

Oracle® Communications
Performance Intelligence Center
Alarm Forwarding Administration Guide
Release 10.3.0
E98802-01

December 2018

Copyright © 2003, 2018 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notices are applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.



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

Table of Contents

Table of Contents	iii
List of Figures	iv
List of Tables	iv
Chapter 1: About This Help Text	1
Overview	1
Scope and Audience	1
General Information	1
Chapter 2: Introduction to Alarm Forwarding.....	2
Alarm Forwarding Key Features.....	2
Alarm Forwarding Architecture	3
Filtering criterias	3
SNMP traps	4
Mails.....	4
Chapter 3: Working in Alarm Forwarding	5
Accessing Alarm Forwarding.....	5
Understanding Alarm Forwarding Components	5
Alarm Forwarding Toolbar	5
Using Alarm Forwarding.....	6
Creating a Filter	6
Editing a Filter	7
Alarm Forwarding Test Connection.....	8
Test Connection for SMTP	8
Test Connection for SNMP.....	8

Chapter4 : SNMP Agent	9
Management Application Forwarding MIB SNMP Overview	9
Management Application Forwarding MIB	9
APPENDIX A: My Oracle Support.....	21

List of Figures

Figure 1: Alarm Forwarding List	5
Figure 2: Create New Filter Dialog	6
Figure 3: Filter Configuration Display	7
Figure 4: Summary Dialog Display	7

List of Tables

Table 1: Alarm Forwarding Toolbar Icons	6
---	---

Chapter 1: About This Help Text

Overview

Management Application Alarm Forwarding (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
- SS7 network (nodes, linksets, links)
- System errors

Scope and Audience

This user's guide provides information about the Management Application Alarm Forwarding. This guide provides definitions and instructions to help the user efficiently and effectively define conditions and destinations for forwarding Alarms. The audience for this manual is the nspManager and nspPowerUser.

General Information

You can find general information about Oracle® Communications Performance Intelligence Center, such as product overview, list of other guides, workstation requirements, login and logout procedures, user preference settings, in the Quick Start Guide. This document is available from the Portal menu or can be downloaded from Oracle Help Center (OHC).

Chapter 2: Introduction to Alarm Forwarding

Alarm Forwarding Key Features

Alarm Forwarding is part of Management Application toolkit.

Key features include:

- A Simple Network Management Protocol (SNMP) agent compliant with ITU x721, X733
- A Dedicated Access Module for HP TeMIP
- Trap sent reliability
 - ✓ Sequence number is added to trap sent.
 - ✓ Telecommunications Management Network (TMN) can check that none were lost.
 - ✓ Re-synchronization is available.
- Acknowledge / Terminate capability from SNMP

Two alarm attributes are writable:

- ✓ Perceived Severity: Setting the value to 5 (clear) terminates the alarm in the Management Application database.
 - ✓ Acknowledged: Setting the value to 1 acknowledges the alarm in the Management Application database.
 - ✓ Terminate or “Acknowledge” action is associated with a user ID in the Management Application database.
- 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.
 - Alarm termination is always forwarded if one events of this alarm has been forwarded.

Also see [*Management Application Forwarding MIB*](#)

Alarm Forwarding Architecture

Alarm Forwarding supports the forwarding of alarms to applications in an external system. It supports the following 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 select a forwarding destination. A Filter List provides the following information for a Filter:

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

Filtering criterias

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

- **Ack state:** Status regarding acknowledging status
- **Alarm Cleared User:** User who manually terminate alarm (if any)
- **Alarm ID:** Internal unique ID to group alarm events with same specific problem on same managed object.
- **Alarm Type:** ITU alarm definition (selection in list) as per [X.721] [X.733] and [X.736]
- **Managed Object Class:** Class of managed object
- **Managed Object ID:** Internal unique ID of managed object
- **Managed Object:** : Name of managed object (allowing placeholders)
- **Perceived Severity:** Perceived severity (selection in list) as per [X.721] [X.733] and [X.736]
- **Probable Cause:** Perceived severity (selection in list) as per [X.721] [X.733] and [X.736]
- **Specific Problem:** Specific problem (selection in list)

- **Trend:** Trend of severity for successive events in alarm. Initial event has MORE_SEVERE trend. It allows to get only opening and closing event for an alarm and avoid repetitive events
- **User Name:** name of acknowledging status

Note: Destination configuration is part of platform configuration. These steps (SMTP server, SNMP version, and target IP) are described in Management Application installation.

For the Alarm configuration to work, ensure that the Target Server is added in hosts file. Remove entry for 127.0.0.1 and add alias localhost for the Target Server in the hosts file.

For Example the /etc/hosts should look like below. Here the entry corresponds to the target server.

```
xx.xx.xx.xxx hostname localhost
```

SNMP traps

SNMP traps are emitted by associated Management Application Alarm Forwarding sub-agent.

Also see [Management Application Forwarding MIB](#).

Mails

Mails are created by Weblogic service according following template:

- Title

Management Appliaction Alarm - <SEVERITY_NAME> event

- Content

Alarm #<ALARM_ID> raised at <ALARM_RAISED_TIME>

Managed object: <MO_NAME> (# <MO_ID>)

Specific Problem: <SPECIFIC_PROBLEM_NAME>

Additional text: <EVENT_ADDITIONAL_TEXT>

Probable cause: <ITU_PROBABLE_CAUSE_NAME>

Event summary :

[critical=<CRITICAL_COUNT>][major=<MAJOR_COUNT>][minor=<MINOR_COUNT>][warning=<WARNING_COUNT>]

Note: ALARM_RAISED_TIME is formatted according default user preferences defined by an Administrator.

Chapter 3: Working in Alarm Forwarding

Accessing Alarm Forwarding

To open Alarm Forwarding, follow these steps:

Note: Management Application only supports the latest versions of IE and Firefox. Before using Management Application, turn off the browser pop up blocker for the Management Application site.

1. Log in to Management Application.

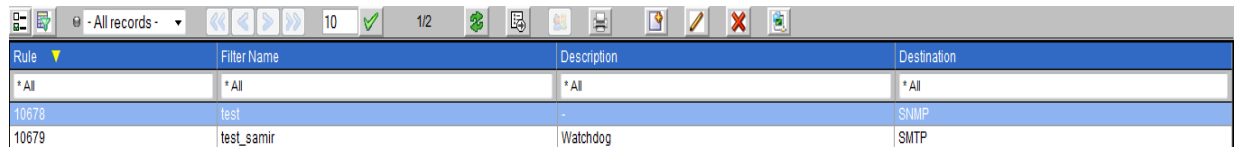
The Management Application board is displayed.

2. Click **Alarm Forwarding**.

The Alarm Forwarding home page is displayed.

Understanding Alarm Forwarding Components




The figure below shows the Alarm Forwarding page with the toolbar and Filters list. Toolbar icons are explained in the table below the figure.



Rule	Filter Name	Description	Destination
* All	* All	* All	* All
10679	test	Watchdog	SMTP

Figure 1: Alarm Forwarding List

Alarm Forwarding Toolbar

Icon	Explanation
	Navigation icon - to move from one record to another << is for first page < is for previous page > Is for next page >> is for last page
	Filter - adds a Filter, defining the types of alarms to be forwarded and their destination
	Column Select Record - sets the order of the columns










	Edit Filter - edits an existing filter's definition
	Delete Filter - deletes a selected filter
	Refresh Page - resets display to include the most current data
	Records Per Page - number of records to display on a page
	Set Size - resets display to include the number of Records per Page
	Filter - to define filters for the list
	Export - to provide option to export list getting displayed.
	Print - to provide facility to print current list.
	Test Connection - tests connections for different protocol(SNMP or SMTP)

Table 1: Alarm Forwarding Toolbar Icons

Note: Do not use the Function Keys (F1 through F12) when using Management Application. Function keys work in unexpected ways. For example, the F1 key does not open Management Application help but opens the help for the browser in use. The F5 key does not refresh a specific screen, but refreshes the entire session and results in a loss of any entered information.

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.

To create a Filter,

1. Click the Add Filter icon  on the toolbar
The Create new Filter dialog is displayed.



Figure 2: Create New Filter Dialog

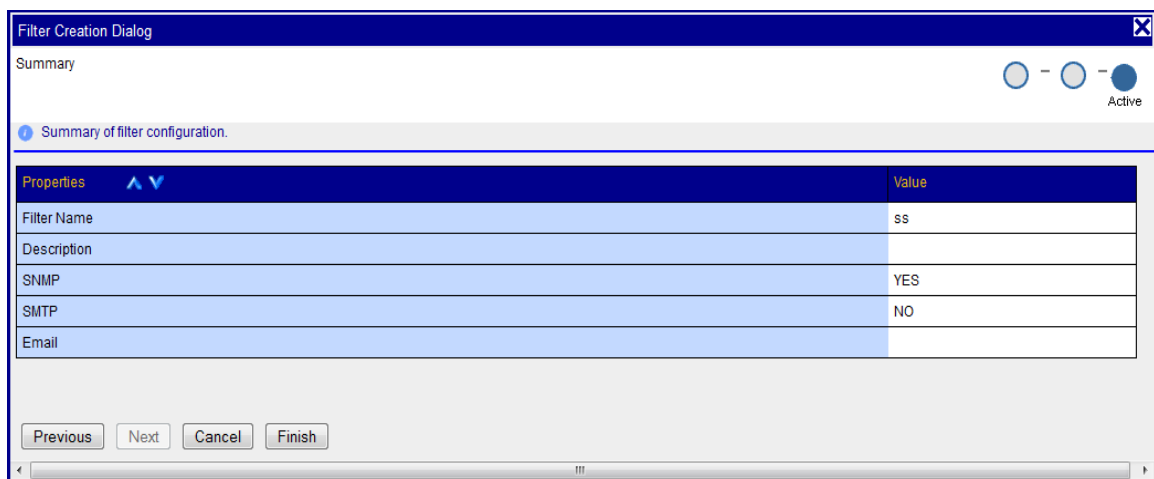
2. Type in a Filter Name and Description.
3. Type in Description.
4. Select Filter and click  (Add).
5. Select a Field, Operator, and Value from the drop-down menus.



The image shows a 'Filter Configuration' dialog box. It has two input fields at the top: 'Filter Name' with the text 'filter2' and 'Description' with the text 'Just testin''. Below these is a section titled 'Filter Configuration' which contains a table with three columns: 'Field', 'Operator', and 'Value'. The 'Field' column has a dropdown menu currently showing 'Select a field...'. The 'Operator' and 'Value' columns also have dropdown menus. There are checkboxes and a plus icon on the left, and a minus icon and a question mark on the right.

Figure 3: Filter Configuration Display


6. Enter an Expression.
7. Select 'Next' to advance to the Destination display.
8. Select SNMP and/or SMTP.
9. Enter Email list (addresses) information.
10. To advance to the Filter Creation Dialog Summary display, select 'Next'



The image shows a 'Filter Creation Dialog' window with a 'Summary' tab. It displays a summary of the filter configuration in a table. The table has two columns: 'Properties' and 'Value'. The 'Properties' column lists 'Filter Name', 'Description', 'SNMP', 'SMTP', and 'Email'. The 'Value' column shows 'ss', an empty field, 'YES', 'NO', and an empty field respectively. At the bottom, there are four buttons: 'Previous', 'Next', 'Cancel', and 'Finish'. The 'Next' button is highlighted.


Properties	Value
Filter Name	ss
Description	
SNMP	YES
SMTP	NO
Email	

Figure 4: Summary Dialog Display

11. If this 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.
12. To add another filter, repeat from [Click the](#) Add Filter icon  on the toolbar

Editing a Filter

To edit an existing Filter:

1. Select a Filter from the Filter table.
2. Click the Edit 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

This section provides additional information referenced from the screen when using the **Test Connection** GUI icon  .

Test Connection for SMTP

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

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 [APPENDIX A: My Oracle Support \(MOS\)](#) to investigate and help determine the correct SMTP configuration.

Test Connection for SNMP

The configurator should check the JMX agent log on the Management Application primary to identify any SNMP agent configuration errors, verify the SNMP address, and the SNMP availability through firewalls. Secured destinations require additional parameters be defined and are described in the 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 [APPENDIX A: My Oracle Support \(MOS\)](#) to investigate and help determine the correct SNMP configuration.

Management Application Forwarding MIB SNMP Overview

The main features of the Simple Network Management Protocol (SNMP) agent of Management Application Forwarding are explained below.

Overview of Management Application Database

- 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.

Acknowledgement or Termination from SNMP

- Change in an alarm's writable attributes is reflected in Application Alarm and System Alarms.
- Setting the NspAlarmAcknowledged attribute of an alarm table entry to True (1) acknowledges that alarm.
- Setting the NspAlarmPerceivedSeverity attribute of an alarm table entry to Cleared (5) terminates an alarm.

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

Management Application Forwarding MIB

Shown here is the NSP-Forwarding-MIB, which is located on the Management Application server at </opt/nsp/nsp-package/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
    LAST-UPDATED      "200602131148Z"
    ORGANIZATION      "Tekelec"
    CONTACT-INFO      "ttprocessing@tekelec.com"
    DESCRIPTION        "Description"
    REVISION           "200602131148Z"
    DESCRIPTION        "NSP module"
    ::= { enterprises 4404 }

nsp      OBJECT IDENTIFIER
    ::= { steleus 8 }

forwarding      OBJECT IDENTIFIER
    ::= { nsp 6 }

nspManagedObjectClassTable      OBJECT-TYPE
    SYNTAX          SEQUENCE OF NspManagedObjectClassEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION      "NSP managed object class table"
    ::= { forwarding 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,
    nspAlarmTrendIndication INTEGER,
    nspAlarmThresholdLevel DisplayString,
    nspAlarmObservedValue DisplayString,
    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 ) , heatingVentCoolingSystemnsplem ( 21
) , humidityUnacceptable ( 22 ) , inputOutputDeviceError ( 23 ) , inputDeviceError
( 24 ) , lanError ( 25 ) , leakDetected ( 26 ) , localNodeTransmissionError ( 27
) , lossOfFrame ( 28 ) , lossOfSignal ( 29 ) , materialSupplyExhausted ( 30 ) ,
multiplexerproblem ( 31 ) , outOfMemory ( 32 ) , ouputDeviceError ( 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.721]

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]"

        ::= { 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
```


APPENDIX A: My Oracle Support

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

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

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

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