter Creation Dialog Summary display, select **Next**.
10. If the information on the Summary display is correct, select finish create this filter. If there are errors in this summary information, select the previous to return to the display to correct the errors.
11. To add another filter, repeat from **Step 1**.

**Editing a Filter**

To edit an existing Filter:
1. Select a Filter from the Filter table.
2. Click the Modify Filter icon on the toolbar. 
The Filter Creation Dialog is displayed.
3. Modify the appropriate field(s) as needed.
   For specific information on fields and options, see Creating a Filter.
4. Click Next.
   The Select Forwarding Destination dialog is displayed.
5. Update Destination information as necessary.
   Note: For SNMP, only one trap destination can be defined. For SMTP, multiple email destinations are permitted.
6. Click Finish to save the record changes.

Alarm Forwarding Test Connection

The user can send a test message to the destination SNMP and/or SMTP using the Connection Test Dialog screen after clicking Test Connection.

![Connection Test Dialog]

Figure 5: Connection Test Dialog

Test Connection for SMTP

The configuring user should verify the SMTP address, SMTP availability thru firewalls, and SMTP access mode. Secured destinations require additional parameters be defined and are described in the Installation Document.

1. If the message was received in the targeted mail box, the test was successful. This procedure is complete.
   If the message is not in the targeted mail box, continue with this procedure.
2. Use the Audit Viewer application to verify if a mail sending error is logged.
3. Contact the *My Oracle Support (MOS)* to investigate and help determine the correct SMTP configuration.

**Test Connection for SNMP**

The configuring user should verify the SNMP address and the SNMP availability thru firewalls. Secured destinations require additional parameters be defined and are described in the *IDIH Installation Document*.

1. Verify the test trap was received by the management system. If the test trap was received by the management system, the test was successful. This procedure is complete.
   
   If the test trap was not received by the management system, continue with this procedure.

2. Contact the *My Oracle Support (MOS)* to investigate and help determine the correct SNMP configuration.
This chapter provides information about how the SNMP Agent functions in the Alarm Forwarding application.

Topics:

- SNMP Overview.....24
- Alarm Forwarding MIB.....24
SNMP Overview

The main features of the Simple Network Management Protocol (SNMP) agent of Alarm Forwarding are:

Overview

- The Management Information Base (MIB) contains Managed Object types, Managed Objects, and opened alarms in specific tables.
- The MIB is loaded at SNMP agent startup with metadata and opened alarms already forwarded.

Validation of Traps Sent

- Traps contain a sequence number (since agent startup) that permits Telecommunications Management Network (TMN) to check that none were lost.
- In case of a gap (lost trap) or if the number is lower, the process is restarted and TNM can re-synchronize its database by querying the opened alarms table.

Acknowledgment or Termination from SNMP

A dedicated Access Module for TeMIP is available to integrate easily with the NSP Forwarding SNMP agent.

Note: SNMP trap forwarding requires the system administrator to configure the destination address, please refer to Configure SNMP Management Server in the IDIH Installation Document.

Alarm Forwarding MIB

Shown here is the Alarm Forwarding MIB, which is located on the NSP server at

```
/usr/TKLC/xIH/apps/forwarding/target/misc/NSP-FORWARDING-MIB
```

```
-- File Name: NSP-FORWARDING-MIB
-- Date: Mon Nov 21 10:18:28 CET 2006
-- Author: AdventNet Agent Toolkit Java Edition - MIB Editor 6

NSP-FORWARDING-MIB DEFINITIONS ::= BEGIN
IMPORTS
    RowStatus, DisplayString
    FROM SNMPv2-TC
    NOTIFICATION-GROUP, OBJECT-GROUP
    FROM SNMPv2-CONF
    enterprises, MODULE-IDENTITY, OBJECT-TYPE, Integer32,
    NOTIFICATION-TYPE
    FROM SNMPv2-SMI;

steleus MODULE-IDENTITY
```

E63646 Revision 02, March 2017
nsp OBJECT IDENTIFIER ::= { enterprises 4404 }

forwarding OBJECT IDENTIFIER ::= { nsp 6 }

nspManagedObjectClassTable OBJECT-TYPE
SYNTAX SEQUENCE  OF  NspManagedObjectClassEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION NSP managed object class table
 ::=  { nspManagedObjectClassTable 1 }

nspManagedObjectClassEntry OBJECT-TYPE
SYNTAX NspManagedObjectClassEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION NSP managed object class entry
INDEX { nspManagedObjectClassId }  
 ::=  { nspManagedObjectClassTable 1 }

NspManagedObjectClassEntry ::= SEQUENCE {
 nspManagedObjectClassId Integer32,  
nspManagedObjectClassName DisplayString,  
nspManagedObjectClassDescription DisplayString,  
nspManagedObjectClassRowStatus RowStatus
}

nspManagedObjectClassId OBJECT-TYPE
SYNTAX Integer32  {-2147483648 .. 2147483647 }  
MAX-ACCESS read-only
STATUS current
DESCRIPTION Value that defines an instance of managed object class in the table
 ::=  { nspManagedObjectClassEntry 1 }

nspManagedObjectClassName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION NSP managed object class instance name
 ::=  { nspManagedObjectClassEntry 2 }

nspManagedObjectClassDescription OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION NSP managed object class instance
description
   ::=  { nspManagedObjectClassEntry  3  }

nspManagedObjectClassRowStatus  OBJECT-TYPE
SYNTAX                  RowStatus { active (1), notInService (2), notReady (3), createAndGo (4), createAndWait (5), destroy (6) }
MAX-ACCESS              read-create
STATUS                  current
DESCRIPTION             SMI v2 required attribute
   ::=  { nspManagedObjectClassEntry  50  }

nspManagedObjectTable   OBJECT-TYPE
SYNTAX          SEQUENCE  OF  NspManagedObjectEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     Description
   ::=  { forwarding  2  }

nspManagedObjectEntry   OBJECT-TYPE
SYNTAX          NspManagedObjectEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     Row Description
INDEX           {  nspManagedObjectId}
   ::=  { nspManagedObjectTable  1  }

NspManagedObjectEntry  ::=  SEQUENCE {
   nspManagedObjectId  Integer32,
   nspManagedObjectName  DisplayString,
   nspManagedObjectClassIdRef  Integer32,
   nspManagedObjectParent  Integer32,
   nspManagedObjectRowStatus  RowStatus
}

nspManagedObjectId      OBJECT-TYPE
SYNTAX                  Integer32  ( -2147483648 .. 2147483647 )
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION             Value that defines an instance of managed object in the table
   ::=  { nspManagedObjectEntry  1  }

nspManagedObjectName    OBJECT-TYPE
SYNTAX                  DisplayString
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION             Column Description
   ::=  { nspManagedObjectEntry  2  }

nspManagedObjectClassIdRef      OBJECT-TYPE
SYNTAX                  Integer32  ( -2147483648 .. 2147483647 )
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION             Value that defines an instance of managed
object class
::=  {  nspManagedObjectEntry  10  }

nspManagedObjectParent  OBJECT-TYPE
SYNTAX                  Integer32
MAX-ACCESS              read-only
STATUS                  current
DESCRIPTION             Value that defines an instance of parent
managed object
::=  {  nspManagedObjectEntry  20  }

nspManagedObjectRowStatus       OBJECT-TYPE
SYNTAX                  RowStatus
MAX-ACCESS              read-create
STATUS                  current
DESCRIPTION             SMI v2 required attribute
::=  {  nspManagedObjectEntry  50  }

nspAlarmsTable  OBJECT-TYPE
SYNTAX          SEQUENCE  OF  NspAlarmsEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     NSP forwarded opened alarms table
::=  { forwarding  3 }

nspAlarmsEntry  OBJECT-TYPE
SYNTAX          NspAlarmsEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     NSP forwarded opened alarms entry
INDEX           {  nspAlarmId  }
::=  { nspAlarmsTable 1 }

NspAlarmsEntry ::= SEQUENCE {
  nspManagedObjectIdRef  Integer32,
nspAlarmId  Integer32,
nspAlarmRowStatus  RowStatus,
nspManagedObjectDN  DisplayString,
nspAlarmLastEventTime  DisplayString,
nspAlarmEventType  INTEGER,
nspAlarmProbableCause  INTEGER,
nspAlarmPerceivedSeverity  INTEGER,
nspAlarmThresholdLevel  DisplayString,
nspAlarmObservedValue  DisplayString,
nspAlarmTrendIndication  INTEGER,
nspAlarmAdditionalText  DisplayString,
nspAlarmSpecificProblem  DisplayString,
nspAlarmFirstDate  OCTET STRING,
nspAlarmClearDate  OCTET STRING,
nspAlarmCriticalCount  Integer32,
nspAlarmMajorCount  Integer32,
nspAlarmMinorCount  Integer32,
nspAlarmWarningCount  Integer32,
nspAlarmAcknowledged  INTEGER
}
nspManagedObjectIdRef  OBJECT-TYPE
SYNTAX               Integer32  (-2147483648 .. 2147483647)
MAX-ACCESS           read-only
STATUS               current
DESCRIPTION          Value that refers to managed object involved in the forwarded alarm
::=  {  nspAlarmsEntry  1  }

nspAlarmId          OBJECT-TYPE
SYNTAX               Integer32  (-2147483648 .. 2147483647)
MAX-ACCESS           read-only
STATUS               current
DESCRIPTION          Value that defines an instance of forwarded alarm
::=  {  nspAlarmsEntry  2  }

nspAlarmRowStatus    OBJECT-TYPE
SYNTAX               RowStatus  { active ( 1 ), notInService ( 2 ), notReady ( 3 ), createAndGo ( 4 ), createAndWait ( 5 ), destroy ( 6 ) } 
MAX-ACCESS           read-create
STATUS               current
DESCRIPTION          SMI v2 required attribute
::=  {  nspAlarmsEntry  50  }

nspManagedObjectDN  OBJECT-TYPE
SYNTAX               DisplayString
MAX-ACCESS           read-only
STATUS               current
DESCRIPTION          Distinguished name that refers to managed object involved in the forwarded alarm
::=  {  nspAlarmsEntry 100  }

nspAlarmLastEventTime OBJECT-TYPE
SYNTAX               DisplayString
MAX-ACCESS           read-only
STATUS               current
DESCRIPTION          Last event time in ASN.1 format for the last event of the NSP forwarded alarm on the managed object
::=  {  nspAlarmsEntry 1000  }

nspAlarmProbableCause OBJECT-TYPE
SYNTAX               INTEGER  { adapterError ( 1 ), applicationSubsystemFailure ( 2 ), bandwidthReduced ( 3 ), callEstablishmentError ( 4 ), communicationsProtocolError ( 5 ), communicationsSubsystemFailure ( 6 ), configurationOrCustomizationError ( 7 ), congestion ( 8 ), corruptData ( 9 ), cpuCyclesLimitExceeded ( 10 ), dataSetOrModemError ( 11 ), degradedSignal ( 12 ), dteDceInterfaceError ( 13 ), enclosureDoorOpen ( 14 ), equipmentMalfunction ( 15 ), excessiveVibration ( 16 ), fileError ( 17 ), fireDetected ( 18 ), floodDetected ( 19 ), framingError ( 20 ), heatingVentCoolingSystemProblem ( 21 ), }
humidityUnacceptable ( 22 ), inputOutputDeviceError ( 23 ), inputDeviceError ( 24 ), lanError ( 25 ), leakDetected ( 26 ), localNodeTransmissionError ( 27 ), lossOfFrame ( 28 ), lossOfSignal ( 29 ), materialSupplyExhausted ( 30 ), multiplexerProblem ( 31 ), outOfMemory ( 32 ), outputDeviceError ( 33 ), performanceDegraded ( 34 ), powerProblem ( 35 ), pressureUnacceptable ( 36 ), processorProblem ( 37 ), pumpFailure ( 38 ), queueSizeExceeded ( 39 ), receiveFailure ( 40 ), receiverFailure ( 41 ), remoteNodeTransmissionError ( 42 ), resourceAtOrNearingCapacity ( 43 ), responseTimeExcessive ( 44 ), retransmissionRateExcessive ( 45 ), softwareError ( 46 ), softwareProgramAbnormallyTerminated ( 47 ), softwareProgramError ( 48 ), storageCapacityProblem ( 49 ), temperatureUnacceptable ( 50 ), thresholdCrossed ( 51 ), timingProblem ( 52 ), toxicLeakDetected ( 53 ), transmitFailure ( 54 ), transmitterFailure ( 55 ), underlyingResourceUnavailable ( 56 ), versionMismatch ( 57 ), authenticationFailure ( 58 ), breachOfConfidentiality ( 59 ), cableTamper ( 60 ), delayedInformation ( 61 ), denialOfService ( 62 ), duplicateInformation ( 63 ), informationMissing ( 64 ), informationModificationDetected ( 65 ), informationOutOfSequence ( 66 ), intrusionDetection ( 67 ), keyExpired ( 68 ), nonRepudiationFailure ( 69 ), outOfHoursActivity ( 70 ), outOfService ( 71 ), proceduralError ( 72 ), unauthorizedAccessAttempt ( 73 ), unexpectedInformation ( 74 )

MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the probable cause values for the alarms as per [X.721], [X.733] and [X.736] for the NSP forwarded alarm on the managed object

::= { nspAlarmsEntry 1001 }

nspAlarmPerceivedSeverity OBJECT-TYPE
SYNTAX INTEGER { indeterminate ( 0 ), critical ( 1 ), major ( 2 ), minor ( 3 ), warning ( 4 ), cleared ( 5 )}
MAX-ACCESS read-write
STATUS current
DESCRIPTION Represents the perceived severity values for the alarms as per [X.733] and [X.736] for the NSP forwarded alarm on the managed object

::= { nspAlarmsEntry 1002 }

nspAlarmTrendIndication OBJECT-TYPE
SYNTAX INTEGER { lessSevere ( 0 ), noChange ( 1 ), moreSevere ( 2 )}
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the trend indication values for the alarms as per [X.733] for the NSP forwarded alarm on the managed object

::= { nspAlarmsEntry 1003 }

nspAlarmThresholdLevel OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the threshold level indication values (real) for the alarms as per [X.733] for the last event of the NSP forwarded alarm on the managed object ::= { nspAlarmsEntry 1004 }

nspAlarmObservedValue OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the threshold observed values (real) for the alarms as per [X.733] for the last event of the NSP forwarded alarm on the managed object ::= { nspAlarmsEntry 1005 }

nspAlarmAdditionalText OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the additional text field for the alarm as per [X.733] for the last event of the NSP forwarded alarm on the managed object ::= { nspAlarmsEntry 1006 }

nspAlarmEventType OBJECT-TYPE
SYNTAX INTEGER { otherAlarm (1),
communicationAlarm (2),
environmentalAlarm (3),
equipmentAlarm (4),
integrityViolation (5),
processingErrorAlarm (10),
qualityOfServiceAlarm (11) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the ITU event type value for the alarms as per [X.721], [X.733] and [X.736] for the NSP forwarded alarm on the managed object ::= { nspAlarmsEntry 1007 }

nspAlarmSpecificProblem OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the specific problem name for the NSP forwarded alarm on the managed object ::= { nspAlarmsEntry 1008 }

nspAlarmFirstDate OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the raised date in ASN.1 format for the NSP forwarded alarm on the managed object
::= ( nspAlarmsEntry 1010 )

nspAlarmClearDate OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the clear date in ASN.1 format for the NSP forwarded alarm on the managed object
::= ( nspAlarmsEntry 1011 )

nspAlarmCriticalCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the number of critical events for the NSP forwarded alarm on the managed object
::= ( nspAlarmsEntry 1012 )

nspAlarmMajorCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the number of major events for the NSP forwarded alarm on the managed object
::= ( nspAlarmsEntry 1013 )

nspAlarmMinorCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the number of minor events for the NSP forwarded alarm on the managed object
::= ( nspAlarmsEntry 1014 )

nspAlarmWarningCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION Represents the number of warning events for the NSP forwarded alarm on the managed object
::= ( nspAlarmsEntry 1015 )

nspAlarmAcknowledged OBJECT-TYPE
SYNTAX INTEGER { false (0), true (1) }  
MAX-ACCESS read-write  
STATUS current  
DESCRIPTION Represents the acknowledged status for the NSP forwarded alarm of the managed object.

::= { nspAlarmsEntry 1016 }

fwdVersion OBJECT-TYPE  
SYNTAX OCTET STRING  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION Current version of the NSP Forwarding SNMP sub-agent.

::= { forwarding 10 }

fwdStatus OBJECT-TYPE  
SYNTAX INTEGER { allGood (0), failure (1) }  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION Global state of the NSP Forwarding SNMP sub-agent.

::= { forwarding 11 }

ituAlarmEvent OBJECT IDENTIFIER  
::= { forwarding 733 }

otherAlarm NOTIFICATION-TYPE  
OBJECTS { nspAlarmId, nspManagedObjectId, nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity, nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue, nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN }  
STATUS current  
DESCRIPTION Represents the event type for other alarms as per [X.721],[X.733] and [X.736].

::= { ituAlarmEvent 1 }

communicationAlarm NOTIFICATION-TYPE  
OBJECTS { nspAlarmId, nspManagedObjectId, nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity, nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue, nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN }  
STATUS current  
DESCRIPTION Represents the event type for the communication alarms as per [X.721],[X.733] and [X.736].

::= { ituAlarmEvent 2 }

environmentalAlarm NOTIFICATION-TYPE  
OBJECTS { nspAlarmId, nspManagedObjectId, nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity, nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue, nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName,
nspManagedObjectDN }

  STATUS                  current
DESCRIPTION             Represents the event type for the environment alarms as per [X.721],[X.733] and [X.736]
 ::= { ituAlarmEvent 3 }

  equipmentAlarm NOTIFICATION-TYPE
OBJECTS                 { nspAlarmId, nspManagedObjectId,
nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity,
nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue,
nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate,
nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount,
nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName,
nspManagedObjectDN }

  STATUS                  current
DESCRIPTION             Represents the event type for the equipment alarms as per [X.721],[X.733] and [X.736]
 ::= { ituAlarmEvent 4 }

  integrityViolation NOTIFICATION-TYPE
OBJECTS                 { nspAlarmId, nspManagedObjectId,
nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity,
nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue,
nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate,
nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount,
nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName,
nspManagedObjectDN }

  STATUS                  current
DESCRIPTION             Represents the event type for the integrity violation as per [X.721],[X.733] and [X.736]
 ::= { ituAlarmEvent 5 }

  processingErrorAlarm NOTIFICATION-TYPE
OBJECTS                 { nspAlarmId, nspManagedObjectId,
nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity,
nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue,
nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate,
nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount,
nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName,
nspManagedObjectDN }

  STATUS                  current
DESCRIPTION             Represents the event type for the processing error alarms as per [X.721],[X.733] and [X.736]
 ::= { ituAlarmEvent 10 }

  qualityOfServiceAlarm NOTIFICATION-TYPE
OBJECTS                 { nspAlarmId, nspManagedObjectId,
nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity,
nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue,
nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate,
nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount,
nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName,
nspManagedObjectDN }

  STATUS                  current
DESCRIPTION             Represents the event type for the quality of service alarms as per [X.721],[X.733] and [X.736]
of service alarms as per [X.721],[X.733] and [X.736]

::= { ituAlarmEvent 11 }

ituAlarmEventGroup NOTIFICATION-GROUP
NOTIFICATIONS { communicationAlarm, environmentalAlarm, equipmentAlarm, integrityViolation, otherAlarm, processingErrorAlarm, qualityOfServiceAlarm }

STATUS current
DESCRIPTION ITU alarm Event notifications
::= { forwarding 500 }

managedObject OBJECT-GROUP
OBJECTS { nspManagedObjectClassDescription, nspManagedObjectClassId, nspManagedObjectClassIdRef, nspManagedObjectClassName, nspManagedObjectClassRowStatus, nspManagedObjectId, nspManagedObjectIdRef, nspManagedObjectName, nspManagedObjectParent, nspManagedObjectRowStatus, nspManagedObjectDN }

STATUS current
DESCRIPTION Data related to NSP managed objects
::= { forwarding 200 }

alarm OBJECT-GROUP
OBJECTS { nspAlarmAcknowledged, nspAlarmAdditionalText, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmFirstDate, nspAlarmId, nspAlarmLastEventTime, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmObservedValue, nspAlarmPerceivedSeverity, nspAlarmProbableCause, nspAlarmEventType, nspAlarmRowStatus, nspAlarmSpecificProblem, nspAlarmThresholdLevel, nspAlarmTrendIndication, nspAlarmWarningCount }

STATUS current
DESCRIPTION Data related to NSP alarms
::= { forwarding 300 }

forward OBJECT-GROUP
OBJECTS { fwdVersion, fwdStatus }
STATUS current
DESCRIPTION Data related to NSP forwarding module
::= { forwarding 100 }

END
**D**

**DSR**

Diameter Signaling Router

A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.

**ENUM**

TElephone NUmber Mapping - A technology for unifying various communications and telephone addresses for private and business numbers, facsimile and mobile phone numbers, SMS services, Instant Messaging and email. ENUM integrates legacy phone numbers with the Domain Name System (DNS). Users can access and maintain a directory that supports all forms of wired communication, mobile communications networks, and the Internet. ENUM allows for an end user to be reached on multiple devices via one phone number and allows the end user to determine which device to contact first or multiple devices simultaneously.

E.164 Number Mapping

**F**

Filter

A value consisting of FNAI, FPFX, FDL, used to filter called party digits.

**I**

Glossary
I

ID
Identifier

IDIH
Integrated Diameter Intelligence Hub

ITU
International Telecommunications Union
An organization that operates worldwide to allow governments and the private telecommunications sector to coordinate the deployment and operating of telecommunications networks and services. The ITU is responsible for regulating, coordinating and developing international telecommunications, and for harmonizing national political interests.

M

MIB
Management Information Database
A database of network management information that is used and maintained by the SNMP protocol.

S

SMTP
Simple Mail Transfer Protocol

SNMP
An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol
S

arranges managed objects into groups.