Oracle® Communications Session Delivery Manager

Maintenance Release Guide
Release 7.3
Formerly Net-Net Central

February 2014

Notices

Contents

1 About this Guide.. 7
Related Documentation.. 7
Related SBC Documentation..8
Revision History..8

2 Net-Net Central 7.3M1 Features and Model Support....................... 9
Content Map for 7.3M1..9
Net-Net Central Features..9
Audible Alarms.. 9
Enabling an Audible Alarm..10
Configuration Element Search.. 10
Using the Configuration Element Search..11
Model Support..11
S-C[x]6.2.0M12..11
Palladion Mediation Engine.. 11
IPFIX..12
Communication Monitor Configuration..12
TLS Configuration.. 13
S-C[x]6.3.0M3..13
Automated Daylight Savings Time (DST) Updates..13
Automated DST Configuration.. 15
SDP Version Change without SDP Body Change.. 16
SDP Version Change without SDP Body Change Configuration..16
S-C[x]6.3.7M1..16
S-C[xz]6.3.9M1..16
S-C[x]6.4.6F2..17
TSCF data flow.. 17
TSCF data flow Configuration..17
TSCF Config.. 17
TSCF Element Id Configuration.. 18
TSCF Keepalive Timer Datagram Configuration.. 18
E-C[xz]6.3.7M1..18
D-C[z]2.1.0..18
Natively Securing Network Topology Information in AVPs..18
Natively Securing Network Topology Information in AVPs Configuration.. 19

3 Net-Net Central 7.3M2 Features and Model Support..................... 21
Content Map for 7.3M2..21
Net-Net Central Features..21
License Information.. 21
S-C[x]6.3.0M4..21
S-D7.1.0M5..21

4 Net-Net Central 7.3M3 Features and Model Support..................... 23
Content Map for 7.3M3..23
Net-Net Central Features..23
Password Change Enhancement..24

Changing a System User Password........24
Configuration Schema Upload........24
Upload a Configuration Schema........24
Diagnostics Tool........24
Retrieving Diagnostics Information........25
Work Order Enhancements........25
Configuring Work Order Enhancements........25
External AAA........26
External AAA for RADIUS Configuration........26
External AAA for Active Directory Configuration........26
TLS Support for ACP........27
Trusted Certificates for ACP over TLS Configuration........28
Entity Certificates for ACP over TLS Configuration........28
TLS Certificate Options........29
Model Support........29
S-C[x]6.3.3M2........29
Specific Action AVP........29
Specific Action AVP Configuration........30
Node-Function AVP........30
Specific Action AVP Global Configuration........30
Node-Function AVP Realm Configuration........31
S-C[x]6.3.9M2........31
SIPREC Ping........31
SIPREC Ping Configuration........31
Personal Profile Manager (PPM) Proxy........32
PPM Proxy Configuration........32
S-C[x]6.4.0M1........33
DDoS Protection from Devices Behind a NAT........33
DDoS Protection from Devices Behind a NAT Realm Configuration........33
DDoS Protection from Devices Behind a NAT Access Control Configuration........33
SDP Alternate Connectivity........34
SDP Alternate Connectivity Configuration........34
Authenticated NTP........34
Authenticated NTP Configuration........34

5 Net-Net Central 7.3M4 Features and Model Support 37

Content Map for 7.3M4........37
Net-Net Central Features........38
GUI Improvements to Multi-Instance Element Tables........38
Enabling Optional Columns........38
Software Licensing........38
SOAP/XML API Updates........39
Security Banner Enhancement........40
Security Banner Enhancement Configuration........40
Setting Permissions for the Security Banner........41
Diameter Director Support for Route Manager........41
Oracle Linux VM........41
Deploying the OVM Template........42
Creating a Guest VM........43
Adding VNICs to the VM........44
Launching and Accessing the VM........44
Configuring the VM with Sysprep........45
Audit Log Improvements........50
Automatic XSD Loading........51
Fault Email Severity Settings........51

Enabling Notify on Clear........ 51
Northbound Fault Management........ 52
Accessing Northbound Fault Management Configuration........ 53
Add/Edit Trap Receivers........ 53
Synchronizing Trap Receiver Alarms........ 54
Global Identifier Configuration During Installation........ 54
Displaying the Global Identifier in NNC........ 55
Setting Permissions for Northbound Fault Management........ 55
SC[z]7.1.2M2........ 56
S-C[x]6.3.3M3/L-CX1.1.3M3........ 56
IMS-AKA Change Client Port........ 56
L-CX1.5.0........ 57
S-C[x]6.4.0M3........ 57
S-C[x]6.3.7M2........ 57
DCZ2.2.0........ 57
Upstream Congestion Control........ 57
Diameter Director Agent........ 59
Diameter Director Group........ 60
Diameter Director Interface........ 60
S-C[xz]6.3.9M3........ 60
E-C[xz]6.4.0M2........ 60
Remote Site Survivability........ 60
S-C[x]6.3.5M1........ 62

A— MIBs........ 63
Northbound Fault Management MIB........ 63

1

About this Guide

The Net-Net Central 7.3 Maintenance Release Guide provides configuration support for Net-Net Central Release Version 7.3M1 and above.

Related Documentation

The following table lists related documents for Oracle Communications Session Delivery Manager:

Document Name	**Document Description**
Release Notes	Contains information about the administration and software configuration of the Oracle Communications Session Delivery Manager feature support new to this release.
Installation Guide	Contains graphical and next mode installation information.
High Availability Guide	Describes Net-Net Central High Availability (HA) and the HA cluster, which is a network of tightly-linked servers. HA provides continuous management of the Net-Net Central system.
Web Services SOAP XML Provisioning API Guide	Provides a full description of the individual interface definitions that make up the Application Programming Interface (API)
Core Functionality Guide	Contains an overview of the Net-Net Central graphical user interface (GUI), detailed information about managing devices in Net-Net Central, and Net-Net Central licenses.
Element Manager Guide	Contains detailed information pertaining to Net-Net Central's Element Manager application and describes the dashboard summary view, audit log, fault, and performance views.
Route Manager Guide	Contains detailed information about centrally automating the management and distribution of routing data.
Quick Start Guide	Contains a brief description of the GUI, along with information on how to add a device and perform basic configuration tasks.
Administration Guide	Contains information about security administration, which lets you create new users and new user groups, and set group-based authorization.

Document Name	Document Description
Configuration Guide: Default View	Contains information about the administration and software configuration of the Oracle Communications Session Delivery Managers using Net-Net Central's default configuration view.

Related SBC Documentation

The following table lists related documents for Oracle Communications Session Delivery Managers and devices:

Net-Net Device Release	Document Name: Number
DCX100	Net-Net Central Diameter Director DCX1.0.0F3 Configuration Guide: 400-0166-30
S-CX6.3.3	Net-Net 4000 S-CX6.3.3 ACLI Reference Guide: 400-0062-63
S-CX6.3.3	Net-Net 4000 S-CX6.3.3 ACLI Configuration Guide: 400-0061-63
L-CX1.3.3	Net-Net 4500 Session Load Balancer Essentials Guide Release Version LCX1.3.3: 400-0140-11
S-C(X)6.3.7	Net-Net 4500 and 3820 Transcoding Configuration Guide Release Version S-C(X)6.3.7
S-D7.0.0M11	N/A
S-D7.0.0M12	N/A
S-D7.2.3F2	Net-Net 9200 Technical Notice Release Version S-D7.2.3F2: 400-0010-723F2
S-CX6.3.0M2	Net-Net 4000 Maintenance Release Guide Version S-CX6.3.0M2
S-CX6.4.0	Net-Net 4000 ACLI Configuration Guide Release Version S-CX6.4.0: 400-0061-64

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
March 2013	1.00	• Initial Release
March 2013	2.00	• Adds chapter for Net-Net Central release 7.3M2 • Updates Related Oracle Communications Session Delivery Manager Documentation.
July 2013	3.00	• Adds chapter for Net-Net Central release 7.3M3
January 2014	4.00	• Adds chapter for Net-Net Central release 7.3M4
February 2014	4.10	• Adds Appendix with Northbound Fault Management MIB details

2

Net-Net Central 7.3M1 Features and Model Support

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net Central Release 7.3M1.

Content Map for 7.3M1

This table provides a listing of all new content in Net-Net Central Release 7.3M1:

Content Type	Description
Net-Net Central Feature	Audible Alarms
Net-Net Central Feature	Configuration Element Search
Model Support	Palladion Mediation Engine
Model Support	Automated DST Updates
Model Support	SDP Version Changes without SDP Body Change
Model Support	TSCF Data Flows
Model Support	TSCF Config
Model Support	Traffic Selectors List
Model Support	Natively Securing Network Topology Information in AVPs

Net-Net Central Features

This section provides features new to the Net-Net Central Release.

Audible Alarms

The Audible Alarms system allows you to set off an audible sound when an activated alarm is triggered.

Alarm events are updated during each refresh cycle of the Alarms table. Search functionality is disabled when audible alarms are active. The Audible Alarms cease to function upon exiting the Fault Manager application.

Alarm Frequency

The alarm will replay at a frequency set in the Audible Alarms configuration. For example, a frequency of 5 will sound the alarm sound every 5 seconds. Setting the frequency to 0 results in the alarm sound playing once.

Audio Files

The Audible Alarms application comes with five alarm sounds (one for each severity). You may replace these files with your own as long as the new.wav files retain the same filenames. The files are located in the directory:

<installed directory>\ACMEConsole\audibleAlarms

The filenames appear as:

- Audio_Emergency.wav
- Audio_Critical.wav
- Audio_Major.wav
- Audio_Minor.wav
- Audio_Warning.wav

Enabling an Audible Alarm

You must configure Audible Alarms in Net-Net Central before launching it from the Fault Manager application..

To configure audible alarms:

1. Click Settings in the Net-Net Central menu bar. A drop-down menu appears.
2. Click Alarms > Audible Alarms.
3. Click the Enable audio alarm check box of each severity you want to enable.
4. Frequency— Click the number to edit the audible alarm frequency. This value is entered in seconds. The default is 5.
5. Click OK.

To launch the Audible Alarms application:

6. Expand the Fault Manager slider and click Alarms.
   The Alarms table appears in the content area.
7. Click Auto Refresh.
8. Refresh interval (secs)— Enter a value in seconds for how often the Alarms table is automatically refreshed.
9. Click OK.
10. Click Start Audible Alarms.
    The button toggles to Stop Audible Alarms.

To shut down the Audible Alarms application:

11. Expand the Fault Manager slider and click Alarms.
    The Alarms table appears in the content area.
12. Click Stop Audible Alarms.
    The button toggles to Start Audible Alarms.

Configuration Element Search

The Configuration Element Search allows you to search and filter the instances within an element type’s paged table.

Attributes that make up the column headings of the table become available as input filters for the search. Column headings that summarize subelements such as Session agent group -> Session agents and from -> addr are not included in the search results.

For example:

Results in the following search filters:

Filter Search Criteria

The search filters you enter must follow these guidelines:

- Standard wild card * and ? characters are supported
    - * matches 0 or more characters
    - ? matches 1 character
- Search filters containing wild card characters must be enclosed in double quotes: “fo*”
- Search filters containing no wild card characters result in an exact match
- Wild card characters cannot be used outside of double quotation marks in combination with an exact match search.

  “A*1” is a valid search filter

  “A*”* is not a valid search filter

Using the Configuration Element Search

1. Click Search from any paged table in Configuration Manager.
   A dialog box appears.
2. Enter desired match values for any filters that appear in the dialog box.
3. Click Apply.
   The filtered search results appear in the table.

   Note: To clear the filtered search results and return to the previous table, you must click Show All.

Model Support

This section provides descriptions, explanations, and configuration information for model support new to the Net-Net Central Release.

S-C[x]6.2.0M12

Palladion Mediation Engine

The Palladion Mediation Engine is a platform that collects SIP, DIAMETER, DNS, ENUM, and MGCP protocol message traffic received from Palladion Probes.

A Probe is software run on COTS hardware; it is deployed within a network and collects packets from span/monitor ports on Ethernet switches, or receives IP-in-IP tunneled packet-traces from Acme PacketOracle Communications Session Delivery Managers. A Probe takes the protocol packets, prepends a receive timestamp and other information, encapsulates the packets, and passes them to Palladion via a secure connection. After receiving protocol traffic from a Probe, Palladion stores the traffic in an internal database, and analyzes aggregated data to provide comprehensive multi-level monitoring, troubleshooting, and interoperability information.

In contrast to the Packet-Trace feature, message logging is performed by software, which sends a copy of sent/received messages over UDP, or by saving such messages in a local file. The copy includes a timestamp, port/vlan information, and IP:port information, but all in ASCII format. Message Logging is performed after all decryption, meaning that SIP/TLS traffic cam be monitored. Because remote message logging sends the protocol messages over UDP, there is no guarantee or confirmation of delivery.

The Oracle Communications Session Delivery Manager provides support for Communications Monitoring, a user-configurable capability that enables the system to function as a Palladion Probe. Acting as a Probe, or as an exporter, the Oracle Communications Session Delivery Manager can:

1. Establish an authenticated, persistent, reliable TCP connection between itself and one or more Palladion Mediation Engines.
2. Optionally ensure message privacy by encrypting the TCP connection using TLS.
3. Use the TCP connection to send a UTC-timestamped, unencrypted copy of a protocol message to the Palladion Engine(s).
4. Accompany the copied message with related data to include: the port/vlan on which the message was sent/ received, local and remote IP:port information, and the transport layer protocol.

IPFIX

The Oracle Communications Session Delivery Manager uses the IPFIX suite of standards to export protocol message traffic and related data to the Palladion Mediation Engine.

- RFC 5101, Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information
- RFC 5102, Information Model for IP Flow Information Export
- RFC 5470, Architecture for IP Flow Information Export
- RFC 5655, Specification of the IP Flow Information Export (IPFIX) File Format
- RFC 5815, Definitions of Managed Objects for IP Flow Information Export

The IPFIX standards describe the use of templates to format the export of specific types of protocol traffic. The Oracle Communications Session Delivery Manager and the Palladion Mediation Engine share ten (10) pre-defined templates that facilitate protocol message exchange, and subsequent processing and analysis by the Palladion Engine.

The pre-defined templates are:

- incoming SIP/DNS over UDP
- incoming SIP over TCP
- incoming SIP over SCTP
- incoming DNS over UDP (entire IP and UDP header not included)
- outgoing SIP/DNS over UDP
- outgoing SIP over TCP
- outgoing SIP over SCTP
- outgoing DNS over UDP (entire IP and UDP header not included)
- media qos and flow record
- IPFIX handshake (used for connection establishment)

Communication Monitor Configuration

Communications Monitor configuration consists of the following steps.

1. Configuration of one or more Oracle Communications Session Delivery Manager/Palladion exporter/collector pairs.

   Configuration of the config object, which defines common operations across all interfaces, is not required. Default values can be retained to enable standard service.
2. Optional assignment of a TLS profile to an exporter/collector pair.

1. Expand the Configuration Manager slider > Global settings
2. Click System.
   The System window appears in the content area.

3. Scroll to the Communications monitor section.
4. SBC group ID — Enter an integer value to assign to the Oracle Communications Session Delivery Manager, in its role as an inform action exporter. The default value is 0.
5. State — Set to enabled to use communication monitoring
6. TLS profile — Enter a TLS profile to be assigned to the network interface. The absence of an assigned TLS profile (the default state) results in unencrypted transmission.
7. Enable qos — Set to enable or disable to export of RTP, SRTP, and QOS data flow information. Set to enabled by default.
8. Scroll to the Monitor collector table.
9. Click Add.
10. Address — Enter the IPv4 address monitored by a Palladion Mediation Engine for incoming IPFIX traffic.
11. Click Apply.
12. Select the Monitor collector you created and click Edit.
13. Port — Enter the port monitored by a Palladion Mediation Engine for incoming IPFIX traffic. The valid range is 1025-65535. The default value is 4739.
14. Click Apply.
15. Repeat Steps 1 through 14 to configure additional as required.

TLS Configuration

The TLS profile contains the information required to run SIP over TLS. You can configure a TLS profile using the ACLI. You can only view TLS profile information with the Net-Net Central.

To configure a TLS profile using ACLI, consult the *Net-Net 4000 S-C(X)6.2.0 Maintenance Release Guide*.

S-C[x]6.3.0M3

Automated Daylight Savings Time (DST) Updates

In addition to configuring DST at the command prompt, the Net-Net Central provides a mechanism to create static or rules-based time updates to reflect your location's seasonal Daylight Savings Time changes. This configuration offsets the Net-Net Central's internal time, obtained via NTP or from configuration. When DST is configured as a configuration element, it is persistent across reboots.

When the DST start date/time is reached, 1 hour is added to the system clock. When the DST end date/time is reached, 1 hour is subtracted from the system clock.

Baseline Configuration

To complete automated DST configuration, you must give a name to the time zone that this system adheres to and the minutes from UTC (offset) from UTC, entered as +/-720.

Static DST Updates

You can configure the Net-Net Central to enact and rescind DST offset on a predefined start and stop date. This is set with the following parameters:

Start/End rule— This parameter is set to static when configuring static DST start and end times.

Start/End month— The month when DST offset begins or ends, entered as 1-12.

Start/End day— The day of the month when DST offset begins or ends, entered as 1-31.

Start/End hour— The hour on the chosen day when DST offset starts or ends, entered as 0-23.

Rules-based DST Updates

You can configure the Net-Net Central to enact and rescind DST offset based on rules that correspond to relative dates in a month. That is, start and stop dates can be the Nth (or last) day-name, in a calendar month, as opposed to a day-number of the month.

Start/End rule— This parameter is set to ordinal number of the start/stop weekday when configuring rules-based DST start and end times. You can set this parameter to any of the following values:

Start/End month— The month when DST offset begins or ends, entered as 1-12.

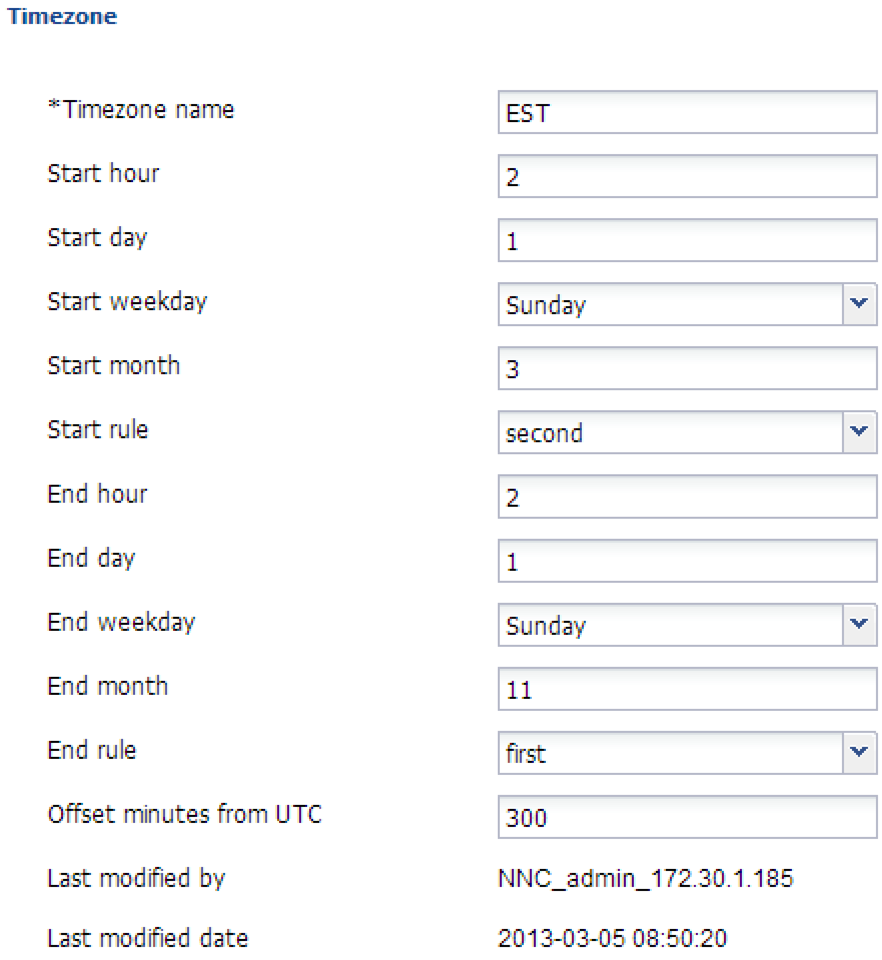
Start/End weekday— The named day when DST offset begins or ends. You can set this parameter to any of the following values:

Start/End hour— The hour on the chosen day when DST offset starts or ends, entered as 0-23.

Start/End day— This parameter is not configured when entering rules based DST updates.

DST Update Examples

The current DST rule for North America is that daylight savings starts on the second Sunday in March at 2:00am and ends on the first Sunday in November at 2:00am. Thus the settings for the Eastern Time Zone would be as follows:

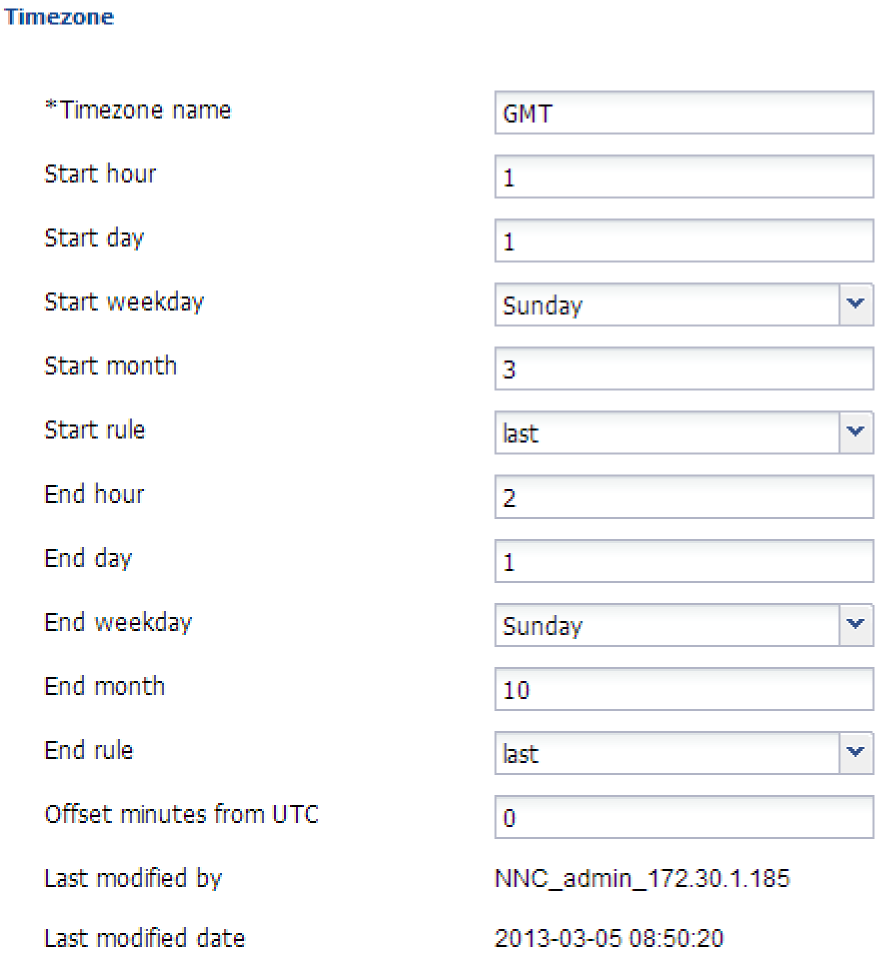


Timezone

*Timezone name	EST
Start hour	2
Start day	1
Start weekday	Sunday
Start month	3
Start rule	second
End hour	2
End day	1
End weekday	Sunday
End month	11
End rule	first
Offset minutes from UTC	300
Last modified by	NNC_admin_172.30.1.185
Last modified date	2013-03-05 08:50:20

Note: The Start day and End day values are ignored.

The European Union directive states that DST starts on the last Sunday in March at 1:00am UTC and ends on the last Sunday in October at 1:00am UTC. Therefore the timezone settings for the UK would be:



Timezone

*Timezone name	GMT
Start hour	1
Start day	1
Start weekday	Sunday
Start month	3
Start rule	last
End hour	2
End day	1
End weekday	Sunday
End month	10
End rule	last
Offset minutes from UTC	0
Last modified by	NNC_admin_172.30.1.185
Last modified date	2013-03-05 08:50:20

Note: The End hour is 2 because this is the local time and 2am BST is 1am UTC.

Automated DST Configuration

1. Expand the Configuration Manager slider > Global settings > Management.
2. Click Timezone.
3. Click Add to create a new Timezone configuration.
4. Timezone name — Enter the time zone name where this Net-Net Central resides.
5. Click Apply.
6. Click OK.
7. Start hour — Enter the hour when DST starts.
8. Start day — Enter the day number of the month when DST starts. This parameter is only configured in static DST rules.
9. Start weekday — Enter the day name when DST starts. This parameter is only configured in non-static DST rules.
10. Start month — Enter the month number that DST starts.
11. Start rule — Set to static when configuring a static DST start date or the ordinal position of the configured dst-start-weekday parameter when configuring a rulesbased DST offset. Valid values are:

    ```
    disabled | static | first | second | third | fourth | last
    ```

12. End hour — Enter the hour when DST ends.
13. End day — Enter the day number of the month when DST ends. This parameter is only configured in static DST rules.

14. End weekday — Enter the day name when DST ends. This parameter is only configured in non-static DST rules.
15. End month — Enter the month number when DST ends.
16. End rule — Set to static when configuring a static DST end date or the ordinal position of the configured dst-end-weekday parameter when configuring a rulesbased DST offset. Valid values are:

    ```
    disabled | static | first | second | third | fourth | last
    ```

17. Offset minutes from UTC — Enter the offset from UTC in minutes. Valid values are +/-720 (a “plus” is not required when entering a positive offset.
18. Click Apply.

SDP Version Change without SDP Body Change

When an SRTP call is made through the Oracle Communications Session Delivery Manager and a UE sends a reINVITE, there may be no change in the SDP contents. When the other UE responds, some devices will increment the o= line’s session version, despite no SDP change. Normally the change in SDP version indicates that the SDP has changed, which would otherwise require the Oracle Communications Session Delivery Manager to modify the media flow set-up. In order to leave the media flows unchanged when session version changes but the rest of the SDP does not, an option is configured in the Media manager configuration.

If the Oracle Communications Session Delivery Manager attempts to modify these media flows when unnecessary, calls could be dropped by the system disrupting media packet sequence number synchronization.

The ignore-reinv-session-ver option is set to handle this situation. When configured, the Oracle Communications Session Delivery Manager compares the current SDP received from a UE against the previously received SDP from the same UE. If the SDP in the newer and older messages is the same, the Oracle Communications Session Delivery Manager ignores any changes to the session-version and will not modify the media flow portion of the call.

Note: When the SDP change is only a reordering of SDP lines without any other change, the option has no effect.

Note: This option is used only to mitigate compatibility issues when running SRTP calls over any of Acme Packet’s IPSec accelerated NIUs for the Net-Net 4500 or 3820. NOT for ETC NIUs.

SDP Version Change without SDP Body Change Configuration

1. Expand the Configuration Manager slider > Global Settings.
2. Click Media manager.
3. Click Add to create the Media manager configuration if one does not exist.
4. Scroll to the Options section, and click Options.
   The Options dialogue box appears.
5. Click ignore-reinv-session-ver in the Available options list to select it.
6. Click >> to move the option to the Selected options list.
   The option name appears along with a description in the lower part of the window.
7. Click OK.
8. Click Apply.

S-C[x]6.3.7M1

There is no new configuration for this maintenance release.

S-C[xz]6.3.9M1

There is no new configuration for this maintenance release.

S-C[x]6.4.6F2

For more information on this release, consult the *Net-Net TSCF Essentials Guide Version SCX6.4.6F2*.

TSCF data flow

Use the following procedure to configure an optional TSCF data flow object. If you are not using TSCF data flows to provide to provide static egress routes, this procedure can be safely ignored.

The size of the associated TSCF address pool (defined as the number or IPv4 addresses contained in the pool), is divided by the Group size value to segment the address pool into smaller address blocks. After determining the start address for each block, the Session Director establishes two static flows for each of the address blocks — a downstream flow, in the access direction, and an upstream flow generally toward a core application server gateway/router that provides forwarding service for pass-thru dataflow.

As a result of the static-flow establishment, each address block consumes 4 NAT entries, 2 for the downstream flow and 2 for the upstream flow. Because the current software release imposes a maximum restriction of 4096 NAT entries per data flow instance, dividing 4096 by 4 provides the largest number of supported address blocks, 1024.

TSCF data flow Configuration

1. Global settings > Security > TSCF > TSCF data flow.
2. Name — Enter the name for a data flow.
3. Group size — Enter the number of UEs to be managed by the data flow. The default value is 128.
4. Upstream rate — Enter the allocated upstream (access-side) bandwidth in KB/s. The valid range is 0-122070. The default value is 0 and allocates all available bandwidth.
5. Downstream rate — Enter the allocated downstream (access-side) bandwidth in KB/s. The valid range is 0-122070. The default value is 0 and allocates all available bandwidth.
6. Realm id — Enter the realm ID to route the upstream data flow.
7. Click Apply.

TSCF Config

Element Id

In topologies that contain multiple TSCF servers, each server must be assigned a unique network-wide identifier, provided by this parameter.

The assignment of a unique TSCF server guarantees unique tunnel identifiers regardless of the number of TSCF servers within the network.

Keepalive Timer Datagram

Keepalive timer datagram specifies the maximum idle time (defined as no transmission activity within the tunnel) before the TSCF server transitions a datagram-based (UDP) tunnel from the active to the persistent state. The integer values 30 through 550 seconds specifies the maximum size of the tolerated idle period for datagram-based tunnels.

In the absence of a user-supplied value for Keepalive timer datagram provides a default timer value for all tunnels regardless of the underlying transport protocol. When Keepalive timer datagram is set to its default value (0), Keepalive timer provides the default timer value for all tunnels, without regard to the transport protocol (TCP or UDP).

TSCF Element Id Configuration

1. Expand the Configuration Manager slider > Global settings > Security > TSCF.
2. Click TSCF config.
3. Press Add to add the accounting configuration in the content area.
4. Element Id — Enter a unique identifier to this TSCF server. The valid range is 0- 1023. The default value is 0.
5. Click Apply.

TSCF Keepalive Timer Datagram Configuration

1. Expand the Configuration Manager slider > Global settings > Security > TSCF.
2. Click TSCF data flow.
3. Keepalive timer datagram — Enter a the maximum idle time (seconds) before the TSCF server transitions to a datagram-based tunnel from the active to persistent state. The valid range is 30-550 seconds.
4. Click Apply.

E-C[xz]6.3.7M1

There is no new configuration for this release.

D-C[z]2.1.0

.

Natively Securing Network Topology Information in AVPs

In many deployment environments, administrators require that their network topology information be hidden across Diameter elements. The Net-Net Diameter Director provides configuration options to implement this security without requiring discrete diameter manipulation rules. By implementing this processing natively, the Net-Net Diameter Director minimizes the processing and configuration overhead required to secure this information.

This is the start of your concept. Concepts answer the question What is...? Here you need to provide conceptual and overview information. For example, provide the background information a user needs to know so that they can be successful in accomplishing their tasks.

There are 6 key AVPs that the Net-Net Diameter Director can secure natively. You secure these AVPs via the Network topology parameter and its applicable arguments, as described below:

- Topology Masking — Changes origin-host and origin-realm AVPs from the source's values to the values used during capabilities negotiation between the Net-Net Diameter Director and the next-hop diameter agent.
- Toplogy Hiding — Changes destination-host and destination-realm AVPs from the source's values to the values used during capabilities negotiation between the NetNet Diameter Director and the next-hop diameter agent.
- Topology Obscuring — Changes session-id to a string encoded by the Net-Net Diameter Director and strips all record-route AVPs from the message.

You can also configure any combination of the above to implement each argument's effects.

You configure this support globally, per diameter-interface, or per diameter-agent. In cases of conflicting configuration, the diameter-agent configuration takes highest precedence, followed by interface, then global. This precedence is not cumulative; that is, any configuration on an agent invalidates the applicable interface's configuration for traffic to that agent.

The system performs the configured function on egress traffic. This provides additional configuration flexibility, giving you the option of performing these functions for either or both Diameter elements involved with the messaging.

Topology Masking

Topology masking is as much a means of establishing compatibility between devices as a security feature. Some devices always expect upstream Diameter traffic to come from a relay. These devices expect the origin-host and origin-realm AVPs in messages to be the same as learned during capabilities negotiation.

In deployments where this security is required or Net-Net Diameter Director needs to appear to be a proxy, use topology masking to change origin-host and origin-realm accordingly.

Topology Hiding

Use topology hiding to further secure networks' topology information from each other. It is common for topology hiding to be implemented in conjunction with topology masking to achieve the resulting cumulative security.

Topology Obscuring

Topology obscuring changes session-id AVPs and removes all record-route AVPs from ingress request and response messages prior to forwarding. When implemented in conjunction with topology masking and hiding, you achieve the maximum level of security.

By definition, topology obscuring is only applicable within the context of stateful applications. The sytem maintains an internal mapping of the original and new sessionIDs. During transit, the system inserts the new session-ID in messages from the originator and inserts the original session-ID in messages from the next-hop server back to the originator.

The format of the new session ID is as follows:

```
New Session-Id = <origin-host>;<timestamp>;<sequence>
```

- <origin-host> — The origin-host value derived from the diameter-director-interface for the egress agent.
- <timestamp> — The time the socket originally connected, per RFC3588.
- <sequence> — An incrementing sequence number from 1 to 4294967295, which is the maximum unsigned 32-bit value. If the sequence reaches the maximum value, the Net-Net Diameter Director generates a new timestamp and re-starts the sequence.

Record-route stripping is a matter of removing these AVPs from requests and responses from the session originator to the next-hop server.

The Net-Net Diameter Director performs topology obscuring only within the context of stateful applications. Any messages associated with a stateless application that transiting a Net-Net Diameter Director element configured for topology obscuring are not affected. Instead, the Net-Net Diameter Director simply logs a message indicating that it forwarded the message without modification.

Network Topology Security and Dynamic Routing

The Net-Net Diameter Director accommodates dynamic routing in paths that include network topology masking, hiding and/or obscuring. Additional user configuration is not required.

Dynamic routing depends on an agent's origin host AVPs to reply to requests. Normally, the Net-Net Diameter Director caches this forwarding information for these agents. Lookups needed to route to these cached endpoints, therefore, fail if the AVP has been changed in transit.

To accommodate this, the Net-Net Diameter Director builds origin host AVPs in such a way that it can recognize messages intended for agents that depend on dynamic routing. The Net-Net Diameter Director creates these AVPs using a pre-specified format that includes a cookie and the AVP. The Net-Net Diameter Director recognizes AVPs in this format and forwards the messages using the route cache.

Natively Securing Network Topology Information in AVPs Configuration

To configure an existing diameter-director agent with topology masking, hiding and obscuring security:

1. Configuration Manager Slider, go to Services -> Diameter director agent.
2. Select the Diameter directer agent you want to modify and click Edit.

3. Scroll to the Network topology table.
4. Click Add. The Add Network topology dialog appears.
5. Name — Select the desired level of topology security the system uses.
6. Click Apply.
7. Click Apply.

3

Net-Net Central 7.3M2 Features and Model Support

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net Central Release 7.3M2.

Content Map for 7.3M2

This table provides a listing of all new content in Net-Net Central Release 7.3M2:

Content Type	Description
Net-Net Central Feature	License Information

Net-Net Central Features

This section provides features new to the Net-Net Central Release.

License Information

You can view the system license information for the Net-Net Central server(s) by clicking Help > License information.

You can view the third-party license information for the Net-Net Central server(s) by clicking Help > About > License info.

S-C[x]6.3.0M4

There is no new configuration support for this release.

S-D7.1.0M5

There is no new configuration support for this release.

4

Net-Net Central 7.3M3 Features and Model Support

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net Central Release 7.3M3.

Content Map for 7.3M3

This table provides a listing of all new content in Net-Net Central Release 7.3M3:

Content Type	Description
Net-Net Central Feature	Password Change Process Enhancement
Net-Net Central Feature	Configuration Schema Upload
Net-Net Central Feature	Diagnostics Tool
Net-Net Central Feature	Work Order Enhancements
Net-Net Central Feature	External AAA
Net-Net Central Feature	TLS Support for ACP
Model Support	Specific Action AVP
Model Support	Node-Function AVP
Model Support	SIPREC Ping
Model Support	Personal Profile Manager (PPM) Proxy
Model Support	DDoS Protection from Devices Behind a NAT
Model Support	SDP Alternate Connectivity
Model Support	Authenticated NTP

Net-Net Central Features

This section provides features new to the Net-Net Central Release.

Password Change Enhancement

You can update system user passwords using the Tools > Passwords... dialog. In previous releases, administrators were required to run through the Net-Net Central installation in order to change system user passwords. Selecting Update system user password under Passwords... displays a table of the following system users:

- SFTP (nncentral)
- Reports and Faults (user email)
- Trap Replay (sudo)

After a new password is validated, if present, all changes replicate across the cluster.

Changing a System User Password

1. Select Tools > Passwords and click Update OS/System passwords.
   The Passwords... dialog appears.
2. Select the type of account you would like to update and click OK.
   The Select account dialog appears.
3. Select the user you want to edit and click Update.
   New password and Confirm new password fields appear in the dialog.
4. Enter the new password twice and click Update.
   A confirmation dialog appears.
5. Click Yes to confirm you changes.
   A dialog appears with a success or error message.

Configuration Schema Upload

You can upload a configuration schema into Net-Net Central by selecting and uploading a configuration file. Net-Net Central validates the schema to ensure it is a proper .XSD file. The uploaded schema is replicated to all members within a cluster.

Upload a Configuration Schema

1. Select the Tools menu and click Upload configuration file.
2. Click Browse... to navigate to a valid .xsd file.
   A file browsing dialog appears.
3. Select the configuration schema you want to upload and click Open.
4. Click Upload to start the upload process.
   A dialog appears with a success or error message.

Diagnostics Tool

The diagnostics tool allows administrators to retrieve files used for troubleshooting and analysis via the Net-Net Central GUI. Types of files collected include:

- Logs
- Databases
- Configuration

Collected files can be found in the directory .../AcmePacket/NNCArchive/NNCDiagnosticsArchive/. The diagnostic tool can initiated on any node in a clustered environment and the files are retrieved from any running cluster member. If a node does not respond within a timeout period of 120 seconds, the Collection status is set to Failed.

Logging Levels

Logging levels can be changed dynamically on all or individual log files. The levels are as follows:

- ERROR
- WARNING
- INFO
- DEBUG
- TRACE

For example, if DeviceService.log is set to ERROR, all subsequent entries will have logs of level ERROR or higher.

Retrieving Diagnostics Information

1. Select the Tools menu and click NNC Diagnostics.
2. Mark the check boxes of any additional diagnostic information you wish to collect.
3. Click Start Collection to initiate the diagnostics tool.
   The Collection Information is updated with the most recent collection date and the collected file name.
4. Click Download Now to save the files to your local machine.

Work Order Enhancements

This feature includes additions to Work Order administration configuration.

HA Software Upgrade/Downgrade Workflow Enhancements

You can restore the original HA pair active/standby configuration during the software upgrade process by enabling Force switchover to restore original HA setup if it is configured in the workflow. This option is disabled by default and can be enabled in the Workflows tab of the Add/Edit work order screen.

Behavior of Work Orders

The Behavior parameter, located in the Settings tab of the Work Order administration screen, previously offered two options:

- Never pause - Executes all work orders on multiple machines.
- Pause after every device - Requires approval before operating on subsequent machines.

The addition of Pause only after 1st device stops the work order after the first device is complete for approval by the administrator, while automatically completing the tasks for subsequent machines.

Configuring Work Order Enhancements

Enabling a Force Switchover to Restore Original HA Setup

1. Expand the Device Manager > Software upgrade and click Work Order Administration.
2. Click Add or select an existing work order from the table and click Edit.
3. Click the Workflows tab.
4. Force switchover to restore original HA setup if it is configured— Click the checkbox to enable this feature.
5. Click Apply.

Setting the Behavior of Work Orders

6. Expand the Device Manager > Software upgrade and click Work Order Administration.
7. Click Add or select an existing work order from the table and click Edit.
8. Click the Settings tab.
9. Force switchover to restore original HA setup if it is configured— Select Pause only after 1st device from the combination box.

10. Click Apply.

External AAA

External Authentication, Authorization, and Auditing/Accounting (AAA) enables you to utilize your existing RADIUS or Active Directory servers for Net-Net Central user authentication. User groups that are created and managed externally must be mapped to internal NNC-local user groups. NNC-local and external users are supported simultaneously, although external users do not have corresponding user records or username/password information stored in Net-Net Central.

The Change authentication, authorization and auditing mechanism permission allows admin/liadmin users to edit external authentication settings.

Add/Edit Groups

The External group name element appears when external AAA is enabled, allowing you to specify which external group is associated with the current NNC-local group. When editing a group, you can test the authentication of a user within the group by clicking the Test group membership button.

External AAA for RADIUS Configuration

Pre-requisites:

- RADIUS server must be configured to use the same shared secret string for all NNC cluster nodes.
- RADIUS server must be configured to return one or more attribute values in the authentication response message to represent the groups a user belongs to.

1. Expand the Security Manager slider > User management.
2. Click Authentication.
3. External authentication, authorization- Select Radius.
   The Radius servers table becomes available for use.
4. Click Add.
   The Add a radius server screen appears.
5. Address- Enter the IP address or DNS name of the RADIUS server.
6. Port- Enter the listening port of the RADIUS server.
7. Click Edit.
8. Shared secret- Enter the string assigned within the RADIUS server configuration to a given RADIUS client (Net-Net Central, in this case).
9. Enter the shared secret again to confirm your input.
10. Click Apply.
11. Password authentication mechanism- Select the protocol used to authenticate the user. Choices are PAP, CHAP, MSCHAPV1, MSCHAPV2, EAPMD5, and EAPMSCHAPV2.
12. Group attribute name- Enter the attribute for the RADIUS server to return, containing group information on an authenticated user. The default is Filter-Id.
13. Click Apply.

External AAA for Active Directory Configuration

Pre-requisites:

- Active Directory must be configured for LDAP over SSL if enabled in Net-Net Central.
- Active Directory must support version 5, if using the Kerbeos protocol.
- Each user object in your Active Directory must store the groups of each member using the "memberOf" attribute.

- Only child groups may be mapped to NNC-local groups when group nesting is in use. This limitation is due to the memberOf attribute not containing a recursive list of predecessors when nesting.

1. Expand the Security Manager slider > User management.
2. Click Authentication.
3. External authentication, authorization- Select Active directory.
   The Active Directory servers table becomes available for use.
4. Click Add.
   The Add a Domain Controller screen appears.
5. Address- Enter the IP address or DNS name of the Domain Controller.
6. Domain- Enter the domain name for the Domain Controller.
7. LDAP port- Enter the listening port number of the LDAP service. The default is 389, 636 if using SSL.
8. Password security- Select one of the following options:
   - Digest-MD5- Use the password cipher based on RFC 2831.
   - LDAP over SSL- Use SSL to encrypt all LDAP traffic.
   - Kerberos- Use the Kerberos protocol to authenticate the user. Additional parameters are required in order to use this option.
9. Skip this step if configuring the Kerberos protocol, otherwise click Apply to finish.

Continue if configuring the Kerberos protocol:

10. Kerberos- Select one of the following options:
    - Kerberos choice 1- Select to specify an existing krb5.conf file.
    - Kerberos choice 2- Select to specify a realm.
11. Enter the required information for your selection and click Apply.

TLS Support for ACP

ACP over TLS adds a layer of security to the communications link between the Oracle Communications Session Delivery Manager and Net-Net Central. Trusted and/or Entity Cerficates must be configured during the installation/ upgrade process with the Setup tool. In order to establish the TLS community for ACP, you must:

1. Import the valid Trusted CA Certificate to Net-Net Central for device authentication during the handshake.
2. If mutual authentication is enabled on your device, you must create a valid Entity Certificate for Net-Net Central to send the device during the handshake. To sign an Entity Certificate by the CA, you must perform the following steps, in order.
   a. Generate a Certificate Signing Request (CSR) and send the request to CA.
   b. Store the signed certificate reply from the CA on a local directory accessible to Net-Net Central.
   c. Import the CA (signer) certificate as a Trusted Certificate.
   d. Import the signed certificate reply.

The current status of TLS support for each device is displayed in the Managed devices screen by enabling the hidden TLS status column.

Valid states for TLS status are:

- enabled
- disabled
- -- (Unknown status or unsupported device)

Note: All cluster members must configure and manage their own certificates.

Note: You must disable TLS over ACP if you plan on downgrading your device to a TLS non-supported image when using the Software Downgrades tool in Net-Net Central.

Trusted Certificates for ACP over TLS Configuration

The process for importing a trusted certificate is as follows:

1. Press Enter to accept the default value of 9 for SBI TLS configuration.

   ```
   Please select an option [9] 9
   ```

2. Enter Y and press Enter to continue. The SBI TLS configuration menu appears.

   ```
   Do you want to continue Yes/No? Y
   ```

3. Enter 2 and press Enter to select the Trusted Certificate configuration.

   ```
   Please select an option [1] 2
   ```

4. Press Enter to accept the default value of 1 for the Import Trusted Certificate dialog.
5. Enter a unique alias name for the certificate to be imported.
6. Enter the full path of the certificate to be imported.
   A success message appears, along with the location on the server of the imported certificate.
7. Enter Y and press Enter to continue. The SBI TLS configuration menu appears.

   ```
   Do you want to continue Yes/No? Y
   ```

You may continue configuring an Entity Certificate if you plan on using mutual authentication, otherwise you can finish your Net-Net Central Installation/upgrade.

Entity Certificates for ACP over TLS Configuration

This section shows you how to configure an Entity Certificate to support ACP over TLS for the firs time.

The following steps occur during the installation/upgrade process for custom options.

1. Press Enter to accept the default value of 9 for SBI TLS configuration.

   ```
   Please select an option [9] 9
   ```

2. Enter Y and press Enter to continue. The SBI TLS configuration menu appears.

   ```
   Do you want to continue Yes/No? Y
   ```

3. Press Enter to accept the default value of 1 for Entity Certificate configuration.

   ```
   Please select an option [1]
   ```

4. Press Enter to accept the default value of 1 for the Entity Certificate creation menu.
   You are prompted to enter the certificate information.
5. Enter the name of your organization unit (OU) and press Enter.
6. Enter the name of your organization (O) and press Enter.
7. Enter the name of your city or locality (L) and press Enter.
8. Enter the name of your state or province (ST) and press Enter.
9. Enter the two-letter country code for this unit (C) and press Enter.
10. Enter the key size (1024, 2048) and press Enter.
11. Enter the validity (day) and press Enter.
12. Enter Y and press Enter to continue.

    ```
    Do you want to continue Yes/No? Y
    ```

13. Enter 3 and press Enter to generate a Certificate Signing Request.

    ```
    Please select an option [1] 3
    ```

14. Enter the absolute path of the certificate request file and press Enter.

    ```
    Enter full path of the certificate request file: [] C:\ssl
    \entityCertRequest.csr

    Operation successful
    ```

15. Send the CSR to the CA to be signed.

16. Follow the instructions in *Trusted Certificates for ACP over TLS Configuration* to import a Trusted Certificate.
17. Enter 4 and press Enter to import the signed Entity Certificate.

```
Please select an option [1] 4

Operation successful
```

You may continue configuring your Net-Net Central Installation.

TLS Certificate Options

The menu changes based on whether you have a previously configured certificate or not. When first configuring SBI TLS, you may only have a few options to create/import a certificate. The following selections appear when previously configured certificates are found.

Enter the number of the corresponding action you want to complete and press Enter.

Entity Certificates

1. - View Entity Certificates
2. - Export Entity Certificate
3. - Generate Certificate Signing Request
4. - Import Signed Entity Certificates
5. - Delete Entity Certificate
6. Quit and back to Main Menu

Trusted Certificates

1. - Import Trusted Certificate
2. - List all Certificates
3. - View Certificate detail
4. - Delete Trusted Certificate
5. Quit and back to Main Menu

Model Support

This section provides descriptions, explanations, and configuration information for model support new to the Net-Net Central Release.

S-C[x]6.3.3M2

Specific Action AVP

When acting as a P-CSCF, Oracle Communications Session Delivery Manager sends the Specific-Action AVP to the PCRF in an AAR message to indicate the subscription types it supports.

The Oracle Communications Session Delivery Manager can be configured to subscribe to one or more of the following subscription types:

- LOSS OF BEARER
- RECOVERY OF BEARER
- RELEASE OF BEARER
- OUT OF CREDIT
- SUCCESSFUL RESOURCES ALLOCATION
- FAILED RESOURCES ALLOCATION

When no subscription types are configured, the Oracle Communications Session Delivery Manager does not include the Specific-Action AVP in its AAR.

Specific Action AVP subscription is configured in the Specific action subscription parameter located in the External policy server configuration element.

Specific Action AVP Configuration

Required. See Authoring Guide for details.

1. Expand the Configuration Manager slider > Services > Signaling > Call admission control.
2. Click External policy server.
3. Specific action subscription - Add 1 or more specific actions. The following are valid specific actions: loss-of-bearer, recovery-of-bearer, release-of-bearer, out-of-credit, successful-resources-allocation, failed-resources-allocation, ip-can-change
4. Click Apply.

Node-Function AVP

The Oracle Communications Session Delivery Manager sends the Node-Functionality (862) AVP in all Rf ACR messages.

The Node-Functionality AVP indicates the function that the message's source plays in the network. The CDF/CGF function that collects the ACR messages can use the information in the Node-Functionality AVP for billing or analysis purposes.

In an IMS network, the Oracle Communications Session Delivery Manager may perform the following functions: P-CSCF, E-CSCF, IBCF, BGCF (when configured as a Net-Net Session Router). In fact, the Oracle Communications Session Delivery Manager might perform different roles simultaneously, so that on a call-by-call basis, the value in the Node-Functionality might change.

To accurately reflect multiple, simultaneous functions that the Oracle Communications Session Delivery Manager performs, the value inserted into the Node-Functionality AVP may be defined per realm. The node functionality value for a call's ACR is taken from the configuration in the ingress realm. Each realm may only be marked with a single Node Functionality value.

The Oracle Communications Session Delivery Manager can still be configured with a single, global Node-Functionality value. This is done in the SIP config's node functionality parameter. When configured, all Oracle Communications Session Delivery Manager-generated ACRs include this value. However, if the node functionality parameter is also configured in a realm config, the ingress realm's node functionality value supersedes the global value.

The Node functionality in a realm config may be configured with an empty string (default). This indicates that this realm should revert to the global Node functionality value.

Specific Action AVP Global Configuration

To configure a global Node Functionality AVP value:

1. Expand the configuration Manager slider > Global settings.
2. Click SIP.
3. Select a SIP configuration and click Edit.
4. Node functionality— Select a global value to insert into the Node-Functionality AVP when the Oracle Communications Session Delivery Manager sends ACRs over the Rf interface to an appropriate destination. The default is P-CSCF. Valid values are:
   - P-CSCF
   - BGCF
   - IBCF

- E-CSCF

5. Click Apply.

Node-Function AVP Realm Configuration

To configure a global Node Functionality AVP value:

1. Expand the configuration Manager slider > Services.
2. Click Realms.
   The Realm table appears in the content area.
3. Select an existing Realm and click Edit or click Add to create a new one.
4. Node functionality— Select the value to insert into the Node-Functionality AVP when the Oracle Communications Session Delivery Manager sends ACRs for calls that enter the system from this realm. The default is empty which uses the global node functionality value configured in the sip-config configuration element. Valid values are:

   - P-CSCF
   - BGCF
   - IBCF
   - E-CSCF
5. Click Apply.

S-C[x]6.3.9M2

SIPREC Ping

This SIPREC ping is a signal that the Oracle Communications Session Delivery Manager transmits to the connected SRS requesting a response pertaining to the message type that you specify for the ping-method. It uses the ping-interval to determine how long it should wait before sending another ping to the SRS.

You can check the connectivity by configuring the following parameters:

- Ping method- SIP message or method for which to ping the SRS.
- Ping interval- Amount of time, in seconds, that the Oracle Communications Session Delivery Manager waits before it pings the SRS in subsequent intervals. For example, if this parameter is set for 60 seconds, the Oracle Communications Session Delivery Manager pings the SRS every 60 seconds.

Once configured the Oracle Communications Session Delivery Manager uses this feature to perform SIP-based pinging to determine if the SRS is reachable or not.

SIPREC Ping Configuration

To configure SIPREC ping:

1. Expand the Configuration Manager slider > Services > Signaling.
2. Click Call recording server.
3. Ping method- Enter the message or method type for which the Oracle Communications Session Delivery Manager uses in a ping request to the SRS to determine if it is reachable or not. Default is blank.

   Valid values are:

BYE	OPTIONS
UPDATE	SUBSCRIBE
CANCEL	NOTIFY

4. Ping interval (sec)— Enter the amount of time, in seconds, that the Oracle Communications Session Delivery Manager waits before it pings the SRS in subsequent intervals. Valid values are 0 to 99999. Default is 0 (zero). The setting of zero disables the ping interval.

Personal Profile Manager (PPM) Proxy

The Personal Profile Manager (PPM) proxyis a web service that runs as part of Avaya Aura Session Manager and Aura System Manager. Local and remote SIP clients may download configuration data from the PPM proxy using SOAP messages over HTTP or HTTPS, enabling soft keys to be customized and contact lists to be loaded. Unfortunately, in enterprise networks certain messages may refer to private IP addresses, which are not routable from remote clients. Acme Packet now incorporates an application proxy in the Net-Net ESD for such messages, replacing the internal IP addresses with the Net-Net ESD's external SIP interface IP address.

The PPM proxy supports incoming messages over HTTP and HTTPS on a configurable IP address / port. If using HTTPS, the PPM proxy uses a selectable server certificate for Transport Layer Security (TLS).

Remote clients accessing the PPM proxy are authenticated by HTTP digest authentication, using their SIP credentials. The PPM proxy forwards such challenges and responses transparently to the PPM web service for which it is configured.

Since the PPM proxy could potentially be a target of a denial-of-service (DoS) attack, the Net-Net ESD allows you to set DoS rules to protect the proxy port as part of standard configurations. For configuring DoS on the Net-Net Session Director, see the *Net-Net 4000 ACLI Configuration Guide*.

PPM Proxy Configuration

1. Expand the Configuration Manager slider > Services > Signaling.
2. Click HTTP-ALG.
3. Click Add.
4. Identifier— Enter a unique identifier for the HTTP proxy. Valid values are alpha-numeric characters.

Public Setting

5. Address— Enter the IPv4 or IPv6 IP address on which the Net-Net SBC is listening for HTTP traffic. Valid values must be in the format of 0.0.0.0..
6. Realm ID— Select the realm that the Net-Net SBC uses to listen for the HTTP request.

Private Settings

7. Address— Enter the IPv4 or IPv6 IP address from which the Net-Net SBC forwards the incoming HTTP request. Valid values must be in the format of 0.0.0.0.
8. SM address— Enter the IPv4 or IPv6 IP address of the destination server to which the HTTP request is forwarded. Valid values must be in the format of 0.0.0.0.
9. Realm ID— Select the realm that the Net-Net SBC uses to proxy the HTTP request. .
10. Click Apply.

Enabling the Proxy

11. Select the PPM proxy you just created and click Edit.
12. Description— Enter a description for the HTTP proxy. Valid values are alpha-numeric characters. Default is blank.
13. State— Set to Enabled.
14. Click Apply.

S-C[x]6.4.0M1

DDoS Protection from Devices Behind a NAT

A DDoS attack could be crafted such that multiple devices from behind a single NAT could overwhelm the Net-Net SBC. The Net-Net SBC would not detect this as a DDoS attack because each endpoint would have the same source IP but multiple source ports. Because the Net-Net SBC allocates a different CAM entry for each source IP:Port combination, this attack will not be detected. This feature remedies such a possibility.

Restricting the Number of Endpoints behind a NAT

Each new source IP address and source IP port combination now counts as an endpoint for a particular NAT device. After the configured value of a single NAT's endpoints is reached, subsequent messages from behind that NAT are dropped and the NATis demoted. This is set with the Max endpoints per nat parameter located in both the Access control and Realm configuration elements.

Counting Invalid Messages from Endpoints behind a NAT

The Net-Net SBC also counts the number of invalid messages sent from endpoints behind the NAT. Once a threshold is reached, that NAT is demoted. Numerous conditions are counted as Errors/Invalid Messages from an endpoint. The aggregate of all messages from endpoints behind the NAT are counted against the NAT device, in addition to the existing count against the endpoint. This threshold is set with the Nat invalid message threshold parameter located in both the Access control and Realm configuration elements.

As a unique case, the absence of a REGISTER message following a 401 response is counted as an invalid message from the end point. And if that endpoint is behind a NAT, this scenario will be counted as invalid message from that NAT device as well. You set a timeout period in which the REGISTER message must arrive at the Net-Net SBC. This period is set with the Wait time for invalid register parameter located in the Realm configuration.

DDoS Protection from Devices Behind a NAT Realm Configuration

1. Expand the Configuration Manager slider > Services.
2. Click Realms.
3. Select an existing Realm and click Edit or click Add to create a new one.
4. Wait time for invalid register— Set the period (in seconds) that the Oracle Communications Session Delivery Manager counts before considering the absence of the REGISTER message as an invalid message.
5. Maximum endpoints per NAT— Set the maximum number of endpoints that can exist behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature. This parameter is also found in the access control configuration element.
6. NAT invalid message threshold— Set the maximum number of invalid messages that may originate behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature. This parameter is also found in the access control configuration element.
7. Click Apply.

DDoS Protection from Devices Behind a NAT Access Control Configuration

1. Expand the Configuration Manager slider > Services > Signaling.
2. Click Access control.
3. Maximum endpoints per NAT— Set the maximum number of endpoints that can exist behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature.
4. Nat invalid message threshold— Set the maximum number of invalid messages that may originate behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature.
5. Click Apply.

SDP Alternate Connectivity

The Oracle Communications Session Delivery Manager can create an egress-side SDP offer containing both IPv4 and IPv6 media addresses via a mechanism which allows multiple IP addresses, of different address families (i.e., IPv4 & IPv6) in the same SDP offer. Our implementation is based on the RFC draft "draft-boucadair-mmusic-altc-09".

Each realm on the Oracle Communications Session Delivery Manager can be configured with an alternate family realm on which to receive media in the Alternate family realm parameter in the realm configuration. As deployed, one realm will be IPv4, and the alternate will be IPv6. The Oracle Communications Session Delivery Manager creates the outbound INVITE with IPv4 and IPv6 addresses to accept the media, each in an a=altc: line and each in its own realm. The IP addresses inserted into the a=altc: line are from the egress realm's and Alternate realm family realm's steering pools. Observe in the image how the red lines indicate the complementary, alternate realms.

You can configure the order in which the a=altc: lines appear in the SDP in the pref-address-type parameter in the realm-config. This parameter can be set to:

- IPv4 - SDP contains the IPv4 address first
- IPv6 - SDP contains the IPv6 address first
- NONE - SDP contains the native address family of the egress realm first

In the 200OK to the INVITE, the callee chooses either the IPv6 or IPv4 address to use for the call's media transport between itself and Oracle Communications Session Delivery Manager. After the Oracle Communications Session Delivery Manager receives the 200OK, the chosen flow is installed, and the unused socket is discarded.

For two realms from different address families to share the same physical interface and vlan, you use a .4 or .6 tag in the network-interface reference. See *Net-Net SCx6.4.0 M-Release Guide* for more information.

SDP Alternate Connectivity Configuration

1. Expand the Configuration Manager slider > Services.
2. Click Realms.
3. Select an existing Realm and click Edit or click Add to create a new one.
4. Alternate family realm— Select the alternate realm, from which to use an IP address in the other address family.
5. Preferred address type— Set the order in which the a=altc: lines suggest preference. Valid values are:
   - NONE — address family type of egress realm signaling
   - IP4 — IPv4 realm/address first
   - IP6 — IPv6 realm/address first
6. Click Apply.

Authenticated NTP

The Oracle Communications Session Delivery Manager can authenticate NTP server requests using MD5. The configured MD5 keys are encrypted and obscured in the ACLI. You configure an authenticated NTP server with its IP address, authentication key, and the key ID. Corresponding key and key IDs are provided by the NTP server administrator.

dfd **Configuration Manager slider** > **Global settings** > **Management**.

Authenticated NTP Configuration

1. Expand the **Configuration Manager slider** > **Global settings** > **Management**.
2. Click NTP.
3. Click Add if there is no existing NTP configuration.
4. IP address— Enter the IP address of the NTP server that supports authentication.
5. Key identifier— Enter the key ID of the key you enter in the next step. This value's range is 1 - 999999999.

6. Key—Enter the key used to secure the NTP requests. The key is a string 1 - 31 characters in length.

   You must re-enter the key to confirm. You must also enter and confirm your configuration password.
7. Click Edit.

5

Net-Net Central 7.3M4 Features and Model Support

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net Central Release 7.3M4.

Content Map for 7.3M4

This table provides a listing of all new content in Net-Net Central Release 7.3M4:

Content Type	Description
Net-Net Central Feature	GUI Improvements to Multi-Instance Elements
Net-Net Central Feature	Software Licensing
Net-Net Central Feature	SOAP/XML Updates
Net-Net Central Feature	Security Banner Enhancements
Net-Net Central Feature	Diameter Director Support for Route Manager
Net-Net Central Feature	Oracle Linux VM Offering
Net-Net Central Feature	Audit Log Enhancements
Net-Net Central Feature	Automatic XSD Loading
Net-Net Central Feature	Fault E-Mail Severity Settings
Net-Net Central Feature	Northbound Fault Management
Model Support	IMS-AKA Change Client Port
Model Support	Upstream Congestion Control
Model Support	Diameter Director Agent
Model Support	Diameter Director Group
Model Support	Diameter Director Interface
Model Support	Remote Site Survivability

Net-Net Central Features

This section provides features new to the Net-Net Central Release.

GUI Improvements to Multi-Instance Element Tables

Affects top-level multi-instance elements tables in ACLI and List view only.

Table Column Size

- Column width state is remembered throughout the session.
- The Session agent table has pre-defined column widths.

Optional Columns

Checking the Retrieve all attributes check box allows the system to collect all attributes other than non-required sub-element attributes and make them available alphabetically in the optional table columns.

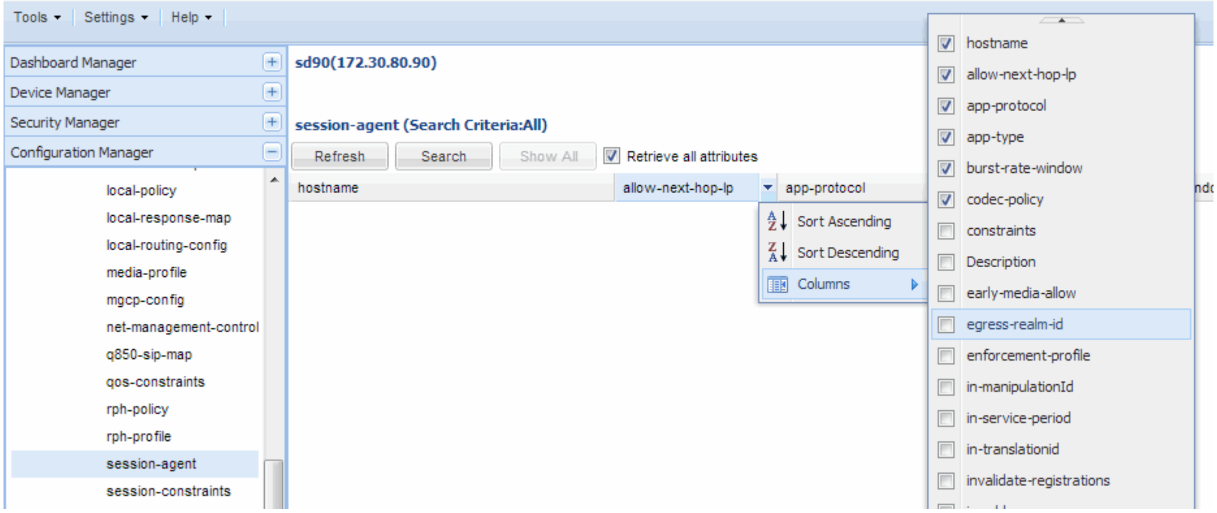
Paging Tool Bar

The state of the table paging is remembered throughout the session. Tables reset to the first page upon resizing the window.

Enabling Optional Columns

To enable the optional columns for multi-instance element tables:

1. Select the check box next to Retrieve all attributes to collect additional instance attributes and make them available as optional columns.



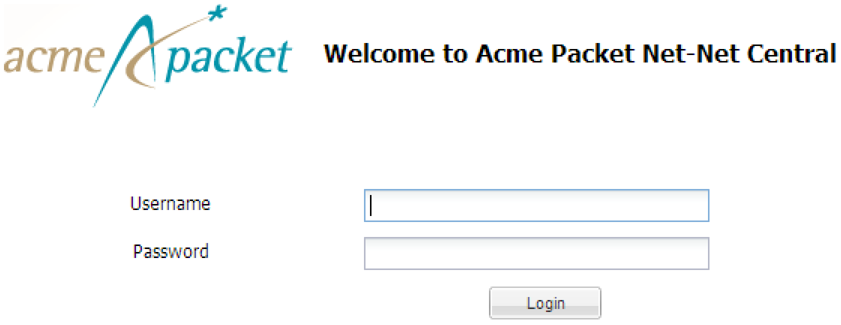
2. Select the drop-down arrow next to the column headers and navigate to Columns.
3. Select the check-boxes corresponding to the attributes you wish to display as additional columns in the table.

Software Licensing

As of NNC 7.3m4 there is no longer be a need to apply a license to enable functionality. The requirement of adding a license in the setup of the application is no longer required. When the user logs into NNC 7.3m4 all application sliders are visible and functional. Please refer to your license agreement with ORACLE on which application you are licensed to use.

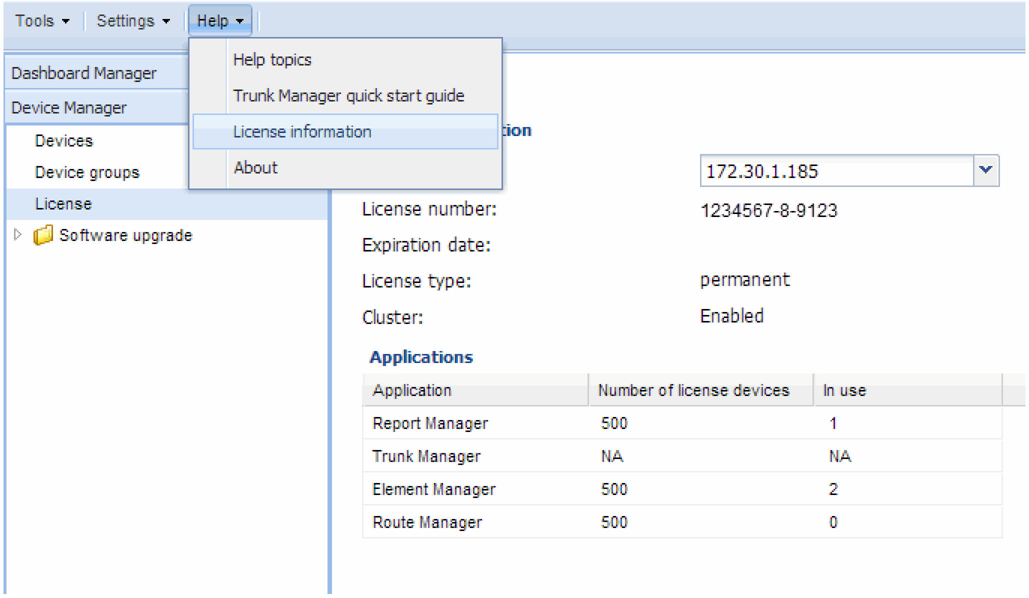
The following license dialogs have been removed from Net-Net Central as a result to the license requirements:

- License contract message on the login screen:



Welcome to Acme Packet Net-Net Central

- License information from the Help menu:



172.30.1.185

License number: 1234567-8-9123

Expiration date:

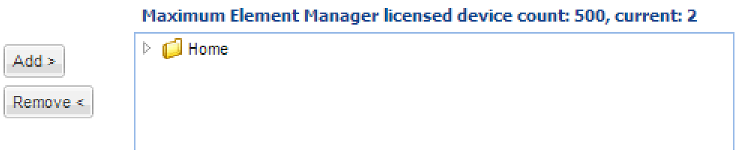
License type: permanent

Cluster: Enabled

Applications

Application	Number of license devices	In use
Report Manager	500	1
Trunk Manager	NA	NA
Element Manager	500	2
Route Manager	500	0

- Maximum device constraint for Configuration Manager, Route Manager, and Collection groups:



Maximum Element Manager licensed device count: 500, current: 2

SOAP/XML API Updates

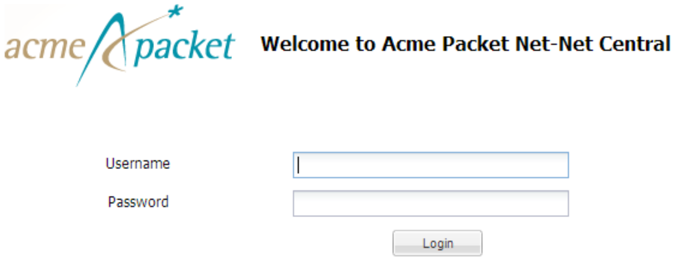
The following SOAP/XML API will be depreciated in the next major release:

API	Description
addDeviceToEMLicense	Adds a device to the Element Manager license.
removeDeviceFromEMLicense	Removes a device from the Element Manager license.
getAllAssociatedDevicesInEMLicense	Returns a list of all associated devices for the Element Manager.

Security Banner Enhancement

The following changes have been made to the Net-Net Central login screen:

- Configurable warning that prompts the user to agree to compliance rules
- Pop-up for custom Terms and Conditions
- Custom warning if compliance box isn't checked

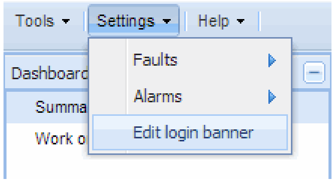


When the Administrator enables the Terms and Conditions review, a hyperlink appears next to the compliance check-box. You need Administrator or LIAdministrator permissions to edit the security banner login page.

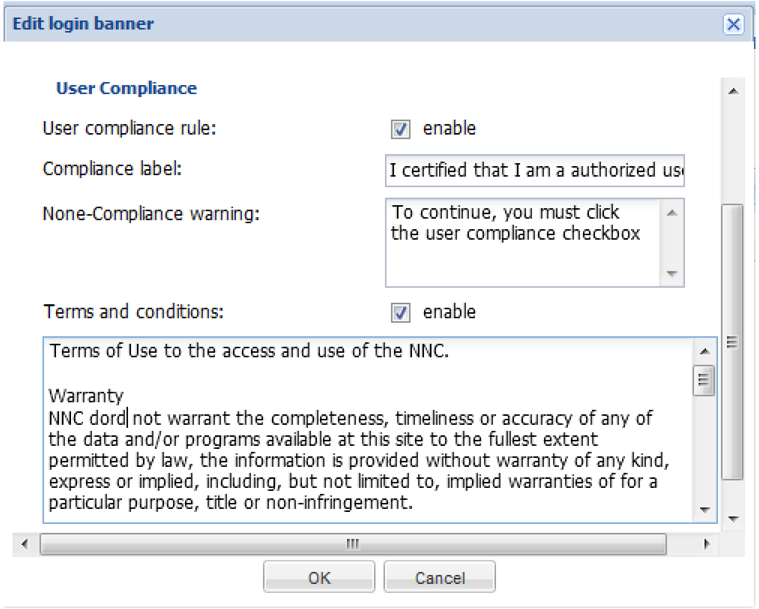
Security Banner Enhancement Configuration

The steps below allow you to enable and configure a compliance check that will appear on the login screen when a user attempts to login.

1. Click the Settings drop-down menu and select Edit login banner.



The Edit login banner dialog appears.



Edit login banner

User Compliance

User compliance rule: ☑ enable

Compliance label: I certified that I am a authorized us

None-Compliance warning: To continue, you must click the user compliance checkbox

Terms and conditions: ☑ enable

Terms of Use to the access and use of the NNC.

Warranty
NNC dord not warrant the completeness, timeliness or accuracy of any of the data and/or programs available at this site to the fullest extent permitted by law, the information is provided without warranty of any kind, express or implied, including, but not limited to, implied warranties of for a particular purpose, title or non-infringement.

2. User compliance rule—set the state of this element to enabled.
    - enabled | disabled
3. Compliance label—Enter the display text for the compliance check-box.

4. None-Compliance warning—Enter the display text for the message a user gets when attempting to login without accepting the terms and conditions.
5. Terms and conditions—Enter the display text for the Terms and conditions dialog.
6. Click OK to submit your changes.

Setting Permissions for the Security Banner

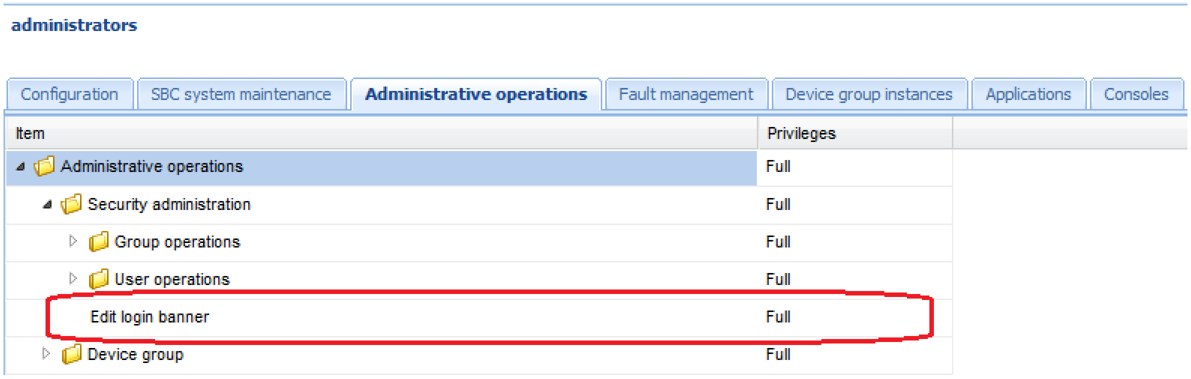
By default, the permission to modify the login banner is set to full for default administration groups. Only user groups created from the default Admin or LIAdmin user groups will have the privileges to configure the login banner. If a new administrator group requires access to the security banner configuration, you must navigate to the Security Manager and set this permission.

To set permissions for login security banner:

1. Expand the Security Manager slider and navigate to Groups.
2. Select a group and click Edit.

   Note: Default user groups cannot be modified.

   The Edit group dialog appears.
3. Click the Administrative operations tab.
4. Expand Administrative operations > Security administration.



Item	Privileges
Administrative operations	Full
Security administration	Full
Group operations	Full
User operations	Full
Edit login banner	Full
Device group	Full

5. Click the Edit login banner operation row in the table under Privilege.
   The drop-down list is activated.
6. Choose the appropriate privilege type.
7. Press <Enter> to accept the selected type.
8. Click Apply.

Diameter Director Support for Route Manager

Net-Net Route Manager supports the configuration and management of Diameter Director devices.

Please see the *Net-Net Central 7.3 Route Manager Guide* for configuration instructions and more information.

Oracle Linux VM

This section contains information about obtaining, installing, and configuring a guest operating system that is required for using Net-Net Central in a virtual environment.

You can install Net-Net Central as part of a virtual machine (VM) if you want to use a virtual environment for your deployment. You can obtain the OVM template from the Acme Packet customer portal site.

You can set up the Net-Net Central VM using Oracle Virtual Machine Manager. OVM transforms your system's hardware resources -including the CPU, RAM, hard disk and network controller- to create a fully functional virtual environment.

Before You Start

Review the following information before proceeding to the instructions. You need to set up your host operating system and install OVM, as well as have the necessary information ready for configuration.

About the OVM Template

The template installs Oracle Linux 6.2 and proceeds to upgrade to 6.4 before Net-Net Central installation. The OVM template includes the following components:

- NNC_OL62_OVM.tar.gz

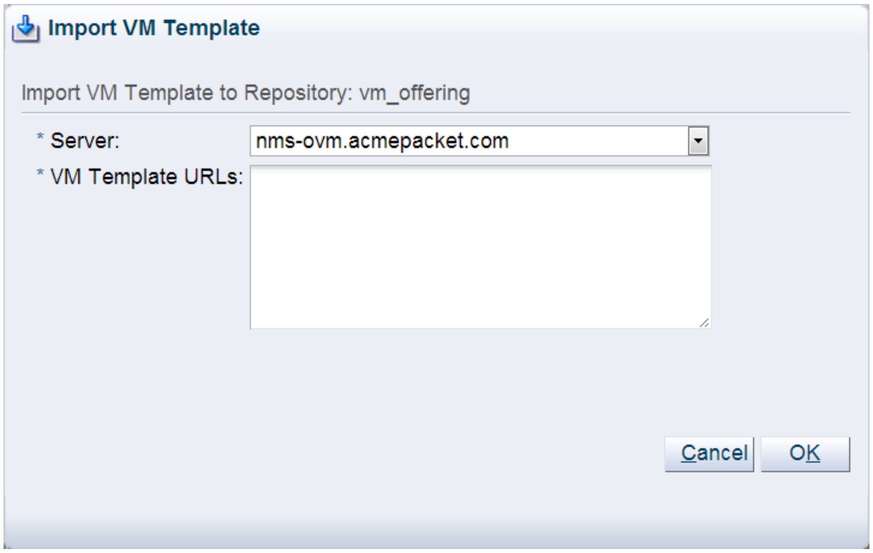
Memory Usage

Do not provision more virtual memory than you have available in physical memory.

Deploying the OVM Template

To deploy an OVM template on Oracle VM Manager:

1. Log into the Oracle VM Manager.
2. Click the Repositories tab.
3. Select the repository you wish to import the template to and click Import VM Template.
   The Import VM Template dialog appears.



Import VM Template

Import VM Template to Repository: vm_offering

* Server: nms-ovm.acmepacket.com

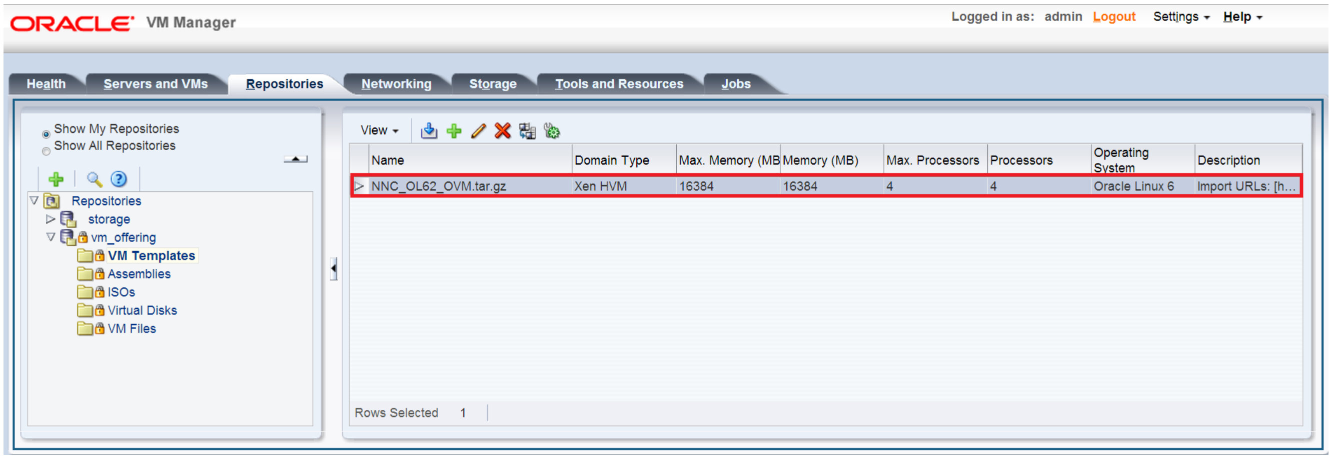
* VM Template URLs:

4. Select an OVM server from the drop down list.
5. Enter the VM template's URLs.

   Note: URLs should point to an HTTP or FTP server hosting the OVM template.

6. Click OK to submit the Import VM template request.

Upon completion, the OVM template appears under <Repository_Name>/VM Templates.



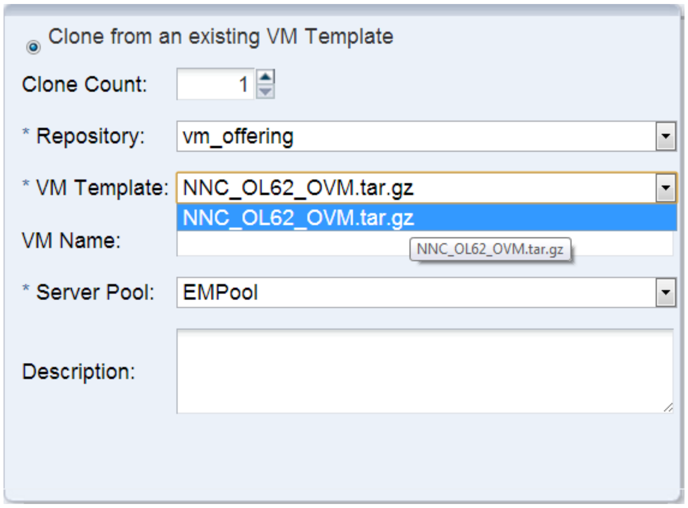
Name	Domain Type	Max. Memory (MB	Memory (MB)	Max. Processors	Processors	Operating System	Description
NNC_OL62_OVM.tar.gz	Xen HVM	16384	16384	4	4	Oracle Linux 6	Import URLs: [h...

Rows Selected 1

Creating a Guest VM

To create a guest VM from the OVM template:

1. Click the Servers and VMs tab.
2. Click Create Virtual Machine.
   The Create Virtual Machine dialog appears.



● Clone from an existing VM Template

Clone Count: 1

* Repository: vm_offering

* VM Template: NNC_OL62_OVM.tar.gz

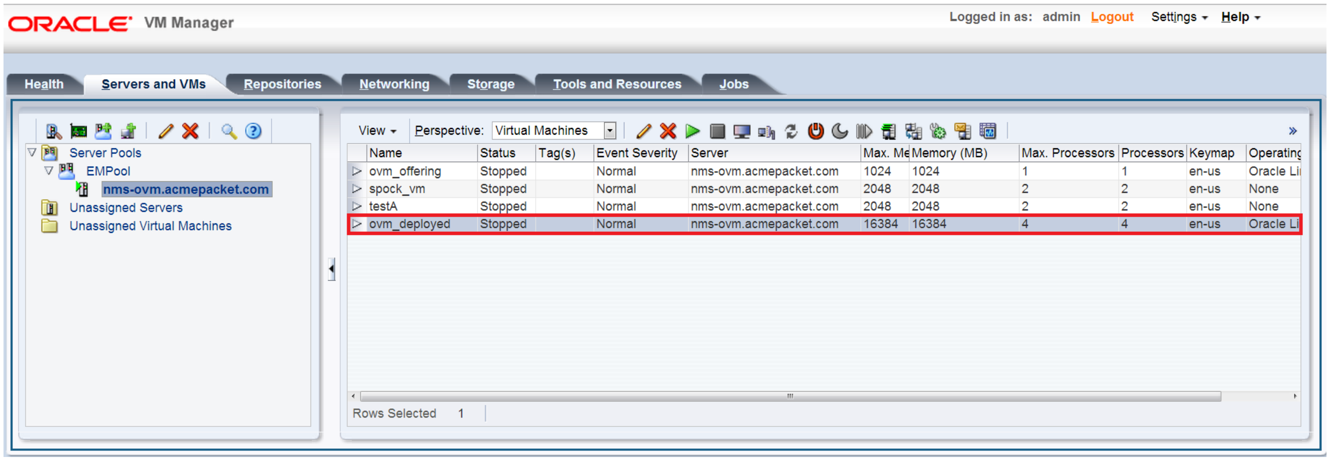
VM Name:

* Server Pool: EMPool

Description:

3. Select Clone from an existing VM template.
4. Clone Count—Select the number of desired VMs to create using the up and down arrows.
5. Repository—Select the repository holding the OVM template from the drop-down menu.
6. VM Template—Select the imported OVM template from the drop-down menu.
7. VM Name—Enter a name for the VM you are creating.
8. Server Pool—Select a server pool from the drop-down menu.
9. Description—Enter an optional description of the VM you are creating.
10. Click Finish to create the VM.

The VM is listed on the OVM Server if successfully provisioned.



Name	Status	Tag(s)	Event Severity	Server	Max. Me	Memory (MB)	Max. Processors	Processors	Keymap	Operating
ovm_offering	Stopped		Normal	nms-ovm.acmepacket.com	1024	1024	1	1	en-us	Oracle Li
spock_vm	Stopped		Normal	nms-ovm.acmepacket.com	2048	2048	2	2	en-us	None
testA	Stopped		Normal	nms-ovm.acmepacket.com	2048	2048	2	2	en-us	None
ovm_deployed	Stopped		Normal	nms-ovm.acmepacket.com	16384	16384	4	4	en-us	Oracle Li

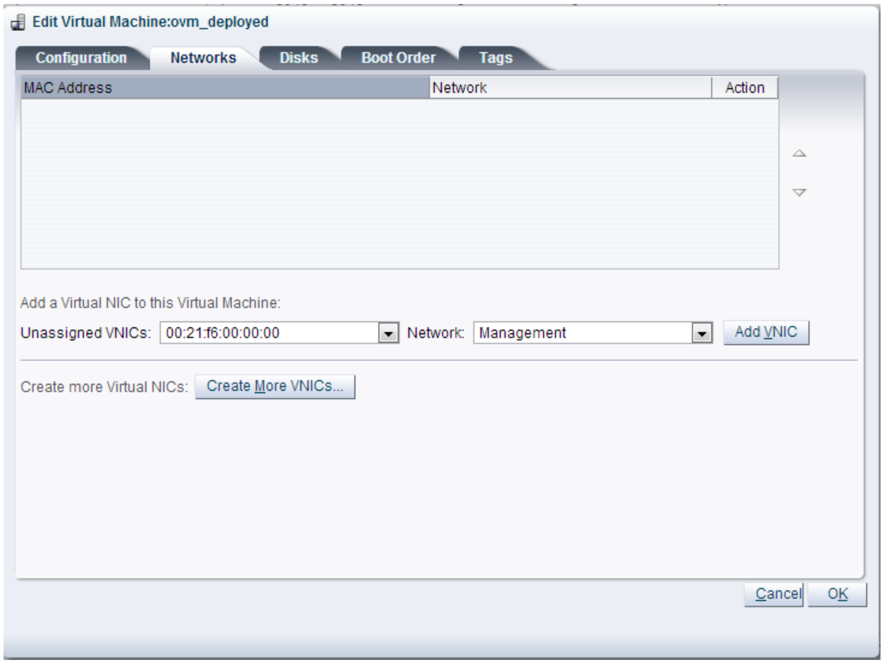
Rows Selected 1

Adding VNICs to the VM

To add VNICs to your guest VMs:

You must have pre-configured VNICs on the server before you can assign them to the Net-Net Central VM. Please consult the documentation for the OVM Manager for information on setting up VNICs on your Network.

1. Select the VM image from the OVM Server table and click the Edit button.
   The Edit Virtual Machine dialog appears.
2. Select the Networks tab.



Add a Virtual NIC to this Virtual Machine:

Unassigned VNICs: 00:21:f6:00:00:00 Network: Management Add VNIC

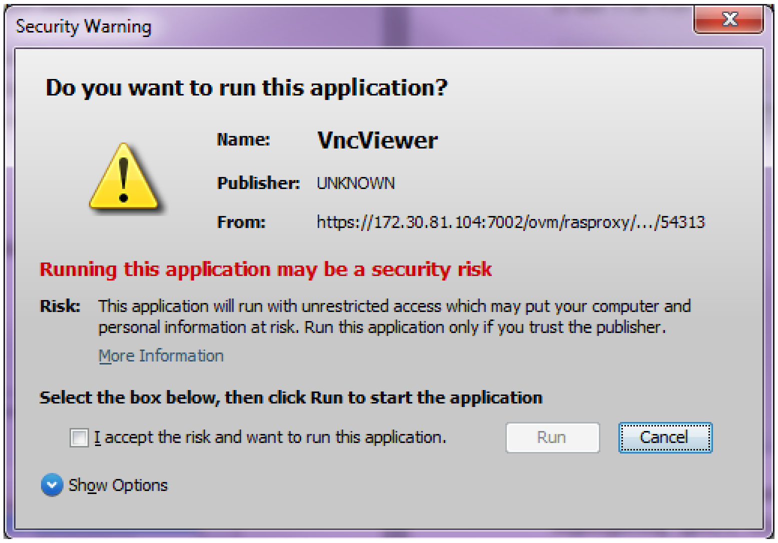
Create more Virtual NICs: Create More VNICs...

3. Unassigned VNICs—Select any VNIC from the drop down list.
4. Network—Select the a network for the VNIC from the drop-down menu.
5. Click Add VNIC to submit the VNIC configuration.
   Repeat steps 3-5 to add any remaining unassigned VNICs.
6. Click OK to close the Edit Virtual Machine dialog and submit your changes.

Launching and Accessing the VM

To launch and access the VM:

1. Select the VM image from the OVM Server table and click the Play button.
2. Click the Start Monitor button to launch VNC Viewer.
3. Click Keep to download the ovm_rasproxy-ws.jnlp file.
4. Run the ovm_rasproxy-ws.jnlp file.
   The following warning may appear. Click the checkbox to accept and click Run.



Security Warning

Do you want to run this application?

Name: VncViewer

Publisher: UNKNOWN

From: https://172.30.81.104:7002/ovm/rasproxy/.../54313

Running this application may be a security risk

Risk: This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the publisher.

More Information

Select the box below, then click Run to start the application

☐ I accept the risk and want to run this application.

Configuring the VM with Sysprep

The sysprep utility guides you through the configuration process for your VM NNC image. If this is your first time installing Net-Net Central, you will want to exercise all options in the sysprep utility to fully configure the VM.

1. Log in with the username 'root' and the password 'root123'.

```
localhost login: root
Password: root123

---------------------------------------------------
This system is a virtual appliance which has been
prepared by Acme Packet to run Net-Net Central.

Operating system: Oracle Linux 6.2
Acme Packet version: 1.0
---------------------------------------------------
===================================================
First time 'root' login detected.
Running /usr/acme/sysprep.sh

Acme Packet Sysprep will walk you through several
steps needed to configure this system for use as
a Net-Net Central server.
===================================================
```

2. Enter Y to continue and press <Enter> to launch the sysprep utility.
   Run Acme Packet sysprep utility? (y/n) y

Changing the root Account Password

For security purposes, you need to change the root account password immediately.

1. Press <Enter> to accept the default value of 1 to change the root account password.

```
[X] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit

Please select an option [1] 1
```

2. Enter Y and press <Enter> to continue.

```
Change password for account 'root'
Do you wish to continue? (y/n) y
```

3. Enter the new password for the account root and press <Enter>. You are prompted to confirm the password.

```
New password:
```

4. Enter the password again and press <Enter>. The confirmation message appears.
5. Press <Enter> to continue.

Changing the nncentral Account Password

For security purposes, you need to change the nncentral account password immediately.

1. Press <Enter> to accept hte default value of 2 to change the nncentral account password. You are prompted about continuing.

```
[ ] 1. Change root password
[X] 2. Change nncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit

Please select an option [1] 2
```

2. Enter Y and press <Enter> to continue. The Change Password prompt appears.

```
Change password for account 'nncentral'
Do you wish to continue? (y/n) y
```

3. Enter the new password for the account nncentral and press <Enter>. You are prompted to confirm the password.

```
New password:
```

4. Enter the password again and press <Enter>. The confirmation message appears.
5. Press <Enter> to continue.

Configuring Networking

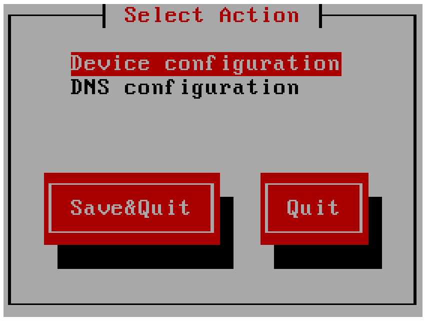
You can configure the ethernet interfaces to use the IP addresses of your network with the following steps.

1. Press <Enter> to accept the default value of 3 to configure networking.

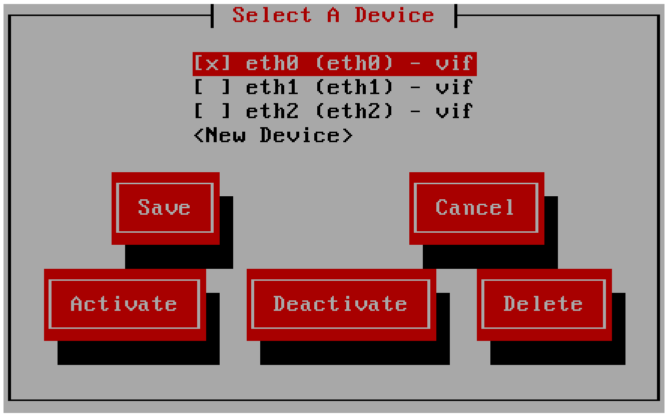
```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[X] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit

Please select an option [3] 3
```

2. Enter Y and press <Enter> to continue.
   The Network utility appears.



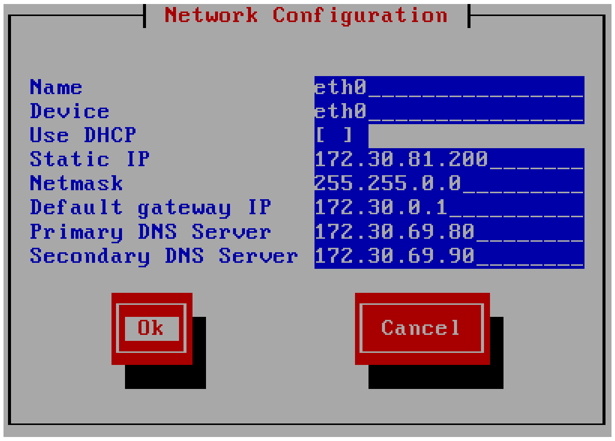
3. Select Device configuration and press <Enter>.
   The device selection dialog appears.



```
[x] eth0 (eth0) - vif
[ ] eth1 (eth1) - vif
[ ] eth2 (eth2) - vif
```

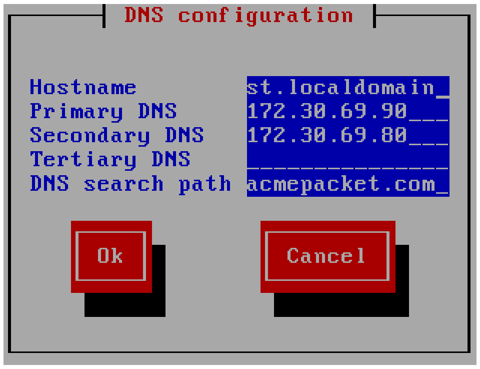
4. Select eth0 and press <Enter>
5. Set the network configuration parameters by using the up and down arrows to reach individual values. Press <Enter> with Ok selected once you are finished.

Note: Acme Packet recommends that users set up eth0 with a static IP address. DHCP is not recommended on eth0.



```
Name                  eth0________________
Device                eth0________________
Use DHCP              [ ]
Static IP             172.30.81.200_______
Netmask               255.255.0.0_________
Default gateway IP    172.30.0.1__________
Primary DNS Server    172.30.69.80________
Secondary DNS Server  172.30.69.90________
```

6. Select Save and press <Enter>.
7. Select DNS configuration and press <Enter>.
8. Set the DNS configuration parameters by using the up and down arrows to reach individual values. Press <Enter> with Ok selected when you are finished.



DNS configuration

```
Hostname          st.localdomain_
Primary DNS       172.30.69.90___
Secondary DNS     172.30.69.80___
Tertiary DNS      _______________
DNS search path   acmepacket.com_
```

9. Select Save & Quit and press <Enter>.

Configuring the Timezone

You need to select the timezone that the VM is operating in.

1. Press <Enter> to accept the default value of 4 to configure the timezone. You are prompted about continuing.

```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[X] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit

Please select an option [4] 4
```

2. Enter Y and press <Enter> to continue.
   The configure timezone utility appears.

3. Enter the corresponding number of the continent or ocean the system is located and press <Enter>.

```
Please select a continent or ocean.
1) Africa                  4) Arctic Ocean         7) Australia
10) Pacific Ocean
2) Americas          5) Asia                                        8)
Europe
3) Antarctica 6) Atlantic Ocean 9) Indian Ocean
```

4. Enter the corresponding number of the country the system is located and press <Enter>.

5. Enter the corresponding number of the time zone region the system is located and press <Enter>.

6. Enter 1 to confirm the selected timezone and press <Enter> to continue.

```
Therefore TZ='America/New_York' will be used.
Local time is now: Tue Nov 20 12:35:36 EST 2012.
Universal Time is now: Tue Nov 20 17:35:36 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
```

Configuring the Network Time Protocol

1. Press <Enter> to accept the default value of 5 to configure optional services.

```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[X] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit
```

```

Please select an option [5] 5
```

2. Enter Y and press <Enter> to continue.
3. Enter Y and press <Enter> to enable the Network Time Protocol. A list of currently defined NTP servers appears.

```
Enabling Network Time Protocol is recommended
Enable Network Time Protocol (NTP)? (y/n) y
```

4. Enter Y and press <Enter> to include the selected NTP server or N to remove it from the NTP configuration.

```
3 NTP servers are currently defined in /etc/ntp.conf
Use NTP server '0.centos.pool.ntp.org'? (y/n) n
Use NTP server '1.centos.pool.ntp.org'? (y/n) n
Use NTP server '2.centos.pool.ntp.org'? (y/n) n
```

5. Enter Y and press <Enter> to add an additional NTP server. Otherwise, enter N and press <Enter> to continue without adding a new server.

```
Add additional NTP servers
Add NTP server (y/n)
```

6. Enter the IP address or DNS name for the additional NTP server and press <Enter>. The Add additional NTP Servers dialog appears again so you can continue adding other values.

```
Enter IP address or DNS name for NTP server: 192.168.1.101
Added NTP server '192.168.1.101' to /etc/ntp.conf
```

7. Enter N and press <Enter> when you are finished adding NTP servers to your configuration.

```
Add NTP server? (y/n) n
Starting ntpd service...
```

8. Press <Enter> to continue.

Configuring Optional Services

You must configue optional services if you wish to enable telnet and ftp.

1. Press <Enter> to accept the default value of 6 to configure optional services.

```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[X] 6. Configure optional services
[ ] 7. Exit

Please select an option [5] 5
```

2. Enter Y and press <Enter> to continue. The configure optional services prompt appears.
3. Enter Y and press <Enter> to enable telnet. Otherwise, enter N and press <Enter> to continue with telnet disabled.

```
Would you like to enable telnet? (y/n)
Enabling telnet...
```

4. Enter Y and press <Enter> to enable FTP. Otherwise, enter Y and press <Enter> to continue with FTP disabled.

```
Would you like to enable ftp?
Enabling ftp...
Updating selinux ftp policy...
```

5. Press <Enter> to continue.

Exiting Sysprep

To exit the sysprep configuration:

1. Press <Enter> to accept the default value of 6 to configure optional services.

```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[X] 7. Exit

Please select an option [7] 7
```

2. Enter Y and press <Enter> to complete the sysprep configuration and reboot the system.

   Note: Rebooting is required to apply configuration changes.

Installing Net-Net Central

You are now able to install Net-Net Central using the typical or custom installation process. Refer to the *Net-Net Central 7.3 Installation Guide* for more information.

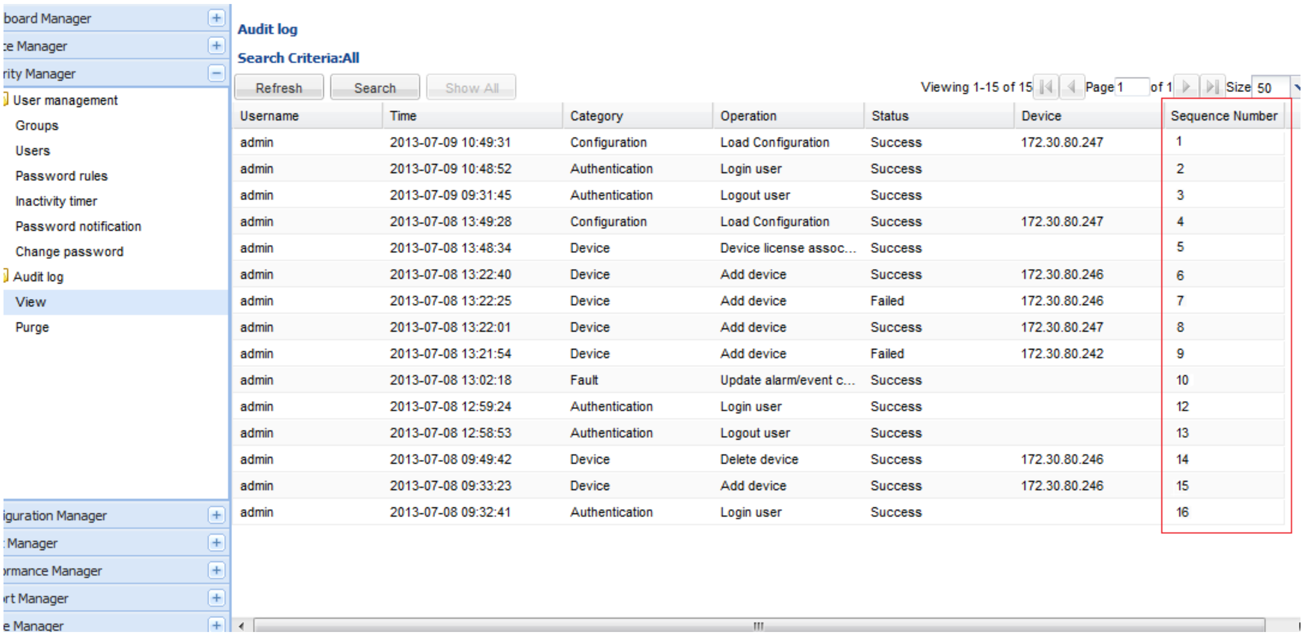
Note: The step to apply a license in the Net-Net Central 7.3 Installation guide is no longer needed to set up Net-Net Central 7.3M4 and above.

Audit Log Improvements

The Audit log now has the ability to sequentially number logs per device and display configuration changes in a comma separated list.

Sequential Numbers

Sequential numbers are generated for device-specific audit logs with a number. Each log entry generates a new sequential number ranging from 1-2^64 to display in the Audit log table. Numbers are not unique across clusters and cannot be referenced between different machines. You must enable the hidden Sequential number column to view it in the Audit Log table.



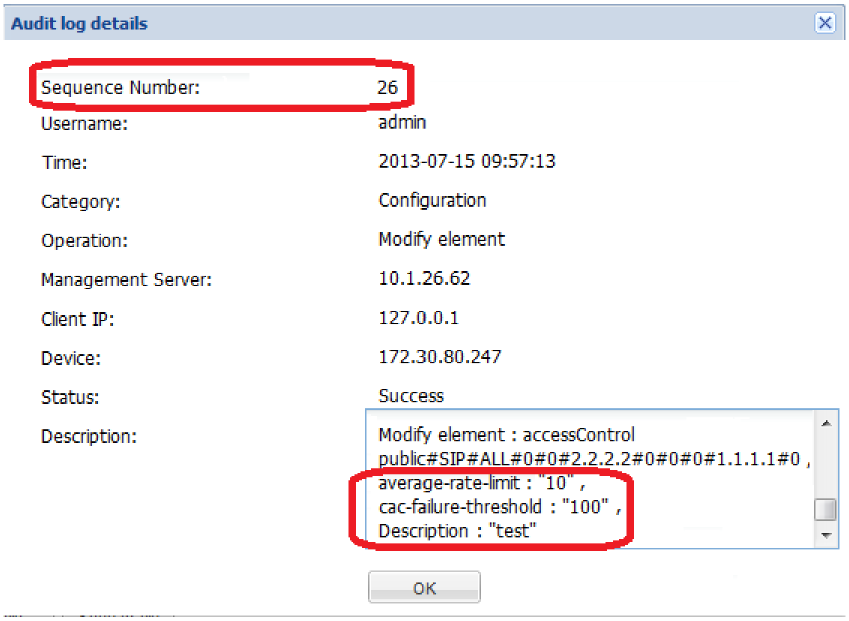
Audit log

Search Criteria:All

Username	Time	Category	Operation	Status	Device	Sequence Number
admin	2013-07-09 10:49:31	Configuration	Load Configuration	Success	172.30.80.247	1
admin	2013-07-09 10:48:52	Authentication	Login user	Success		2
admin	2013-07-09 09:31:45	Authentication	Logout user	Success		3
admin	2013-07-08 13:49:28	Configuration	Load Configuration	Success	172.30.80.247	4
admin	2013-07-08 13:48:34	Device	Device license assoc...	Success		5
admin	2013-07-08 13:22:40	Device	Add device	Success	172.30.80.246	6
admin	2013-07-08 13:22:25	Device	Add device	Failed	172.30.80.246	7
admin	2013-07-08 13:22:01	Device	Add device	Success	172.30.80.247	8
admin	2013-07-08 13:21:54	Device	Add device	Failed	172.30.80.242	9
admin	2013-07-08 13:02:18	Fault	Update alarm/event c...	Success		10
admin	2013-07-08 12:59:24	Authentication	Login user	Success		12
admin	2013-07-08 12:58:53	Authentication	Logout user	Success		13
admin	2013-07-08 09:49:42	Device	Delete device	Success	172.30.80.246	14
admin	2013-07-08 09:33:23	Device	Add device	Success	172.30.80.246	15
admin	2013-07-08 09:32:41	Authentication	Login user	Success		16

Configuration Changes

When a top-level element or sub-element is edited, the modified attributes are displayed alphabetically in the description field of the Audit log details with their new values.



Sequence Number: 26
Username: admin
Time: 2013-07-15 09:57:13
Category: Configuration
Operation: Modify element
Management Server: 10.1.26.62
Client IP: 127.0.0.1
Device: 172.30.80.247
Status: Success
Description: Modify element : accessControl public#SIP#ALL#0#0#2.2.2.2#0#0#0#1.1.1.1#0 , average-rate-limit : "10" , cac-failure-threshold : "100" , Description : "test"

Automatic XSD Loading

Net-Net Central automatically attempts to load the XSD of a C-Series device in the event the release was not provided with your version of Net-Net Central. New configuration elements can be configured from the List and ACLI view in the even that your SBC version is not supported a Net-Net Central release.

The XSD will be loaded during the following procedures:

- Adding a Device
- Loading a Configuration
- Updating SBC Software (via the NNC GUI)

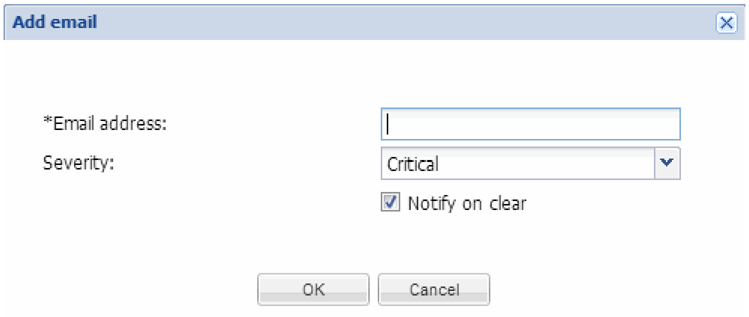
Fault Email Severity Settings

The Clear event is no longer available from the Severity settings drop down list. You can set the Notify on clear option, in addition to Severity, when adding or editing a fault email recipients. You can check the status of Notify on clear for existing recipients via the column on the Fault email recipients table.

Enabling Notify on Clear

To enable an email notification on all clear events:

1. Click Settings in the top tool bar. A drop-down menu appears.
2. Click Fault email notifications.
   The Fault email recipients dialog box appears.



*Email address:
Severity: Critical
☑ Notify on clear

3. Click Add. The Add email dialog box appears.

   Note: The Notify on clear option does not appear until you select a Severity. Not all severities offer clear events.

4. Email address—Enter the recipient's email address you want to attach to the alarm severity.
5. Severity—Click the severity from the drop-down list that you want to set for this email notification.
6. Notify on clear—Select the check-box to enable email notification of clear events .
7. Click OK.

Northbound Fault Management

Net-Net Central Northbound Fault Management allows you to configure destination receivers to receive forwarded traps in either Net-Net Central or ITU X.733 standard formats. You can specify selected traps on devices using the ITU X.733 format in the Add/Edit trap receiver dialog. A maximum of 10 trap receivers may be configured at once, regardless of format.

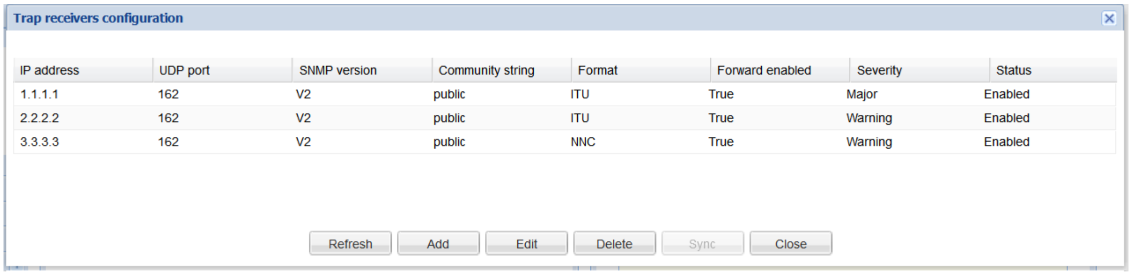
High Availability

When running Net-Net Central within a clustered environment, northbound alarm notifications can be sent from any of the nodes in the cluster. All nodes/hosts must be specified as potential northbound alarm originators if the third-party destination requires configuring alarm originator IP addresses in an acceptance list.

All members of the cluster must share the same global identifier.

Trap Receiver Table

The trap receiver table shown below illustrates an example of configured trap receivers. the users have the ability to add/edit/delete trap receivers, as well as manually launch a process that re-synchronizes alarms for selected devices. Each operation is explained in the following sections.



IP address	UDP port	SNMP version	Community string	Format	Forward enabled	Severity	Status
1.1.1.1	162	V2	public	ITU	True	Major	Enabled
2.2.2.2	162	V2	public	ITU	True	Warning	Enabled
3.3.3.3	162	V2	public	NNC	True	Warning	Enabled

Trap Receiver Alarm Synchronization

The synchronization filter allows you to specify a window of time to synchronize alarms across devices. The Date and time from fields default to the current date and time. The Date and time to fields default to 24 hours earlier.

When enabled, the synchronization filter re-sends previous traps nortbound, depending on the time window set by the user. It is up to the user to differentiate between which traps are new and which are duplicates.

Global Identifiers

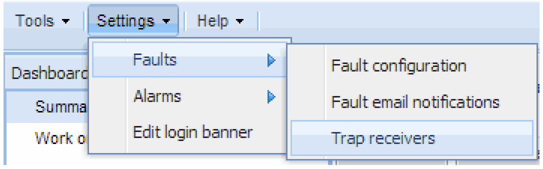
You must configure a global identifier for standalone or clustered Net-Net Central servers to satisfy the northbound managed object instance value. The global identifier configuration can be found in the Net-Net Central typical and custom installation procedures.

Note: The global identifier must be the same for all nodes in a clustered system.

Accessing Northbound Fault Management Configuration

To access Northbound Fault Management configuration:

Click Settings > Faults > Trap receivers.

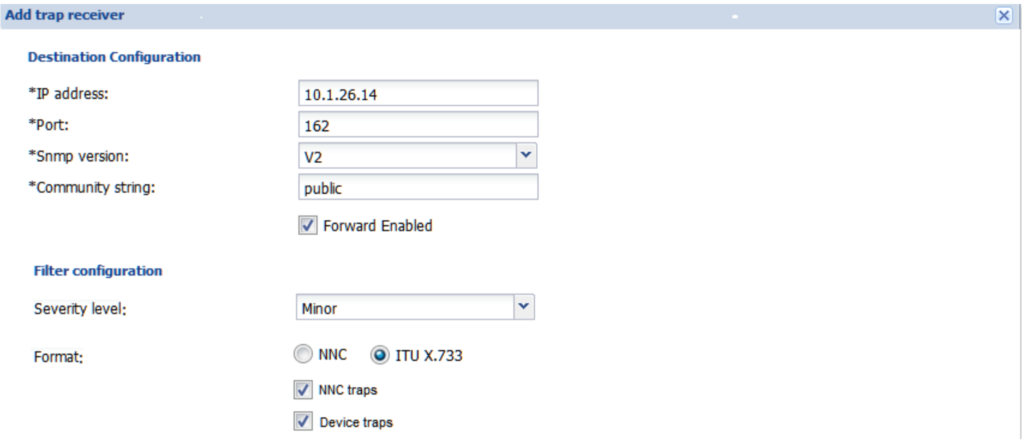


The Trap receiver table appears in the content area.

Add/Edit Trap Receivers

To add or edit a trap receiver from the Trap receiver table:

1. Click Add to configure a new trap receiver or Edit to modify an existing one.
   The Add/Edit trap receiver dialog appears.



Add trap receiver

Destination Configuration

*IP address: 10.1.26.14

*Port: 162

*Snmp version: V2

*Community string: public

☑ Forward Enabled

Filter configuration

Severity level: Minor

Format: ○ NNC ● ITU X.733

☑ NNC traps

☑ Device traps

2. IP address—Enter the IP address of the trap receiver.
3. Port—Enter the port number of the trap receiver.
4. SNMP version—Select V2 from the drop-down menu.
5. Community String—SNMP community name of the trap receiver.
6. Forward Enabled—Check this box to enable trap forwarding to the receiver.
7. Severity Level—Forwards alarms of equal or higher severity than selected.
8. Format—Select the format for forwarded traps.
   - NNC—Forwards backwards-compatible Net-Net Central formatted traps.
   - ITU X.733—Forwards ITU X.733 formatted traps.
9. NNC traps—Check this box to forward all traps generated by the Net-Net Central server.

   Note: When selected, this option only forwards NNC traps. The check box for devices is disabled.

10. Device traps—Check this box to forward all traps from managed devices.

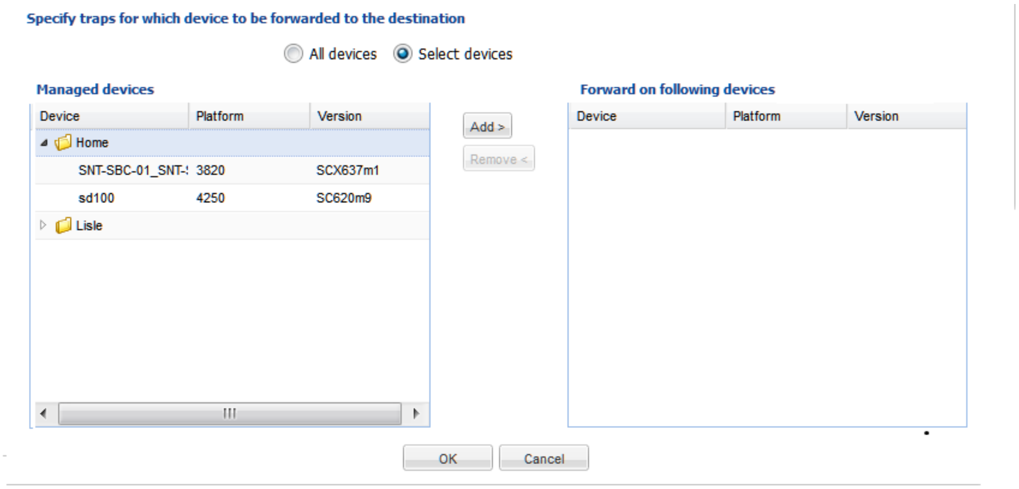
    Note: This option is only available for ITU X.733 format.

11. Click OK if you are configuring a device using the Net-Net Central format or do not wish to filter ITU X.733 device trap forwarding. Otherwise, continue to the filter configuration steps.

Optional Filter configuration

12. Click the radio button for Select devices from the Add/Edit trap receiver dialog.

    Note: Filter configuration is only enabled for the ITU X.733 format.



Specify traps for which device to be forwarded to the destination

○ All devices ● Select devices

Managed devices

Device	Platform	Version
Home		
SNT-SBC-01_SNT-!	3820	SCX637m1
sd100	4250	SC620m9
Lisle		

Forward on following devices

Device	Platform	Version

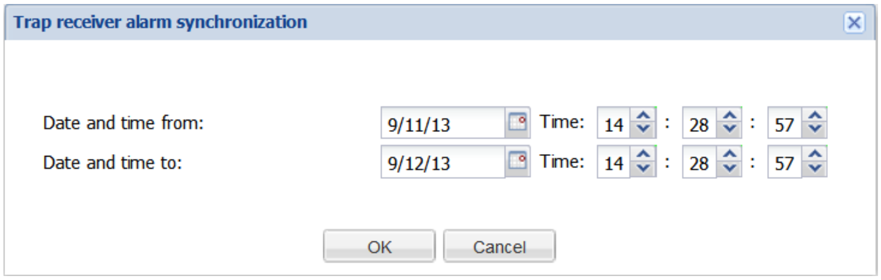
The filter dialog becomes available.

13. Expand the device group folders and select the device(s) you want to forward from the Managed devices table.
14. Click Add to move the selected device(s) to the Forward on following devices table.
15. Click OK to finish.

Synchronizing Trap Receiver Alarms

To sync trap receiver alarms:

1. Click Sync from the Trap receiver table.
   The Trap receiver synchronization dialog appears.

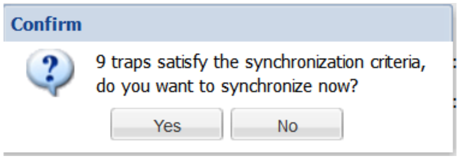


Trap receiver alarm synchronization

Date and time from: 9/11/13 Time: 14 : 28 : 57

Date and time to: 9/12/13 Time: 14 : 28 : 57

2. Select a date from value using the calendar dialog.
3. Set a time from value using the arrows.
4. Select a date to value using the calendar dialog.
5. Set a time to value using the arrows.
6. Click OK to submit the sync.
   A confirmation dialog appears with the number of traps to be synchronized.



Confirm

9 traps satisfy the synchronization criteria, do you want to synchronize now?

7. Click Yes to confirm.

Global Identifier Configuration During Installation

To configure global identifiers from the typical and custom installation procedures:

1. Enter the number corresponding to Net-Net Central global identifier configuration and press <Enter>

```
[X]  1 - Net-Net Central global identifier configuration
```

```
[ ]   2 - HTTP/HTTPS configuration
[ ]   3 - Fault Management configuration
[ ]   4 - Quit setup

Please select an option [1] 1
```

2. Enter Y and press <Enter> to continue.
3. Enter a global unique identifier for the system.

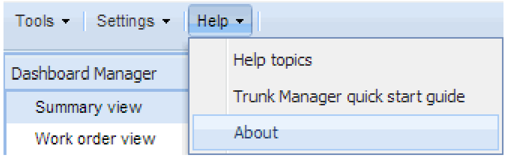
```
Global identifier
Enter global identifier: [Acme NNC]
```

4. Press <Enter> to submit and continue with the installation procedure.

Displaying the Global Identifier in NNC

To display the global identifier in the about information:

1. Select Help > About.

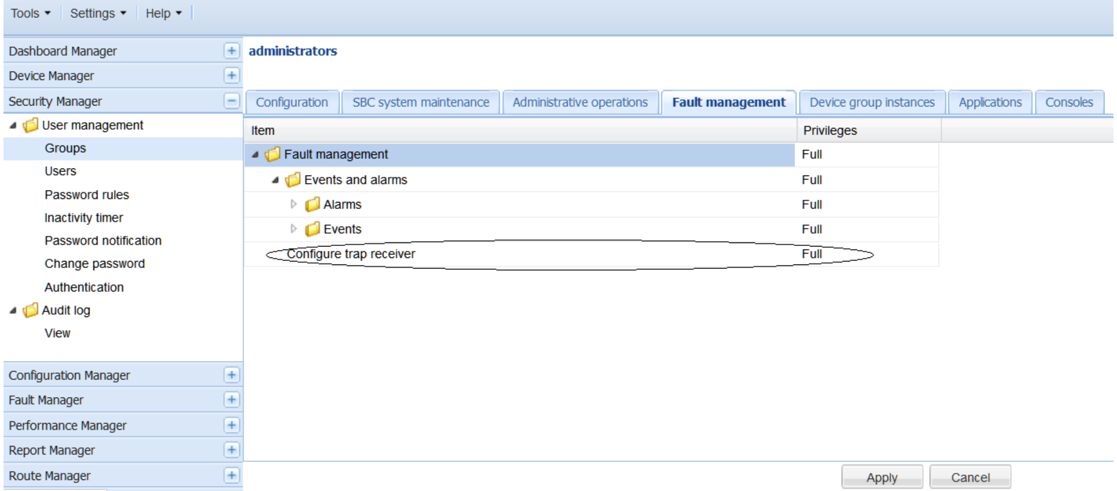


2. Expand the Net-Net Central information by clicking the arrow. The Global ID appears below the Version and OS information.

Setting Permissions for Northbound Fault Management

To set permissions for northbound fault management:

1. Expand the Security Manager slider and navigate to Groups.
2. Select a group and click Edit. The Edit group dialog appears.
3. Click the Fault management tab.
4. Expand Fault management > Events and alarms.



administrators

Item	Privileges
Fault management	Full
Events and alarms	Full
Alarms	Full
Events	Full
Configure trap receiver	Full

5. Click the Configure trap receiver operation row in the table under Privilege. The drop-down list is activated.
6. Choose the appropriate privilege type.
7. Press <Enter> to accept the selected type.
8. Click Apply.

SC[z]7.1.2M2

Documentation will be made available upon release.

S-C[x]6.3.3M3/L-CX1.1.3M3

IMS-AKA Change Client Port

Release S-CX6.3.3M3 brings the SBC into compliance with 3GPP TS 33.203, Access Security for IP-Based Services. Releases prior to S-CX6.3.3M3 failed to change the protected client ports after a successful re-registration.

Release S-CX6.3.3M3 brings the SBC into compliance with 3GPP TS 33.203, Access Security for IP-Based Services. Previous releases did not comply with requirements specified in Section 7.4, Authenticated re-registration, which reads in part:

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P CSCF handle this replacement and which SAs to apply to which message.

When security associations are changed in an authenticated re-registration then the protected server ports at the UE (port_us) and the P-CSCF (port_ps) shall remain unchanged, while the protected client ports at the UE (port_uc) and the P-CSCF (port_pc) shall change.

If the UE has an already active pair of security associations, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol. In particular, if the UE considers the SAs no longer active at the P-CSCF, e.g., after receiving no response to several protected messages, then the UE should send an unprotected REGISTER message."

For more information, see the *Net-Net 4000 Maintenance Release Guide*.

IMS-AKA Change Client Port Configuration

To configure IMS-AKA Change Client Port:

1. Navigate to **Configuration Manager** > **Global settings** > **Security**.
2. Click IMS-AKA profile. The IMS-AKA profile table appears in the content area.
3. Click Add to create a new IMS-AKA profile
4. Name—Enter the name you want to give this IMS-AKA profile. This is the value you will use to apply the profile to a SIP port configuration. This parameter is required, and it has no default value.
5. Protected server port—Enter the port number of the protected server port, which is the port on which the Net-Net SBC receives protected messages. The protected server port should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor.
6. Start protected server port(Protected server port in SCX6.3.3M2/LCX1.3.3M2)—Enter the start value for the pool of port numbers available following a successful re-authentication. Like the protected server port, the protected client port pool should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor.

   Note: Any existing configuration for Protected client port will be mapped to both Start protected client port and End protected client port parameter values.

7. End protected client port—Enter the end value for the pool of port numbers available following a successful re-authentication. Ensure that this value is greater than the value assigned to Start protected client port. Note that the maximum supported pool contains 5 entries. Like the protected server port, the protected client port pool should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP

interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor. The default value is 0. The value range for this parameter is 1025-65535.

8. Click Apply.

L-CX1.5.0

There is no new configuration for this release.

S-C[x]6.4.0M3

There is no new configuration for this release.

S-C[x]6.3.7M2

There is no new configuration for this release.

DCZ2.2.0

Upstream Congestion Control

The Net-Net Diameter Director can detect that upstream devices are congested and throttle traffic to those devices. Upstream devices can provide clues about the extent to which they are congested by sending responses such as DIAMETER_TOO_BUSY, or by simply failing to respond, causing timeouts. When these conditions become evident, the Net-Net Diameter Director can intelligently reduce the transaction rate sent towards the device. It also provides a means of resuming traffic rates when the upstream device is no longer congested.

In addition, the Net-Net Diameter Director can apply differentiated rate-limiting and prioritization based on Application-ID, Command-Code and configurable AVPs for upstream stations in congested state.

You configure how you want the Net-Net Diameter Director to handle congested upstream devices by configuring:

- Diameter director constraints
  - Application constraints
  - Application message constraints
- Congestion control policy

You can apply congestion control based on interface and/or agent, with agent configuration taking precedence.

For more information, consult the *Net-Net Diameter Director Essentials Guide Version D-Cz2.2.0*.

Application Constraint Configuration

To configure application constraints:

1. Navigate to **Configuration Manager** > **Services** > **Diameter Director**.
2. Click Diameter director constraints. The Diameter director constraints table appears in the content area.
3. Click Add to create a new congestion control policy.
4. Name—Enter the identifier or name for this diameter director constraint. This parameter is required.
5. Click Apply.
6. Select the diameter director constraint in the table and click Edit.
7. Scroll to the Application constraints table and click Add to create a new application constraint.

8. Application name—Enter a name assigned to this profile. This name must correspond to an application name within the state machine XML.
9. Click Apply.
10. Select the application constraint from the table and click Edit.
11. Maximum inbound burst rate—Enter the maximum number of inbound messages at the burst rate for this application type. The valid range is 0-999999. The default value is 0.
12. Maximum inbound sustained rate—Enter the maximum number of inbound messages at the sustained rate for this application type. The valid range is 0-999999. The default value is 0.
13. Maximum outbound burst rate—Enter the time, in milleseconds that the Net-Net Diameter Director uses between measurements, from which it evaluates an applicable element's congested state. The valid range is 0-999999. The default value is 0.
14. Maximum outbound sustained rate—Enter the maximum number of outbound messages at the sustained rate for this application. The valid range is 0-999999. The default value is 0.
15. Time to resume—Enter the duration, in seconds, that must elapse before the system evaluates the status of a congested far end device. The device status cannot be changed back to "un-congested" until this timer expires and all thresholds are no longer exceeded. The valid range is 0-999999. The default value is 0.
16. Transaction timeout threshold—Enter the time, in milleseconds, that the Net-Net Diameter Director waits for a response from an applicable element before it labels that elements as congested. The valid range is 0-4294967296. The default value is 0.
17. Scroll to the Application message constraints table and click Add.
18. Message type—Select a value for the message type. Specific values are listed in the table below:
19. Maximum inbound burst rate—Enter the maximum number of inbound messages at the burst rate for this application type. The valid range is 0-999999. The default value is 0.
20. Maximum inbound sustained rate—Enter the maximum number of inbound messages at the sustained rate for this application type. The valid range is 0-999999. The default value is 0.
21. Maximum outbound burst rate—Enter the time, in milleseconds that the Net-Net Diameter Director uses between measurements, from which it evaluates an applicable element's congested state. The valid range is 0-999999. The default value is 0.
22. Maximum outbound sustained rate—Enter the maximum number of outbound messages at the sustained rate for this application. The valid range is 0-999999. The default value is 0.
23. Click Apply.
24. Click Apply.

Congestion Control Policy Configuration

To configure Congestion Control Policy:

1. Navigate to **Configuration Manager** > **Services** > **Diameter Director**.
2. Click Congestion control policy. The Congestion control policy table appears in the content area.
3. Click Add to create a new congestion control policy.
4. Name—Enter the identifier or name for this congestion control policy. This parameter is required.
5. Click Apply.
6. Select the congestion control policy in the table and click Edit.
7. Allow threshold—Enter the maximum number of result-code messages the system allows before denoting the element as congested.
8. Congestion action—Enter the behavior the Net-Net Diameter Director exhibits when it finds an applicable element to be congested.
   - drop—The Net-Net Diameter Director does not respond to requests directed towards the congested element.
   - reject—The Net-Net Diameter Director sends the configured response to devices that send requests to the congested element. Messages sent include the configured result-code and/or the experimental-result-code.

- constraints—The Net-Net Diameter Director uses the configured congestion-contraints profile to shape the traffic stream.

9. Congestion window—Enter the time, in milleseconds that the Net-Net Diameter Director uses between measurements, from which it evaluates an applicable element's congested state. The valid range is 0-999999. The default value is 0.
10. Constraint name—Enter the name of the diameter-director-constraint that this policy applies when the congestion action is set to constraints.
11. Experimental result codes—Click Add to open the dialog to enter an identifier (numeric) of the result code the system receives.
12. Reject experimental result code—Enter the value to include in the Experimental Result Code AVP when the Net-Net Diameter Director chooses this congestion control policy with a reject action. This parameter must be configured along with the reject exp vendor id parameter.
13. Reject experimental vendor id—Enter the vendor ID to accompany the Experimental Result Code when the Net-Net Diameter Director chooses this congestion control policy with a reject action.
14. Reject result code—Enter the value to include in the Result Code AVP when the Net-Net Diameter Director chooses this congestion control policy with a reject action.
15. Result codes—Click Add to open the dialog to enter an identifier (numeric) of the result code the system receives and with which the system measures the element's level of congestion.
16. Time to resume—Enter the duration, in seconds, that must elapse before the system evaluates the status of a congested far end device. The device status cannot be changed back to "un-congested" until this timer expires and all thresholds are no longer exceeded. The valid range is 0-999999. The default value is 0.
17. Transaction timeout threshold—Enter the time, in milleseconds, that the Net-Net Diameter Director waits for a response from an applicable element before it labels that elements as congested. The valid range is 0-4294967296. The default value is 0.
18. Click Apply.

Diameter Director Agent

The Diameter Director Agent is the representation of a remote Diameter agent. For all Diameter agents that may connect to the Net-Net Diameter Director, a Diameter Director Agent must be created. Diameter Director Agents must be in the same realm as a Diameter Director Interface to communicate. If there is no Diameter Director Interface that a Diameter Director Agent can point to, no connection will be made.

For more information, see the Diameter Director Agent section of the Diameter Director Configuration chapter in the *Net-Net Central Configuration Guide: Default View*.

Diameter Director Agent Configuration

To configure Diameter Director Agent:

1. Navigate to **Configuration Manager** > **Services** > **Diameter director**.
2. Click Diameter director agent. The Diameter Director agent table appears in the content area.
3. Double click a hostname to configure.
4. On demand max inactivity—Time in seconds that must elapse before the Net- Net PD will disconnect from an on-demand peer. The value range for this parameter is 0 to 65535.
5. signaling-monitor—Valid values are enabled or disabled.
6. DNS Realm ID—Realm to which this agent issues SRV and NAPTR resolution requests if the target DNS server is not in the same realm as the agent. If the target DNS server is in the same realm as the agent, you can leave this field empty. The system only uses this field if the IP address is empty. This function also requires a resolvable diameter-director-agent hostname.
7. Congestion policy name—Constraint policy applied to this Diameter Director agent. The default is empty, and only congestion control policy names are valid values.
8. Click Apply.

Diameter Director Group

A Diameter Director Group combines several Diameter Director Agents into a single logical entity. Each configured Diameter Director Agent may only belong to one Diameter Director Group. For more information, see the Diameter Director Groups section of the Load Balancing & Redundancy chapter in the *Net-Net Central Configuration Guide: Default View*.

Diameter Director Group Configuration

To configure Diameter Director group:

1. Navigate to **Configuration Manager** > **Services** > **Diameter director**.
2. Click Diameter director group. The Diameter Director group table appears in the content area.
3. Double click a group name to configure.
4. Signaling monitor—Valid values are enabled or disabled.
5. Click Apply.

Diameter Director Interface

The Diameter Director Interface is the Diameter application interface that runs on the Net-Net Diameter Director. Since there can only be one Diameter Director Interface active in a realm, it is defined by that realm, which is configured in the realm-id parameter. When a message is received on a Diameter Director Interface, the Net-Net Diameter Director then determines how and where to route it. Each Diameter Director Interface is configured with a root Diameter Director Policy that sets the starting point of the routing process. For more information, see the Diameter Director Interface section of the Diameter Director Configuration chapter in the *Net-Net Central Configuration Guide: Default View*.

Diameter Director Interface Configuration

To configure the Diameter Director interface:

1. Navigate to **Configuration Manager** > **Services** > **Diameter director** > **Diameter director interface**.
2. Click Diameter Director interface. The Diameter Director interface table appears in the content area.
3. Double click on the realm to configure.
4. Signaling monitor—Valid values are enabled and disabled.
5. congestion policy name—Constraint policy applied to this Diameter Director interface. The default is empty, and only congestion control policy names are valid values.

S-C[xz]6.3.9M3

There is no new configuration for this release.

E-C[xz]6.4.0M2

Remote Site Survivability

Release E-C[xz]6.4.0 M2 includes a new feature called Remote Site Survivability. This feature is the Net-Net Enterprise Session Director’s ability of a Remote Office/Branch Office (ROBO) to detect the loss of communication over SIP-based telephony, to the Enterprise’s core call processing Data Center. When loss of communication is detected over the SIP service, the ROBO Net-Net Enterprise Session Director dynamically switches into Survivable Mode, locally handling call processing and providing limited additional server functionality.

Note: Remote Site Survivability supports SIP only. It does not support the H.323.

The following are features of Remote Site Survivability:

- Works with or without High Availability (HA) operation.
- Configurable in real-time - no reboot required to enable this feature.
- Allows configuration of the feature via the Net-Net Enterprise Session Director Web GUI
- Maintains Historical Recording (HDR) statistics about being in survivability mode, such as:
    - Whether or not the Net-Net Enterprise Session Director is in survivable mode using the ACLI command, show health.
    - Length of time the Net-Net Enterprise Session Director was in survivable mode (records number of times and amount of time in survivability mode)
    - Number of SIP messages handled in survivable mode
    - Number of SIP users registered locally in survivable mode (both existing based on cache, and separately - new registrations).

Configuring Remote Site Survivability using Net-Net Central

You can enable Survivability using the survivability mode configuration. You must also configure the service tag string on the SIP interface for which the Net-Net Enterprise Session Director checks the health score.

The order in which to configure Survivability is:

1. Configure a service-tag for an IP interface.
2. Enable Survivability mode on the Net-Net Enterprise Session Director.
3. Configure a ping-method for the session agent to use to determine whether or not the Net-Net Enterprise Session Director is down.
4. Configure the service health of the IP interface.

Use the following procedure to configure Survivability on the Net-Net ESD.

Configuring a Service Tag for an IP Interface

To configure a Service tag for an IP interface:

1. Navigate to **Configuration Manager** > **Services**.
2. Click Realms. The Realms table appears in the content area.
3. Select a SIP realm in the table and click Edit.
4. Select a SIP interface service in the table and click Edit.
5. Service tag—Enter a character string that identifies a group of session agents for the current SIP interface. When Survivability is enabled, the Net-Net Enterprise Session Director monitors the health of the session agents using this Service tag.
6. Click Apply.

Configuring Survivability Mode

To configure a Service tag for an IP interface:

1. Select List view from the view selection drop-down.
2. Navigate to **Session router** > **Survivability**.
3. Click Realms. The Realms table appears in the content area.
4. Select a SIP realm in the table and click Edit.
5. Select a SIP interface service in the table and click Edit.
6. State—Enter the operational state of Survivability. Valid values are:
    - Enabled
    - Disabled (default)

7. Service tag—Enter the name of the service tag (associated with an IP interface) for which the Net-Net Enterprise Session Director will initiate Survivability. If entering more then one service-tag name, separate each entry with a comma. Default for this parameter is blank.
8. Reg expires—Enter a value, in seconds, that the Net-Net Enterprise Session Director must reach before it enters Survivability mode. When the failed REGISTER attempts reach this limit, the Net-Net Enterprise Session Director goes into Survivability mode (if it is enabled). Valid values are 0 to 2147483647 seconds. Default is 30 seconds.
9. Prefix length—Enter the maximum digits allowed for a phone extension. Valid values are 0 to 10 digits. Default is 4 digits.
10. Click Apply.

Configuring Service Health for a List of Service Tag

To configure a the service health for a list of service tags:

1. Select List view from the view selection drop-down.
2. Navigate to **Session router** > **Service Health**.
3. Click Add.
4. service-tag-string—Enter a list of service tags (associated with IP interfaces) on which the Net-Net Enterprise Session Director checks the service health. Default is blank.
5. Click OK.
6. Navigate to the SA health profile table and click Add.
   the Add SA health profile dialog appears.
7. session-agent-hostname—Enter the hostname of the session agent on which the Net-Net Enterprise Session Director monitors the service health.
8. session-agent-health—Enter the health score that the Net-Net Enterprise Session Director uses to determine whether or not the health of the session-agent has decremented and gone out of service or incremented and came back into service. Valid values are 0 to 100 percent. Default is 100. For example, if this parameter is set to 100, and if the health score of the session-agent falls beneath 100 percent, Survivability mode begins (if enabled). If the health of the session-agent comes back up to 100 percent, Survivability mode ends and the system returns to Normal mode.

   Note: For cases where there are two session agents, each session agent could have a service health of 50.
9. Click OK.
10. Click Apply.

Configuring Ping Method for a Session Agent

To configure the ping method for a session agent:

1. Navigate to **Configuration Manager** > **Services** > **Agents**.
2. Click Session agents. The Session agent table appears in the content area.
3. Select a session agent in the table and click Edit.
4. Ping method—Indicate the SIP message/method to use to ping a session agent. The ping confirms whether the session agent is in service. If this field is left empty, no session agent is pinged. Default is blank. Setting this field to OPTIONS is recommended.
5. Click Apply.

S-C[x]6.3.5M1

There is no new configuration for this release.

A

MIBs

Northbound Fault Management MIB

A new SNMP MIB for northbound fault management is defined as follows:

```
------------------------------------------------------------------
--------------
--ACMEPACKET-ITU-X733-MIB:  ORACLE NNC Fault Management
Northbound MIB file
--
--June 2013
--
--Copyright (c) by ORACLE, Inc.
--All rights reserved.
------------------------------------------------------------------
--------------
--This MIB provides a means to gather information about the
--Acme Management Interface running at the Net-Net NNC and/or
Device
--
APNNCItuX733Alarm-MIB DEFINITIONS ::= BEGIN

    IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Integer32,
Unsigned32,
    enterprises
        FROM SNMPv2-SMI
    OBJECT-GROUP, NOTIFICATION-GROUP
        FROM SNMPv2-CONF
    DisplayString, TruthValue
      FROM SNMPv2-TC;

    apNNCItuX733AlarmModule MODULE-IDENTITY
        LAST-UPDATED        "201307200000Z"
        ORGANIZATION        "ORACLE, Inc"
        CONTACT-INFO
              "       Customer Service
                        Postal: ORACLE, Inc
                                100 Crosby Drive
                                Bedford, MA 01730
                                US
                        Tel:    1-781-328-4400
                        E-mail: support@oracle.com"
        DESCRIPTION     "The Net-Net NNC ITU X733 MIB for ORACLE"
        REVISION        "201307200000Z"
        DESCRIPTION     "Initial version"
        ::= { apEMSModule 6 }

    acmepacket OBJECT IDENTIFIER ::= { enterprises 9148 }
    acmepacketMgmt OBJECT IDENTIFIER ::= { acmepacket 3}
    apEMSModule OBJECT IDENTIFIER ::= { acmepacketMgmt 8 }

    apNNCItuX733AlarmMIBObjects OBJECT IDENTIFIER ::= 
{ apNNCItuX733AlarmModule 1 }

    apNNCItuX733NotificationObjects OBJECT IDENTIFIER ::= 
{ apNNCItuX733AlarmModule 2 }

    apNNCItuX733NotificationId     OBJECT-TYPE
        SYNTAX                  Unsigned32
        MAX-ACCESS           accessible-for-notify
        STATUS                  current
        DESCRIPTION
            "Unique identifier for the notification."
        ::= {apNNCItuX733NotificationObjects 1}

    apNNCItuX733ManagedObjectClass OBJECT-TYPE
        SYNTAX                  DisplayString
        MAX-ACCESS           accessible-for-notify
        STATUS                  current
        DESCRIPTION
            "Type of managed object."
        ::= {apNNCItuX733NotificationObjects 2}

    apNNCItuX733ManagedObjectInstance OBJECT-TYPE
        SYNTAX                     DisplayString
        MAX-ACCESS              accessible-for-notify
        STATUS                     current
        DESCRIPTION
            "Managed object instance."
        ::= {apNNCItuX733NotificationObjects 3}

    apNNCItuX733PerceivedSeverity OBJECT-TYPE
        SYNTAX                        INTEGER {
                                cleared(1),
                                indeterminate(2),
                                critical(3),
                                major(4),
                                minor(5),
                                warning(6)
                                }
        MAX-ACCESS              accessible-for-notify
        STATUS                     current
        DESCRIPTION
            "Represents the perceived severity values for the 
alarms as per[X.733]"
        ::= {apNNCItuX733NotificationObjects 4}

    apNNCItuX733EventTime      OBJECT-TYPE
        SYNTAX                     DisplayString (SIZE (1..64))
        MAX-ACCESS              accessible-for-notify
        STATUS                     current
        DESCRIPTION
            "Timestamp of event."
        ::= {apNNCItuX733NotificationObjects 5}
    apNNCItuX733EventType       OBJECT-TYPE
        SYNTAX               INTEGER {
                other(1),
                communicationsAlarm(2),
                qualityOfServiceAlarm(3),
                processingErrorAlarm(4),
                equipmentAlarm(5),
                environmentalAlarm(6),
                integrityViolation (7),
                operationalViolation (8),
                physicalViolation (9),
                securityServiceOrMechanismViolation (10),
                timeDomainViolation (11)
                }
        MAX-ACCESS              accessible-for-notify
        STATUS                     current
        DESCRIPTION
            "Represents the event type values for the alarms as
per [X.733] and [X.736]"
        ::= {apNNCItuX733NotificationObjects 6}

    apNNCItuX733ProbableCause      OBJECT-TYPE
        SYNTAX                  INTEGER {
                other (1),
                adapterError (2),
                applicationSubsystemFailure (3),
                bandwidthReduced (4),
                callEstablishmentError (5),
                communicationsProtocolError (6),
                communicationsSubsystemFailure (7),
                configurationOrCustomizationError (8),
                congestion (9),
                corruptData (10),
                cpuCyclesLimitExceeded (11),
                dataSetOrModemError (12),
                degradedSignal (13),
                dteDceInterfaceError (14),
                enclosureDoorOpen (15),
                equipmentMalfunction (16),
                excessiveVibration (17),
                fileError (18),
                fireDetected (19),
                floodDetected (20),
                framingError (21),
                heatingVentCoolingSystemProblem (22),
                humidityUnacceptable (23),
                inputOutputDeviceError (24),
                inputDeviceError (25),
                lanError (26),
                leakDetected (27),
                localNodeTransmissionError (28),
                lossOfFrame (29),
                lossOfSignal (30),
                materialSupplyExhausted (31),
                multiplexerProblem (32),
                outOfMemory (33),
                ouputDeviceError (34),
                performanceDegraded (35),
                powerProblem (36),
                pressureUnacceptable (37),
                processorProblem (38),
                pumpFailure (39),
                queueSizeExceeded (40),
                receiveFailure (41),
                receiverFailure (42),
                remoteNodeTransmissionError (43),
                resourceAtOrNearingCapacity (44),
                responseTimeExecessive (45),
                retransmissionRateExcessive (46),
                softwareError (47),
                softwareProgramAbnormallyTerminated (48),
                softwareProgramError (49),
                storageCapacityProblem (50),
                temperatureUnacceptable (51),
                thresholdCrossed (52),
                timingProblem (53),
                toxicLeakDetected (54),
                transmitFailure (55),
                transmitterFailure (56),
                underlyingResourceUnavailable (57),
                versionMismatch (58),
                authenticationFailure (59),
                breachOfConfidentiality (60),
                cableTamper (61),
                delayedInformation (62),
                denialOfService (63),
                duplicateInformation (64),
                informationMissing (65),
                informationModificationDetected (66),
                informationOutOfSequence (67),
                intrusionDetection (68),
                keyExpired (69),
                nonRepudiationFailure (70),
                outOfHoursActivity (71),
                outOfService (72),
                proceduralError (73),
                unauthorizedAccessAttempt (74),
                unexpectedInformation (75)
                }

        MAX-ACCESS          accessible-for-notify
        STATUS              current
        DESCRIPTION
            "Represents the probable cause values for the alarms
as per[X.733]"
        ::= {apNNCItuX733NotificationObjects 7}

    apNNCItuX733AdditionalText        OBJECT-TYPE
        SYNTAX                     OCTET STRING (SIZE (1..2048))
        MAX-ACCESS              accessible-for-notify
        STATUS                     current
        DESCRIPTION
            "Represents free form text description."
        ::= {apNNCItuX733NotificationObjects 8}

    apNNCItuX733ThresholdInformation      OBJECT-TYPE
        SYNTAX                         DisplayString (SIZE
(1..255))
        MAX-ACCESS                     accessible-for-notify
        STATUS                         current
        DESCRIPTION
            "Identifies that it is a threshold crossing event."
        ::= {apNNCItuX733NotificationObjects 9}

    apNNCItuX733SpecificProblem       OBJECT-TYPE
        SYNTAX                     DisplayString (SIZE (1..64))
        MAX-ACCESS              accessible-for-notify
        STATUS                     current
        DESCRIPTION
            "Identifies refinement to probable cause of the 
alarm."
        ::= {apNNCItuX733NotificationObjects 10}

    apNNCItuX733CorrelationNotificationIds      OBJECT-TYPE
        SYNTAX                              DisplayString
        MAX-ACCESS                       accessible-for-notify
        STATUS                              current
        DESCRIPTION
            "A set of notification identifiers for event 
correlation."
        ::= {apNNCItuX733NotificationObjects 11}

    apNNCItuX733AdditionalInformation        OBJECT-TYPE
        SYNTAX                            DisplayString
        MAX-ACCESS                     accessible-for-notify
        STATUS                            current
        DESCRIPTION
            "Represents the additional text field for the alarm 
as per[X.733] "
        ::= {apNNCItuX733NotificationObjects 12}

    apNNCItuX733ProposedRepairAction           OBJECT-TYPE
        SYNTAX                              DisplayString
        MAX-ACCESS                       accessible-for-notify
        STATUS                              current
        DESCRIPTION
            "Suggestion for resolving the problem."
        ::= {apNNCItuX733NotificationObjects 13}

    apNNCItuX733Notifications          OBJECT IDENTIFIER ::= 
{ apNNCItuX733AlarmModule 3 }
    apNNCItuX733NotificationsPrefix    OBJECT IDENTIFIER ::= 
{ apNNCItuX733Notifications 0 }

    apNNCItuX733Notification NOTIFICATION-TYPE
        OBJECTS {
            apNNCItuX733NotificationId,
            apNNCItuX733ManagedObjectClass,
            apNNCItuX733ManagedObjectInstance,
            apNNCItuX733PerceivedSeverity,
            apNNCItuX733EventTime,
            apNNCItuX733EventType,
            apNNCItuX733ProbableCause,
            apNNCItuX733AdditionalText,
            apNNCItuX733ThresholdInformation,
            apNNCItuX733SpecificProblem,
            apNNCItuX733CorrelationNotificationIds,
            apNNCItuX733AdditionalInformation,
            apNNCItuX733ProposedRepairAction
            }
    STATUS current
        DESCRIPTION
            "The notification will be generated whenever a trap 
is received from devices managed by NNC or a trap is generated by 
NNC server its self."
    ::= { apNNCItuX733NotificationsPrefix 1 }

    apNNCItuX733ModuleConformance OBJECT IDENTIFIER ::= 
{ apNNCItuX733AlarmModule 4 }

    apNNCItuX733Groups OBJECT IDENTIFIER ::=
{ apNNCItuX733ModuleConformance 1 }
    apNNCItuX733NotificationsGroups OBJECT IDENTIFIER ::=
{ apNNCItuX733ModuleConformance 2 }
    apNNCItuX733NotificationObjectsGroups OBJECT IDENTIFIER ::=
{ apNNCItuX733ModuleConformance 3 }

    apNNCItuX733NotificationsGroup NOTIFICATION-GROUP
        NOTIFICATIONS {
          apNNCItuX733Notification
        }
    STATUS current
    DESCRIPTION "NNC northbound X.733 format trap"
    ::= { apNNCItuX733NotificationsGroups 1 }

    apNNCItuX733NotificationObjectsGroup OBJECT-GROUP
        OBJECTS {
            apNNCItuX733NotificationId,
            apNNCItuX733ManagedObjectClass,
            apNNCItuX733ManagedObjectInstance,
            apNNCItuX733PerceivedSeverity,
            apNNCItuX733EventTime,
            apNNCItuX733EventType,
            apNNCItuX733ProbableCause,
            apNNCItuX733AdditionalText,
            apNNCItuX733ThresholdInformation,
            apNNCItuX733SpecificProblem,
            apNNCItuX733CorrelationNotificationIds,
            apNNCItuX733AdditionalInformation,
            apNNCItuX733ProposedRepairAction
       }
    STATUS current
    DESCRIPTION "Objects for NNC northbound X.733 notifications."
    ::= { apNNCItuX733NotificationObjectsGroups 1 }

END
```