ECX640 Web GUI User Guide

ECX640 Web GUI User Guide
Release 6.4.0

2014

ORACLE

Notices

Contents

Preface

About this Guide - ECX640 WebGUI

The E-CX6.4.0 Maintenance Release Guide provides information about the contents of maintenance releases related to release E-CX6.4.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release of the Net-Net OS from prior releases. When applicable, this guide contains explanations of defect fixes to the software and step-by-step instructions, if any, for how to enables these fixes on your system. This guide contains explanations of adaptations including conceptual information and configuration steps.

Purpose of this Document

Designed as a supplement to the main documentation set supporting release E-CX6.4.0, this document informs you of changes made to the software in the maintenance releases of E-CX6.4.0. Consult this document for content specific to maintenance releases. For information about general release features, configuration, and maintenance, consult the Related Documentation listed in the section below and then refer to the applicable document.

Organization

The Maintenance Release Guide is organized chronologically by maintenance release number, started with the oldest available maintenance release and ending with the most recently available maintenance release.

This document contains a Maintenance Release Availability Matrix, showing when and if given maintenance releases have been issued and the date of issue. Each available maintenance release constitutes one chapter of this guide.

In certain cases, a maintenance release will not have been made generally available. These cases are noted in the Maintenance Release Availability Matrix. When Oracle has not made a maintenance release available, there will be no corresponding chapter for that release. Therefore, you might encounter breaks in the chronological number of maintenance release.

Related Documentation

The following table lists related documents that are new to E-C[xz]6.4.0.

Document Name	Document Description
Enterprise Session Border Controller Release Notes	Contains information about new features in this Release, including fixed issues and software limitations.
Enterprise Session Border Controller Configuration Guide	Contains information about the administration, management, and software configuration of the SBC for Enterprises and Service Providers.

The following table lists related S-CX6.3.0 documents you can use as reference.

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3800 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3800 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the SBC's support for its Administrative Security license.

Revision History

Date	Revision Number	Description
April 4, 2013	Revision 1.00	New document that presents the Net-Net Session Director Web GUI (Configuration, SIP Monitor and Trace, System File Management, and Configuration).
May 10, 2013	Revision 1.01	Added the following note: Note: After upgrading your Net-Net ESD software, you should clear your browser cache before using the Net-Net ESD Web GUI.
June 28, 2013	Revision 1.01	Incorporated EC[xz]6.4.0M1 information.
February 28, 2014	Revision 1.0.2	• Clarifies that the monitor and trace maximum message storage capacity is cumulative for all report types.

1

Overview

Introduction

This chapter provides information about the following aspects of the Enterprise Session Director:

- Browser Support
- GUI Logging in/Logging out
- GUI Tool Functions

Note: For information about configuring the Net-Net ESD to allow Web GUI access, see the Installation Wizard section of the *Net-Net® Enterprise Session Director Configuration Guide*.

Browser Support

You can use any of the following Web browsers to access the Web GUI:

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Enterprise Session Director software, you should clear your browser cache before using the Enterprise Session Director Web GUI.

Logging in Logging out

This section provides information and procedures for logging into the Web GUI.

User and Administrator Access

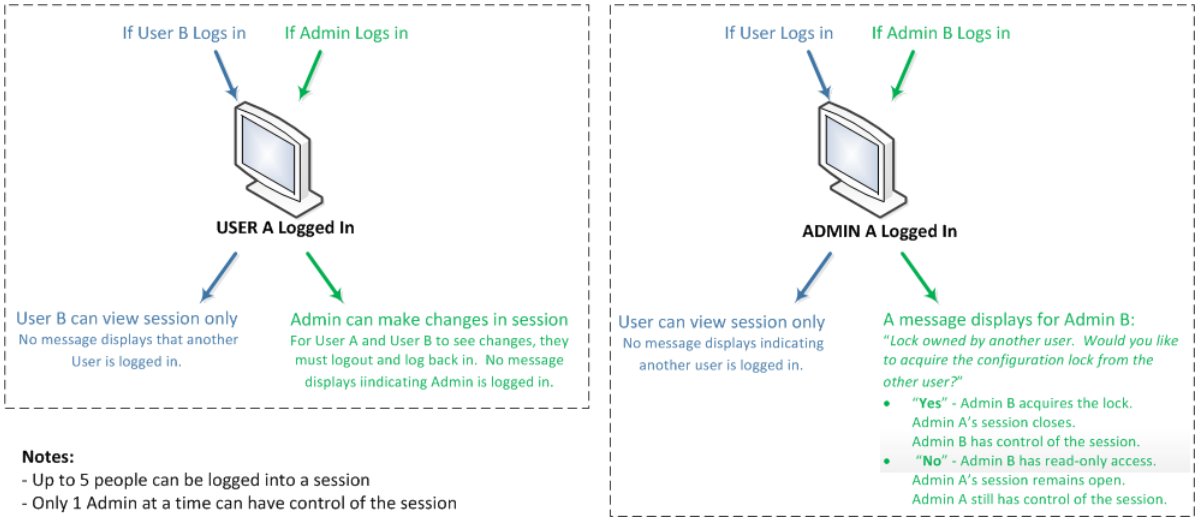
You can login to the Web GUI using your Web browser. There are two types of user logins:

- User - Allows viewing (read-only) access to the Web GUI.
- Administrator - Allows Superuser access to the Web GUI.

For specific rules that apply to the User and Administrator when using the Configuration, SIP Monitor and Trace, and System tabs, see the respective chapters in the *Oracle Enterprise Session Border Controller SE/VME Web GUI User Guide*.

Simultaneous Logins

The Web GUI allows simultaneous logins for both the User and Administrator. However, session availability to the User and Admin is dependant on which type of user is logged into the session. The following illustration shows a scenario of a User and an Administrator logged into a Web GUI session.



Up to five people can log into the same session (same IP address) at the same time. However, only one Administrator at a time can have full control of a simultaneous session. If more than five users attempt to log in, the following error message displays:

```
User limit reached. Please try again later.
```

Radius Server in the Network

The Web interface supports authentication functionality similar to a user logging in via TELNET, Secure Shell (SSH), and SSH File Transfer Protocol (SFTP).

The Web GUI supports RADIUS authentication. The following table indicates the functions available to the Administrator and User levels.

IF	THEN
RADIUS server is configured as userclass=admin	Administrator has full access to all features and functions after logging into the GUI.
RADIUS server is configured as userclass=user	User has the following limited acess to the features and functions after logging into the GUI: Full access to all SIP Monitor and Trace features and functions Can download the following files in System File Management: • Local route table (LRT) • SPL Plug-in (SPL) • Backup configuration • SIP Trunk Xpress bootstrap • Playback media • Log Note: A user with User privilege cannot upload files in System File Management.

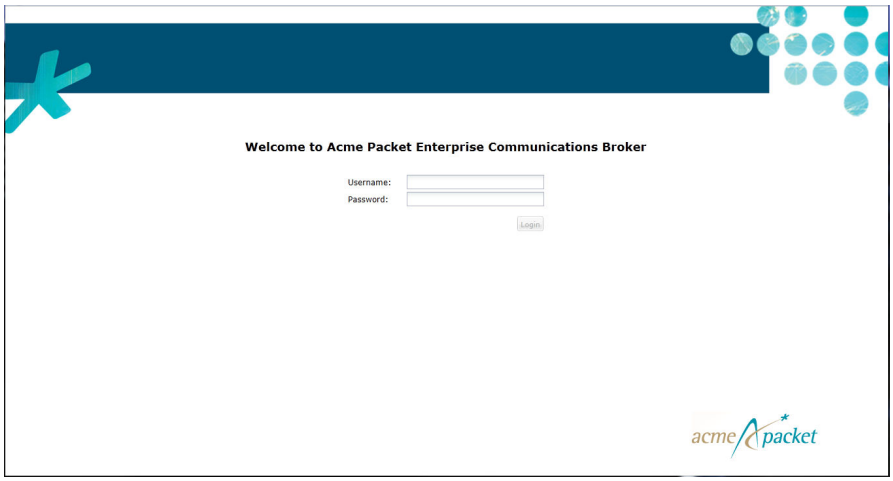
Logging In

To login to the GUI:

1. On your PC, open an Internet Browser.
2. Start the GUI by using either the HTTP or HTTPS login:

```
http://<Server IP address>
https://<Server IP address>
```

Note: Logging in using HTTP and/or HTTPS is dependant on the setting made by your Administrator during the installation of the Web GUI. Your Administrator can change this setting using the ACLI. For more information, see the Net-Net Enterprise Session Director Configuration Guide.

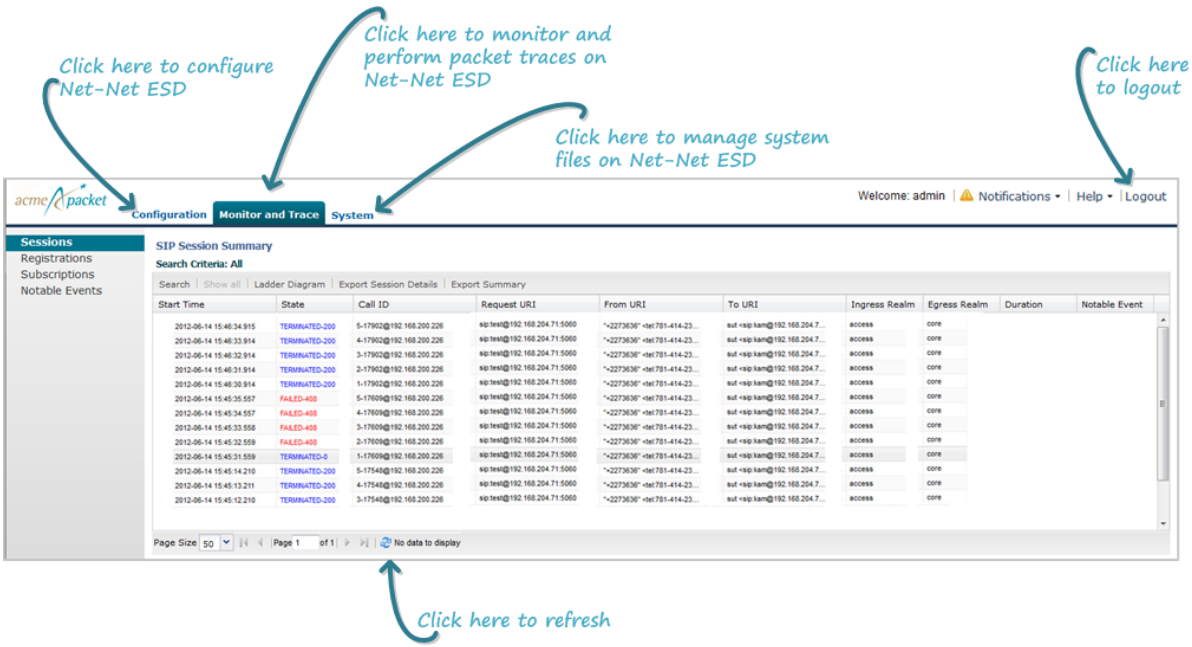


3. Enter your GUI username and password. The default username for the User level is “user” and the default password is “acme.” The default username for an Administrator level is “admin”, and the default password is "packet". If you changed a default password, use that one.

   To change passwords, you use the secret command from the ACLI to change the login password for user and/or the config password for admin.

   For more information about setting passwords, see the *Oracle Enterprise Session Border Controller Configuration Guide*.

   If RADIUS is enabled on the Enterprise Session Director, the Enterprise Session Director performs authentication similar to how it behaves with TELNET/SSH sessions.
4. Click <Login>.



The following table describes the tabs on this page.

Tab	Description
Configuration	Allows you to configure your Enterprise Session Director.
Monitor and Trace	Allows you to use data collected by the Monitor and Trace tool. For information about using the Monitor and Trace tool, see the *Oracle Enterprise Session Border Controller SE/VME Web GUI User Guide*. You enable configure Monitor and Tracing and set filters from the ACLI. For information about configuring the Monitor and Trace tool, see the *Oracle Enterprise Session Border Controller Configuration Guide*.
System	Allows you to: • Manage the system files on the Enterprise Session Director. Using this feature, you can manage specific system files, backup the Enterprise Session Director configuration, and view log files for troubleshooting purposes. • Reboot your Enterprise Session Director.

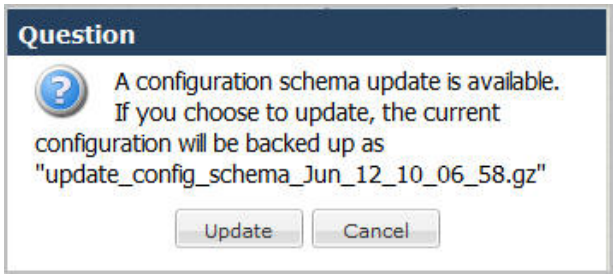
5. Click on the applicable tab to perform configuration, use monitoring and tracing or to manage the Enterprise Session Director system files.

Logging Out

To logout of the GUI, click Logout in the upper right corner of the page. The system logs you out and returns to the login dialog.

Prompt for Configuration Schema Update

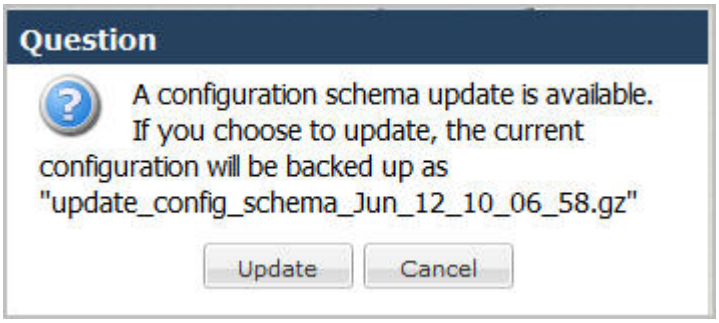
When upgrading your Web GUI software from E-C[xz]6.4.0 GA to any subsequent release, after first login into the GUI, the following prompt displays:



This prompt provides you the option of whether or not to update the configuration parameters in your previous software with any new parameters that were added in the subsequent release. For each configuration screen in Basic Mode, if new parameters were added for you to configure, this update adds those new parameters.

To update the configuration schema:

1. Log into the Web GUI. The following prompt displays.

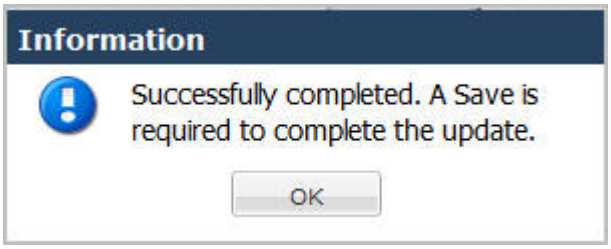


2. Click Update. The current configuration is backed up and the configuration schema is updated.

   Note: If required, you can reinstall the backed up configuration at a later time using the System tab in the Web GUI.

   If you click Cancel, the update is bypassed and no new parameters are added. If you cancel the update, the update prompt displays each time you log into the Web GUI, until you choose to update the configuration schema.

   The following message displays.



3. Click the Save link in the upper left corner of the screen.

GUI Tool Functions

The GUI provides global tools that enhance your user interface experience in the GUI. These tools apply to the entire GUI interface. There are also GUI tools that apply to specific functions within each tab.

This section provides a description of each global tool and each tab-specific GUI tool:

Global Tools

- About Link
- Help Link
- Customizing the Page Display

- Configuration Tools
- Refresh
- Changing Number of Data Items on the Page
- Pop-up Context Menu

Global Tools

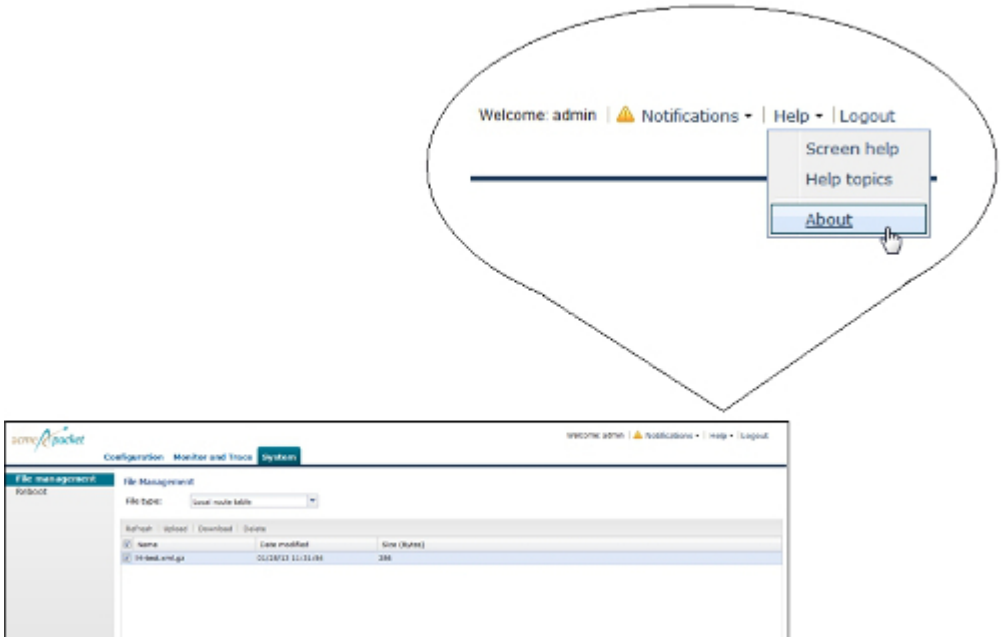
The following paragraphs describe the tools you can use to enhance your Web GUI experience. These tools apply to the Configuration, Monitor and Trace, and System tabs.

About Link

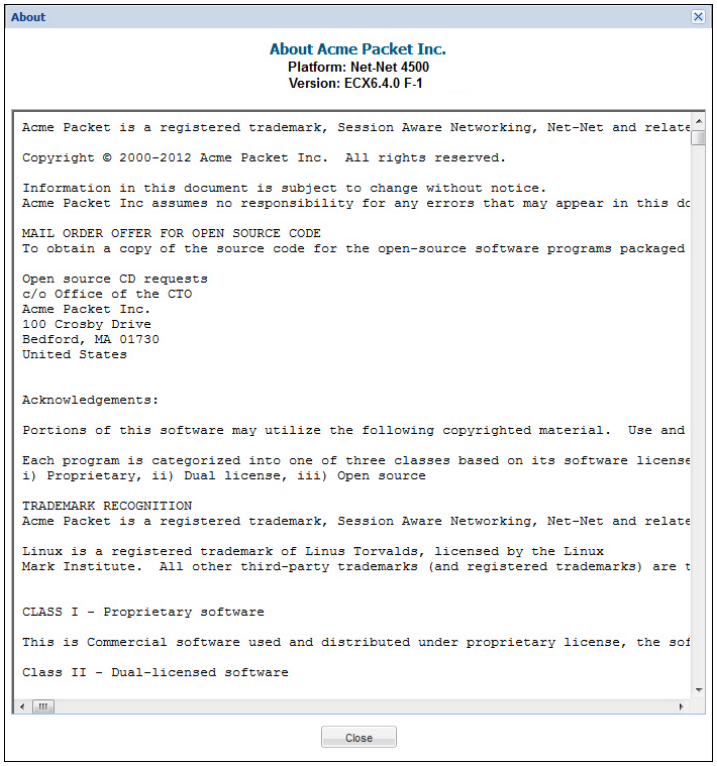
You can display information about the software and licenses currently loaded on the Net-Net ESD. The “About” link allows you to display the current version of software, as well as the licenses associated with the software. You can access the “About” link at the **Help** > **About** Menu in the upper right corner of the screen.

To display the About information:

1. From any page in the Web GUI, click **Help** > **About** in the upper right corner of the screen.



The following information displays.



This box displays the following about the system you are currently logged into:

- Platform type
- Software version number
- Legal notices
- Copyright information
- Open Source Mailing Address
- Trademark recognition
- Licensing information

2. Click <Close> to close the About box.

Help Link

The Help link in the Web GUI has three types of help methods:

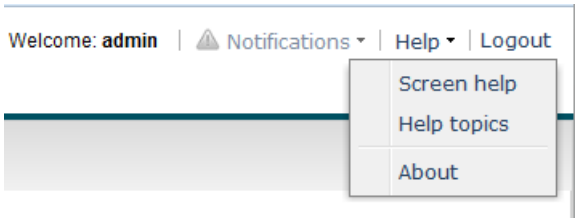
- Screen Help - Quick pointers that indicate specific tasks you can perform.
- Help Topics - Menu of elements that provide more specific help about the Web GUI.

Each of these help methods is described below.

Screen Help

Screen Help provides an overlay on the current screen with pointers that indicate specific tasks you can perform. When you select **Help** > **Screen** help in the upper right corner of the page, an overlay displays with screen pointers to specific areas of the blurred-out screen. Clicking anywhere on the screen closes this help method.

You can display screen help on the main screens for each tab (Configuration tab (expert and basic modes), Monitor and Trace tab, and System tab).

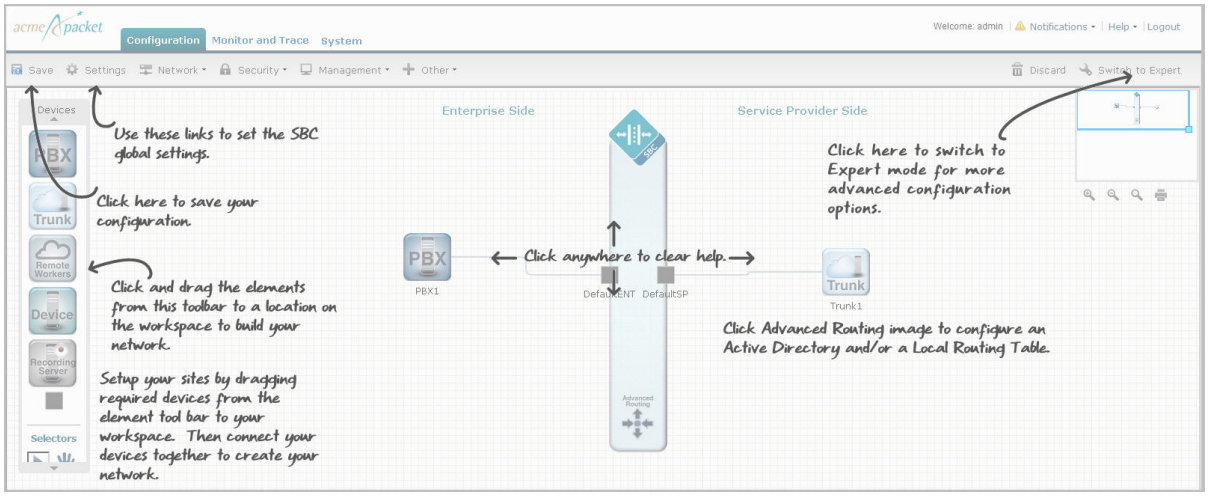


To display Screen Help:

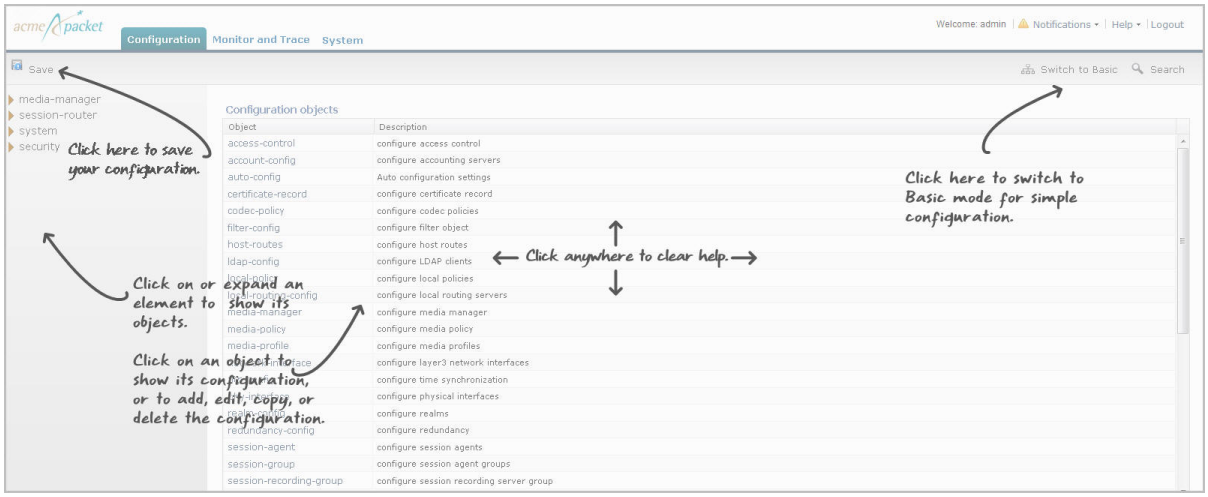
Select **Help** > **Screen** help in the upper right corner of the screen. An overlay displays on the screen with help pointers to tasks you can perform.

The following illustrations show the screen help for each tab. If a User is logged into a session as “view-only”, some of the screen help pointers are not applicable.

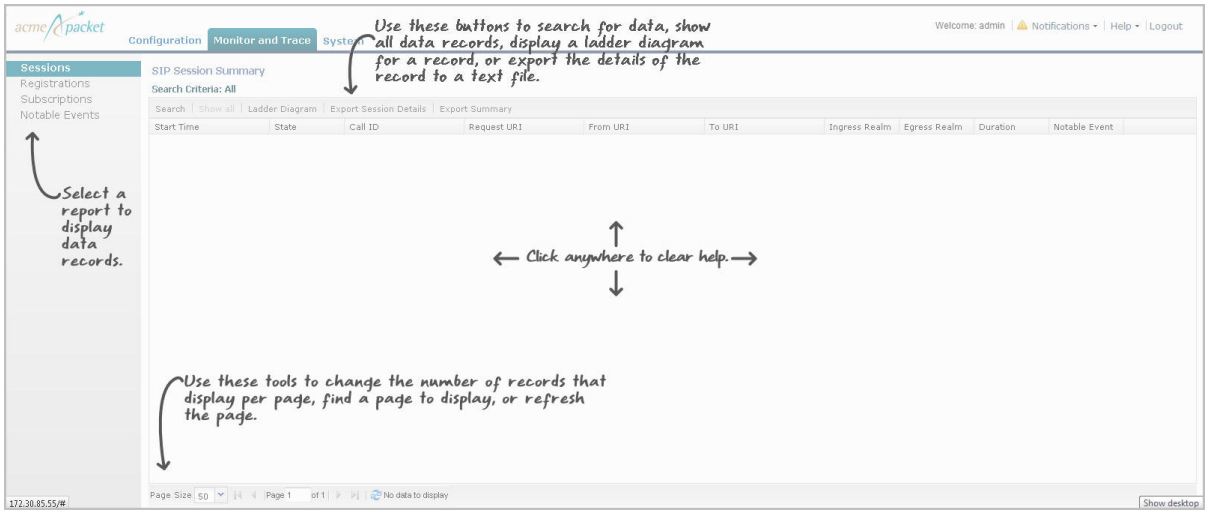
Configuration Tab (Basic mode)



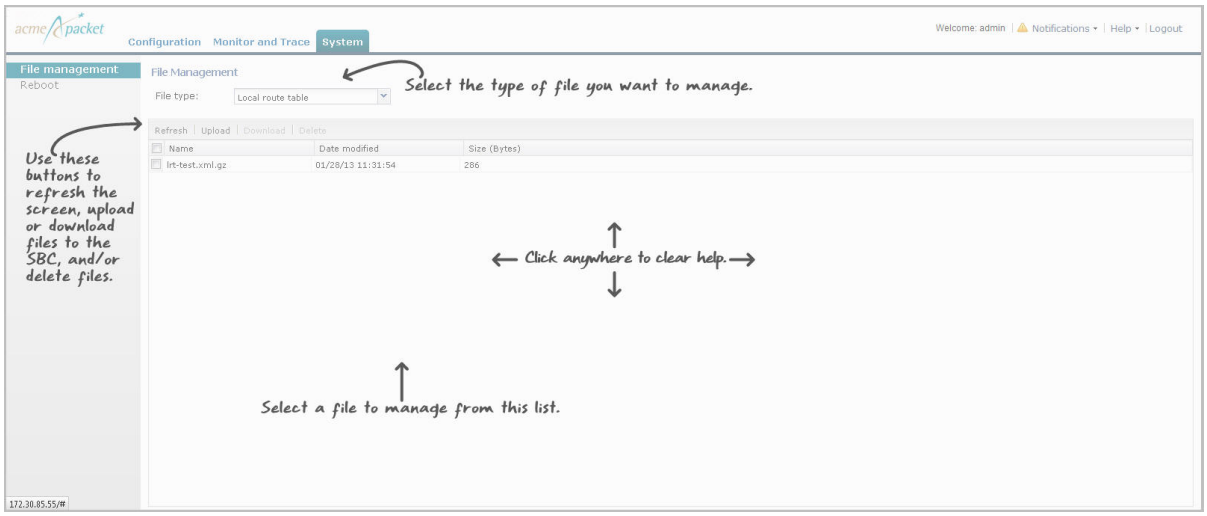
Configuration Tab (Expert mode)



Monitor and Trace Tab



System Tab

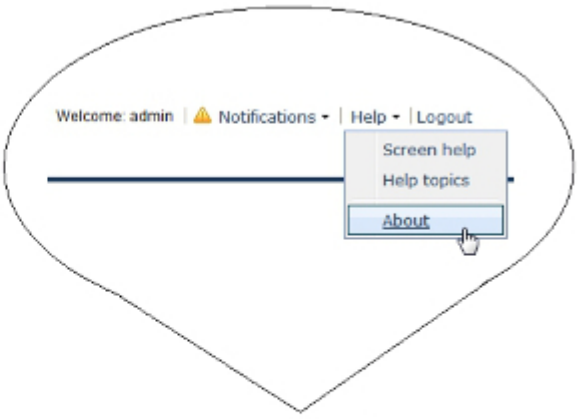


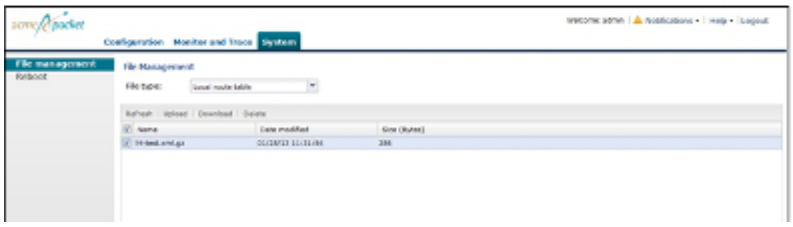
Help Topics

The Web GUI provides more detailed online help for the Configuration tab, Monitor and Trace tab, and System tab if required. You can select **Help** > **Help Topics** to display a menu of help topics you can click on to get more information about a topic. You can access help from any page in the Web GUI.

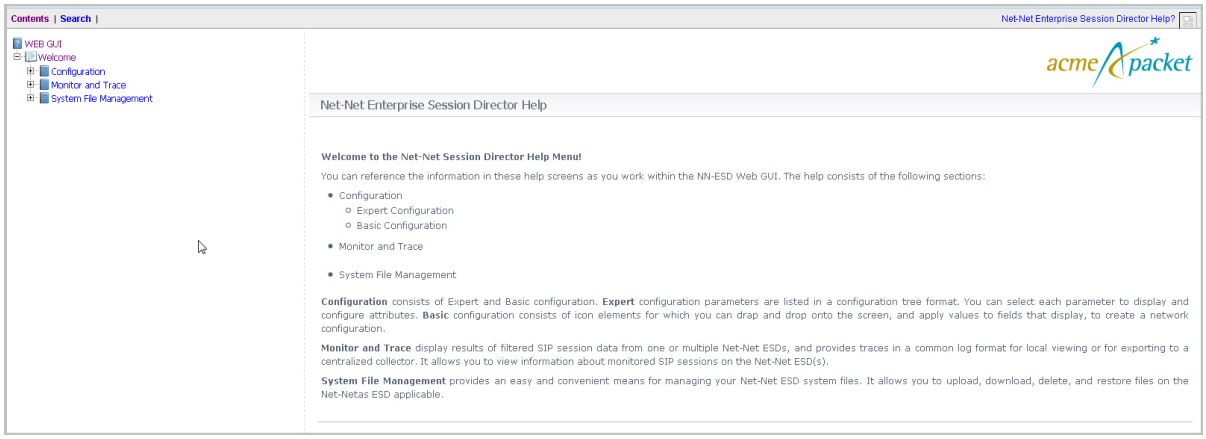
To display Help:

1. From any page in the Web GUI, select Help->Help topics in the upper right corner on the screen.





A new tab opens in your browser that contains a menu that provides help for the various aspects of your device.



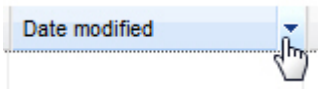
2. Click on an element in the menu for help about that element
3. Close the tab by clicking the “x” in the upper right corner of the tab. Or drag the tab away from the browser to keep it open in a separate window while you continue to work in the Web GUI.

Customizing the Page Display

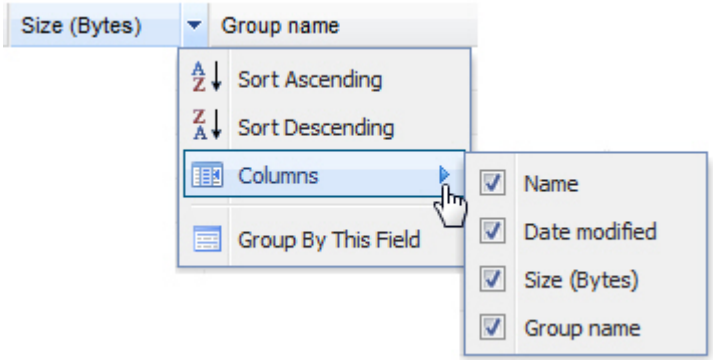
You can customize the data presented on the pages in the Web GUI by changing whether or not specific columns display and how they display. You can also sort the order of item entries. Customizing the page display is available throughout the Web GUI.

To customize the page display within any report:

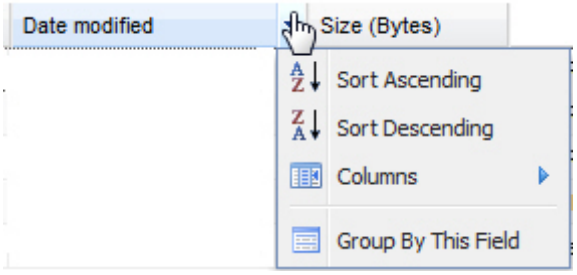
1. Position the cursor over a column heading. A pointer displays on the right hand side of the box. For example:



2. Click the down arrow to display the menu. For example:



3. Click Sort Ascending to sort the data in the table in ascending order.
4. Click Sort Descending to sort the data in the table in descending order.
5. Click Columns to access and customize a list of column names. For example:

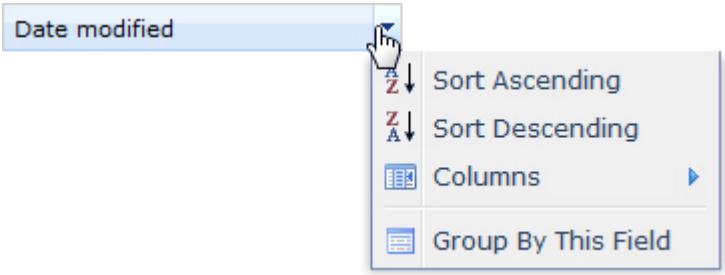


6. Place a checkmark in the box to display that heading/column in the window. Remove the checkmark to hide the heading/column in the window.

Group by Field

The Group by This Field option is available from the System tab only.

When on the System tab, the Group by This Field option displays in the column drop-down box.



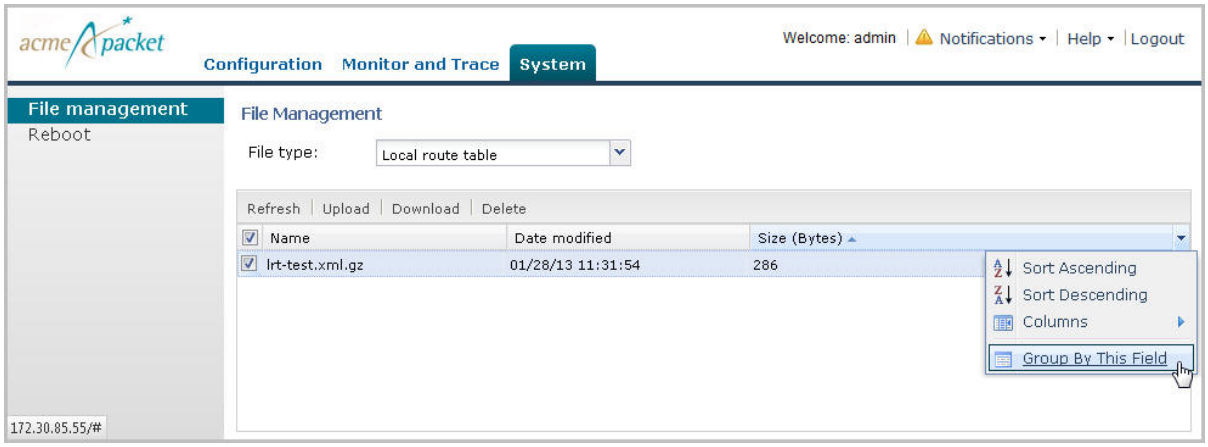
This option allows you to group items on a page according to the column heading you select.

Group By Field Configuration

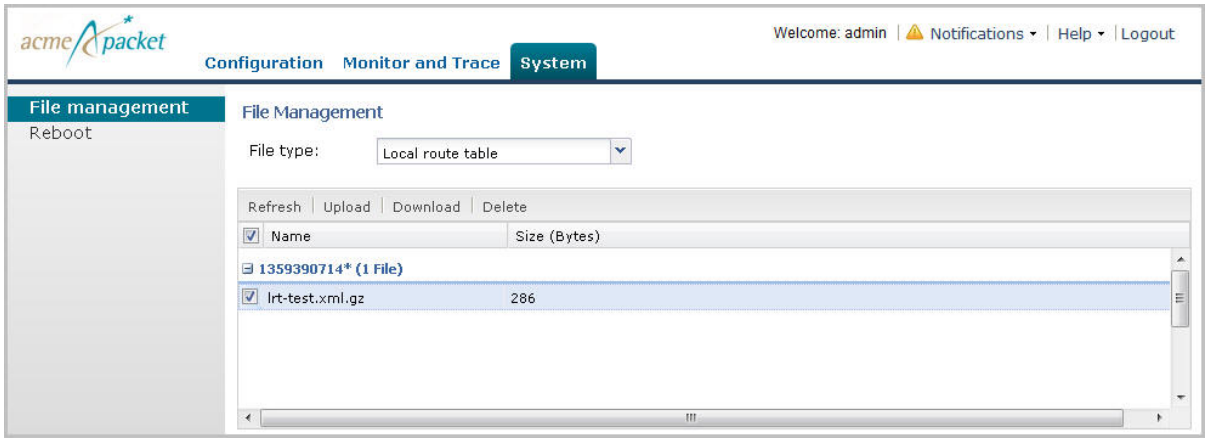
To group items by field:

1. Select a column from the window.
2. Click the down-arrow and select Group By This Field.

   The following window shows the "Size" column selected for Local route table system files.



The following window displays after selecting "Group By This Field."



The above window shows the file(s) grouped by the size of the files.

Group By This Field Configuration

To change the column to group by:

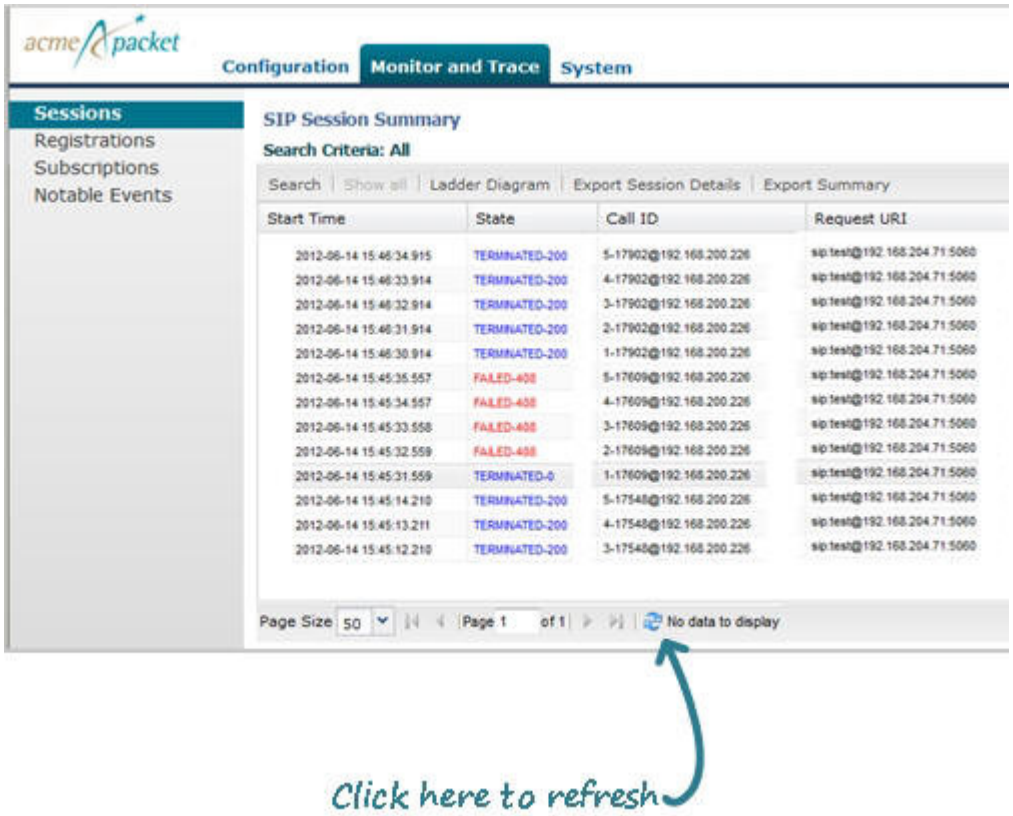
1. Display the column you want to group by, using the procedure in Customizing the Page Display (12).
2. Select a column from the window.
3. Click the down-arrow and select "Group By This Field."

Monitor and Trace Tools

The Web GUI provides specific tools within the Monitor and Trace tab that you can use to enhance your experience in displaying data. The following paragraphs describe each of these tools.

Refresh

Click the at the bottom of any page to update the window with the latest data.

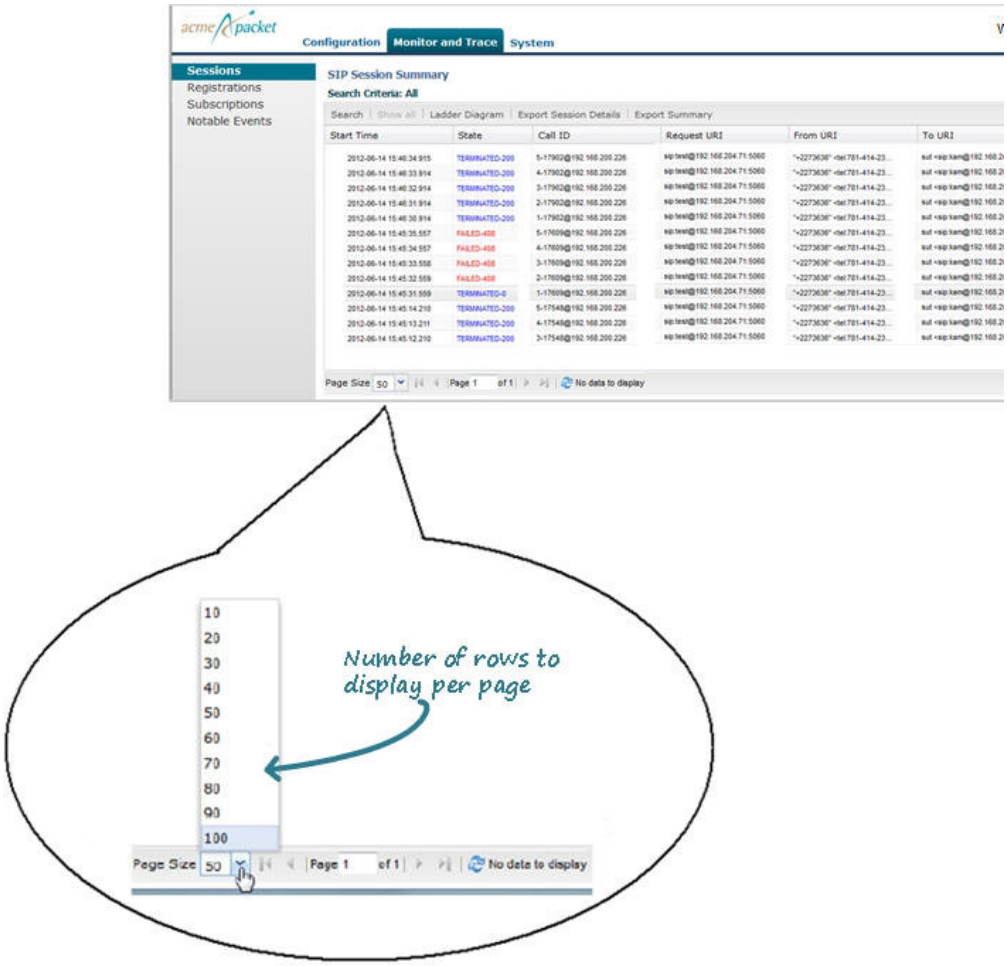


Changing Number of Data Items on the Page

By default, 50 data items are shown per page. You can change the number of items that display on a page.

To change the number of data items displayed in Monitor and Trace:

1. At the bottom left corner of the window, click the down arrow next to Size. The drop down list of values appears.

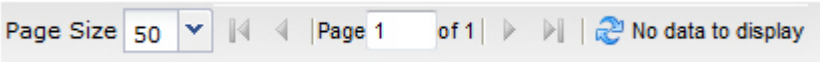


2. Click the number of data items you want to display per page. Default is 50. Valid values are 10 to 100 in increments of 10.

Navigating Pages

To navigate through multiple pages in Monitor and Trace:

1. Use the navigation arrows located at the bottom left corner of the window to navigate through the desired pages (first, previous, next, last). Or enter the page number you want to view in the page box

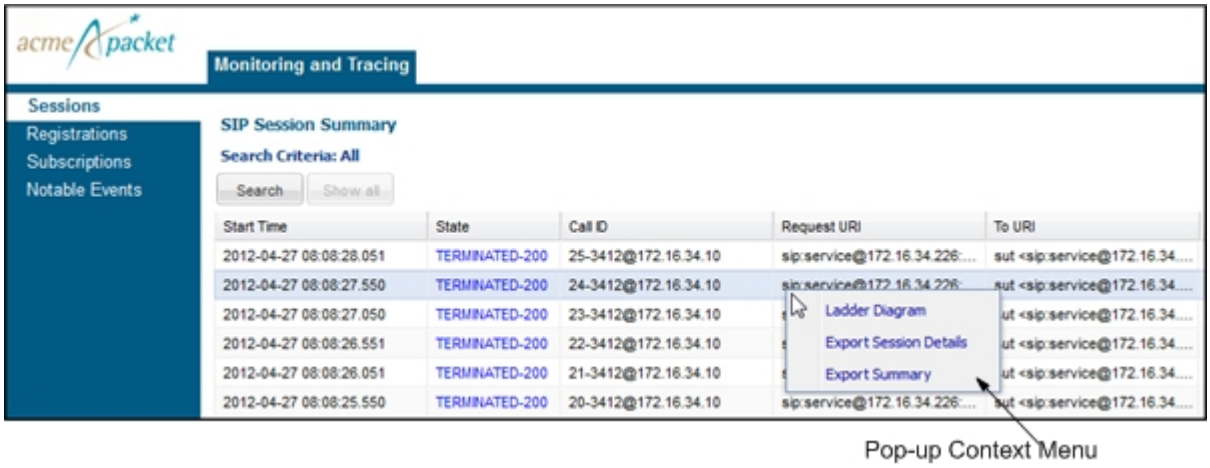


Pop-up Context Menu

The pop-up context menu feature allows you to select a specific record in the display and view its ladder diagram, export session details, or export session summary. All reports (Sessions, Registrations, Subscriptions, and Notable Events) support a pop-up context menu that you can use to select a Ladder diagram, Export Session Details, and Export Session Summary. You display the pop-up context menu by selecting a record and right clicking to show a menu.

To display the pop-up context menu in any report in Monitor and Trace:

1. Click on a record in the report page.



2. Right-click the mouse to display the pop-up context menu.
3. Drag the mouse to an option on the menu and left-click the mouse to select it.

   The applicable page displays or the export begins, depending on the option you selected (Ladder Diagram, Export Session Details, or Export Summary).

Configuration Tools

The Web GUI provides specific tools within the Configuration tab that you can use to enhance your experience in configuring the Net-Net ESD. The following paragraphs describe each of these tools.

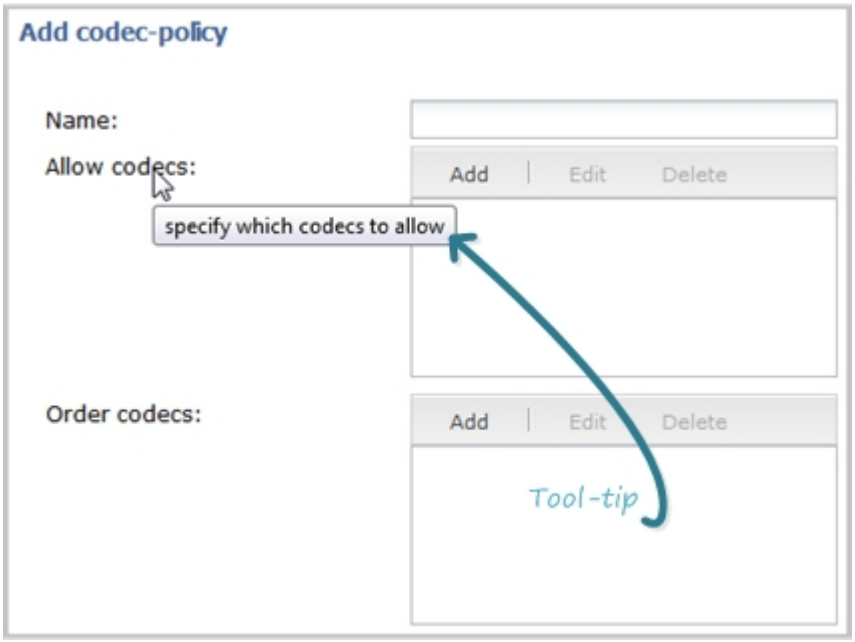
Tool Tips

A tool-tip is a brief description of a specific field on the configuration screens in the Web GUI. You can scroll over a field and display quick information about that field in a temporary pop-up box.

The tool-tip feature is available on the configuration tab in both Expert and Basic modes.

To view a tool-tip description:

1. On any configuration screen, scroll the mouse over the field title.



A box displays allowing you to view a brief description about the field. For example, in the above illustration, the tool-tip for the “Allow codecs” field is “specify which codecs to allow”. This tool-tip gives brief information for what you should be entering in this field. If a default exists for the field, the default value also displays.

2. To close the tool-tip, scroll off of the field. Or click at another location within the page.

2

Configuration

Introduction

This chapter provides information and procedures for configuring the NN-ESD. You can configure the parameters for the NN-ESD using either of two modes:

- Basic Mode - Recommended for most users. Allows you to configure the parameters of the NN-ESD using a graphical drag-and-drop method. You can configure basic or advanced parameters using this method. (
- Expert Mode - Recommended only for complex configuratons which are unique. Allows you to configure the parameters of the NN-ESD using a tree structure method. This method provides the minimum parameters required to configure the NN-ESD. You can access more advanced parameters from this mode if required.

The information in this chapter provides a general description of how to use the Basic and Expert Modes when configuring your network. It provides procedures for configuring a Enterprise Session Director in a basic network. It does not provide procedures for configuring advanced features on the Enterprise Session Director. For information about configuring advanced features and for parameter descriptions, refer to the *Net-Net® Enterprise Session Director Configuration Guide*.

Topics include:

- Workspace Tools
- Basic Mode
- Export Mode
- Error Messages

User and Administrator Access Rules

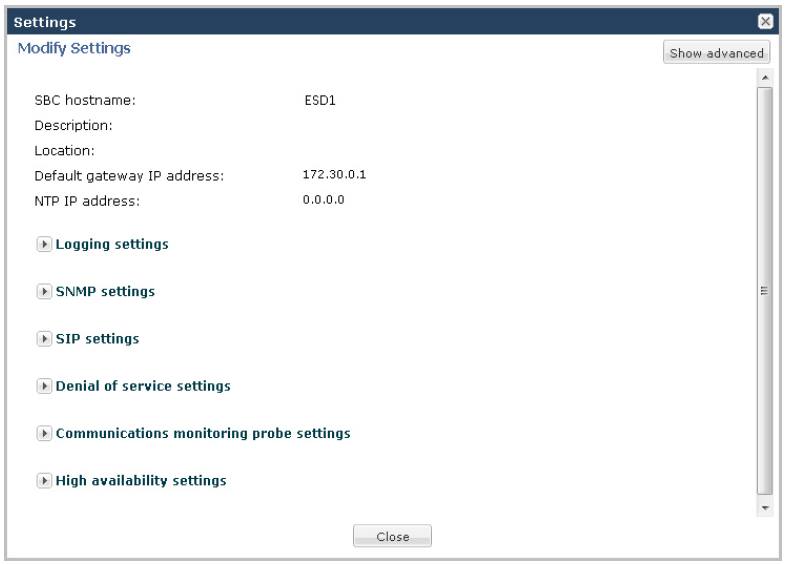
There are two types of users that can configure the Enterprise Session Director using the Web GUI - User and Administrator. For Basic and Expert configuration modes, there are access rules that apply to both a User and an Administrator. The following table identifies these rules.

Type	Rule
User	A user: Has view (read-only) access only. Can view basic and advanced configuration information. Does not have access to the Expert Mode.

Type	Rule
	Cannot save and activate configurations. Cannot add configurations. Cannot edit configurations.
Administrator	An Administrator: Can add, edit, and view configurations. Can add, edit, and view advanced configuration information. Can save and activate configurations. Can switch between Basic and Expert Modes (if both modes enabled). See Basic/Expert Switching Flow Chart for more information.

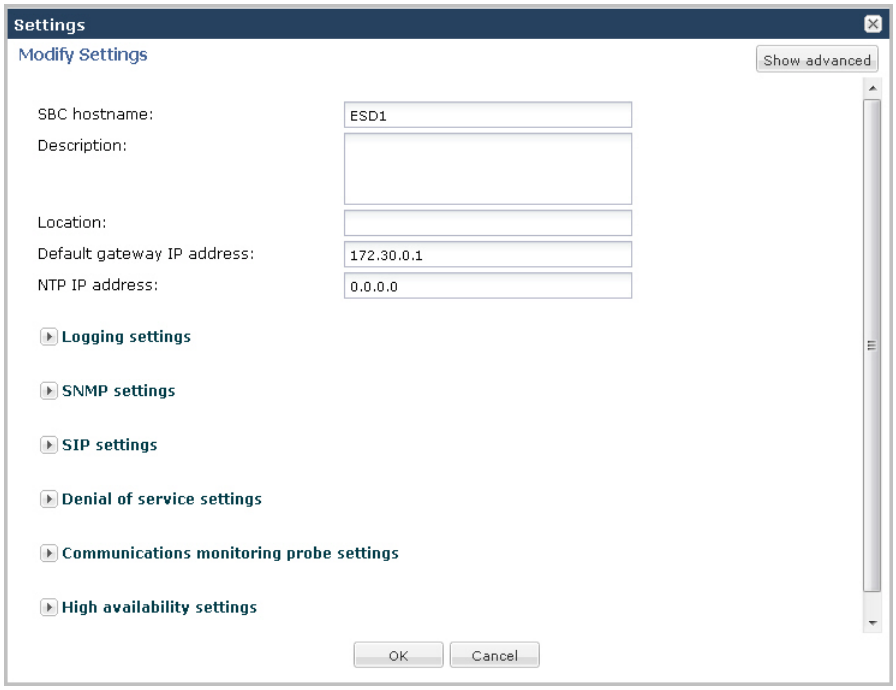
The following examples show a User view and an Administrator view of the global settings for the Enterprise Session Director.

Example of User View



A User can also view advanced configurations if applicable, by clicking the <Show advanced> button.

Example of Admin View



An Administrator can configure global settings and advanced settings.

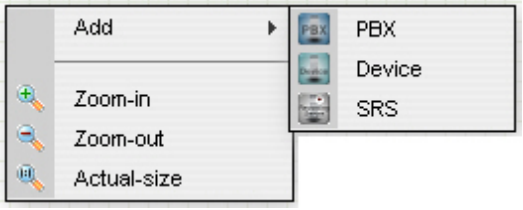
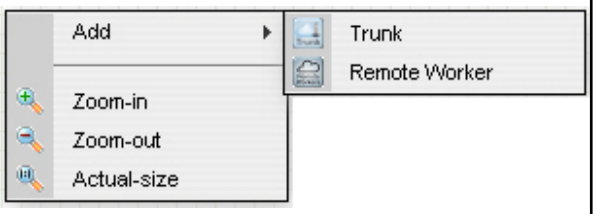
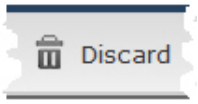
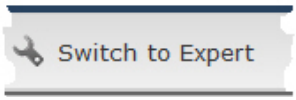
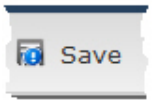
Workspace Tools

The Configuration tab provides specific workspace tools you can use within the Basic and Expert mode screens. These tools can help you manage the items in your workspace, provide an easy way to save and activate your configuration, and allow you to search for elements in your configuration if required.

The following tables identify the workspace tools for both Basic and Expert Modes.

Basic Mode Tools

Tool	Description
	Zoom-in: Used to increase the viewing size of the current window and all its contents.
	Zoom-out: Used to decrease the viewing size of the current window and all its contents.
	Actual size: Used to display the current window and all its contents on a one-on-one ratio (actual size).
	Print: Provides a view of the image that you can print from your browser.
Enterprise Add Menu	Add Menus - These menus can be accessed by right-clicking the mouse on the Enterprise side or the Service Provider side. **Add** > **PBX/Device/SRS**- Allows you to add a PBX, a Device, or a Session Recording Server (SRS) to your Enterprise configuration. You can use this menu in lieu of

Tool	Description
	dragging and dropping these elements from the Device tools.
Service Provider Add Menu 	**Add** > **Trunk/Remote Worker** Allows you to add a Trunk or a Remote Worker, to your Service Provider configuration. You can use this menu in lieu of dragging and dropping these elements from the Device tools. You can use the following tools from either menu instead of from the workspace tools in the upper right corner of the screen, if required: Zoom-in: Allows you to view a workspace and all of its elements in a closer proximity. Zoom-out: Allows you to view a workspace and all of its elements in a more distant proximity. Actual Size:: Allows you to view a workspace and all of its elements in its actual size.
	Edit/Delete Menu - This menu can be accessed by selecting an element on the screen and then right-clicking the mouse. Edit: Allows you to edit the configuration of the element on which you right-clicked. Delete: Allows you to remove the element from the workspace AND the configuration.
	Discard - Allows you to disregard all configuration changes made in the current session. Only the changes that have not yet been saved are discarded.
	Switch to Expert - (Displays only if Expert Mode enabled) Switches from Basic view to Expert view. Note: Before you can switch to Expert Mode, you must save AND activate your configuration in Basic Mode (or click <Discard> to discard your changes). You can then switch to Expert Mode. Expert Mode shows the configuration you entered during Basic Mode. Warning: FromExpert Mode, you can switch back to Basic Mode if you DO NOT save your changes. If you save your changes, and you still want to switch back to Basic Mode, you must initiate the run setup command in the ACLI again, but you will lose all the configuration changes you made in both modes.
	Save - Allows you to verify and save the current configuration in Basic Mode. A prompt also displays giving you a choice of whether or not to activate the configuration.

Tool	Description
Notifications Save changes	Note: After clicking <Save>, a notification icon in the upper right corner of the screen indicates the configuration still needs to be activated. You can continue to make changes to the configuration as required. When finished, you can select **Notifications** > **Save changes** to save and activate the configuration. The notification icon grays-out after saving and activating.
Show advanced	Show advanced - This button displays in configuration dialog boxes that allow for more advanced parameters to be displayed. Oracle recommends that only Administrators configure these advanced parameters. When clicking this button, the advanced parameters display in italics, and the button toggles to a Hide advanced button. Note: When configuring some advanced parameters, a field may be required but the Web GUI does not indicate it is required. You may be able to save the configuration even if you do not specify a value in the field. If you do not specify a field that is required, the Enterprise Session Director ignores the element in the configuration. No error message displays when you refrain from entering a required parameter.
Hide advanced	Hide advanced - This button displays in configuration dialog boxes that allow for more advanced parameters to be hidden. Oracle recommends that only Administrators configure these advanced parameters. When clicking this button, the advanced parameters are hidden from view, and the button toggles to a Show advanced button.

Expert Mode Tools

Tool	Description
Search	Search - Allows you to perform a search of any configuration element or sub-element on the Enterprise Session Director. You perform the search by entering a keyword which is not case sensitive. Special characters are allowed.
Switch to Basic	Switch to Basic - Switches from Expert view to Basic view. Note: If you save your configuration in Expert Mode, you cannot switch to Basic Mode. Warning: FromExpert Mode, you can switch back to Basic Mode if you DO NOT save your changes. If you save your changes, and you still want to switch back to Basic Mode, you must initiate the run setup command in the ACLI again, but you will lose all the configuration changes you made in both modes.
Save	Save - Allows you to verify and save the current configuration in Expert Mode. A prompt also displays

Tool	Description
Notifications Save changes	giving you a choice of whether or not to activate the configuration. Note: After clicking <Save>, a notification icon in the upper right corner of the screen indicates the configuration still needs to be activated. You can continue to make changes to the configuration as required. When finished, you can select Notifications->Save changes to save and activate the configuration. The notification icon grays-out after saving and activating.
Show advanced	Show Advanced - Allows you to show advanced sub-elements within the configuration tree of objects. Oracle recommends the advanced sub-elements be used by Administrators only. This link toggles the show/hide advanced parameters. Note: When configuring some advanced parameters, a field may be required but the Web GUI does not indicate it is required. You may be able to save the configuration even if you do not specify a value in the field. If you do not specify a field that is required, the Enterprise Session Director ignores the element in the configuration. No error message displays when you refrain from entering a required parameter.
Hide advanced	Hide Advanced - Allows you to hide advanced sub-elements within the configuration tree of objects. This link toggles the show/hide advanced parameters.

Basic Mode

The Basic mode of configuring the NN-ESD allows you to use a graphical drag-and-drop feature. In this mode, you can access basic and advanced parameters to set up your network configuration.

Note: It is recommended that only Administrators configure advanced parameters.

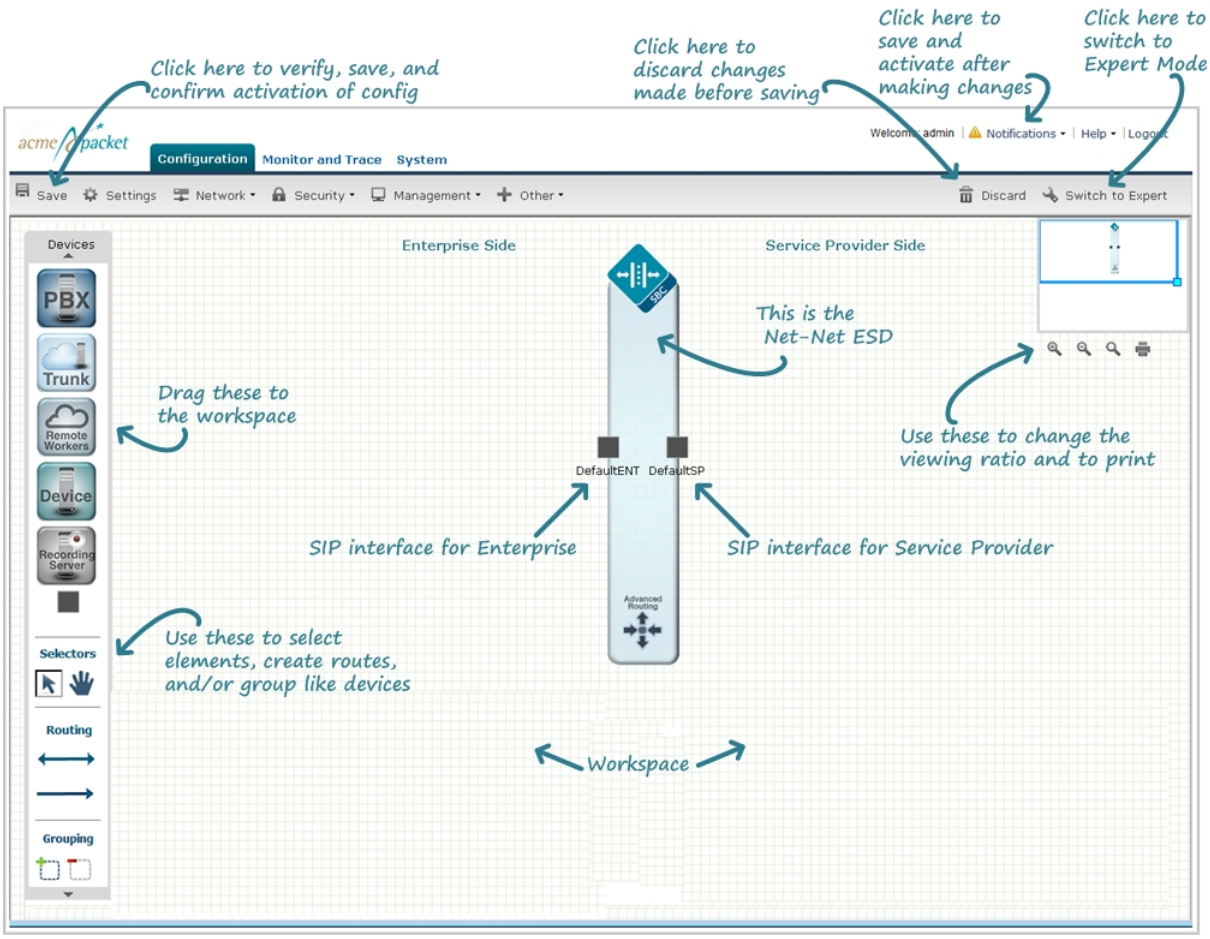
Accessing Basic Mode

You can access the Basic mode of configuration by clicking the Configuration tab in the Web GUI.

To access Basic mode:

After logging into the Web GUI, click on the Configuration tab. The following displays.

Note: If “Expert Mode” was set as the default during the Installation Setup Wizard in the ACLI, you cannot switch to Basic Mode. If you want to configure in Basic Mode, contact your Adminstrator.



This page displays the Basic method for configuring the Net-Net ESD. It displays a workspace you can use to configure your network. The Enterprise Session Director is centered in the middle between the Enterprise network on the left and the Service Provider network on the right.

To begin populating your network, you can use the Device tool bar on the left of the screen to drag and drop selected elements to the workspace. Elements in the toolbar are associated specifically with Enterprise or Service Provider. If you drag and drop an element to an incorrect location in the workspace, the following error message displays:

This icon cannot be placed here.

The following table identifies the Device toobar elements specific to the Enterprise and Service Provider, and provides a description for each element.

Device Toolbar

Element	Description
Elements for Enterprise	When adding any of the Enterprise elements below, a dialog box displays for you to configure the device.
	PBX - Drag-and-drop icon Adds a Private Branch Exchange (PBX) to your Enterprise network. A PBX is a privately owned telephone switching system for handling multiple telephone lines. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

Element	Description
	Device - Drag-and-drop icon Adds a network device (router, media device, phone, etc.) to your Enterprise network. A device can be any network device used to setup the Enterprise Local Area Network (LAN).
	Recording Server - Drag-and-drop icon Adds a session recording server (SRS) to your Enterprise network. An SRS is a 3rd party call recorder or the Net-Net ISR's Record and Store Server (RSS)). It controls the recording of media transmitted in the context of a communications session between multiple user agents.
	SIP Network Interface - Drag-and-drop icon Adds a Session Initiation Protocol (SIP) network interface to the Enterprise side of the Enterprise Session Director. You can add up to five (5) SIP interfaces. **Note:** You can associate a SIP interface to any configured network interface.
Elements for Service Provider	When adding any of the Service Provider elements below, a dialog box displays for you to configure the device.
	Trunk - Drag-and-drop icon Adds a SIP Trunk to the Service Provider network. A SIP trunk is a service offered to Enterprises by a Service Provider that permits the Enterprises with PBXs installed, to use IP communications (including Voice over IP (VoIP)) outside of their Enterprise network on an Internet connection.
	Remote Worker - Drag-and-drop icon Adds a Remote Worker to the Service Provider network. A Remote Worker is a device that is setup outside the network but is still connected to the Enterprise Session Director from the remote location.
	SIP Network Interface - Drag-and-drop icon Adds a SIP network interface to the Service Provider side of the Enterprise Session Director. You can add up to five (5) SIP interfaces. **Note:** You can associate a SIP interface with any configured network interface.
Elements for Both	
	Selection Tool - Select this then click on any element in your workspace. This tool allows you to select any element in your network.
	Image Mover - Select this then click on the image in your workspace. This tool allows you to move the entire image of your network around within the workspace.

Element	Description
	Two-Way Local Policy - Select this first then click on the center of an icon in your network. This tool allows you to create a two-way route (local policy) between devices within your local network, or between the devices on the Enterprise side and the Service Provider side. When adding a two-way route, a dialog box displays for you to configure the route.
	One-Way Local Policy - Select this first then click on the center of an icon in your network. This tool allows you to create a one-way route between devices within your local network, or between the devices on the Enterprise side and the Service Provider side. When adding a one-way route, a dialog box displays for you to configure the route.
	Grouping Tool - Select the devices in your network that you want to group, then select the grouping tool. This tool allows you to create a grouping around like devices in your network (i.e., multiple PBXs, multiple routers, etc.). When creating a group, a dialog box displays for you to configure the group.
	Ungrouping Tool - Select the group you want to ungroup first, then select the ungrouping tool to ungroup the devices. This tool allows you to remove a grouping from around like devices in your network (i.e., multiple PBXs, multiple routers, etc.). When removing a group, the group configuration information is removed (not the device configurations within the group).

As you place an element in the workspace, the element connects to the SIP interface on the Enterprise Session Director automatically, and a configuration dialog box displays allowing you to configure the element for your network.

You can use the workspace tools on the upper right corner of the screen to zoom in, zoom out, display actual size, or print the current screen.

Note: For more information about the workspace tools, see Workspace Tools.

Icon Connections Supported

The Enterprise and Service Provider icons can be connected in two ways - either using a one-way local policy route or a two-way local policy route. Specific icons can connect when using advanced routing as well. The following table indicates the icons that you can connect via a one-way or two-way local policy, and the icons that are applicable to advanced routing.

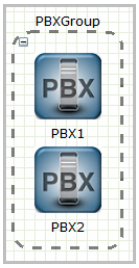
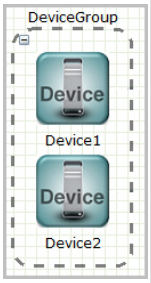
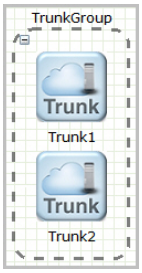
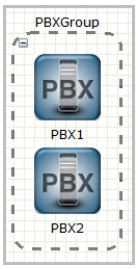
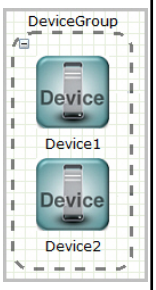
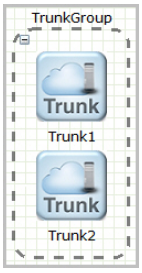
One-way Local Policy

From	To

	PBX	PBXGroup (PBX1, PBX2)	Device	DeviceGroup (Device1, Device2)	Trunk	TrunkGroup (Trunk1, Trunk2)	Remote Workers
PBX	Yes	Yes	Yes	Yes	Yes	Yes	No
PBXGroup (PBX1, PBX2)	Yes	Yes	Yes	Yes	Yes	Yes	No
Device	Yes	Yes	Yes	Yes	Yes	Yes	No
DeviceGroup (Device1, Device2)	Yes	Yes	Yes	Yes	Yes	Yes	No
Trunk	Yes	Yes	Yes	Yes	No	No	No
TrunkGroup (Trunk1, Trunk2)	Yes	Yes	Yes	Yes	No	No	No
Remote Workers	Yes	Yes	Yes	Yes	No	No	No

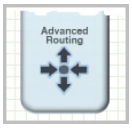
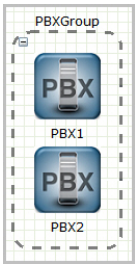
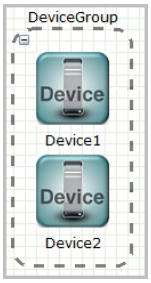
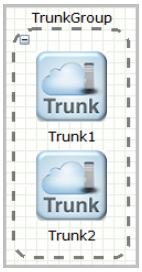
Two-way Local Policy

From	To

							
	Yes	Yes	Yes	Yes	Yes	Yes	No
	Yes	Yes	Yes	Yes	Yes	Yes	No
	Yes	Yes	Yes	Yes	Yes	Yes	No
	Yes	Yes	Yes	Yes	Yes	Yes	No
	Yes	Yes	Yes	Yes	No	No	No
	Yes	Yes	Yes	Yes	No	No	No
	No	No	No	No	No	No	No

Advanced Routing Local Policy

From	To

	
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes

Setting Up a Typical Network

You can quickly and easily setup your network using the Basic Mode method to configure the devices. Use this procedure to setup your typical network.

Note: You must drag-and-drop the devices from the Device tool bar into the space below the titles of “Enterprise Side” and/or Service Provider Side. The application does not allow you to place icons above the titles.

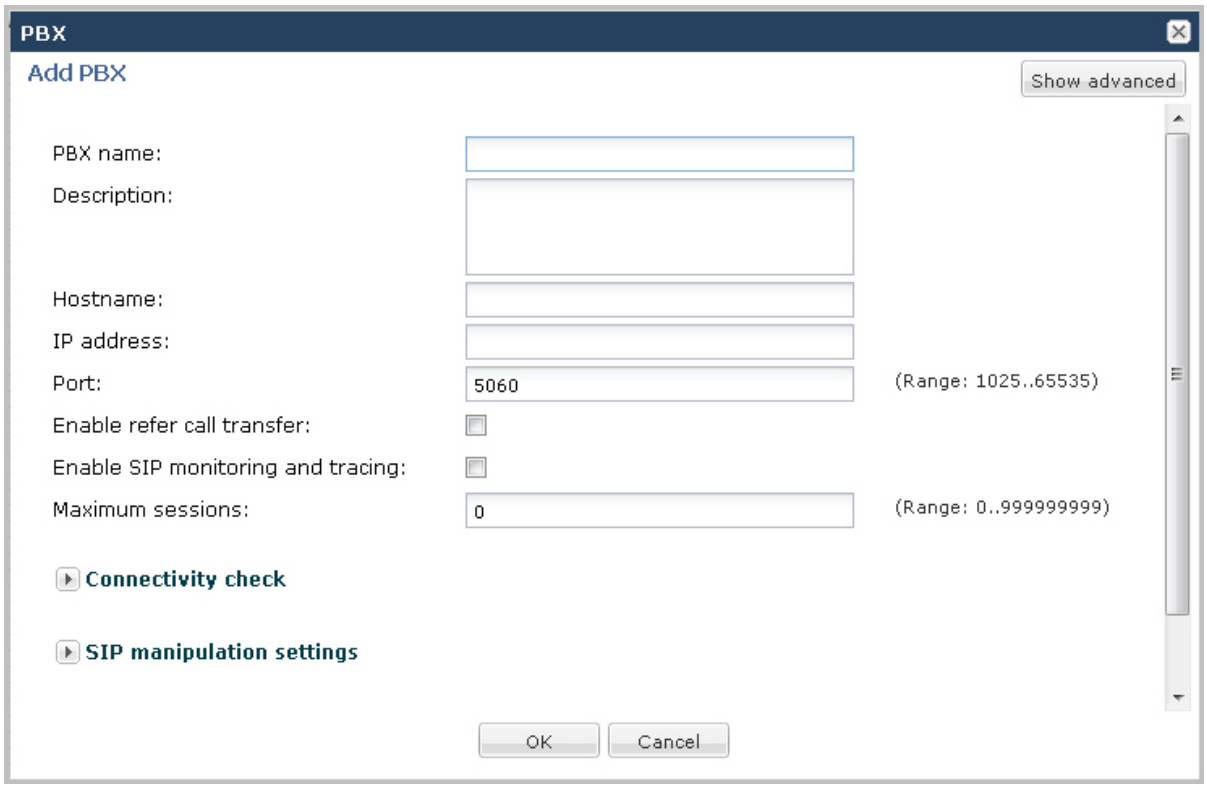
To setup your network, you perform the following:

- Add a PBX to the Enterprise Side
- Add a SIP Trunk to the Service Provider Side
- Add a Local Policy (2-way route) between the PBX and the SIP Trunk
- Verify the Network Interface on the Enterprise Session Director is correct on the Enterprise and Service Provider sides

Add a PBX

To add a PBX to the Enterprise side:

1. Click on the PBX icon in the device tool bar, and drag it to the Enterprise side in the workspace. The following dialog box displays.



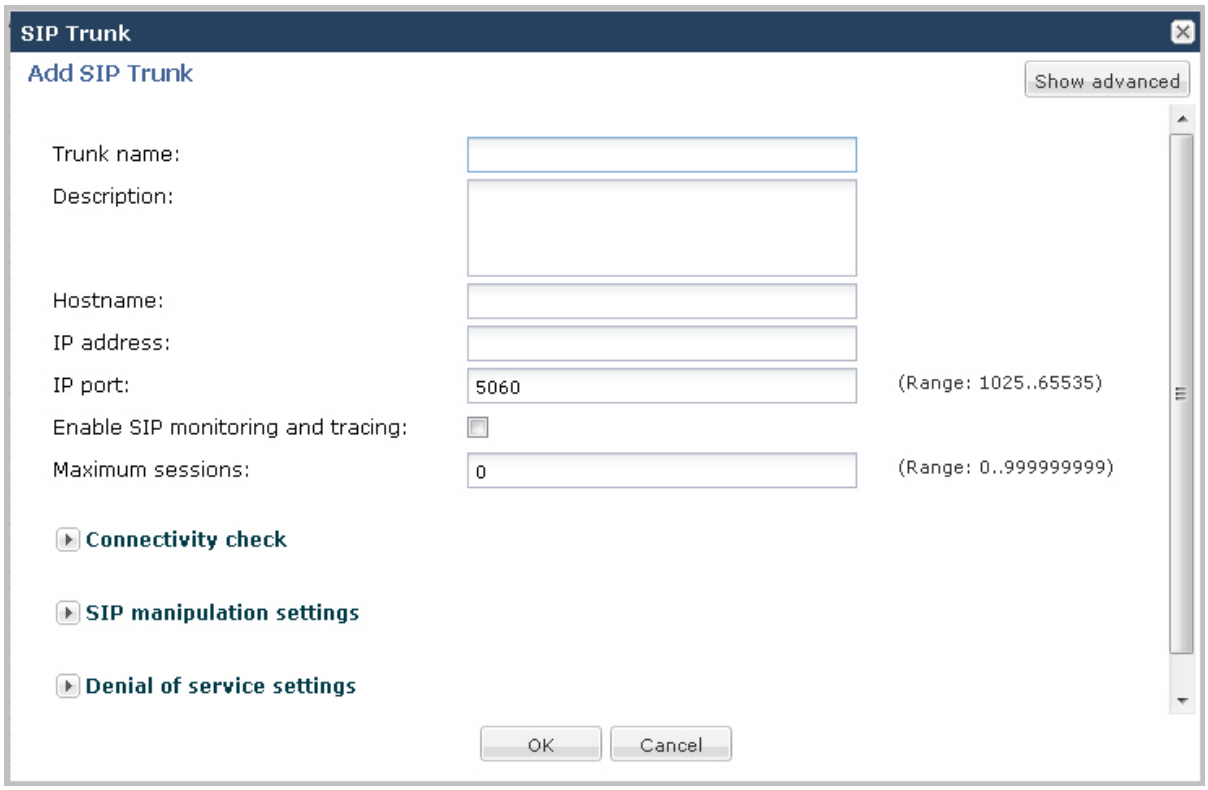
2. In the PBX name field, enter the name to assign to this PBX in the Enterprise network. For example, PBX1. Valid values are alpha-numeric characters.
3. (optional) In the Description field, enter a description for this PBX. For example, PBX for Enterprise. Valid values are alpha-numeric characters.
4. In the Hostname field, enter the hostname of the Enterprise Session Director to which this PBX is connected. For example, ESD1. Valid values are alpha-numeric characters.
5. (optional) In the IP address field, enter the IP address of this PBX. Enter the address in dotted decimal format. For example, 1.1.1.1. Default is 0.0.0.0.

   Note: By default, the Port on the PBX is 5060. Also, setting all other parameters in this dialog box is optional. If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the *Net-Net® Enterprise Session Director Configuration Guide* for more information. Oracle recommends that only Administrators add or modify adavanced parameters.
6. Click <OK> to save your settings. The PBX displays in your Enterprise workspace with the name of the PBX displayed beneath the icon. You can edit the PBX configuration anytime if required, by double-clicking the icon and modifying the configuration in the dialog box.

Add a Trunk

To add a SIP Trunk to the Service Provider side:

1. Click on the Trunk icon in the device tool bar, and drag it to the Service Provider side in the workspace. The following dialog box displays.



2. In the Trunk name field, enter the name to assign to this SIP Trunk in the Service Provider network. For example, TrunkA. Valid values are alpha-numeric characters.
3. (optional) In the Description field, enter a description for this SIP Trunk. For example, Trunk between SP and Ent. Valid values are alpha-numeric characters.
4. In the Hostname field, enter the hostname of the Enterprise Session Director to which this Trunk is connected. For example, ESD1. Valid values are alpha-numeric characters.
5. (optional) In the IP address field, enter the IP address of this SIP Trunk. Enter the address in dotted decimal format. For example, 2.2.2.2. Default is 0.0.0.0.

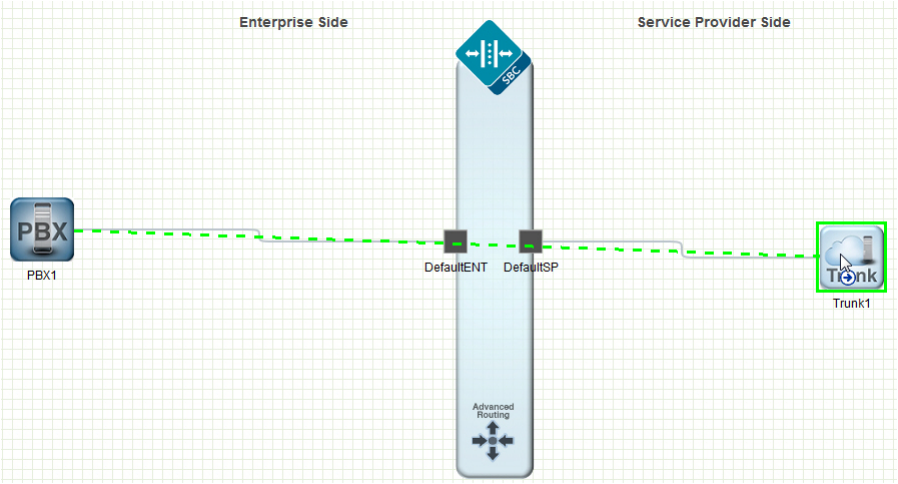
   Note: By default, the IP Port on the SIP Trunk is 5060. Setting all other parameters in this dialog box is optional. If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the *Net-Net® Enterprise Session Director Configuration Guide* for more information. Oracle recommends that only Administrators add or modify advanced parameters.
6. Click <OK> to save your settings. The Trunk displays in your Enterprise workspace with the name of the Trunk displayed beneath the icon. You can edit the Trunk configuration anytime if required, by double-clicking the icon and modifying the configuration in the dialog box.

Add a Local Policy

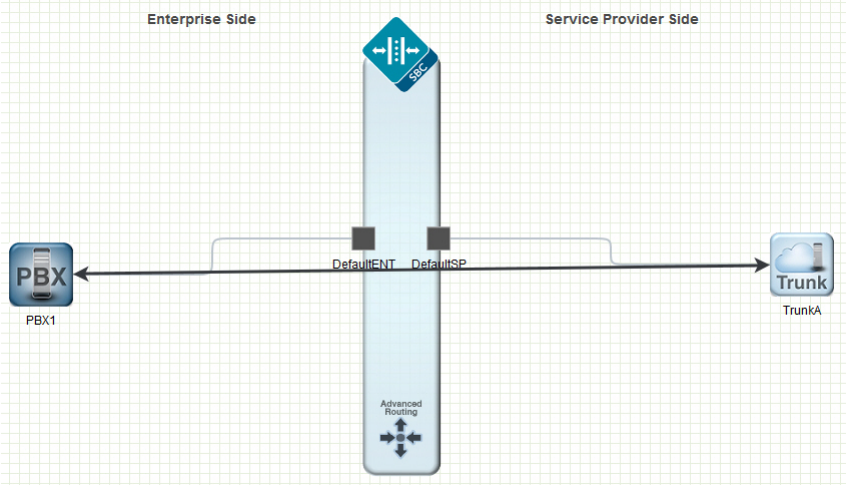
To add a Local Policy (2-way route) between the PBX and the SIP Trunk:

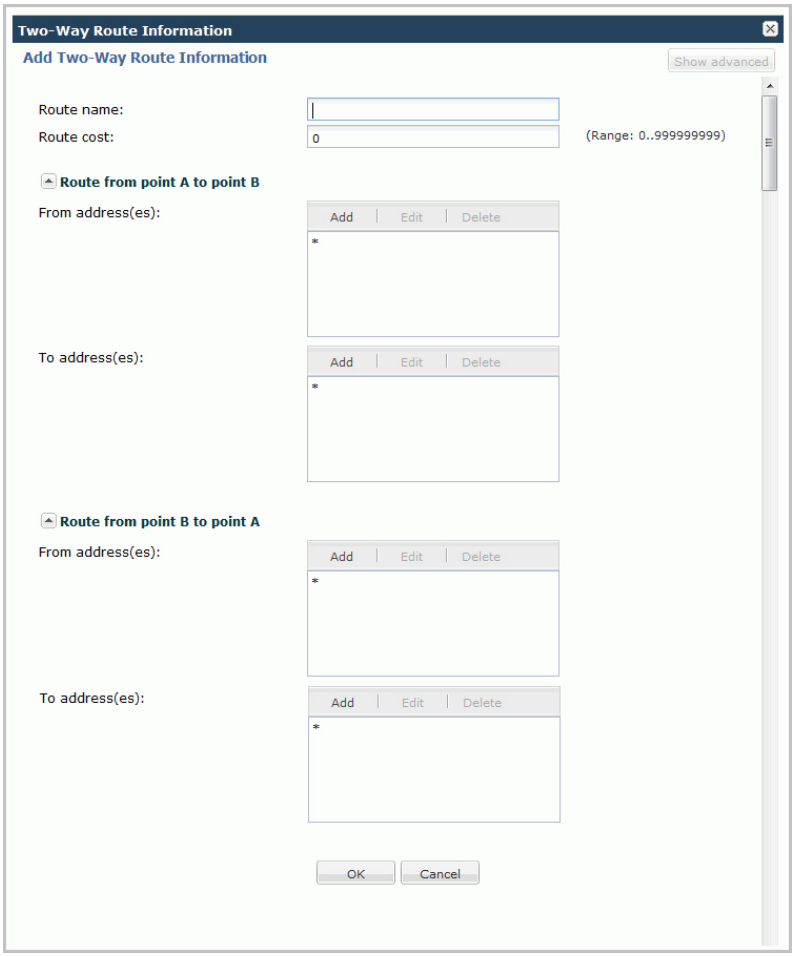
1. In the connectors section of the device tool bar, click on the 2-way arrow to select it.
2. Click in the center of the PBX icon in the Enterprise network. A small arrow displays.

3. Holding down the left mouse button, drag the mouse over to the Trunk icon, making sure a green border appears around the Trunk icon.



4. Release the left mouse button. This draws a 2-way arrow (local-policy) between the PBX and the Trunk. A dialog box displays.





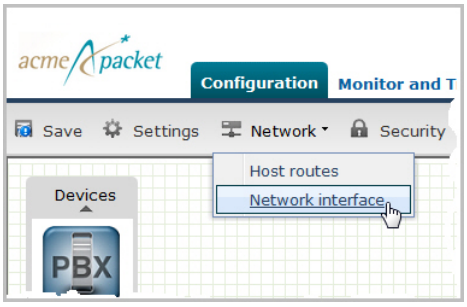
5. In the Route name field, enter a name for this route. For example, RouteA.
6. Click <OK>. You can edit the local policy configuration anytime if required, by double-clicking the 2-way arrow and modifying the configuration in the dialog box.

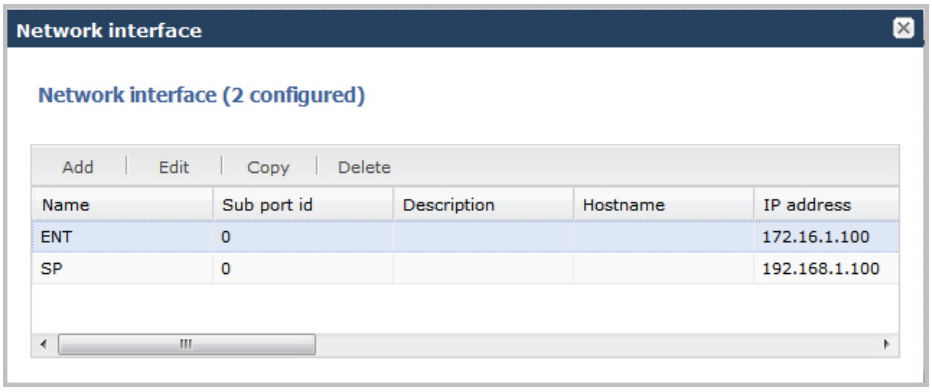
Note: If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the Net-Net® Enterprise Session Director Configuration Guide for more information. Acme Packet recommends that only Administrators add or modify advanced parameters.

Modify Enterprise Network Interface

To modify the Enterprise network interface:

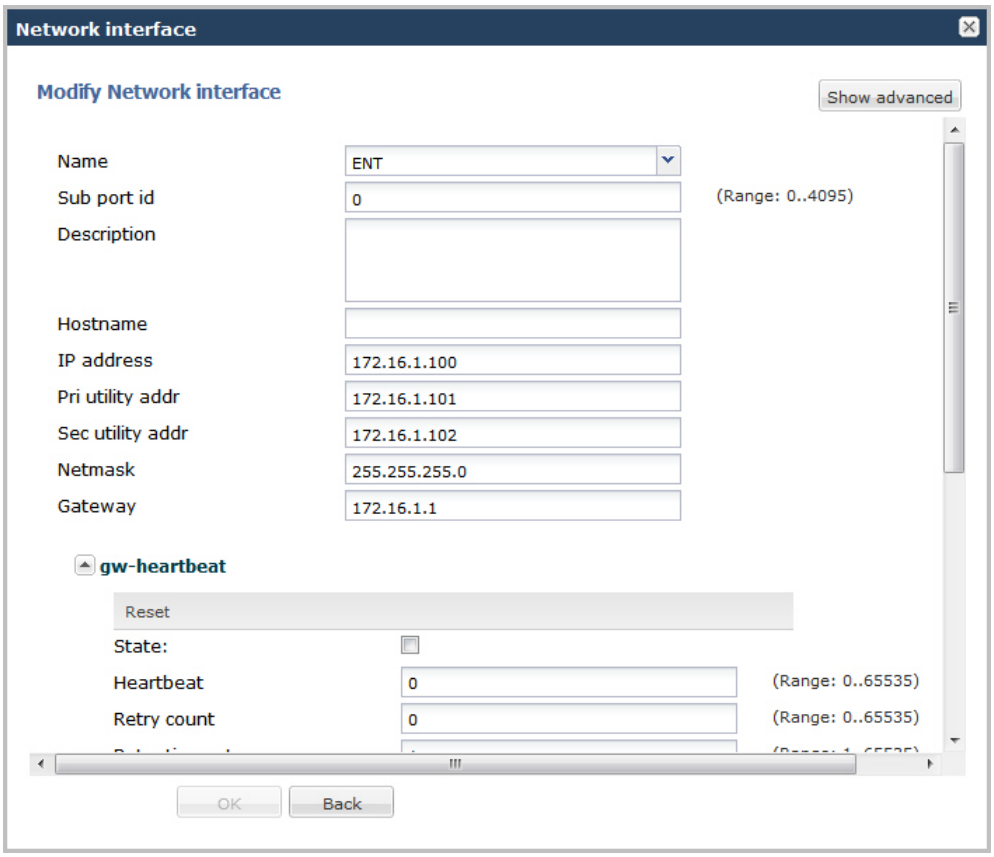
1. From the Main Menu, select **Network** > **Network interface**. The following dialog box displays.





The list in the above dialog box shows the current default settings.

2. From the list of network interfaces, select ENT (Enterprise) and click <Edit>. The following dialog box displays.



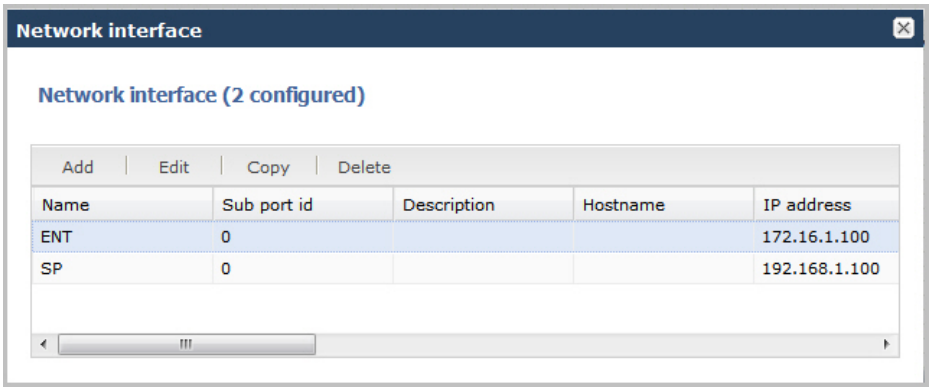
3. In the IP address field, enter the IP address of the network interface on the Enterprise side. Enter the address in dotted decimal format. Default is 172.16.1.100.
4. In the Netmask field, enter the netmask address of the network interface on the Enterprise side. Enter the address in dotted decimal format. Default is 255.255.255.0.
5. In the Gateway field, enter the IP address of the gateway associated with the network interface on the Enterprise side. Enter the address in dotted decimal format. Default is 172.16.1.1.

   For a High Availibility (HA) environment:

6. In the Pri utility address field, enter the IP address of the primary Enterprise Session Director. Enter the address in dotted decimal format. Default is 172.16.1.101.
7. In the Sec utility address field, enter the IP address of the secondary (backup) Enterprise Session Director. Enter the address in dotted decimal format. Default is 172.16.1.102.

Note: If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the *Net-Net® Enterprise Session Director Configuration Guide* for more information. Oracle recommends that only Administrators add or modify advanced parameters.

8. Click <OK> to save the changes. The following dialog box displays.

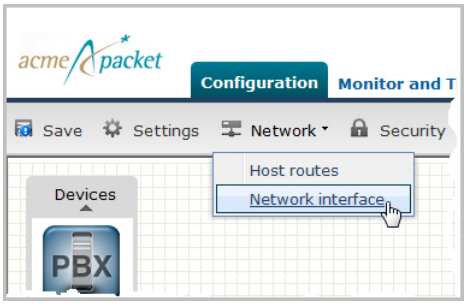


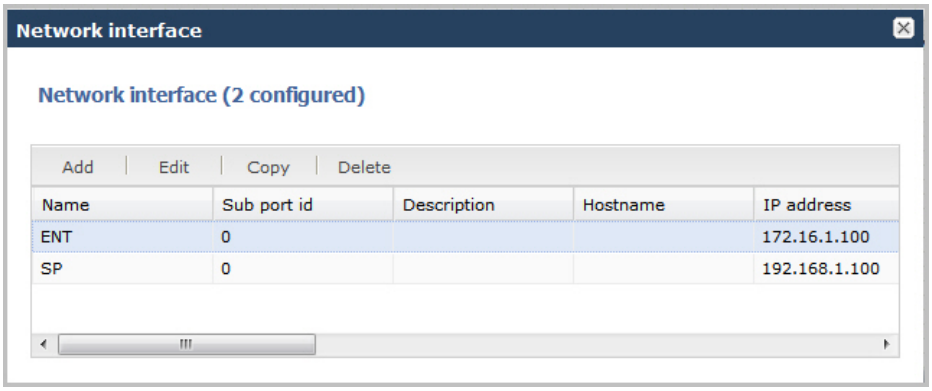
9. Modify the Service Provider network address using the procedure in Modify Service Provider Network Interface.

Modify Service Provider Network Interface

To modify the Service Provider network interface:

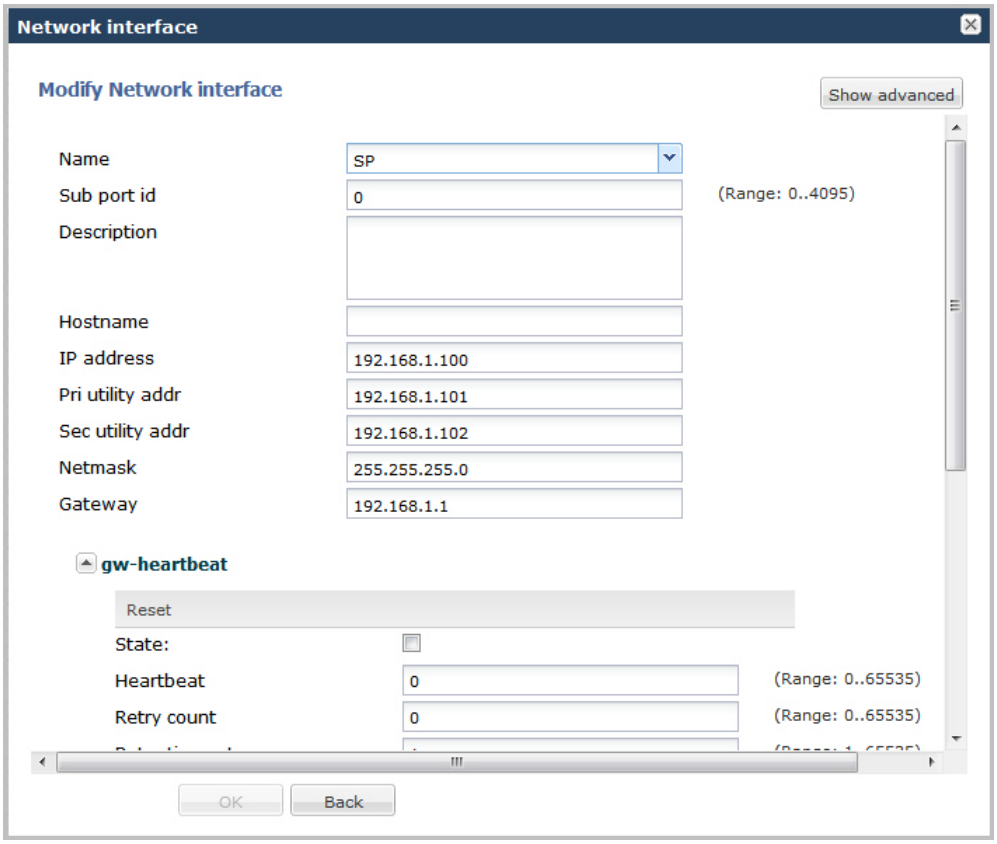
1. From the Main Menu, select **Network** > **Network interface** . The following dialog box displays.





The list in the above dialog box shows the current default settings.

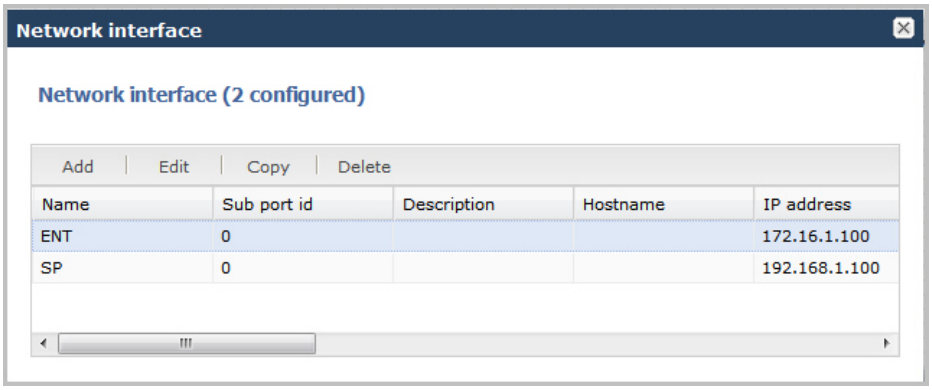
2. From the list of network interfaces, select SP (Service Provider) and click <Edit>. The following dialog box displays.



3. In the IP address field, enter the IP address of the network interface on the Service Provider side. Enter the address in dotted decimal format. Default is 192.168.1.100.
4. In the Netmask field, enter the netmask address of the network interface on the Service Provider side. Enter the address in dotted decimal format. Default is 255.255.255.0.
5. In the Gateway field, enter the IP address of the gateway associated with the network interface on the Service Provider side. Enter the address in dotted decimal format. Default is 192.168.1.1.

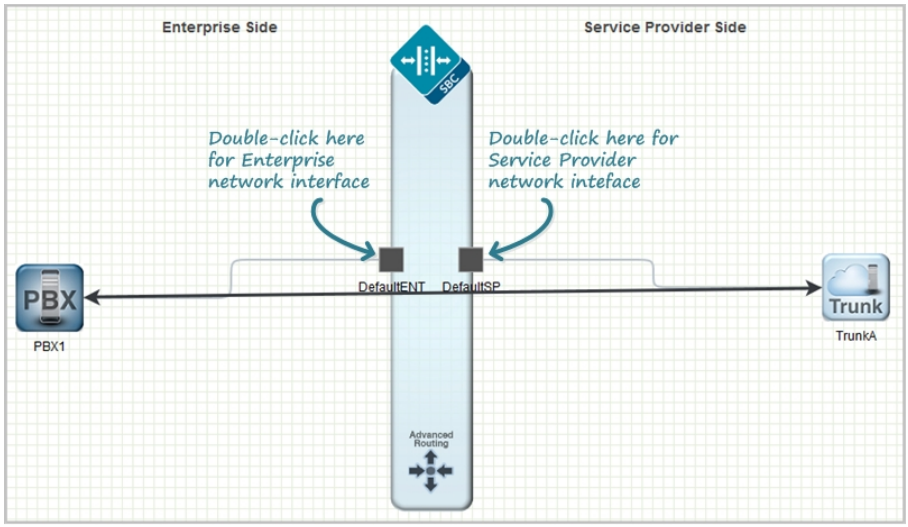
   For a High Availibility (HA) environment:
6. In the Pri utility address field, enter the IP address of the primary Enterprise Session Director. Enter the address in dotted decimal format. Default is 192.168.1.101.
7. In the Sec utility address field, enter the IP address of the secondary (backup) Enterprise Session Director. Enter the address in dotted decimal format. Default is 192.168.1.102.

   Note: If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the *Net-Net® Enterprise Session Director Configuration Guide* for more information. Oracle recommends that only Administrators add or modify advanced parameters.
8. Click <OK> to save the changes. The following dialog box displays.



9. Click the x in the upper right corner to close this dialog box.

Note: You can modify additional parameters if required, for the Enterprise and Service Provider network interfaces by clicking on the network interface icons on the Enterprise Session Director. For more information on setting advanced parameters, see your *Net-Net® Enterprise Session Director Configuration Guide.*



Save and Activate Network Configuration

When you have completed creating your network, the Save button allows you to verify, save, and activate the configuration on the Enterprise Session Director. Clicking <Save> verifies and saves the current configuration to the Enterprise Session Director's last-saved configuration, stored in flash memory. It also displays a prompt that allows you to activate the configurationas the running configuration if required.

A notification icon displays grayed-out in the upper right corner of the screen. After clicking <Save>, the Notifications menu becomes active. This menu will remain active allowing you to continue making changes to the configuration, and when you are ready to save and activate the configuration, you can select **Notifications** > **Save Changes** and then choose to activate the configuration.

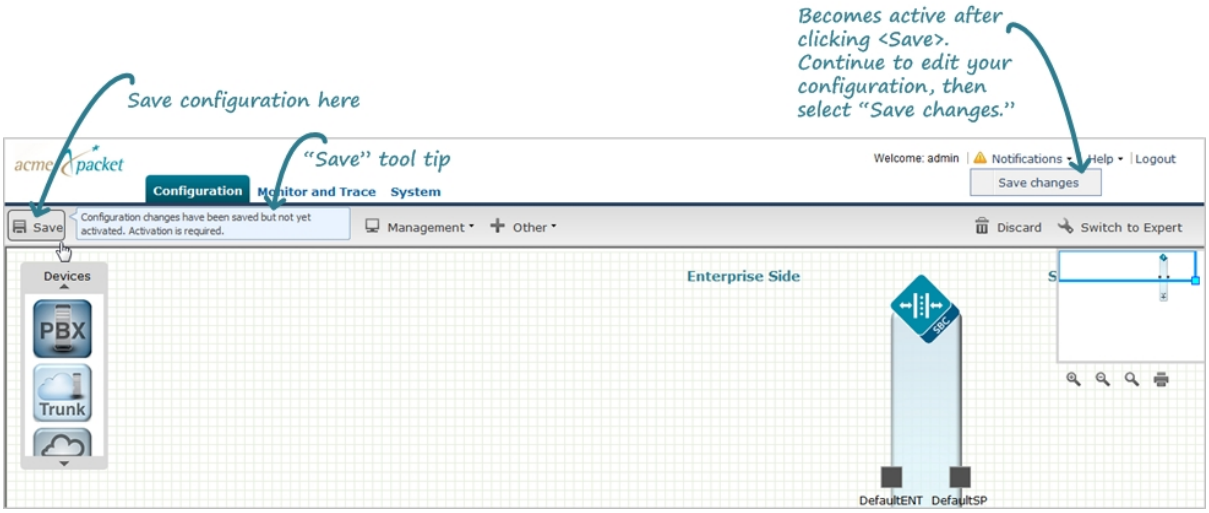
To save your Enterprise Session Director configuration:

1. Click <Save> to verify and save your configuration. This saves the current configuration to the Enterprise Session Director's last-saved configuration, stored in flash memory.

   Note: Placing the pointer over the <Save> button displays the following tool tip: Configuration changes have been made but not yet activated. Activation is required.

   The following prompt displays: Do you want to activate the configuration?

2. Click <Activate> to activate the current configuration in Basic Mode and make it the running configuration. Or click <Cancel> to cancel the activate function. The configuration is still saved in memory. If you click <Cancel>, you can continue to make changes to the configuration. After you clicked <Save> in Step 1, a notification icon became active in the upper right corner of the screen. When you complete your changes, you can then select **Notifications** > **Save changes** from this notification menu and then activate your configuration.



You have completed a basic Enterprise Session Director configuration. Your network is ready to use and you can begin sending/receiving calls.

Other Basic Mode Functions

In Basic Mode, you can also configure specific features on your Net-Net ESD. This section provides a description and procedures for configuring the following features:

- Global Settings
- Host Routes
- Security
- Management Settings
- Global Settings
- Additional Features

For more information about the features in this section, and for a description of the parameters, see the *Net-Net® Enterprise Session Director Configuration Guide*.

Note: When configuring some advanced parameters, a field may be required but the Web GUI does not indicate it is required. You may be able to save the configuration even if you do not specify a value in the field. If you do not specify a field that is required, the Enterprise Session Director ignores the element in the configuration. No error message displays when you refrain from entering a required parameter.

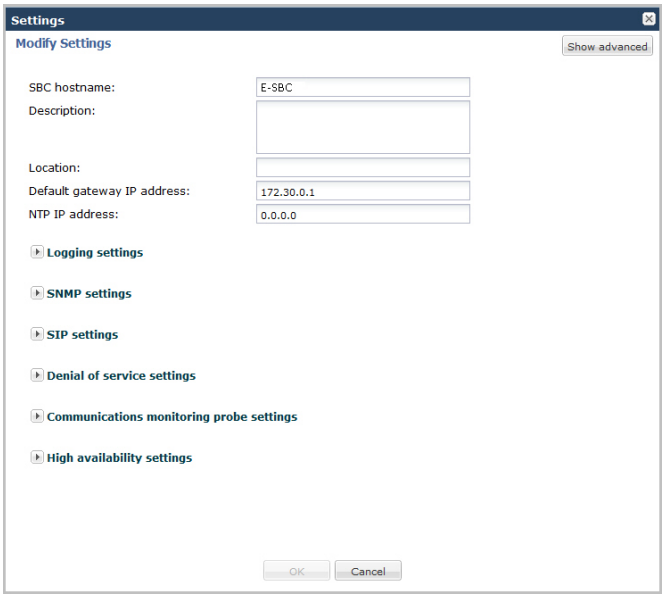
Global Settings

You can set specific global settings on your Enterprise Session Director on the Enterprise side, if required. Global settings include configuring:

- SBC hostname
- Description
- Location
- Default gateway IP address
- Network Time Protocol IP address

To configure global settings:

1. Click on Settings in the Main Menu. The following dialog box displays.



Note: The SBC hostname, Description (optional), and Default gateway IP address fields were automatically populated when you configured the Enterprise side network interface.

2. In the SBC hostname, Description, and Default gateway IP address fields, modify the values if required.
3. In the Location field, enter a geographical location of your Enterprise network. Valid values are alpha-numeric characters. For example, Boston. Default is blank.
4. In the NTP IP address field, enter the IP address of your Network Time Protocol (NTP) server. For example, 172.30.1.4. Default is 0.0.0.0.
5. Click <OK>.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Enable restart on critical failure

For more information on this setting, see Initiating Packet Capture in the *Net-Net® Enterprise Session Director Configuration Guide*.

Additional Global Settings

You can set the following additional global settings on the Enterprise Session Director if required:

- Logging
- SNMP
- SIP
- Denial of service (DoS)
- Communication Monitor Probe
- High Availability (HA)

Each of these global settings is described in the following paragraphs.

Logging Settings

The Enterprise Session Director generates two types of logs - syslogs and process logs. Syslogs conform to the standard used for logging servers and processes as defined in RFC 3164.

Process logs are Oracle proprietary logs. Process logs are generated on a pertask basis and are used mainly for debugging purposes. Because process logs are more data inclusive than syslogs, their contents usually encompass syslog log data. A special application must be run on a remote server to receive process logs. Please contact your

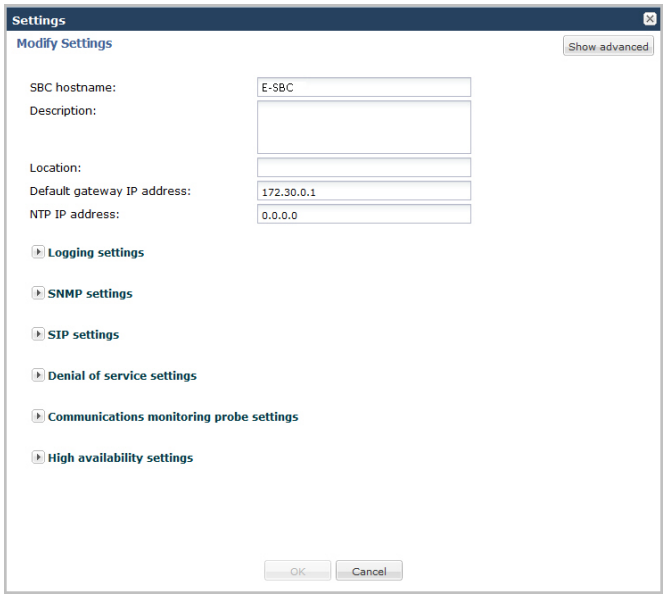
Oracle sales representative directly or through email at support@acmepacket.com for more information about the process log application.

Syslog and process log servers are both identified by an IPv4 address and port pair.

For more information about logging, see the section, Syslog and Process Logs Configuration in the *Net-Net® Enterprise Session Director Configuration Guide*.

To set logging on the Enterprise Session Director:

1. Click on Settings in the Main Menu. The following dialog box displays.



2. Click on Logging settings to expand the dialog box. The following displays.

3. In the SysLog server IP address field, enter the IPv4 address of a syslog server. Enter the address in dotted-decimal format. For example, 134.5.4.3. Default is blank.
4. In the Process log level field, select the starting log level of all processes running on the Enterprise Session Director. Each individual process running on the system has its own process log. Default is NOTICE. Valid values are:

CRITICAL	INFO
MINOR	TRACE
WARNING	BUG
NOTICE (default)	

5. Click <OK>.

SNMP Settings

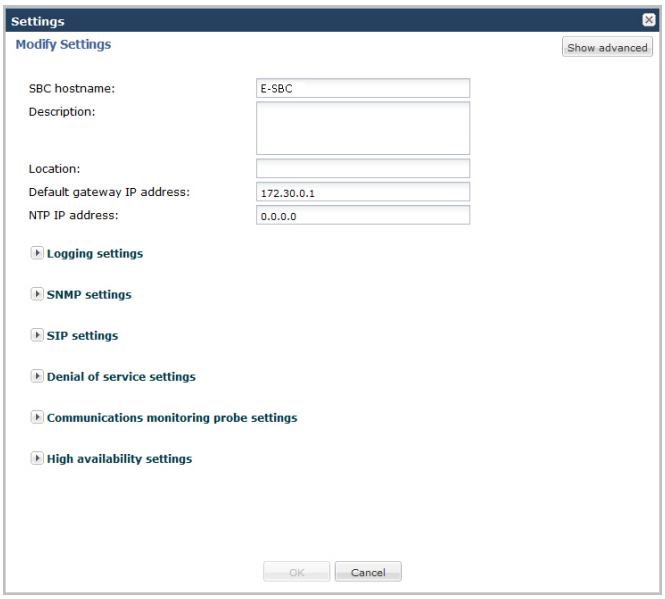
Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP is used to support monitoring of network-attached devices for conditions that warrant administrative attention. SNMP is comprised of three groups of settings on the Enterprise Session Director. These settings are system-wide configurations including MIB contact information, SNMP community settings, and trap receivers.

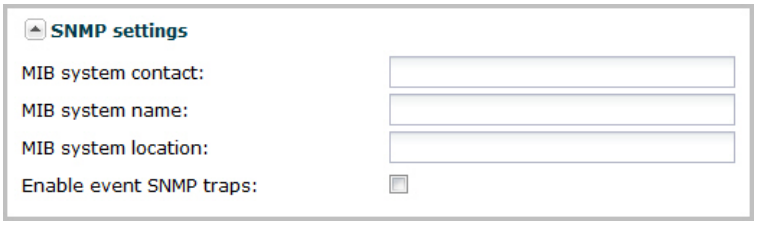
For more information about SNMP, see the section, SNMP in the *Net-Net® Enterprise Session Director Configuration Guide*.

To set SNMP on the Enterprise Session Director:

1. Click on Settings in the Main Menu. The following dialog box displays.



2. Click on SNMP settings to expand the dialog box. The following displays.



3. In the MIB system contact field, enter the contact information used within the Enterprise Session Director's MIB transactions. The SNMP agent sends this information to a Network Management System (NMS) in response to an SNMP Get for the MIB-II sysContact MIB variable. This parameter's value can be a textual identification of your company's contact person for the Enterprise Session Director and/or information about how to contact that person. For example, John Doe. Valid values are alpha-numeric characters. Default is blank.
4. In the MIB system name field, enter the identification of this Enterprise Session Director presented within MIB transactions. This value, along with the target name of the Enterprise Session Director (identified in the boot parameters) are the values reported for MIB-II when an SNMP GET is issued by the NMS for the MIB-II sysName variable. For example. Test System: This parameter has no direct relation to the hostname parameter in the system configuration element. By convention, this is the node's FQDN. For SNMP MIB-II sysName GETs, the Enterprise Session Director returns SNMP communications in the following format:

   ```
   <targetName>[.<mib-system-name>]"
   ```

   The "targetName" is the value configured in the target name (tn) boot parameter and mib-system-name is the value configured in this field.

   Valid values are alpha-numeric characters. Default is blank.
5. In the MIB system location field, enter the physical location of this Enterprise Session Director that is reported within MIB transactions. This parameter is reported when an SNMP GET is issued by the NMS for the MIB-II

sysLocation variable. This parameter has no direct relation to the location field in the system configuration element. For example, Oracle. Valid values are alpha-numeric characters. Default is blank.

6. In the Enable event SNMP traps field, place a checkmark in the box to enable the Enterprise Session Director to report event SNMP traps. Uncheck to the box to disable this feature. Default is disabled.
7. Click <OK>.

SIP Settings

Session Initiation Protocol (SIP) is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions. Sessions may consist of one or several media streams.

Dialog Transparency

Dialog transparency prevents the Enterprise Session Director from generating a unique Call-ID and modifying dialog tags. With dialog transparency enabled, the Enterprise Session Director is prevented from generating a unique Call-ID and from modifying the dialog tags; the Enterprise Session Director passes what it receives. Therefore, when a call made on one Enterprise Session Director is transferred to another UA and crosses a second Enterprise Session Director, the second Enterprise Session Director does not note the context of the original dialog, and the original call identifiers are preserved end to end. The signalling presented to each endpoint remains in the appropriate context regardless of how many times a call crosses through a Enterprise Session Director or how many Enterprise Session Directors a call crosses.

Without dialog transparency enabled, the Enterprise Session Director's SIP B2BUA rewrites the Call-ID header and inserted dialog cookies into the From and To tags of all messages it processes. These dialog cookies are in the following format: SDxxxxxNN-. Using these cookies, the Enterprise Session Director can recognize the direction of a dialog. However, this behavior makes call transfers problematic because one Enterprise Session Directors' Call-ID might not be properly decoded by another Enterprise Session Director. The result is asymmetric header manipulation and failed call transfers.

IPv6 Reassembly and Fragmentation Support

As it does for IPv4, the Enterprise Session Director supports reassembly and fragmentation for large signaling packets when you enable IPV6 on your system.

The Enterprise Session Director takes incoming fragments and stores them until it receives the first fragment containing a Layer 4 header. With that header information, the Enterprise Session Director performs a look-up so it can forward the packets to its application layer. Then the packets are re-assembled at the applications layer. Media fragments, however, are not reassembled and are instead forwarded to the egress interface.

On the egress side, the Enterprise Session Director takes large signaling messages and encodes it into fragment datagrams before it transmits them.

Note that large SIP INVITE messages should be sent over TCP. If you want to modify that behavior, you can use the SIP interface's option parameter max-udplength=xx for each SIP interface where you expect to receive large INVITE packets.

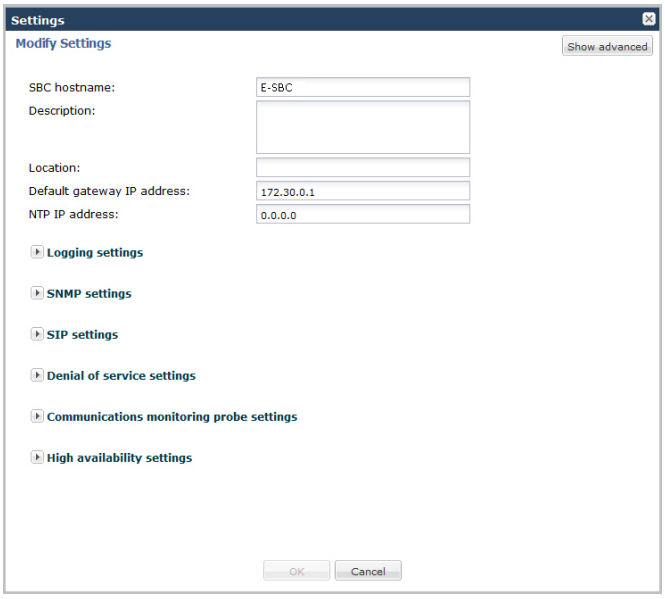
Other than enabling IPv6 on your Enterprise Session Director, there is no configuration for IPv6 reassembly and fragmentation support. It is enabled automatically.

For more information about dialog transparency and IPv6 reassembly and fragmentation support, see the Net-Net® Enterprise Session Director Configuration Guide.

SIP Features on Net-Net ESD

To set SIP features on the Enterprise Session Director:

1. Click on Settings in the Main Menu. The following dialog box displays.



2. Click on SIP settings to expand the dialog box. The following displays.

3. In the Enable dialog transparency field, place a check mark in the box to enable dialog transparency. Uncheck the box to disable this feature. Default is enabled.
4. In the Allow SIP UDP fragmentation field, place a check mark in the box to allow (enable) SIP UDP fragmentation. Uncheck the box to prevent (disable) SIP UDP fragmentation from occurring. Default is disabled.
5. In the Set INVITE expires at 100 response field, place a check mark in the box to enable the process of an INVITE expiring after the Enterprise Session Director receives a response of 100 (continue). Uncheck the box to disable this feature. Default is disabled.
6. Click <OK>.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Maximum SIP message length
- SIP options

For more information on these settings, see “Fraud Prevention” and SIP Options Tag Handling in the *Net-Net® Enterprise Session Director Configuration Guide*.

SNMP Settings

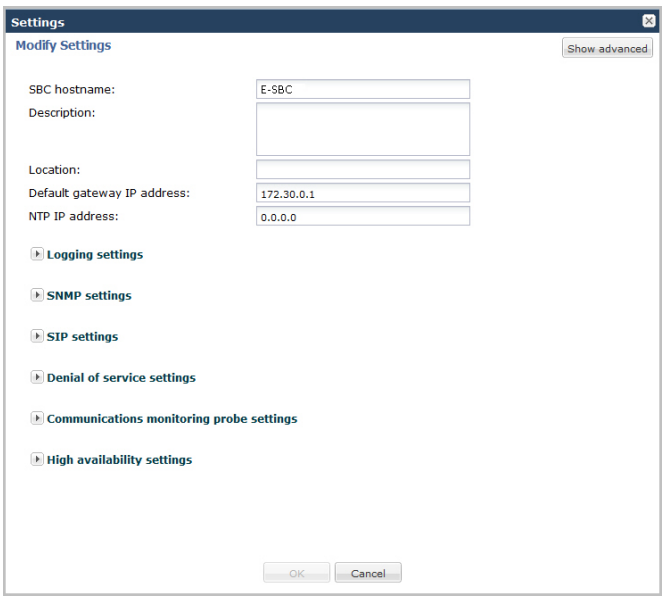
Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP is used to support monitoring of network-attached devices for conditions that warrant administrative attention. SNMP is comprised of three groups of settings on the Enterprise Session Director. These settings are system-wide configurations including MIB contact information, SNMP community settings, and trap receivers.

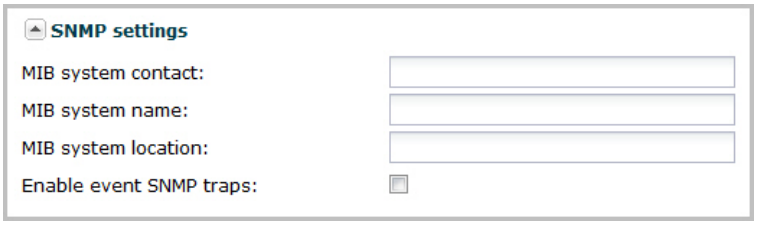
For more information about SNMP, see the section, SNMP in the *Net-Net® Enterprise Session Director Configuration Guide*.

To set SNMP on the Enterprise Session Director:

1. Click on Settings in the Main Menu. The following dialog box displays.



2. Click on SNMP settings to expand the dialog box. The following displays.



3. In the MIB system contact field, enter the contact information used within the Enterprise Session Director's MIB transactions. The SNMP agent sends this information to a Network Management System (NMS) in response to an SNMP Get for the MIB-II sysContact MIB variable. This parameter's value can be a textual identification of your company's contact person for the Enterprise Session Director and/or information about how to contact that person. For example, John Doe. Valid values are alpha-numeric characters. Default is blank.
4. In the MIB system name field, enter the identification of this Enterprise Session Director presented within MIB transactions. This value, along with the target name of the Enterprise Session Director (identified in the boot parameters) are the values reported for MIB-II when an SNMP GET is issued by the NMS for the MIB-II sysName variable. For example. Test System: This parameter has no direct relation to the hostname parameter in the system configuration element. By convention, this is the node's FQDN. For SNMP MIB-II sysName GETs, the Enterprise Session Director returns SNMP communications in the following format:

   ```
   <targetName>[.<mib-system-name>]"
   ```

   The "targetName" is the value configured in the target name (tn) boot parameter and mib-system-name is the value configured in this field.

   Valid values are alpha-numeric characters. Default is blank.
5. In the MIB system location field, enter the physical location of this Enterprise Session Director that is reported within MIB transactions. This parameter is reported when an SNMP GET is issued by the NMS for the MIB-II sysLocation variable. This parameter has no direct relation to the location field in the system configuration element. For example, Oracle. Valid values are alpha-numeric characters. Default is blank.
6. In the Enable event SNMP traps field, place a checkmark in the box to enable the Enterprise Session Director to report event SNMP traps. Uncheck to the box to disable this feature. Default is disabled.
7. Click <OK>.

Denial of Service Settings (DoS)

The Enterprise Session Director Denial of Service (DoS) protection functionality protects softswitches and gateways with overload protection, dynamic and static access control, and trusted device classification and separation at Layers 3-5. The Enterprise Session Director itself is protected from signaling and media overload, but more importantly the feature allows legitimate, trusted devices to continue receiving service even during an attack. DoS protection prevents the Net-Net ESD host processor from being overwhelmed by a targeted DoS attack from the following:

- IP packets from an untrusted source as defined by provisioned or dynamic ACLs
- IP packets for unsupported or disabled protocols
- Nonconforming/malformed (garbage) packets to signaling ports
- Volume-based attack (flood) of valid or invalid call requests, signaling messages, and so on.

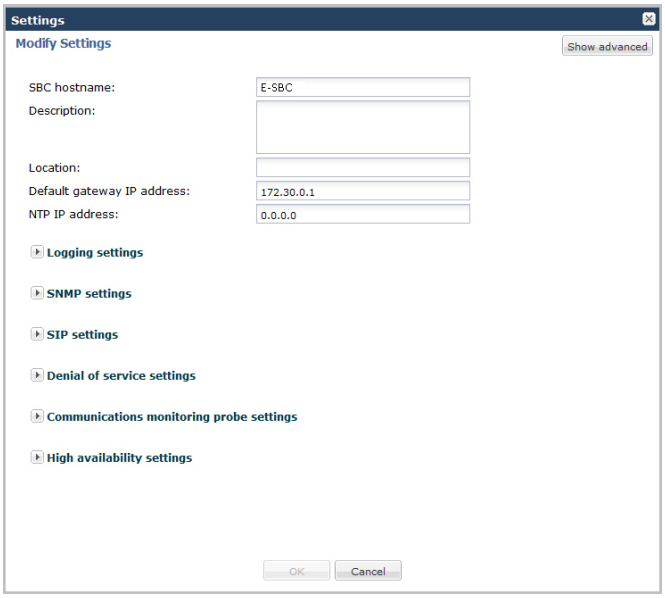
The Server Edition and VM Edition support of Denial of Service (DoS) protection differs from the Oracle Hardware Platforms Edition because of the absence of Oracle network interface hardware. Consequently DoS protection is implemented in software and consumes CPU cycles when responding to attacks.

In addition, the Server Edition and VM Edition handle media packet fragments differently, processing them in the datapath rather than in the host application code. Protection against fragment attacks is still present by ensuring fragments are never kept more than 5 ms.

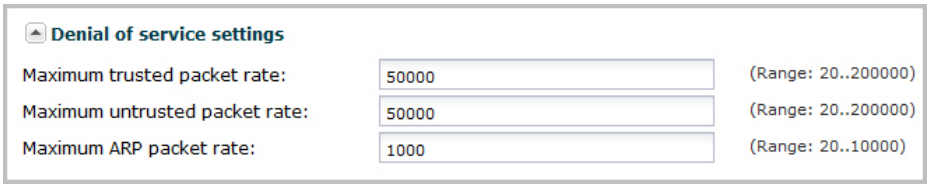
For more information about DoS, see SIP Security in the *Net-Net® Enterprise Session Director Configuration Guide*.

To set DoS features on the Enterprise Session Director:

1. Click on Settings in the Main Menu. The following dialog box displays.



2. Click on Denial of service settings to expand the dialog box. The following displays.



3. In the Maximum trusted packet rate field, enter the maximum trusted packet rate, in packets per seconds. Valid values are 20 to 200,000. Default is 50,000.
4. In the Maximum untrusted packet rate field, enter the maximum untrusted packet rate, in packets per seconds. Valid values are 20 to 200,000. Default is 50,000.
5. In the Maximum ARP packet rate field, enter the maximum ARP packet rate, in packets per seconds. Valid values are 20 to 10,000. Default is 1000.

6. Click <OK>.

Communication Monitoring Probe Settings

Palladion is Oracle's Communication Experience Manager. The manager is powered by the Palladion Mediation Engine, a platform that collects SIP, DNS, ENUM, and protocol message traffic received from Palladion Probes. The mediation engine stores the traffic in an internal database, and analyzes aggregated data to provide comprehensive multi-level monitoring, troubleshooting, and interoperability information.

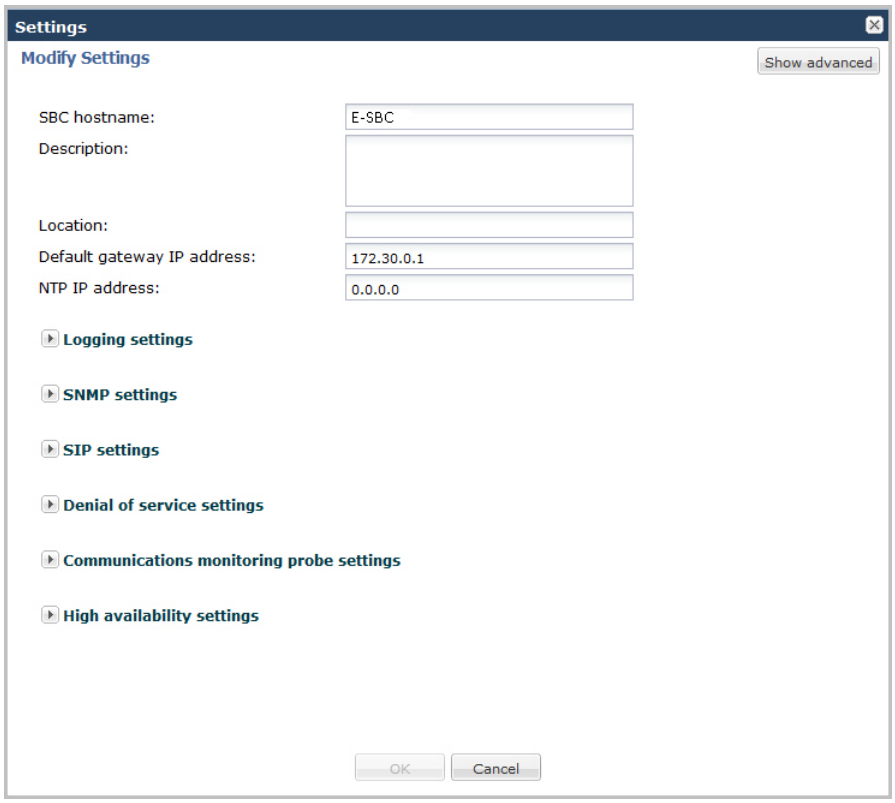
Palladion simplifies the operation of software-based Palladion probes by enabling the transmission of Internet Protocol Flow Information Export (IPFIX) data to one or more Palladion Mediation Engines, possibly on different sub-nets. This enhancement requires a slight change in the ACLI hierarchy -- specifically, the removal of the network-interface parameter from the comm-monitor configuration object, and its transfer to the monitor-collector configuration object.

Note: The Palladion Communications Monitor Probe communicates over the media interface for signaling and Quality of Service (QoS) statistics using IPFIX. QoS reporting is done via Call Detail Records (CDR) (accounting).

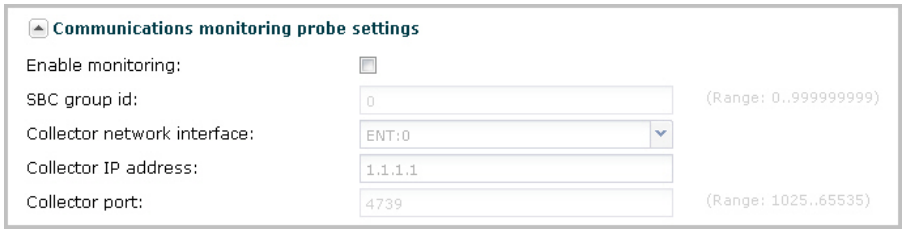
For more information about the Communications Monitoring Probe, see the Communications Monitoroing Probe chapter in the Net-Net® Enterprise Session Director Configuration Guide.

To set Communication Monitoring Probe features on the Enterprise Session Director:

1. Click on Settings in the Main Menu. The following dialog box displays.



2. Click on Communications monitoring probe settings to expand the dialog box. The following displays.



3. In the Enable Monitoring field, place a check mark in the box to enable the Communication Monitor Probe to monitor the network. Uncheck the box to disable monitoring. Default is disabled.

   Note: After checking the Enable monitoring box, all remaining fields are enabled for you to edit.

4. In the SBC group id field, enter an integer value to assign to the Net-Net ESD, that indicates its role as an information exporter. Valid values are 0 to 999999999. Defaul is zero (0).
5. In the Collector network interface field, enter the network interface and port whose traffic is exported to the Palladion Mediation Engine. Valid values are alpha-numeric characters. Default is the Enterprise network interface and port (ENT:0).
6. In the Collector IP address field, enter the IP address monitored by a Palladion Mediation Engine for incoming IPFIX traffic. Enter the address in dotted decimal format (0.0.0.0). Default is 1.1.1.1.
7. In the Collector port field, enter the port monitored by a Palladion Mediation Engine for incoming IPFIX traffic. Valid values are 1025 to 65535. Default is 4739.
8. Click <OK>.

High Availability (HA) Settings

Enterprise Session Directors can be deployed in pairs to deliver high availability (HA). Two Enterprise Session Directors operating in this way are called an HA node. Over the HA node, media and call state are shared, keeping sessions/calls from being dropped in the event of a failure.

Two Enterprise Session Directors work together in an HA node, one in active mode and one in standby mode.

- The active Enterprise Session Director checks itself for internal process and IP connectivity issues. If it detects that it is experiencing certain faults, it will hand over its role as the active system to the standby Enterprise Session Director in the node.
- The standby Enterprise Session Director is the backup system, fully synchronized with active Enterprise Session Director's session status. The standby Enterprise Session Director monitors the status of the active system so that, if needed, it can assume the active role without the active system having to instruct it to do so. If the standby system takes over the active role, it notifies network management using an SNMP trap.

To produce seamless switchovers from one Enterprise Session Director to the other, the HA node uses shared virtual MAC and virtual IP addresses for the media interfaces in a way that is similar to VRRP (virtual router redundancy protocol). When there is a switchover, the standby Enterprise Session Director sends out a gratuitous ARP messages using the virtual MAC address, establishing that MAC on another physical port within the Ethernet switch. To the upstream router, the MAC and IP are still alive, meaning that existing sessions continue uninterrupted.

Within the HA node, the Enterprise Session Directors advertise their current state and health to one another in checkpointing messages; each system is apprised of the other's status. Using Oracle's HA protocol, the Enterprise Session Directors communicate with UDP messages sent out and received on the rear interfaces.

The standby Enterprise Session Director shares virtual MAC and IPv4 addresses for the media interfaces (similar to VRRP) with the active Enterprise Session Director. Sharing addresses eliminates the possibility that the MAC and IPv4 address set on one Enterprise Session Director in an HA node will be a single point of failure. The standby Enterprise Session Director sends ARP requests using a utility IPv4 address and its hard-coded MAC addresses to obtain Layer 2 bindings.

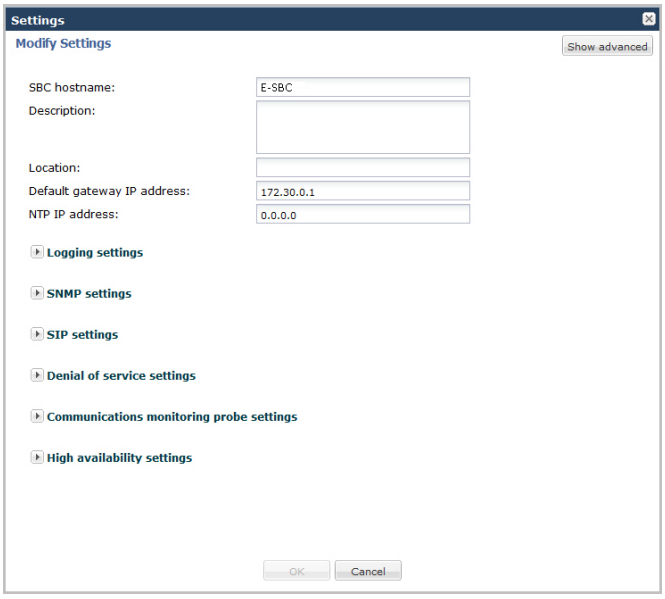
The standby Enterprise Session Director assumes the active role when:

- It has not received a checkpoint message from the active Enterprise Session Director for a certain period of time.
- It determines that the active Enterprise Session Director's health score has decreased to an unacceptable level.
- The active Enterprise Session Director relinquishes the active role.

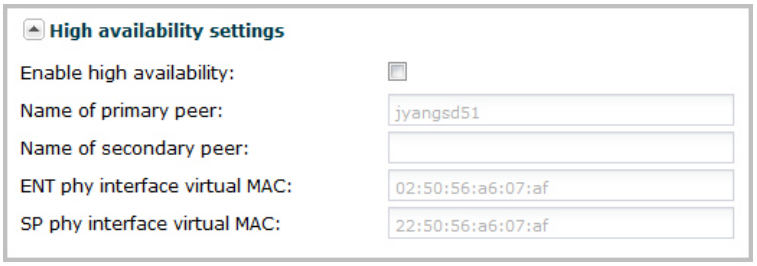
For more information about HA on the Enterprise Session Director, see the High Availability chapter in the *Net-Net® Enterprise Session Director Configuration Guide*.

To set HA features on the Enterprise Session Director:

1. Click on Settings in the Main Menu. The following dialog box displays.



2. Click on High availability settings to expand the dialog box. The following displays.



3. In the Enable high availability field, place a check mark in the box to enable HA on the Enterprise Session Director.

   Note: After checking the Enable high availability box, all remaining fields are enabled for you to edit.

4. In the Name of primary peer field, enter the name of the primary Enterprise Session Director peer. Valid values are alpha-numeric characters. Default is <primary peer name>.

   Note: This field is automatically populated with the primary peer name that you entered when you ran the Installation Wizard.

5. In the Name of secondary peer field, enter the name of the secondary system you are using for HA purposes to peer with the primary system. Valid values are alpha-numeric characters. Default is blank.
6. In the ENT phy interface virtual MAC field, enter the MAC address of the Enterprise's physical interface on the Enterprise Session Director.

   Note: This field is automatically populated with the Enterprise's MAC address that was entered when you ran the Installation Wizard.

7. In the SP phy interface virtual MAC field, enter the MAC address of the Service Provider's physical interface on the Enterprise Session Director.

   Note: This field is automatically populated with the Service Provider's MAC address that was entered when you ran the Installation Wizard.

8. Click <OK>.

Packet Capture Settings (Advance Configuration only)

The Server and VM Edition support of packet tracing differs from the other Oracle platforms such as Net-Net 3800 and Net-Net 4500. When enabled, packets are captured that meet specific criteria. The packets are logged into a file in

the /opt/traces directory in a PCAP-formatted format as well as being displayed to the ACLI session from which the capture was executed.

You can enable or disable packet capture on the Enterprise Session Director. The default filter uses port 5060 on the specified interface to capture both ingress and egress ICMP traffic. This does not support sending the captured packets off the box in RFC2003 IP in IP format. Therefore the capture-receiver element supported by the other platforms has been removed.

For more information on packet capture, see Packet Trace/PCAP in the *Net-Net® Enterprise Session Director Configuration Guide*.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Enable packet capture
- Capture receiver network interface
- Capture receiver IP address

For more information on these settings, see Initiating Packet Capture in the *Net-Net® Enterprise Session Director Configuration Guide*.

Host Routes

Host routes let you insert entries into the Enterprise Session Director's routing table. These routes affect traffic that originates at the Enterprise Session Director’s host process. Host routes are used primarily for steering management traffic to the correct network.

When traffic is destined for a network that is not explicitly defined on a Enterprise Session Director, the default gateway (located in the system config) is used. If you try to route traffic to a specific destination that is not accessible through the default gateway, you need to add a host route. Host routes can be thought of as a default gateway override.

Certain SIP configurations require that the default gateway is located on a front media interface. In this scenario, if management applications are located on a network connected to a rear-interface network, you will need to add a host route for management connectivity.

When source-based routing is used, the default gateway must exist on a front media interface. Host routes might be needed to reach management applications connected to a wancom port in this kind of situation as well.

For more information about Host Routes, see the section, Host Routes in the *Net-Net® Enterprise Session Director Configuration Guide*.

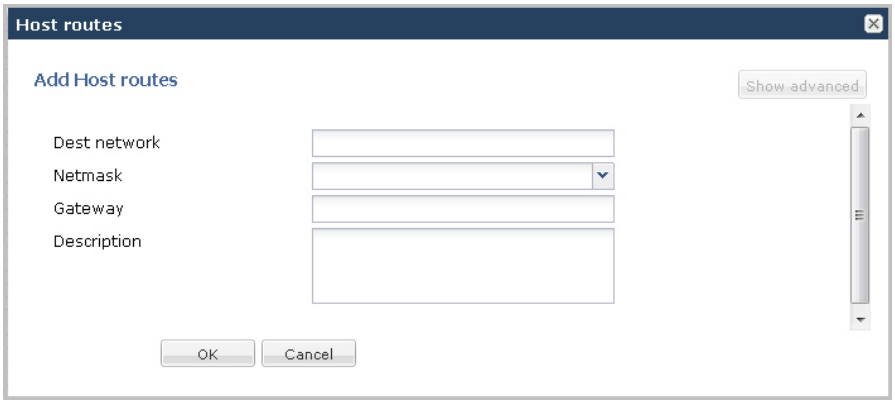
Adding a Host Route

Use the following procedure to add a host route to your configuration.

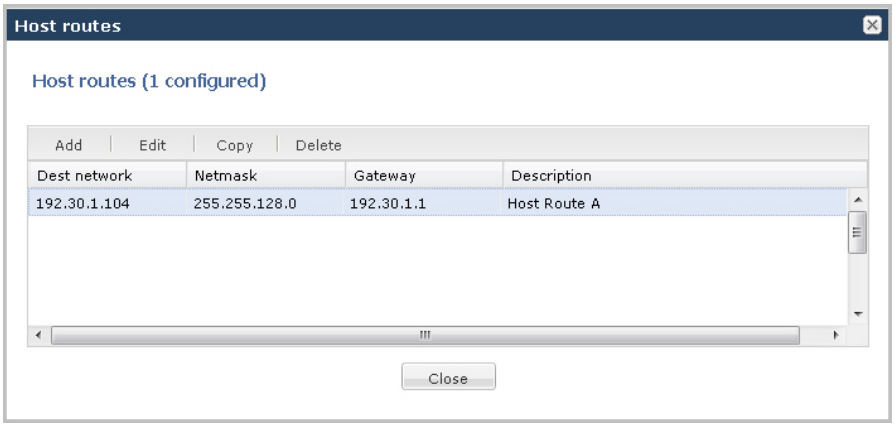
To add a host route:

1. From the Main Menu, click **Network** > **Host routes**. The following displays.

2. Click <Add>. The following dialog box displays.



3. In the Dest network field, enter the IPv4 address of the destination network that this host route points toward. Enter the address in dotted decimal format. For example, 192.30.1.104. Default is blank.
4. In the Netmask field, select the netmask from the drop-down list associated with the destination network you entered for the Dest network parameter. For example, 255.255.128.0. Default is blank.
5. In the Gateway field, enter the gateway for which traffic destined for the address defined in the Dest network parameter, should use as its first hop. Enter the address in dotted decimal format. For example, 192.30.1.1. Default is blank.
6. In the Description field, enter a description for this host route. Valid values are alpha-numeric characters. For example, Host Route A. Default is blank.
7. Click <OK> to save the host route. The host route you created displays in the Host Routes table.



8. Click <Close>.

Security

Enterprise Session Director security is designed to provide security for VoIP and other multi-media services. It includes access control, DoS attack, and overload protection, which help secure service and protect the network infrastructure (including the Enterprise Session Director). In addition, Enterprise Session Director security lets legitimate users to still place call during attack conditions; protecting the service itself.

Enterprise Session Director security includes the Net-SAFE framework's numerous features and architecture designs. Net-SAFE is a requirements framework for the components required to provide protection for the Enterprise Session Director (ESD), the service provider's infrastructure equipment (proxies, gateways, call agents, application servers, and so on), and the service itself.

For more information about Security on the Enterprise Session Director, see Chapter 18, Security, in the *Net-Net® Enterprise Session Director Configuration Guide*.

To configure security in your network, you can configure:

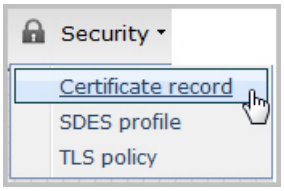
- Certificate record
- SDES Profile (for advanced Administrators only)
- TLS Policy

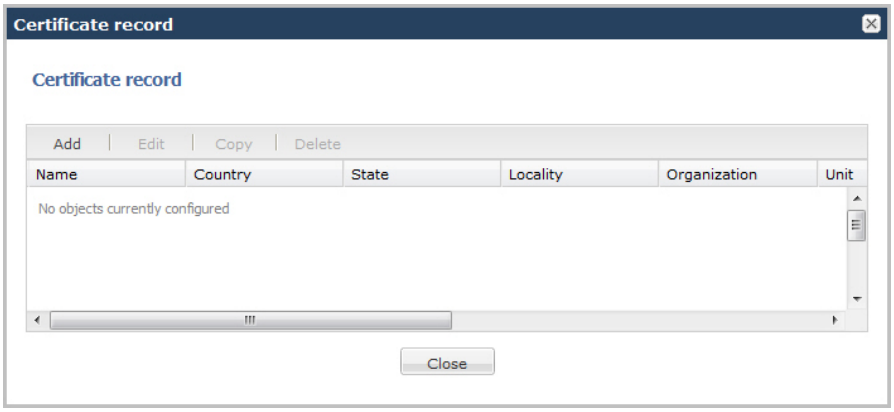
Adding a Certificate Record

Use the following procedure to add a certificate record to your configuration.

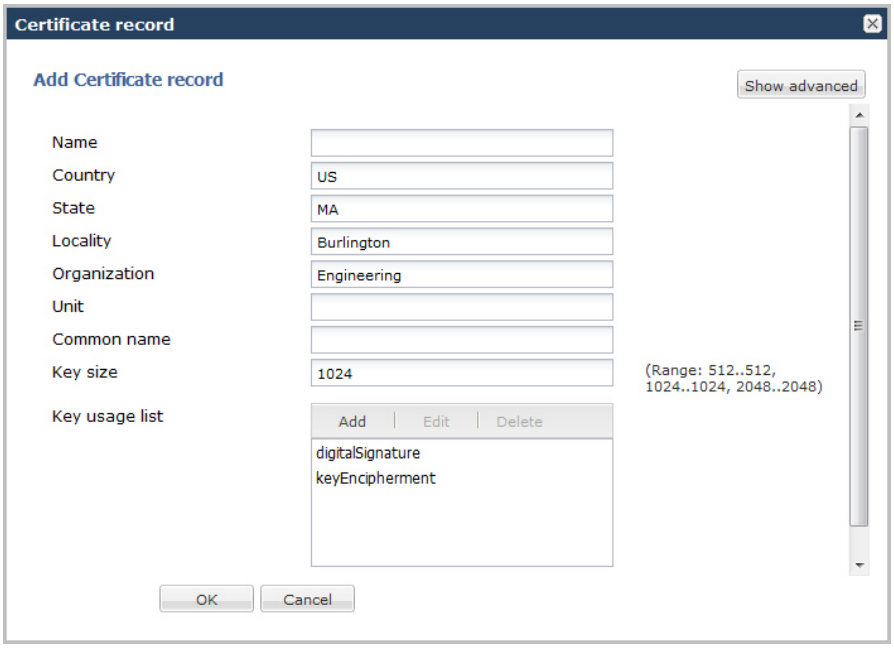
To add a certificate record:

1. From the Main Menu, click **Security** > **Certificate record**. The following displays.





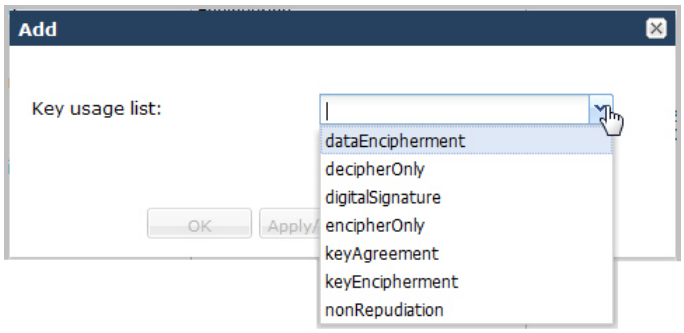
2. Click <Add>. The following dialog box displays.



3. In the Name field, enter a name for the certificate record. For example, acmepacket. Valid values are alpha-numeric characters. Default is blank.
4. In the Country field, enter the name of the country where the certificate is being used. The default is US.
5. In the State field, enter the name of the state where the certificate is being used. The default is MA.

6. In the Locality field, enter the name of the locality within the state where the certificate is being used. Default is Burlington.
7. In the Organization field, enter the name of the organization holding the certificate. The default is Engineering.
8. In the Unit field, enter the name of the unit that is holding the certificate within the organization. Valid values are alpha-numeric characters. Default is blank.
9. In the Common name field, enter a common name for the certificate record. Valid values are alpha-numeric characters. Default is blank.
10. In the Key size field, enter the size of the encrypted key for the certificate. The default is 1024. Valid values are:
    - 512
    - 1024
    - 2048
11. In the Key usage list field, select the usage extensions you want to use with this certificate record. This parameter can be configured with multiple values. Default is a combination of digitalSignature and keyEncipherment.

    To add additional usage extensions to the list, click <Add>. The following dialog box displays.



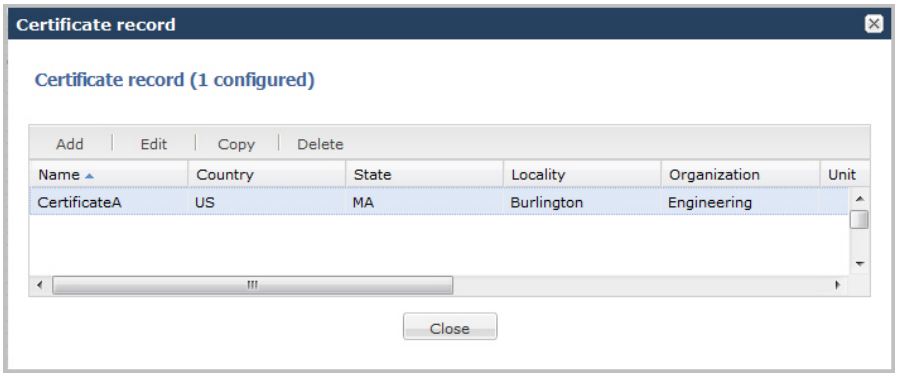
    In the Key usage list field, select an additional usage extension(s) to add the key usage list. Valid values are:

    - dataEncipherment
    - decipherOnly
    - digitalSiggnature
    - encipherOnly
    - keyAgreement
    - keyEncipherment
    - nonRepudiation

    Note: For more information on these usage extensions, see Chapter 18, the section, Key Usage Control, of the *Net-Net® Enterprise Session Director Configuration Guide*.

    To add the usage extension to the list and apply another one, click <Apply/Add Another>.

    When you have completed adding usage extensions, click <OK>.
12. Click <OK> to save the certificate record. The certificate record you created displays in the Certificate Record table.



13. Click <Close>.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Alternate name
- Trusted state
- Extended key usage list
- Options

For more information about these settings, see Chapter 18, the section, "Configuring Certificates, in the *Net-Net® Enterprise Session Director Configuration Guide*.

Adding an SDES Profile

Session Description Protocol Security Descriptions (SDES) for Media Streams is a way to negotiate the key for Secure Real-time Transport Protocol (SRTP). It provides confidentiality, message authentication, and replay protection for RTP media and control traffic.

Adding an SDES profile to the Enterprise Session Director is for Administrators only. For more information about SDES, and for configuring an SDES profile, see Chapter 18, the section, Key Exchange Protocols in the *Net-Net® Enterprise Session Director Configuration Guide*.

Adding a TLS Policy

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity.

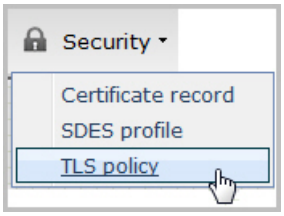
The TLS policy configuration holds the information required to run SIP over TLS. You can configure an end entity certificate and a trusted certification authority (CA) certificate(s) for a TLS policy. CA certificates are certificates that are issued by a CA to itself or to a second CA for the purpose of creating a defined relationship between the two CAs. A certificate that is issued by a CA to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy. Once the trusted root has been established, it can be used to authorize subordinate CAs to issue certificates on its behalf.

For more information about TLS, see Chapter 18, the section, Transport Layer Security, in the Net-Net® Enterprise Session Director Configuration Guide.

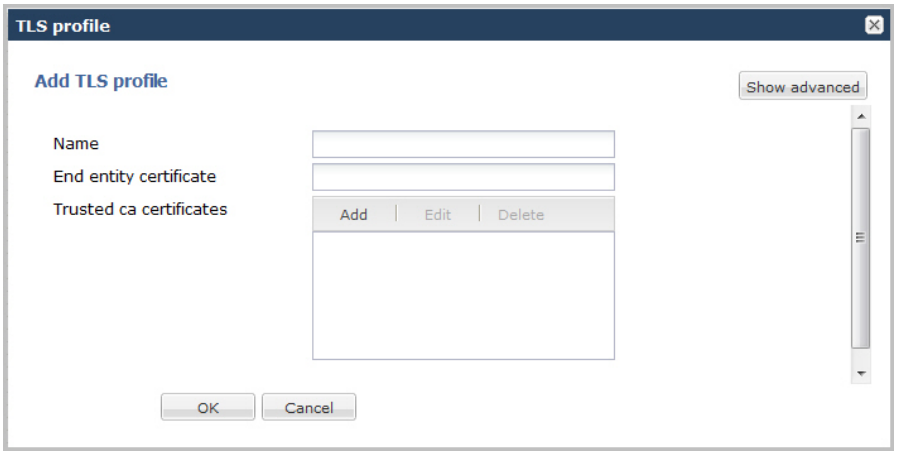
Use the following procedure to add a TLS policy to your configuration.

To add a TLS policy:

1. From the Main Menu, click **Security** > **TLS policy**. The following displays.



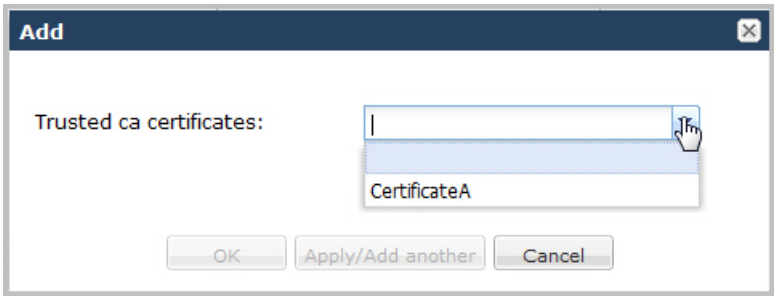
2. Click <Add>. The following dialog box displays.



3. In the Name field, enter a name for the TLS profile. For example, TLS1. Valid values are alpha-numeric characters. Default is blank.
4. In the End entity certificate field, enter the name of the entity certification record. Valid values are alpha-numeric characters. Default is blank.
5. In the Trusted ca certificates field, select the names of the trusted CA certificate records.

   To add a trusted CA certificate, click <Add>.

   The following dialog box displays.

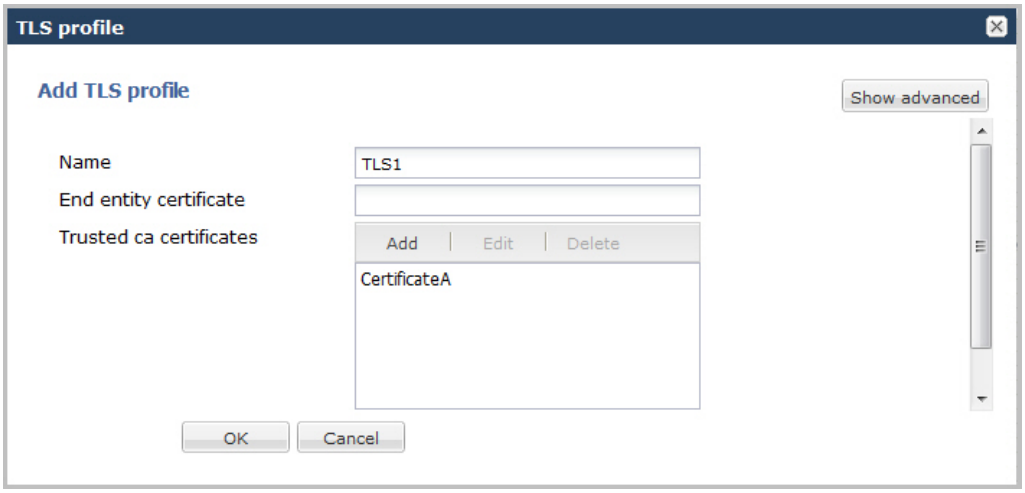


In the Trusted ca certificates field, select the certificate to trust for this TLS profile.

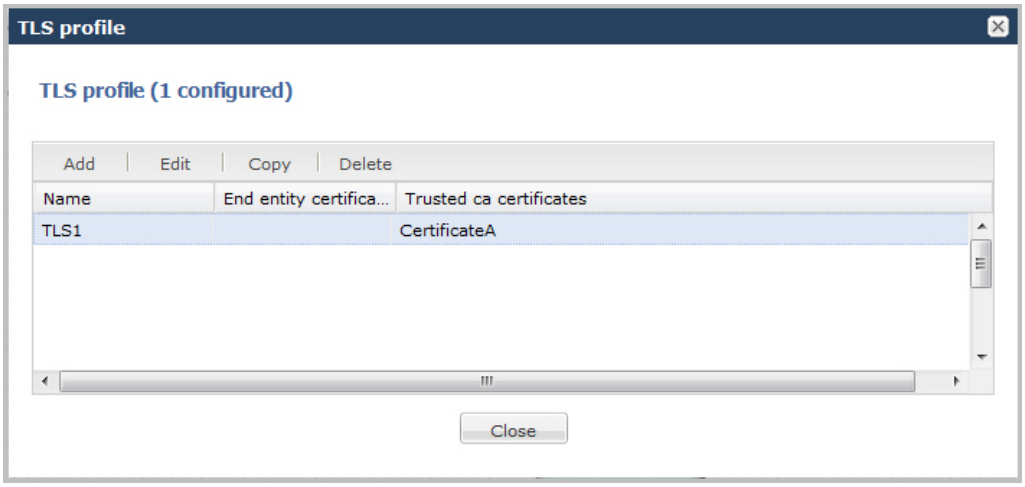
Note: You must add a certificate record to the Net-Net ESD configuration is order to select a value for this field. To add a certificate record, see Adding a Certificate Record.

To add the certificate to the list and apply another one, click <Apply/Add Another>.

When you have completed adding certificates, click <OK>. The following displays.



6. Click <OK>. The profile you created displays in the TLS Profile table.



7. Click <Close>.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Cipher list
- Verify depth
- Mutual authenticate
- TLS version
- Options
- Certificate status check
- Certificate status profile list
- Enable/disable ignore dead responder

For more information about these settings, see Chapter 18, the section, Transport Layer Security, in the *Net-Net® Enterprise Session Director Configuration Guide*.

Management Settings

Management settings in Basic Mode allow you to configure the following features on the Enterprise Session Director:

- Accounting
- SNMP Community
- Trap Receiver
- Web Server

Configuring Accounting

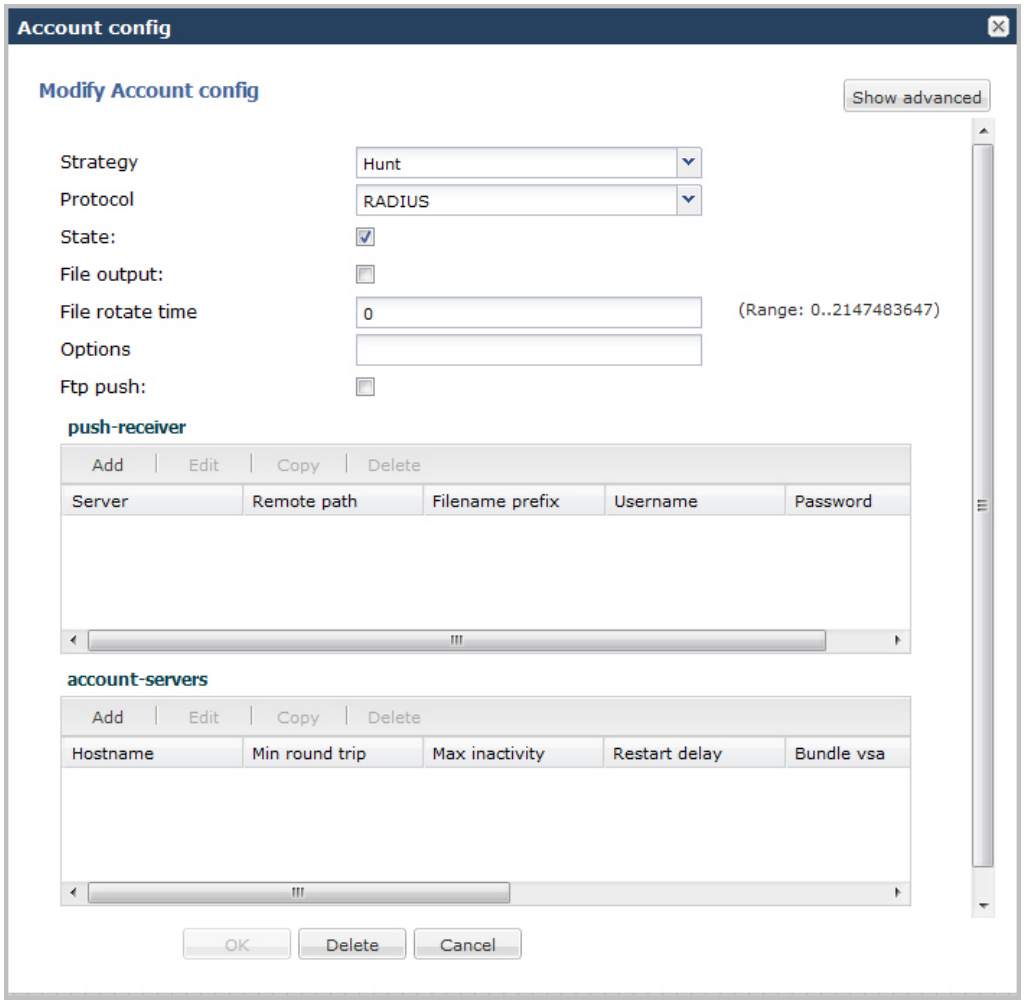
The Enterprise Session Director offers support for RADIUS, an accounting, authentication, and authorization (AAA) system. RADIUS servers are responsible for receiving user connection requests, authenticating users, and returning all configuration information necessary for the client to deliver service to the user.

You can configure your Enterprise Session Director to send call accounting information to one or more RADIUS servers. This information can help you to see usage and Quality of Service (QoS) metrics, monitor traffic, and even troubleshoot your system.

For information about how to configure the Enterprise Session Director for RADIUS accounting, refer to the *Net-Net 4000 Accounting Guide*. The Accounting Guide contains all RADIUS information, as well as information about:

- Accounting for SIP and H.323
- Local CDR storage on the Enterprise Session Director, including CSV file format settings
- Ability to send CDRs via FTP to a RADIUS sever (the FTP push feature)
- Per-realm accounting control
- Configurable intermediate period
- RADIUS CDR redundancy
- RADIUS CDR content control

The following is an example of the Accounting dialog box.



For configuring the parameters in the above dialog box, and for configuring more advanced parameters, see the *Net-Net 4000 Accounting Guide*.

Configuring SNMP Community

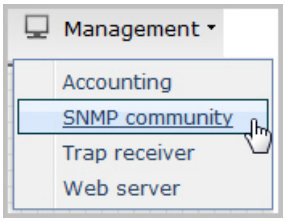
A Simple Network Management Protocol (SNMP) community is a name (string) used as a password by the SNMP manager to communicate with the SNMP agent. The SNMP community string allows access to other devices' statistics. It is used to support monitoring of network-attached devices for conditions that warrant administrative attention. If an SNMP community is configured, the Enterprise Session Director sends the community string along with all SNMP requests.

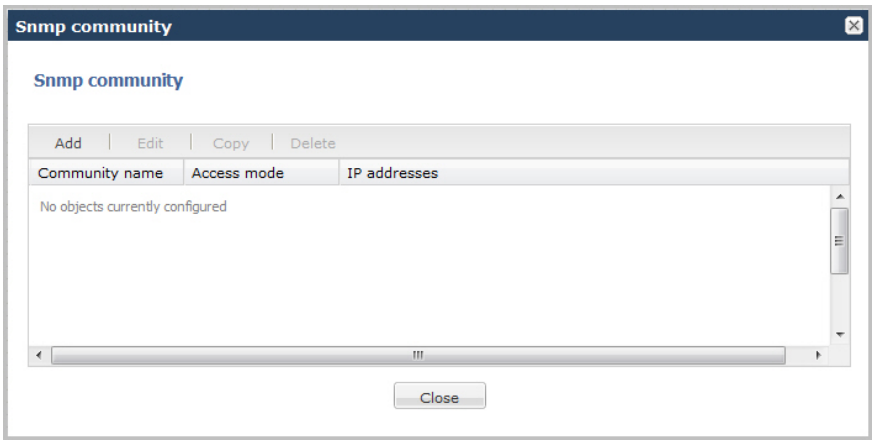
Note: SNMP community strings are used only by devices which support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

For more information about configuring an SNMP community, see Configuring SNMP, in the *Net-Net® Enterprise Session Director Configuration Guide*.

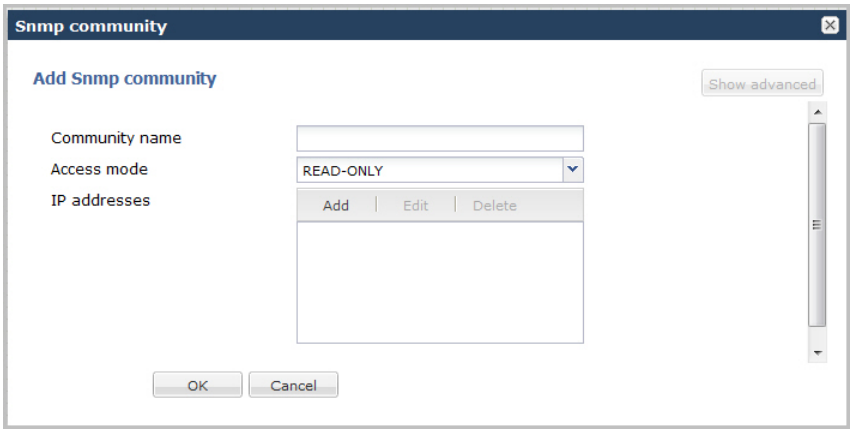
To configure an SNMP community:

1. From the Main Menu, click **Management** > **SNMP community**. The following displays.



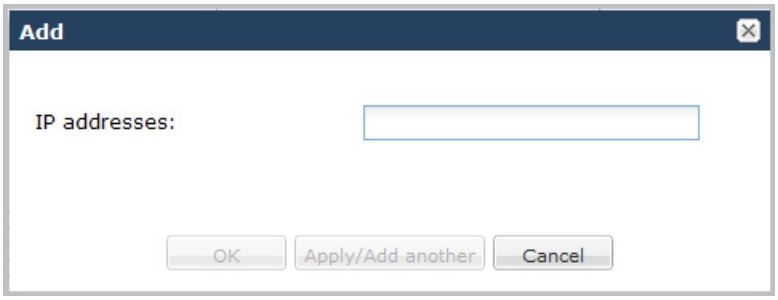


2. Click <Add>. The following dialog box displays.



3. In the Community name field, enter an SNMP community name of an active community where this Enterprise Session Director can send or receive SNMP information. A community name value can also be used as a password to provide authentication, thereby limiting the NMSs that have access to this Net-Net system. With this field, the SNMP agent provides trivial authentication based on the community name that is exchanged in plain text SNMP messages. For example, public. Valid values are alpha-numeric characters. Default is blank.
4. In the Access mode field, enter the access level for all Network Management Systems (NMSs) defined within this SNMP community. The access level determines the permissions that other NMS hosts can wield over this Enterprise Session Director. Default is READ-ONLY. Valid values are:
   - READ-ONLY—allows GET requests.
   - READ-WRITE—allows both GET and SET requests.
5. In the IP addresses field, select one or multiple IPv4 addresses that are valid within this SNMP community. These IPv4 addresses correspond with the IPv4 address of NMS applications that monitor or configure this Enterprise Session Director. Include the IPv4 addresses of all servers where NMSs are installed.

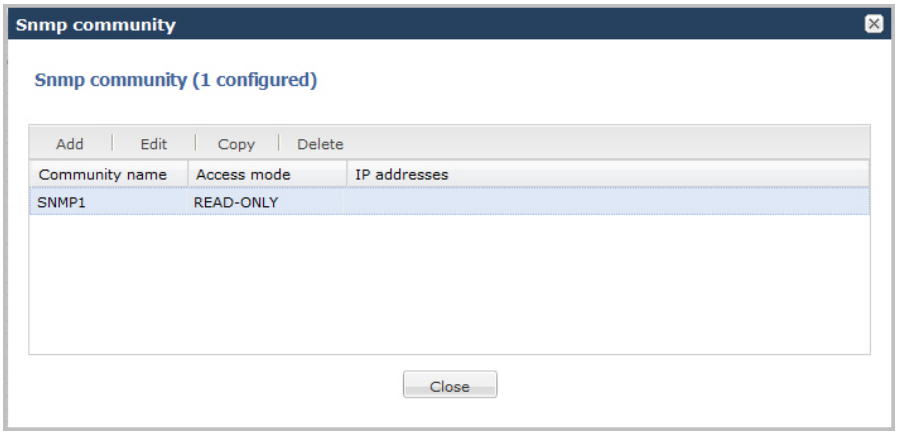
   To add an IP address, click <Add>. The following dialog box displays.



In the IP addresses field, enter an IPv4 address that is valid within this SNMP community.

To add the address to the list and apply another one, click <Apply/Add Another>.

When you have completed adding IP addresses, click <OK>. The following displays.



6. Click <Close>.

Configuring a Trap Receiver

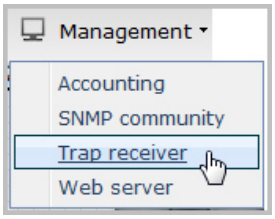
A trap receiver is an application used to receive, log, and view SNMP traps for monitoring the Enterprise Session Director. An SNMP trap is the notification sent from a network device, the Enterprise Session Director in this case, that declares a change in service. Multiple trap receivers can be defined on a Enterprise Session Director either for redundancy or to segregate alarms with different severity levels to individual trap receivers.

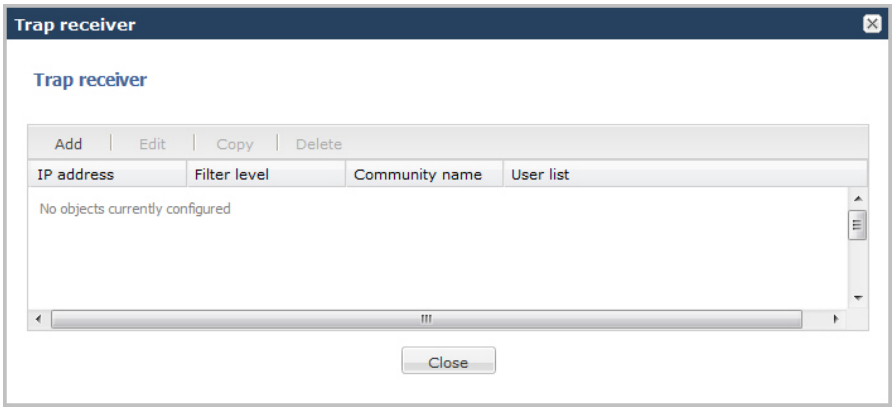
Each server that a NMS is installed on, should be configured as a trap receiver on all Enterprise Session Director's managed by an NMS.

For more information about configuring a trap receiver, see the section, Trap Receiver Configuration, in the Net-Net® Enterprise Session Director Configuration Guide.

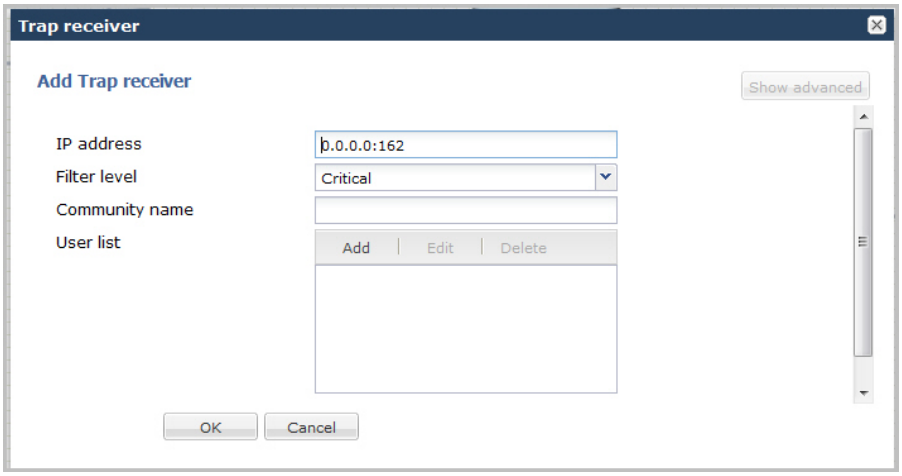
To configure a trap receiver:

1. From the Main Menu, click **Management** > **Trap receiver**. The following displays.





2. Click <Add>. The following dialog box displays.



3. In the IP address field, enter the IPv4 address and port number of an authorized NMS. This value is the IPv4 address of an NMS where traps are sent. If you do not specify a port number, the default SNMP trap port of 162 is used. Enter the IP address in dotted decimal format. Default is 0.0.0.0:162.
4. In the Filter level field, select the filter level threshold that indicates the severity level at which a trap is sent to the trap receiver. Default is Critical. Valid values are:
   - All
   - Critical
   - Major
   - Minor

   The following table maps Syslog and SNMP alarms to trap receiver filter levels.

Filter Level	Syslog Severity Level	(SNMP) Alarm Severity Level
All	Emergency (1) Critical (2) Major (3) Minor (4) Warning (5) Notice (6) Info (7) Trace (8) Debug (9)	Emergency Critical Major Minor Warning
Critical	Emergency (1) Critical (2)	Emergency Critical
Major	Emergency (1) Critical (2) Major (3)	Emergency Critical Major
Minor	Emergency (1) Critical (2) Major (3)	Emergency Critical Major

Filter Level	Syslog Severity Level	(SNMP) Alarm Severity Level
	Minor (4)	Minor

When configuring the trap-receiver element for use with Network Management Systems, Oracle recommends that the filter-level parameter be set to All.

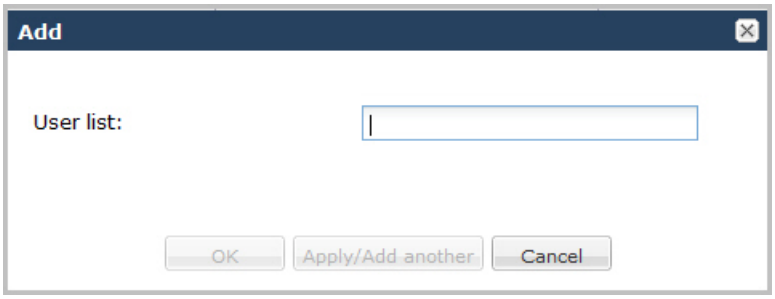
5. In the Community name field, enter the SNMP community name to which this trap receiver belongs. For example, Public. Valid values are alpha-numeric characters. Default is blank.

   Note: For information about configuring an SNMP community, see Configuring SNMP Community.

6. In the User list field, add the user name(s) of users allowed to receive secure traps.

   Note: If SNMPv3 is enabled on the Enterprise Session Director, but no users are listed for this field, a warning message is sent during a verify-config execution. For more information about SNMPv3, see Appendix B Additional SNMP Support, of the *Net-Net® Enterprise Session Director Configuration Guide*.

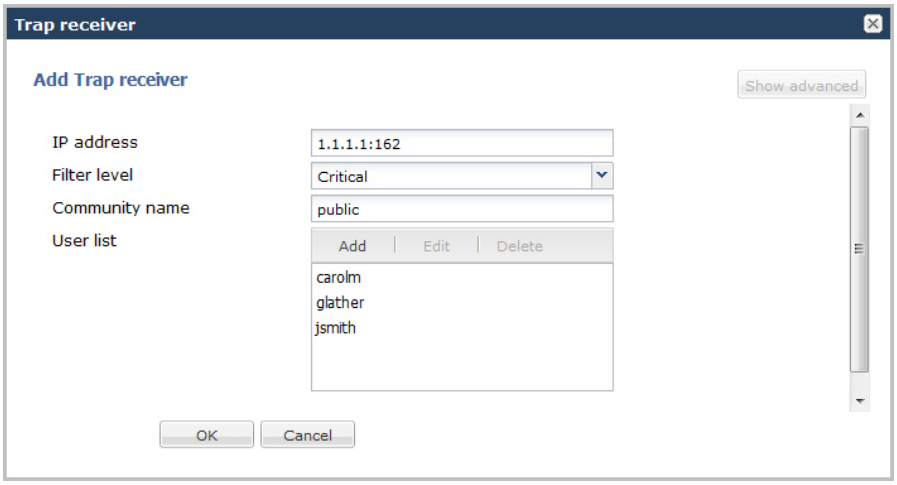
   To add a User, click <Add>. The following dialog box displays.



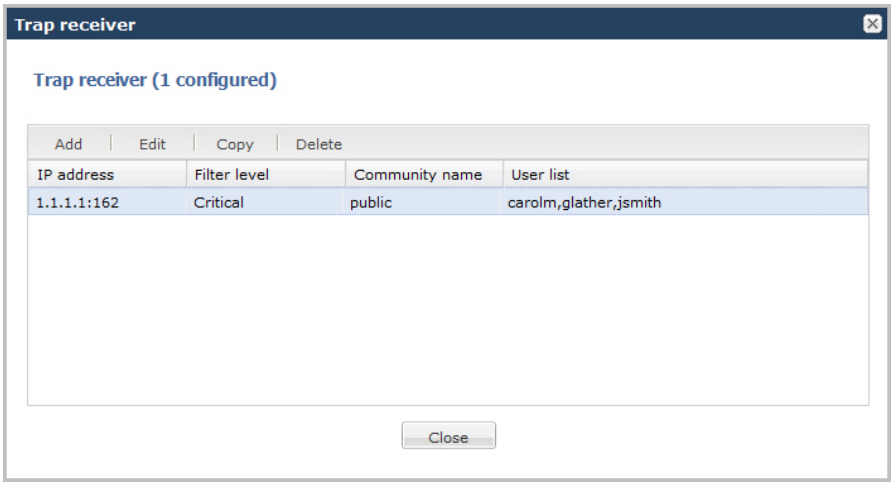
   In the User list field, enter the user name of a user allowed to receive secure traps.

   To add the User to the list and apply another one, click <Apply/Add Another>.

   When you have completed adding Users, click <OK>. The following displays.



7. Click <OK>. The following displays.



8. Click <Close>.

Configuring a Web Server

The Release E-C[xz]6.4.0 Web server is a software application that helps to deliver Web content that you can access through the Internet. The Web server runs the Enterprise application called the Web GUI.

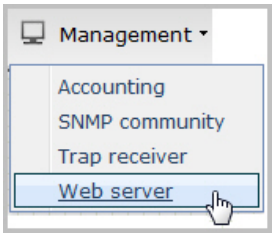
Every Web server has an IP address and sometimes a domain name. For example, if you enter the URL http://www.acmepacket.com/index.html in your browser, this sends a request to the Web server whose domain name is acmepacket.com. The server then fetches the page named index.html and sends it to your browser.

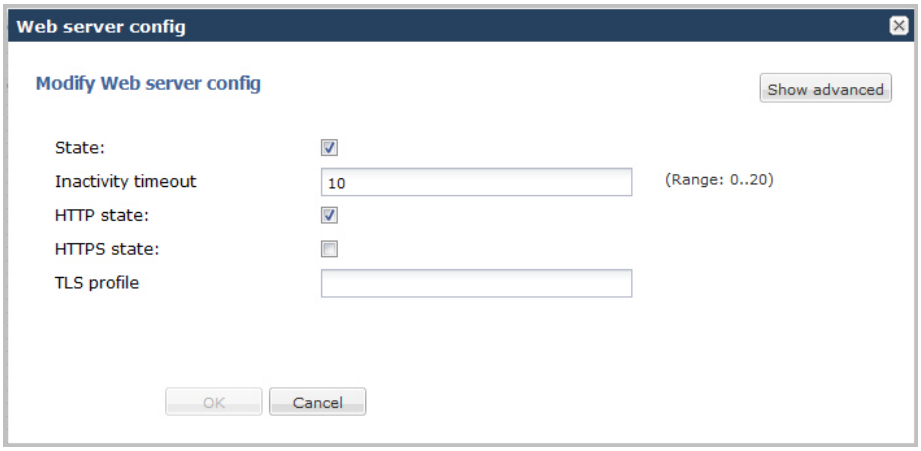
If you enter http://132.45.6.5, and this address has been configured by your Administrator to access the Web GUI, the server fetches the page and displays the Web GUI login to your browser.

This section provides a procedure for configuring the Web server in your network. For information about configuring the Web server using TLS, see Chapter 22 of the *Net-Net® Enterprise Session Director Configuration Guide*.

To configure the Web server:

1. From the Main Menu, click **Management** > **Web server** . The following displays.





2. In the State field, specify whether or not to enable the Web GUI. Default is enabled. A check mark indicates enabled, and a blank box indicates disabled.
3. In the Inactivity timeout field, enter the amount of time, in minutes, that the Web GUI must have remained inactive before it ends the Web session. For example, if this timeout value is set as 5, after 5 minutes of no activity, the Web session disconnects. Default is 10. Valid values are 0 to 20. Zero (0) disables this parameter.

   Note: The following HTTP state and HTTPS state parameters may have already been set via the GUI installation wizard on your Enterprise Session Director. You can edit these parameters if required.
4. In the HTTP state field, specify whether or not to enable HTTP for accessing the Web server. Default is enabled. A check mark indicates enabled, and a blank box indicates disabled.
5. In the HTTPS state field, specify whether or not to enable HTTPS (secure connection) for accessing the Web server. Default is disabled. A check mark indicates enabled, and a blank box indicates disabled.
6. In the TLS profile field, enter the Transport Layer Security (TLS) Protocol profile name to use with HTTPS. Valid values are alpha-numeric characters. Default is blank.

   Note: To create a TLS profile, see Adding a TLS Policy. If you specify a TLS profile, and HTTP is enabled, the Enterprise Session Director checks against the TLS profile table for a match. If there is no match, the applicable errors display during the verification of the configuration.
7. Click <OK>.

Advanced Settings

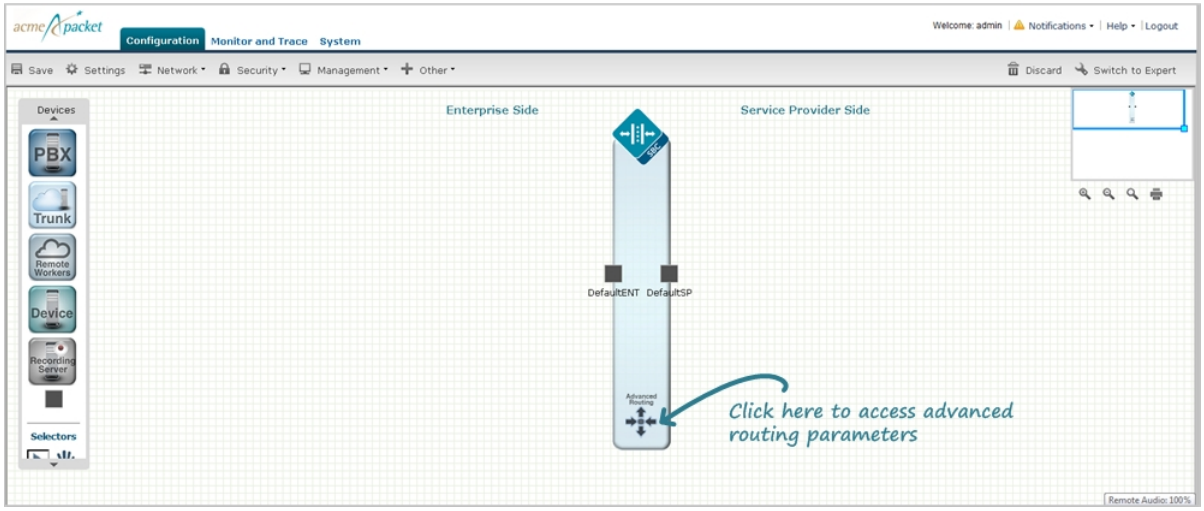
An Administrator can configure the following more advanced parameters:

- HTTP Port
- HTTPS Port

For more information about these settings, see Appendix D, Manual Web Server Configuration in the *Net-Net® Enterprise Session Director Configuration Guide*.

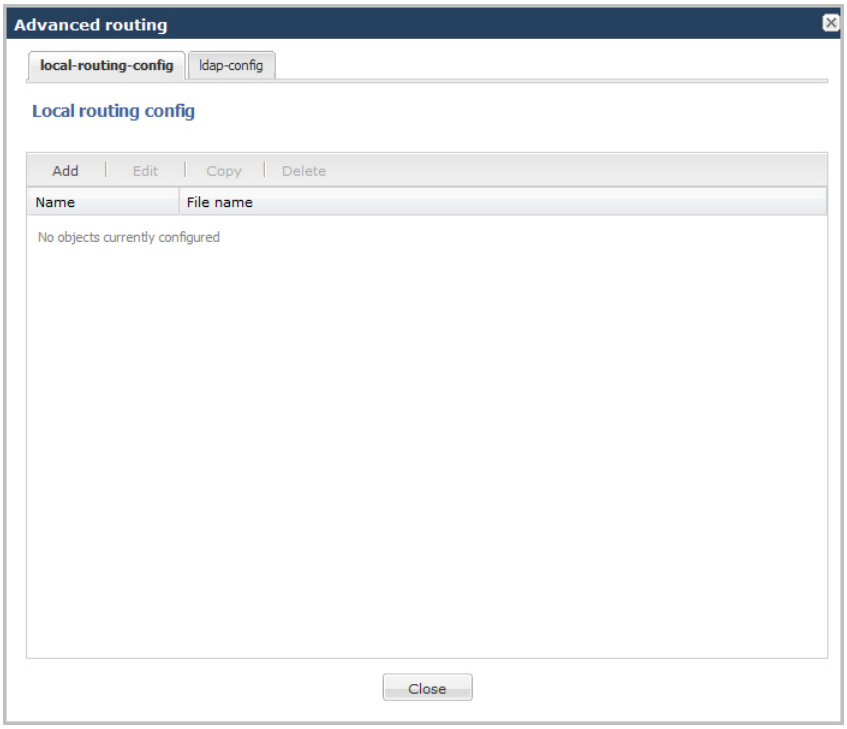
Advanced Routing

After adding a one-way or two-way local policy route, you can configure the routes with more advanced parameters if required. This feature is recommended for experienced administrators. You can access the advanced routing parameters by clicking Advanced Routing on the Enterprise Session Director.

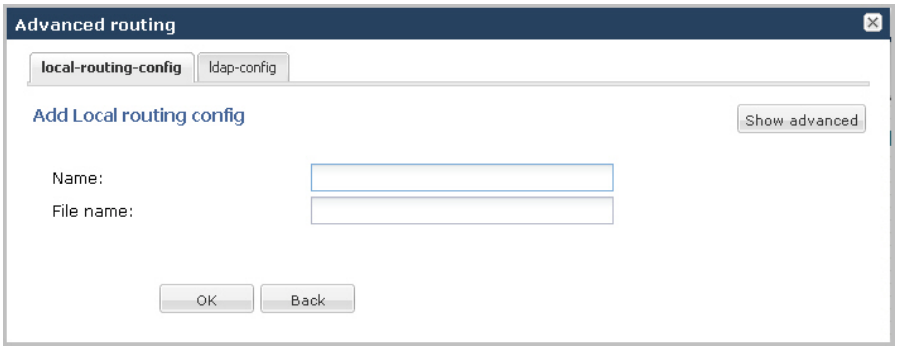


To configure advanced parameters:

1. Double-click Advanced Parameters on the Enterprise Session Director. The following displays:

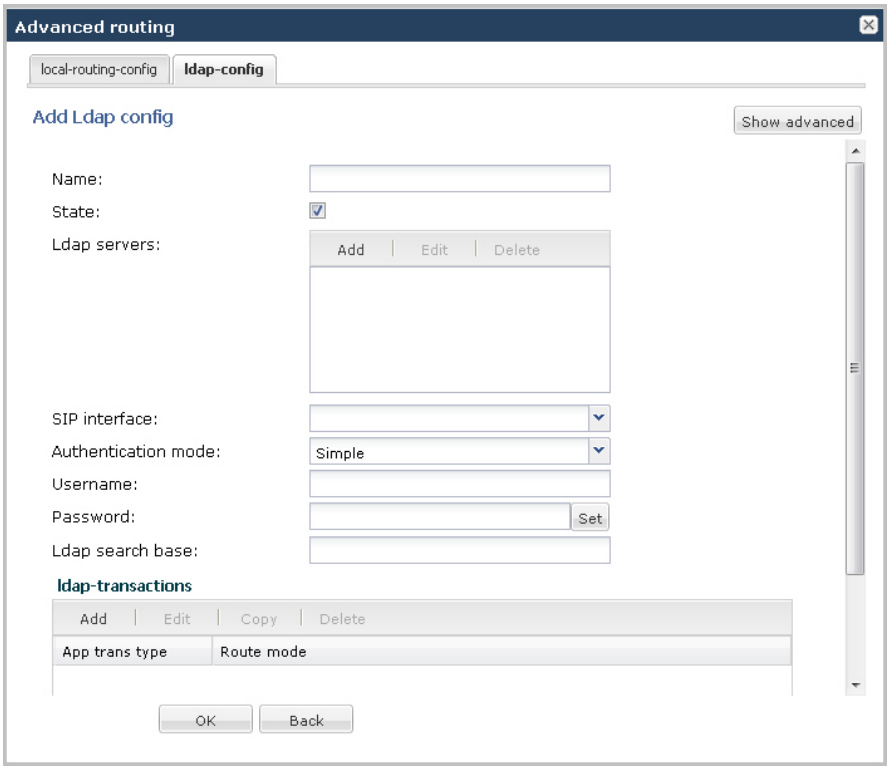


2. On the local-routing-config tab, click <Add>. The following displays.



Local-routing-config Tab

3. In the Name field, enter the name (a unique identifier) for the local route table; this name is used for reference in the local policy attributes when to specify that local routing should be used. There is no default for this parameter, and it is required.
4. In the File name field, enter the name for the file from which the database corresponding to this local route table will be created. You should use the .gz format, and the file should be placed in the /code/lrt/ directory. There is no default for this parameter and it is required.
5. Click <OK>.
6. Click the ldap-config tab. The following displays.



Ldap-config Tab

1. In the Name field, enter a name to assign to this LDAP configuration. This is a unique identifier. Valid values are alpha-numeric characters. Default is blank.
2. In the State field, specify whether or not to enable the operational state of the LDAP configuration. When the state is disabled, ESD does not attempt to establish any connection with the corresponding LDAP Server(s). Default is enabled.
3. In the ldap-servers field, click <Add> and enter the IP address(es) and optionally the port number(s) for each LDAP Server(s) you want to add to the LDAP configuration. When more than one server is specified, each server address should be separated by a space and the list enclosed within parentheses. The first server listed is considered the primary LDAP Server, and the remaining servers are considered the secondary LDAP Servers. The HUNT strategy is used to determine the active LDAP Server (where the ESD selects the first LDAP Server; if unreachable, it selects the second LDAP Server; it that is unreachable, it selects the third LDAP Server, etc.). Default ports used are 389 (for LDAP over TCP) and 636 (LDAP over TLS). IP Address must be entered in dotted decimal format (0.0.0.0). Default is blank.
4. In the SIP Interface field, select the SIP interface from the list that issues an LDAP query. This list contains all of the current SIP interfaces configured on the Enterprise Session Director. Default values are:

   - Default ENT - Default Enterprise SIP interface
   - Default SP - Default Service Provider SIP interface

5. In the Authentication mode field, select the authentication mode to use in the LDAP bind request. Default is Simple. Valid value is:

   - Simple (default) - No specific password encryption is done when sending the bind request. You can use an LDAPS connection with the LDAP Server to maintain security (see ldap-sec-type).

6. In the Username field, enter the username that the LDAP bind request uses for authentication before access is granted to the LDAP Server. Valid values are alpha-numeric characters. Default is blank.

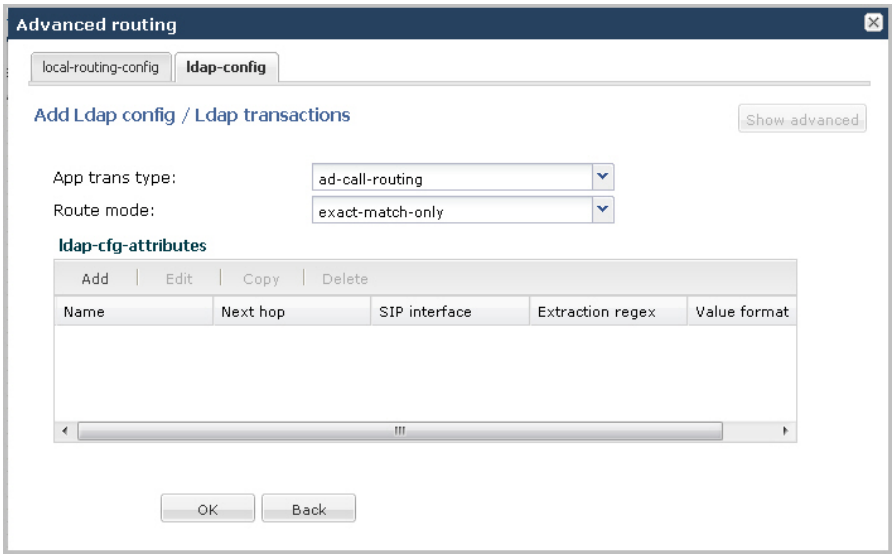
7. In the Password field, click <Set>. Then enter the password to be paired with the username attribute, that the LDAP bind request uses for authentication before access is granted to the LDAP Server. Valid values are alpha-numeric characters. Default is blank.
8. In the Confirm password field, re-enter the password you specified in Step 7, and click <OK>.
9. In the Ldap search base field, enter the base Directory Number you can use for LDAP search requests. Valid values are alpha-numeric characters. Default is blank. For example, cn=users, dc=englab, dc=acmepacket, dc=com.

LDAP Transactions

You use the LDAP transactions to configure the application transaction type for LDAP, determine route priority in the route list, and configure the LDAP configuration attributes. You configure this object for LDAP search queries in call routing.

To configure LDAP transactions:

1. In the ldap-transactions sections, click <Add>. The following displays.



2. In the App trans type field, select the application transaction type to use for LDAP. This value allows the ESD to add call routing updates to the Active Directory. Default is ad-call-routing. Valid value is:
   - ad-call-routing (default)
3. In the Route mode field, select the route priority that the Enterprise Session Director uses in the route list. This parameter determines which routes are created, and the priority of those routes within the route list. Default is exact-match-only. Valid values are:
   - exact-match-only (default) - If there is an exact match between the dialed telephone number and an LDAP attribute value in the search response entry, a route is created corresponding to that LDAP attribute. If there is an exact match on multiple attributes, the ordering of LDAP attributes in the LDAP configuration determines the priority for each route. For example, an enterprise that uses the same phone number for both Lync and IP-PBX phones, if the msRTCSIP-Line attribute is configured first, the corresponding next hop (Lync Server) would be used to create the first route in the route list.
   - attribute-order-only - The ordering of LDAP attributes in the LDAP configuration determines the priority for each route. So if the msRTCSIP-Line attribute is configured first, the corresponding next hop (Lync Server) would be used to create the first route in the route list. If there is a valid value present in the search response entry for a LDAP attribute, a route is created corresponding to that LDAP attribute. Note: The LDAP attribute must have a valid value in the response; a match is not necessary for that attribute. If an entry is returned in the search response, there must be a match on at least one other attribute. For example, the dialed telephone number could be +17813284392 (IP-PBX Phone#), and the msRTCSIP-Line in the response could be +17814307069 (Lync phone#). A route is created for the Lync phone#, even though the dialed telephone number is the PBX Phone#.

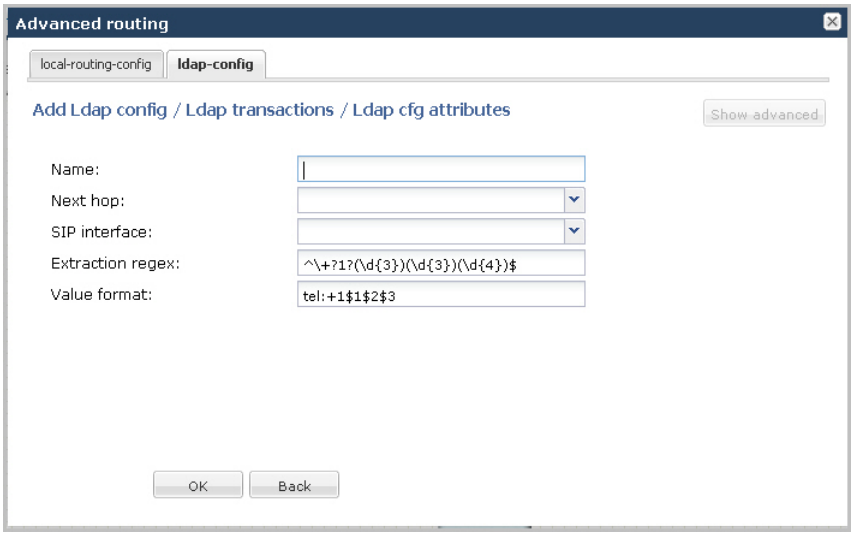
- exact-match-first - If there is an exact match between the dialed telephone number and an LDAP attribute value in the search response entry, the corresponding route gets the highest priority in the route list. For the rest of the routes, the ordering of LDAP attributes in the LDAP configuration determines the priority for each route. So if the msRTCSIP-Line attribute is configured first, the corresponding next hop (Lync Server) would be used to create the second highest priority route in the route list. If there is a valid value present in the search response entry for an LDAP attribute, a route is created corresponding to that LDAP attribute. Note: The LDAP attribute must have a valid value in the response; a match is not necessary for that attribute. If an entry is returned in the search response, there must be a match on at least one other attribute. For example, the dialed telephone number could be +17813284392 (IP-PBX Phone#), and the msRTCSIP-Line in the response could be +17814307069 (Lync phone#). A route is created for the Lync phone#, even though the dialed telephone number is the PBX Phone#.

LDAP Config Attributes

You use the LDAP config attributes object to configure the Active Directory attribute name, next hop for routing SIP requests, the realm for the next hop, a regular expression pattern, and a format for the attribute value. You configure this object for LDAP search queries in the Active Directory.

To configure LDAP config attributes:

1. In the ldap-cfg-attributes section, click <Add>. The following displays.



2. In the Name field, enter the Active Directory attribute name. Default is blank. Valid values are alpha-numeric characters. Some examples of Active Directory attribute names are:
   - ipPhone and msRTCSIP-Line for Lync phone number
   - telephoneNumber for IP PBX phone number
   - mobile for Mobile phone number
3. In the Next hop field, enter the Active Directory's next hop when routing SIP requests. Default is blank. Valid values are alpha-numeric characters. Some examples of the Active Directory's next hop are:
   - SAG (Session Agent Group) name, specified by entering an sag: prefix
   - SA (Sesson Agent) name
   - IP Address
4. In the SIP interface field, select the name of the SIP interface associated with the next hop. This value determines the network interface to which to route the SIP request. This list contains all of the current SIP interfaces configured on the Enterprise Session Director. Default values are:
   - Default ENT - Default Enterprise SIP interface
   - Default SP - Default Service Provider SIP interface
5. In the Extraction regex field, enter the regular expression pattern used to break down the string of digits in the phone number extracted from the request URI of the SIP request. The variables extracted from the phone number

can be used in the attribute-value-format parameter. The default regex is "^\+?1?(\d{2})(\d{3})(\d{4})$". This value assumes that the phone number is a North American phone number specified in the E.164 format. It extracts three variables from the phone number:

- $1 is the area code
- $2 and $3 are the next 3 and 4 digits in the phone number

  Valid values are alpha-numeric characters.

6. In the Value format field, enter the format for the attribute value. These format values are extracted from the phone number using the extraction-regex parameter. The default parameter is "tel:+1$1$2$3". This value assumes that the phone number is a North American phone number specified in the E.164 format, and it recreates the phone number in E.164 format.

   In addition to the E.164 format, Oracle's Active Directory uses other formats as well to store the phone numbers. You can customize the value specified for this parameter to enable successful queries for phone numbers in other formats.

   Valid values are alpha-numeric characters.
7. Click <OK>.

Additional Features

Using the Web GUI, an Administrator can perform configuration on other features on the Enterprise Session Director. These features include:

- Configuring Media Profile
- Configuring Translation Rules
- Configuring SIP Features
- Configuring SIP Manipulations (including Multipurpose Internet Mail Extensions (MIME), ISDN User Part (ISUP) and Session Description Protocol (SDP) rules)
- Adding an SPL

This section provides procedures for configuring each of these features.

Configuring Media Profile

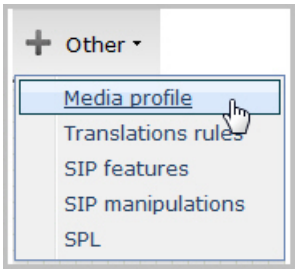
A Media Profile is a group of parameters that the Enterprise Session Director uses as a rule when sending/receiving media over the network. You can configure the following parameters for a Media Profile:

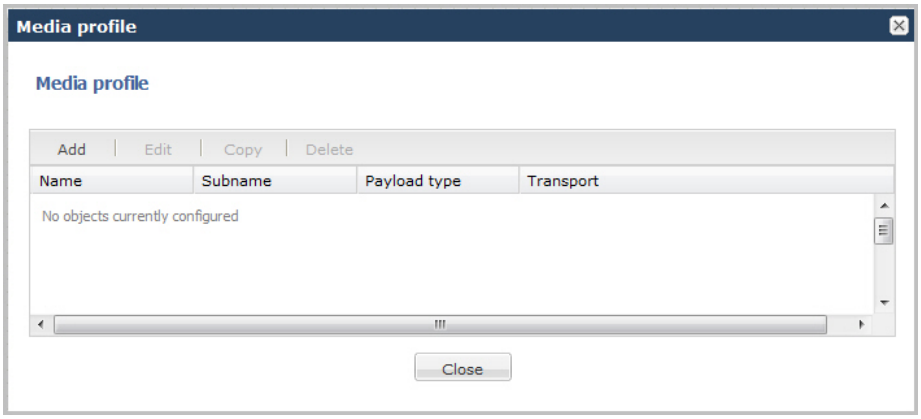
- Name
- Subname
- Payload type
- Transport

For more information about configuring a Media Profile, see the section, Media Profiles per Realm in the Net-Net® Enterprise Session Director Configuration Guide.

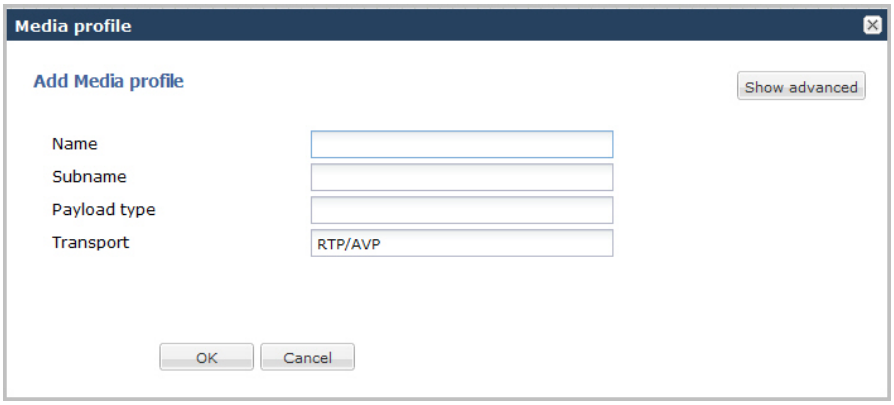
To configure a Media Profile:

1. From the Main Menu, click **Other** > **Media profile** . The following displays.





2. Click <Add>. The following dialog box displays.



3. In the Name field, enter the name for this media profile. For example, you might set the name of the media profile as PCMU. Valid values are alpha-numeric characters. Default is blank.
4. In the Subname field, enter the subname for this media profile. Valid values are alpha-numeric characters. You must use a combination of alpha and numeric characters. Default is blank.
5. In the Payload type field, enter the payload type number that corresponds to the encoding name you entered in Step 3. This value identifies the format in the SDP media lines. Valid values are alpha-numeric characters. Default is blank.

Note: The Payload type value must be numeric if you use the RTP/AVP transport method.

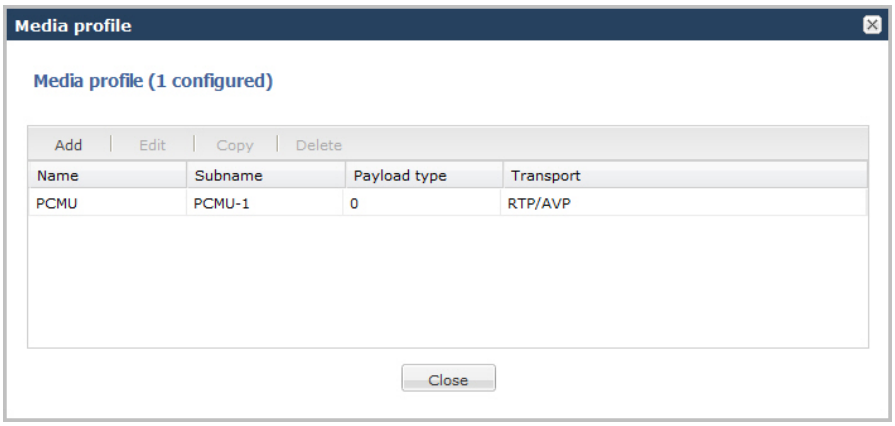
The following is a table of standard audio and visual payload encodings defined in H. Schulzrinne, GND Fokus, RTP Profile for Audio and Visual Conferences with Minimal Control, RFC 1890, and in the RTP Parameters document in IANA's Directory of Generally Assigned Numbers.

Payload Type	Encoding Name	Audio (A)/Visual (V)	Clock Rate (Hz)
0	PCMU	A	8000
1	1016	A	8000
2	G721	A	8000
3	GSM	A	8000
4	G723	A	8000
5	DVI4	A	8000
6	DVI4	A	16000
7	LPC	A	8000

Payload Type	Encoding Name	Audio (A)/Visual (V)	Clock Rate (Hz)
8	PCMA	A	8000
9	G722	A	8000
10	L16	A	44100
11	L16	A	44100
12	QCELP	A	8000
13	reserved	A	
14	MPA	A	90000
15	G728	A	8000
16	DVI4	A	11025
17	DVI4	A	22050
18	G729	A	8000
19	reserved	A	
20	unassigned	A	
21	unassigned	A	
22	unassigned	A	
23	unassigned	A	
dyn	GSM-HR	A	8000
dyn	GSM-EFR	A	8000
dyn	L8	A	var.
dyn	RED	A	
dyn	VDVI	A	var.
24	unassigned	V	
25	CelB	V	90000
26	JPEG	V	90000
27	unassigned	V	
28	nv	V	90000
29	unassigned	V	
30	unassigned	V	
31	H261	V	90000
32	MPV	V	90000
33	MP2T	AV	90000
34	H263	V	90000
35-71	unassigned	?	
72-76	reserved for RTCP conflict avoidance	N/A	N/A

Payload Type	Encoding Name	Audio (A)/Visual (V)	Clock Rate (Hz)
77-95	unassigned	?	
96-127	dynamic	?	
dyn	BT656	V	90000
dyn	H263-1998	V	90000
dyn	MP1S	V	90000
dyn	MP2P	V	90000
dyn	BMPEG	V	90000

6. In the Transport field, enter the type of transport protocol to specify in the Media Profile. Default is RTP/AVP. Valid values are:
   - RTP/AVP
   - UDP
7. Click <OK>. The following displays.



8. Click <Close>.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Media type
- Required bandwidth
- Frames per packet
- Parameters

For more information about these settings, see the section, H.323 features in the *Net-Net® Enterprise Session Director Configuration Guide*.

Configuring Translation Rules

Enterprise Session Director number translation is used to change a layer-5 endpoint name according to prescribed rules. Number translations can be performed on both the inbound and the outbound call legs independently, before and after routing occurs.

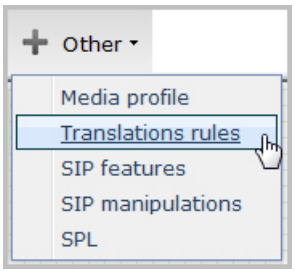
Number translation is used for SIP, H.323, and SIP/H.323 interworking configurations. Number translation takes place twice for both H.323 and SIP calls. The first number translation is applied to the incoming leg of the call, before the outgoing route is selected. The second number translation is applied to the outgoing leg of the call after the outgoing route is selected.

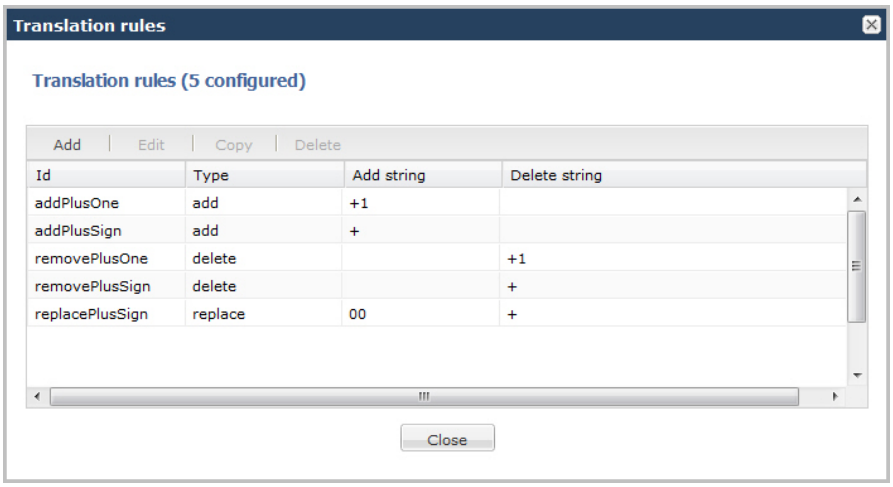
Number translation can be used to strip address prefixes added by external gateways. It can also be used to add a string tag to an address in order to implement a local policy routing scheme, and then remove the tag upon egress from the Net- Net ESD. The most common use of number translation is to add or remove a “1” or a + from a phone number sent from or addressed to a device.

For more information about configuring a translation rules, see the section, Translation Rules in the Net-Net® Enterprise Session Director Configuration Guide.

To configure a Translation Rules:

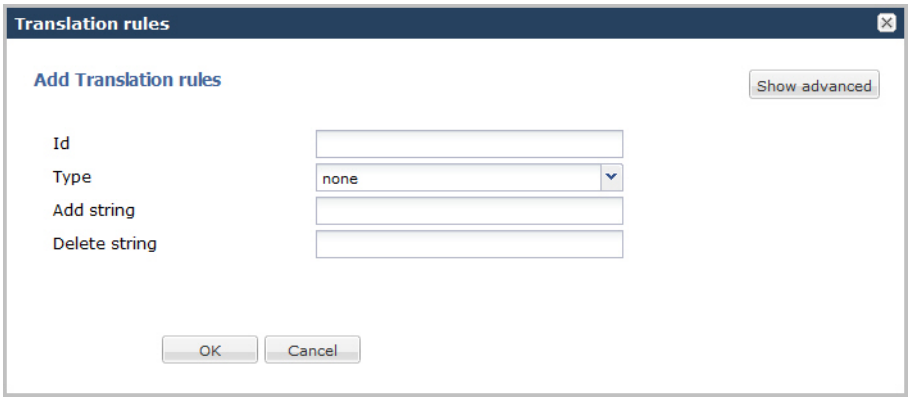
1. From the Main Menu, click **Other** > **Translation** rules. The following displays.





The Translation rules table displays the default translation rules for the Enterprise Session Director. You can select a rule to edit or add a new rule as required.

2. To add new rules, click <Add>. The following dialog box displays.



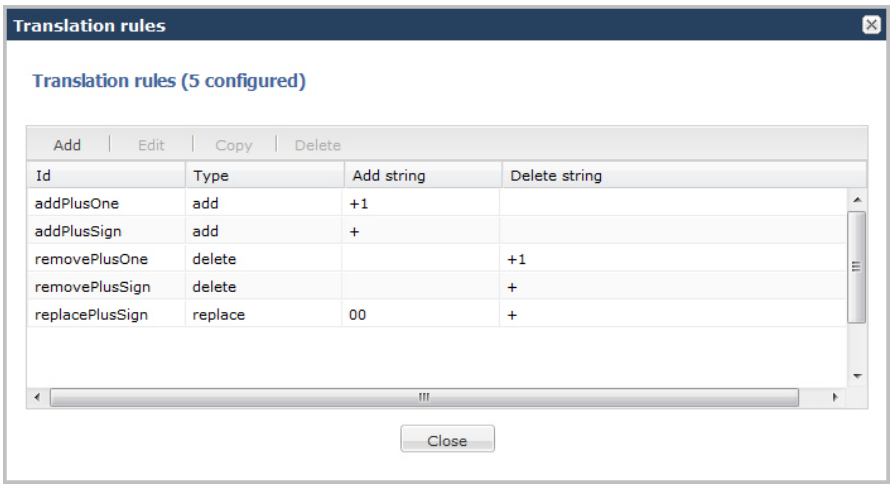
3. In the Id field, enter a descriptive ID name for this translation rule. Valid values are alpha-numeric characters. Default is blank.
4. In the Type field, select the type of translation rule you want to configure. Default is none. Valid values are:
   - add—Adds a character or string of characters to the address

- delete—Deletes a character or string of characters from the address
- none—Translation rule is disabled
- replace—Replaces a character or string of characters within the address

5. In the Add string field, enter the string to be added during address translation to the original address. The value in this field should always be a real value; i.e., this field should not be populated with at-signs (@) or dollar-signs ($). Valid values are alpha-numeric characters. Default is blank.
6. In the Delete string field, enter the string to be deleted from the original address during address translation. Unspecified characters are denoted by the at-sign symbol (@).Valid values are alpha-numeric characters. Default is blank.

   Note: The @ character only works if the type parameter is set to delete. This parameter supports wildcard characters or digits only. For example, valid entries are: delete-string=@@@@@, or delete-string=123456. An invalid entry is delete-string=123@@@.

   When the type is set to replace, this value is used in conjunction with the add-string value. The value specified in the delete-string field is deleted and the value specified in the add-string field is inserted. If no value is specified in the delete-string parameter and the type field is set to replace, then nothing is inserted into the address.
7. Click <OK>. The following displays.



Id	Type	Add string	Delete string
addPlusOne	add	+1	
addPlusSign	add	+	
removePlusOne	delete		+1
removePlusSign	delete		+
replacePlusSign	replace	00	+

8. Click <Close>.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Add Index
- Delete Index

For more information about these settings, see the section, Translation Rules in the *Net-Net® Enterprise Session Director Configuration Guide*.

Configuring SIP Features

SIP extensions that require specific behavior by UAs or proxies are identified by option tags. Option tags are unique identifiers used to designate new options (for example, extensions) in SIP. These option tags appear in the Require, Proxy-Require, and Supported headers of SIP messages.

Option tags are compatibility mechanisms for extensions and are used in header fields such as Require, Supported, Proxy-Require, and Unsupported in support of SIP.

The option tag itself is a string that is associated with a particular SIP option (i.e., an extension). It identifies this option to SIP endpoints.

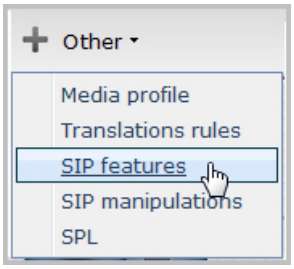
You configure the SIP feature element to define option tag names and their treatment by the Enterprise Session Director when the option tag appears in a Supported header, a Require header, and a Proxy-Require header. If an

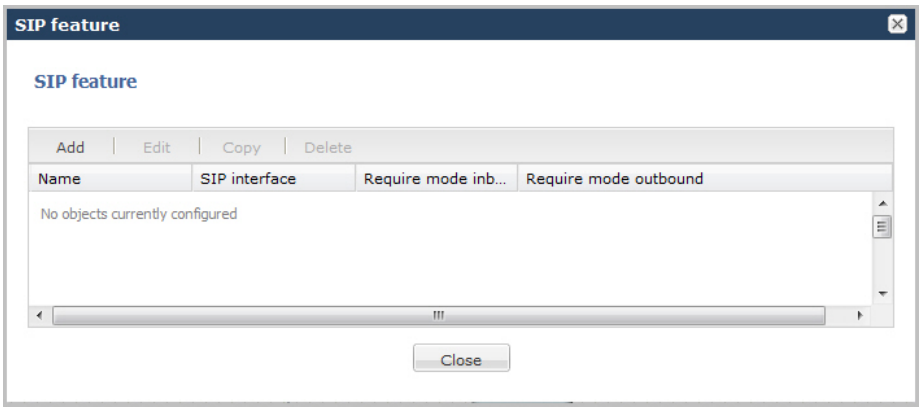
option tag is encountered that is not configured as a SIP feature, the default treatments apply. You only need to configure option tag handling in the SIP feature element when non-default treatment is required.

For more information about configuring a SIP Options Tag, see the section, SIP Options Tag Handling in the Net-Net® Enterprise Session Director Configuration Guide.

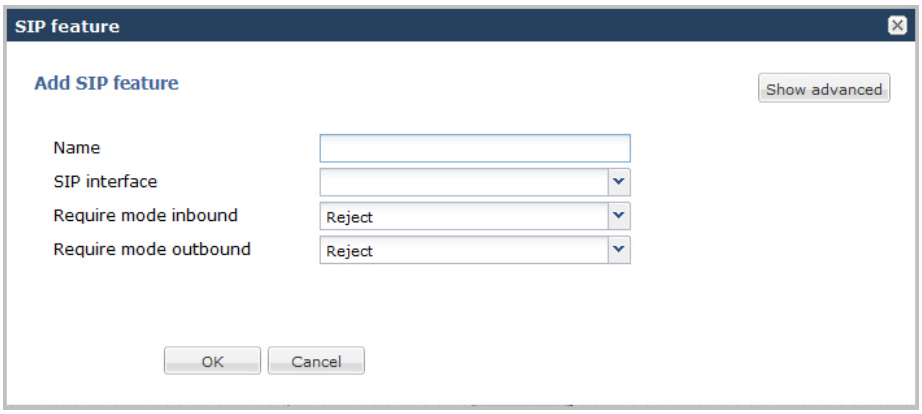
To configure a SIP Options Tag:

1. From the Main Menu, click **Other** > **SIP features**. The following displays.





2. Click <Add>. The following dialog box displays.



3. In the Name field, enter a name for the option tag that appears in the Require, Supported, or Proxy-Require headers of inbound and outbound SIP messages. You must enter a unique value. Valid values are alpha-numeric characters. Default is blank.

   Note: Valid option tags are registered with the IANA Protocol Number Assignment Services under Session Initiation Protocol Parameters. Because option tags are not registered until the SIP extension is published as a RFC, there might be implementations based on Internet-Drafts or proprietary implementations that use unregistered option tags.

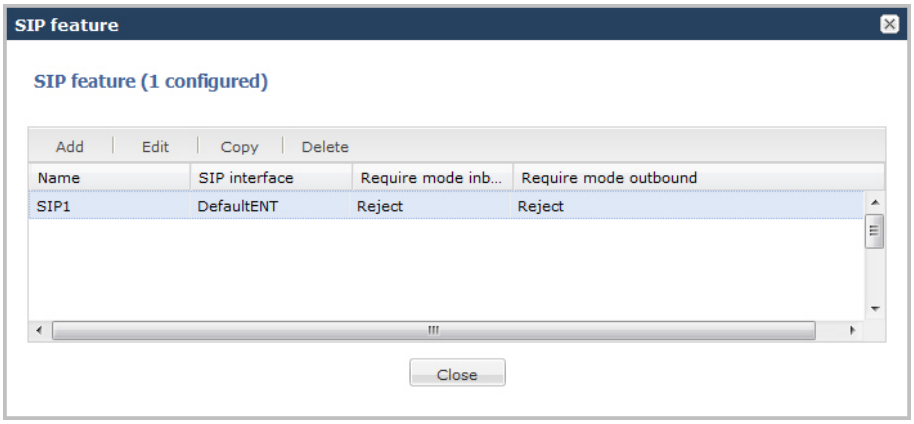
4. In the SIP interface field, select the SIP interface for which to apply this SIP feature. Default is blank. Valid values are:

   - DefaultENT—Default Enterprise SIP interface.

- DefaultSP—Default Service Provider SIP interface.

Note: The drop-down list for the SIP interface field may contain other SIP interfaces if they have been configured in your network.

5. In the Require mode inbound field, select the require proxy mode to define how the option tag is treated when encountered in an incoming SIP message's Proxy-Require header. Default is reject. Valid values are:
   - pass—Indicates the Back-to-Back User Agent (B2BUA) should include the tag in the corresponding outgoing message.
   - reject—Indicates the B2BUA should reject the request with a 420 (Bad Extension) response. The option tag is included in an Unsupported header in the reject response.
6. In the Require mode outbound field, select the require mode to define how the option tag is treated when it is encountered in an outbound SIP message's Require header. The default value is reject. Valid values are:
   - pass—Indicates the B2BUA should include the tag.
   - reject—Indicates the B2BUA should reject the request with a 420 (Bad Extension) response. The option tag is included in an Unsupported header in the reject response.
7. Click <OK>. The following displays.



8. Click <Close>.

Advanced Settings

An Administrator can configure the following more advanced parameters:

- Support mode inbound
- Proxy require mode inbound
- Support mode outbound
- Proxy required mode outbound

For more information about these settings, see the section, SIP Options Tag Handling in the *Net-Net® Enterprise Session Director Configuration Guide*.

Configuring SIP Manipulations

SIP Header Manipulation provides the flexibility to add, remove, or modify any attribute in a SIP message on the Enterprise Session Director. The most common reason for doing this is to fix an incompatibility problem between two SIP endpoints. This could range from anything such as Softswitch/PSTN incompatibility or an issue between two different IP PBX platforms in a multi-site Enterprise where calls between them fail due to issues in the SIP messaging.

The SIP header and parameter manipulation feature allows you to add, modify, and delete SIP headers and parts of SIP headers called SIP header elements. SIP header elements are the different subparts of the header, such as the header value, header parameter, URI parameter and so on (excluding the header name).

To enable the SIP header and parameter manipulation functionality, you create header manipulation rulesets in which you specify header manipulation rules, as well as optional header element rules that operate on specified header elements. You then apply the header manipulation ruleset as inbound or outbound for a session agent or SIP interface.

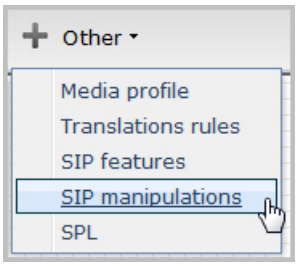
Header manipulation rules operate on the header you specify when you configure the rule. A header manipulation rule can also be configured with a list of element rules, each of which would specify the actions you want performed for a given element of this header.

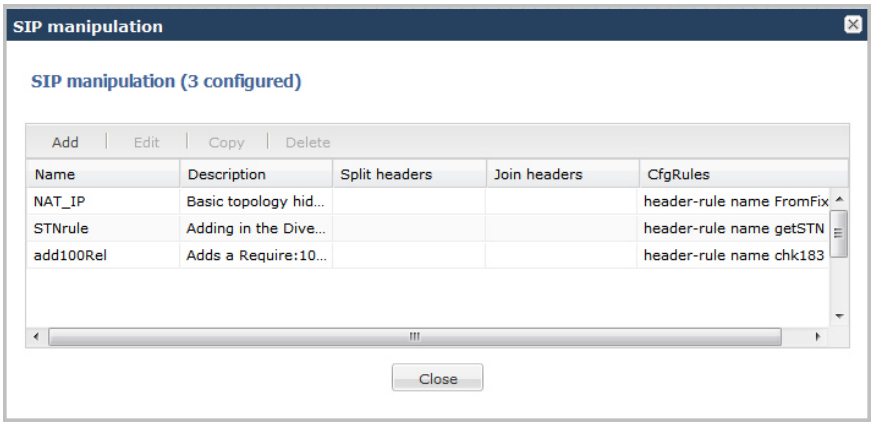
Header element rules perform operations on the elements of a header. Header elements include all subparts of a header; excluding the header name. For example, header value, header parameter, URI parameter, and so on.

For more information about configuring SIP Manipulation, see the section, Static SIP Header and Parameter Manipulation in the Net-Net® Enterprise Session Director Configuration Guide.

To configure SIP Manipulation:

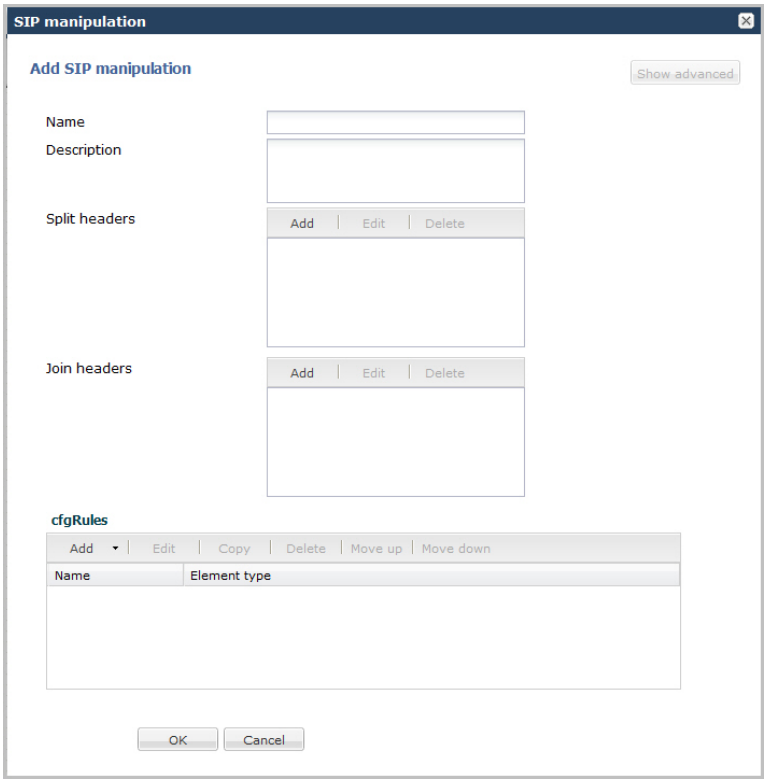
1. From the Main Menu, click **Other** > **SIP manipulation**





The SIP manipulation table displays the default header manipulation rules for the Enterprise Session Director. You can select a rule to edit or add a new rule as required.

2. To add a new rule, click <Add>. The following dialog box displays.



3. In the Name field, enter the name of the header to which this rule applies. The name you enter here must match a header name. This is a case-insensitive string that is compared to the header name for matching. You need to create a rule using the long form of the header name and a rule using the compact form of the header name. Valid values are alpha-numeric characters. Default is blank.

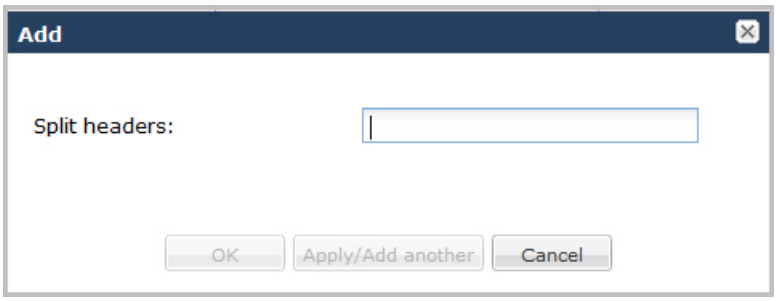
   Note: The Request-URI header is identified as request-uri.

4. In the Description field, enter a description for this header manipulation rule. Valid values are alpha-numeric characters. Default is blank.

Specify Split Headers

In the Split headers field, enter the elements of the message header that you want the Enterprise Session Director to split.

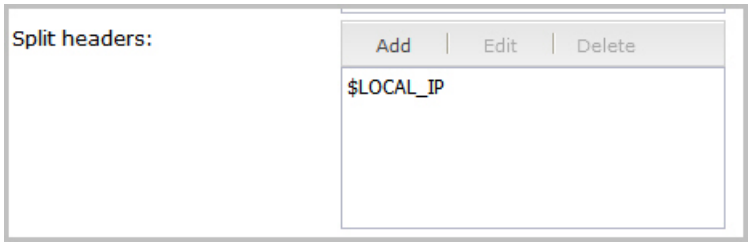
Click <Add>. The following displays.



In the Split headers field, enter the header element you want to split. For example, $LOCAL_IP.

To add the element to the list and apply another one, click <Apply/Add Another>.

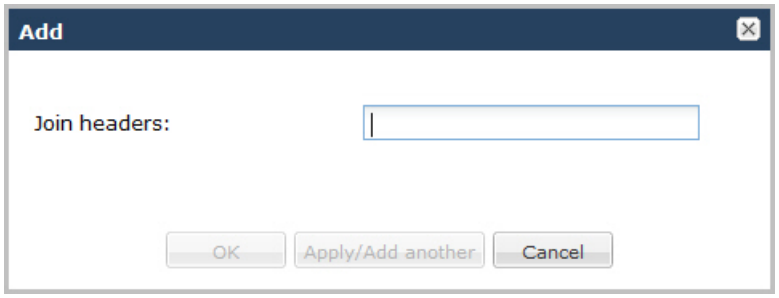
When you have completed adding header elements to the Split header list, click <OK>. The following displays.



Specify Join Headers

In the Join headers field, enter the header element you want the Enterprise Session Director to join.

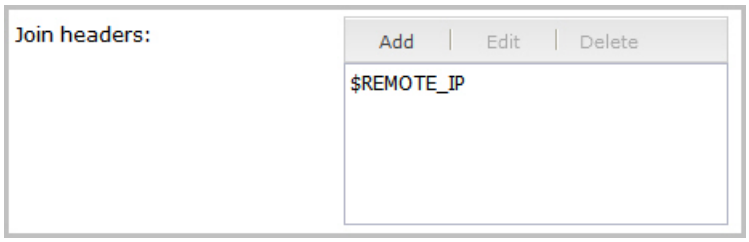
Click <Add>. The following displays.



In the Join headers field, enter the header element you want to join. For example, $REMOTE_IP.

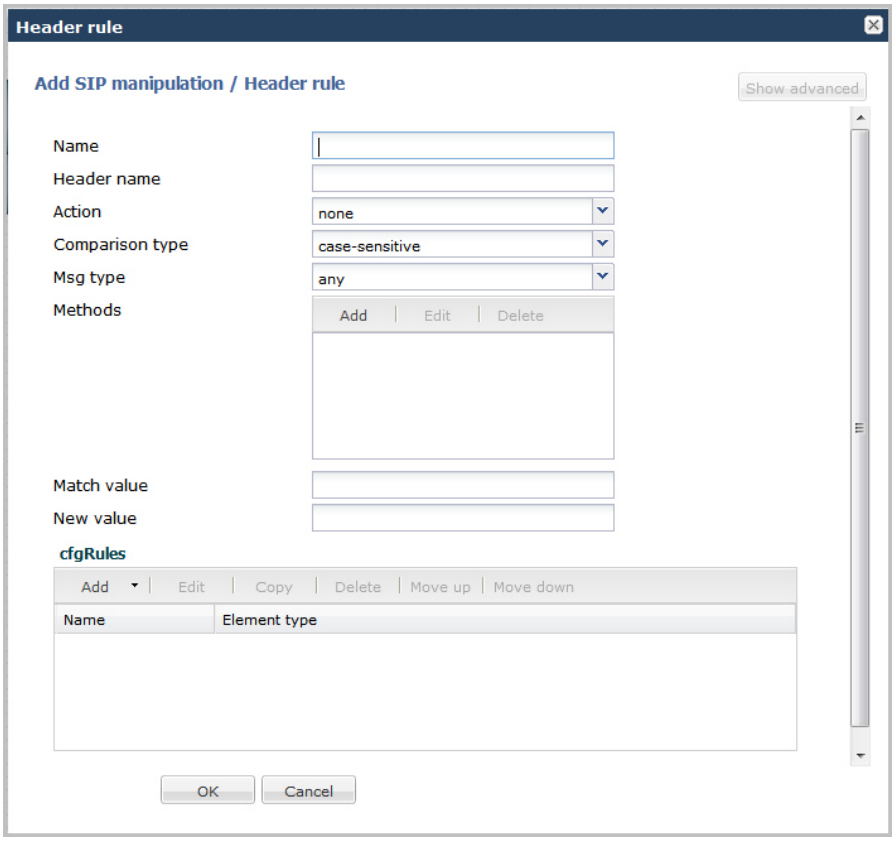
To add the element to the list and apply another one, click <Apply/Add Another>.

When you have completed adding header elements to the Join header list, click <OK>. The following displays.



Specify Configuration Rule

1. In the cfgRules field, enter the rule to use in the Enterprise Session Director configuration. These rules use the "Split" and Join headers you specified above.
2. Click <Add>, and select header-rule from the drop-down list. The following displays.



3. In the Name field, enter a name you want to use for this rule set. Valid values are alpha-numeric characters. Default is blank.
4. In the Header name field, enter the name of the header to which this rule applies. The name you enter here must match a header name. This is a case-insensitive string that is compared to the header name for matching. You need to create a rule using the long form of the header name and a rule using the compact form of the header name. Valid values are alpha-numeric characters. Default is blank.

   Note: The Request-URI header is identified as request-uri.

5. In the Action field, select an action you want applied to the header specified in the Name parameter. Default is none. Valid values are:
   - add—Adds a new header, if that header does not already exist.
   - delete—Deletes the header, if it exists.
   - find-replace-all—Finds all matching headers and replaces it with the header you specified for “Split” and Join.
   - log—Logs the header.
   - manipulate—Manipulates the elements of this header to the element rules configured.
   - monitor—Monitors the header.
   - store—Stores the header.
   - none—(default) No action is taken.
   - reject—Rejects the header.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the header.
6. In the Comparison type field, select the way that you want SIP headers to be compared. This choice dictates how the Enterprise Session Director processes the match rules against the SIP header. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to header rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to header rule regardless of the case of the header.

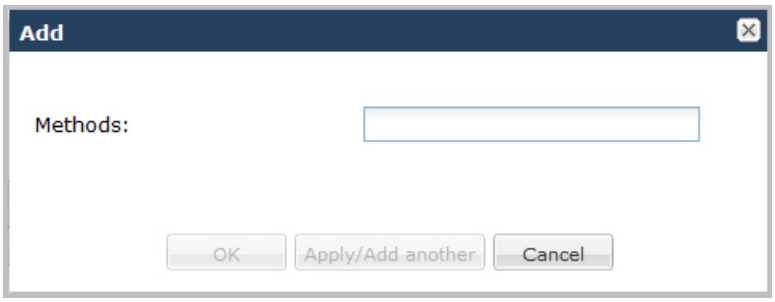
- case-sensitive—(default) Header is compared to the header rule and case must be exactly the same or it is rejected.
- pattern-rule—Header is compared to the header rule and the pattern must be exactly the same or it is rejected.
- refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
- refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.

7. In the Msg type field, select the message type to which this header rule applies. Default is any. Valid values are:

- any—(default) Requests, replies, and out-of-dialog messages
- out-of-dialog—Out of dialog messages only.
- reply—Reply messages only
- request—Request messages only

8. In the Methods field, specify the SIP method names to which you want to apply this header rule.

Click <Add>. The following diplays.

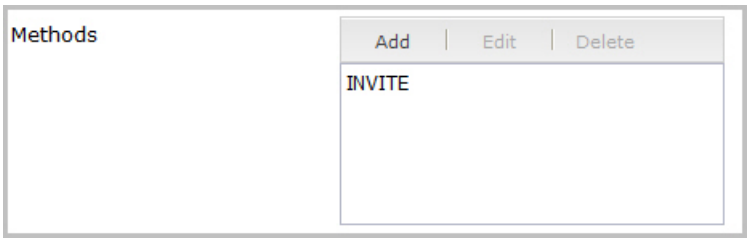


In the Methods field, enter SIP method names to which you want to apply this header rule. For example, INVITE, ACK, BYE.

Note: This field is empty by default. If you leave the method field empty, the header rule applies to all methods.

To add the method to the list and apply another one, click <Apply/Add Another>.

When you have completed adding methods, click <OK>. The following displays.



9. In the Match value field, enter the value you want to match against the element value for an action to be performed.

10. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

  For example:

  sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
- Pre-defined parameters always start with a $. The following table describes the pre-defined parameters.

Pre-defined Parameters Table

Parameter	Description
$ORIGINAL	Original value of the element is used.
$LOCAL_IP	IP address of the SIP interface on which the message was received for inbound manipulation; or sent on for outbound manipulation.
$REMOTE_IP	IP address the message was received from for inbound manipulation; or being sent to for outbound manipulation.
$REMOTE_VIA_HOST	Host from the top Via header of the message is used.
$TRUNK_GROUP	Trunk group is used.
$TRUNK_GROUP_CONTEXT	Trunk group context is used.

The following table describes the Operators.

Operators Table

Operator	Description
+	Append the value to the end. For example: acme”+”packet generates acmepacket
+^	Prepends the value. For example: acme”+^”packet generates packetacme
-	Subtract at the end. For example: 112311”-”11 generates 1123
-^	Subtract at the beginning. For example: 112311”-^”11 generates 2311

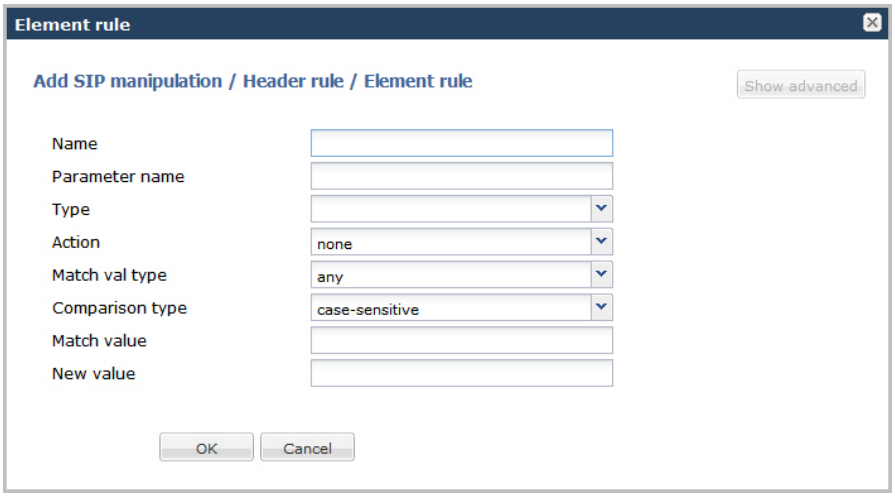
Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
$ORIGINAL+”my name is \”john\””
$ORIGINAL-^781+^617
```

Specify Element Rule

Header element rules perform operations on the elements of a header. Header elements include all subparts of a header; excluding the header name. For example, header value, header parameter, URI parameter, and so on.

1. In the cfgRules field, click <Add>, and then select element-rule from the drop-down list. This allows you to define the element rules you want to use to be performed on the elements of the header specified by the header rule. The following dialog box displays.



2. In the Name field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the Parameter name field, enter the parameter name to which this rule applies. The parameter name depends on the element name you entered in step 2. For uri-param, uri-user-param, and header-param it is the parameter name to be added, replaced, or deleted. For all other types, it serves to identify the element rule and any name can be used. Valid values are alpha-numeric characters. Default is blank.
4. In the Type field, select the type of element on which to perform the action. Default is blank. Valid values are:
   - header-param—Perform the action on the parameter portion of the header.
   - header-param-name—Perform the action on the header parameter name.
   - header-value—Perform the action on the header value.
   - mime—Perform the action on Multipurpose Internet Mail Extensions (MIME).
   - reason-phrase—Perform the action on reason phrases.
   - status-code—Perform the action on status codes.
   - teluri-param—Perform the action on a SIP telephone Uniform Resource Identifier (URI).
   - uri-display—Perform the action on the display of the SIP URI.
   - uri-header—Perform the action on a header included in a request constructed from the URI.
   - uri-header-name—Perform the action on a SIP URI header name.
   - uri-host—Perform the action on a Host portion of the SIP URI.
   - uri-param—Perform the action on the parameter included in the SIP URI.
   - uri-param-name—Perform the action on the name parameter of the SIP URI.
   - uri-phone-number-only—Perform the action on a SIP URI phone number only.
   - uri-port—Perform the action on the port number portion of the SIP URI.
   - uri-user—Perform the action on the user portion of the SIP URI.
   - uri-user-only—Perform the action on the user portion only of the SIP URI.
   - uri-user-param—Perform the action on the user parameter of the SIP URI.
5. In the Action field, enter the action you want applied to the element specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete-element—Deletes the element, if it exists.
   - delete-header—Delete the header where this element exists.

- find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
- log—Logs the element.
- none—(default) No action is taken.
- reject—Rejects the element.
- replace—Replaces the element
- sip-manip—Manipulates the SIP elements of this header to the element rules configured.
- store—Stores the element.

6. In the Match val type field, select the type of value that needs to be matched to the match-field entry for the action to be performed. Default is any. Valid values are:

- any—(default) Element value in the SIP message is compared with the match-value field entry. If the match-value field is empty, all values are considered a match.
- fqdn—Element value in the SIP message must be a valid FQDN to be compared to the match-value field entry. If the match-value field is empty, any valid FQDN is considered a match. If the element value is not a valid FQDN, it is not considered a match.
- ip—Element value in the SIP message must be a valid IP address to be compared to the match-value field entry. If the match-value field is empty, any valid IP address is considered a match. If the element value is not a valid IP address, it is not considered a match.

7. In the Comparison type field, select the way that you want SIP elements to be compared. This choice dictates how the Enterprise Session Director processes the match rules against the SIP header. Default is case-sensitive. Valid values are:

- boolean—Header is compared to header rule and must match exactly or it is rejected.
- case-insensitive—Header is compared to header rule regardless of the case of the header.
- case-sensitive—(default) Header is compared to the header rule and case must be exactly the same or it is rejected.
- pattern-rule—Header is compared to the header rule and the pattern must be exactly the same or it is rejected.
- refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
- refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.

8. In the Match value field, enter the value you want to match against the element value for an action to be performed.

9. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

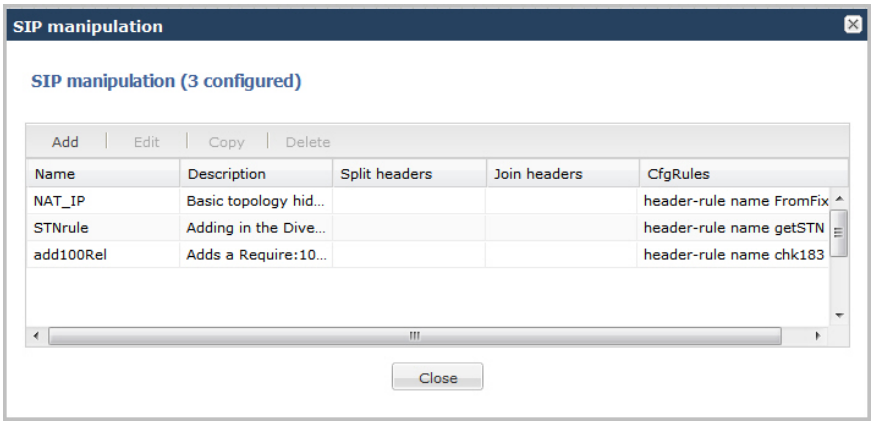
  For example:

  sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
- Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
- Operators parameters - For valid values, see the Operators Table.

  Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
$ORIGINAL+”my name is \”john\””
$ORIGINAL-^781+^617
```

10. Click <OK>. The Header Rule dialog box displays.



11. Click <Close>.

Configuring MIME Rules

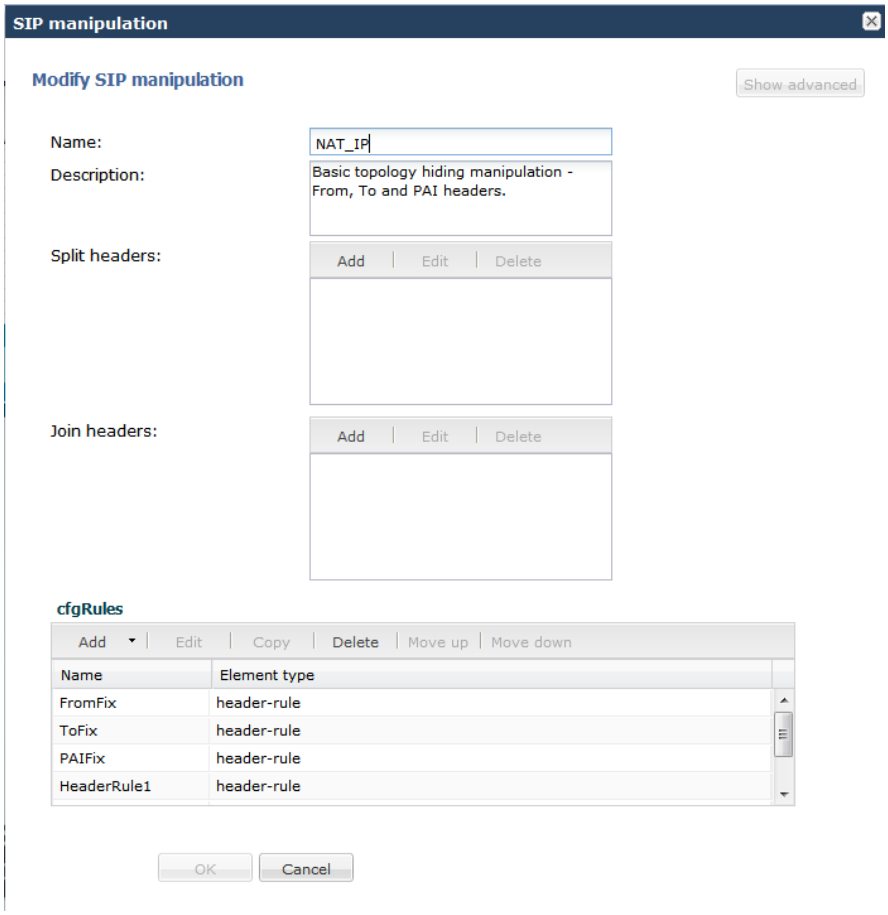
Using the SIP Head Manipulation Rule (HMR) feature set, you can manipulate Multipurpose Internet Mail Extensions (MIME) types in SIP message bodies. While you can manipulate the body of SIP messages or a specific content type using other iterations of SIP HMR, this version gives you the power to change the MIME attachment of a specific type within the body by using regular expressions.

To achieve this, you use the find-replace-all action type, which enables the search for a particular string and the replacement of all matches for that type. Although you use find-replace-all to manipulate MIME attachments, it can also be used to achieve other goals in SIP HMR. Note that using find-replace-all might consume more system resources than other HMR types. Therefore this powerful action type should only be used when another type cannot perform the type of manipulation you require.

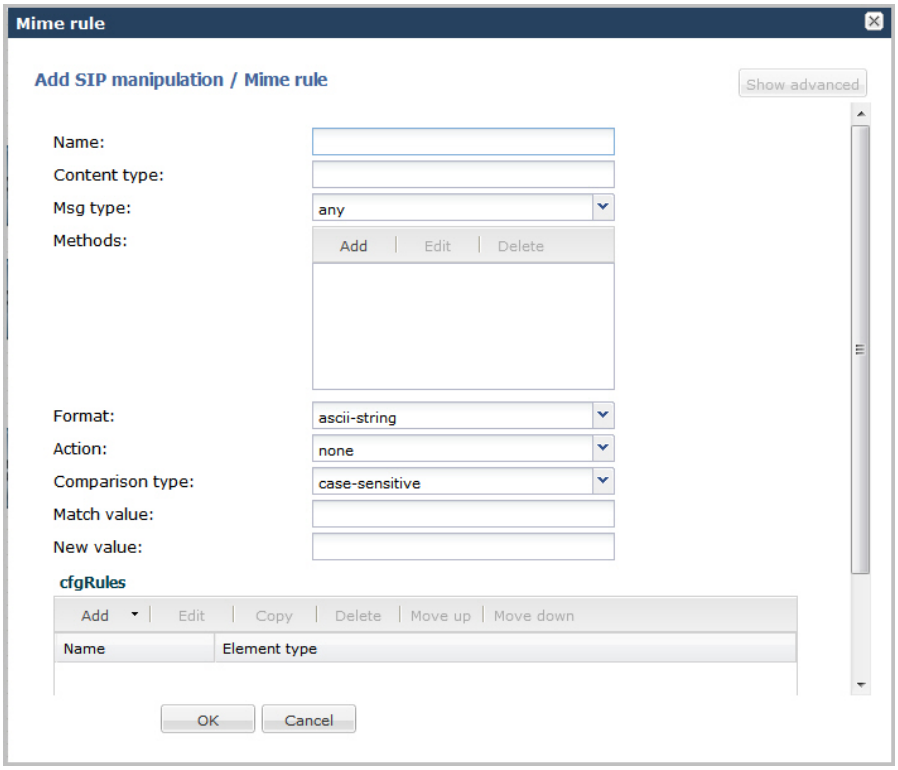
For more information about configuring MIME rules, see the section, MIME Support in the *Net-Net® Enterprise Session Director Configuration Guide*.

To configure MIME rules:

1. After adding a new SIP manipulation rule, go to the SIP Manipulation dialog box.

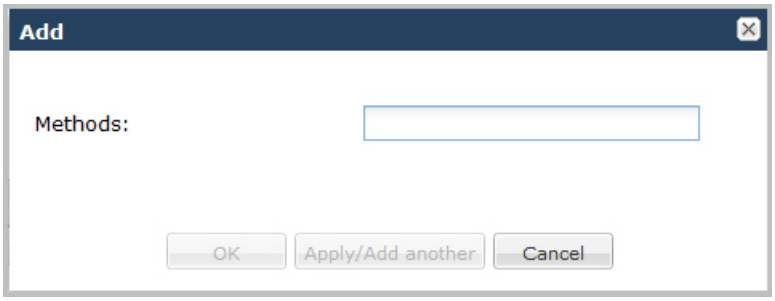


2. In the cfgrules field, click <Add> and select mime-rules from the drop-down list. This allows you to specify mime rules for the header rules you configured. The following dialog box displays.



3. In the Name field, enter a name you want to use for this MIME rule. Valid values are alpha-numeric characters. Default is blank.
4. In the Content type field, enter the content type of the MIME. For example, application/sipfrag or application/sdp. This value is the content type that the Enterprise Session Director looks for in the MIME. Valid values are alpha-numeric characters. Default is blank.
5. In the Msg type field, specify the type of message to which this MIME rule applies. Default is any. Valid values are:
   - any—Both Requests and Reply messages
   - out-of-dialog—Out of dialog messages only.
   - reply—Reply messages only
   - request—Request messages only
6. In the Methods field, specify the SIP method names to which you want to apply this MIME rule.

   Click <Add>. The following diplays.

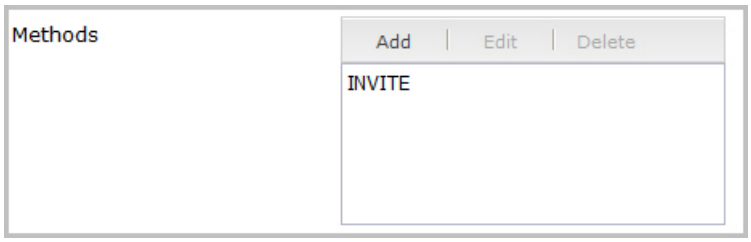


   In the Methods field, enter SIP method names to which you want to apply this MIME rule. For example, INVITE, ACK, BYE.

   Note: This field is empty by default. If you leave the method field empty, the MIME rule applies to all methods.

   To add the method to the list and apply another one, click <Apply/Add Another>.

When you have completed adding methods, click <OK>. The following displays.



7. In the Format field, select the format to apply to this MIME rule. Default is ascii-string. Valid values are:
   - ascii-string - a character-encoding scheme that represents text (128 ASCII codes, 7 bits)
   - binary-ascii - encoding scheme where each byte of an ASCII character is used; can use up to 256 bit patterns
   - hex-ascii - encoding scheme that uses a string of numbers (no spaces) to represent each ASCII character.
8. In the Action field, enter the action you want applied to the MIME rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete—Deletes the element, if it exists.
   - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
   - log—Logs the element.
   - manipulate—Manipulates the elements of this header to the element rules configured.
   - monitor—Monitors the header for this element.
   - none—(default) No action is taken.
   - reject—Rejects the element.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the element.
9. In the Comparison type field, select the way that you want the MIME to be compared with this MIME rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
   - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
   - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
   - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
   - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
10. In the Match value field, enter the value you want to match against the element value for an action to be performed.
11. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
    - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

      For example:

      sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
    - Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
    - Operators parameters - For valid values, see the Operators Table.

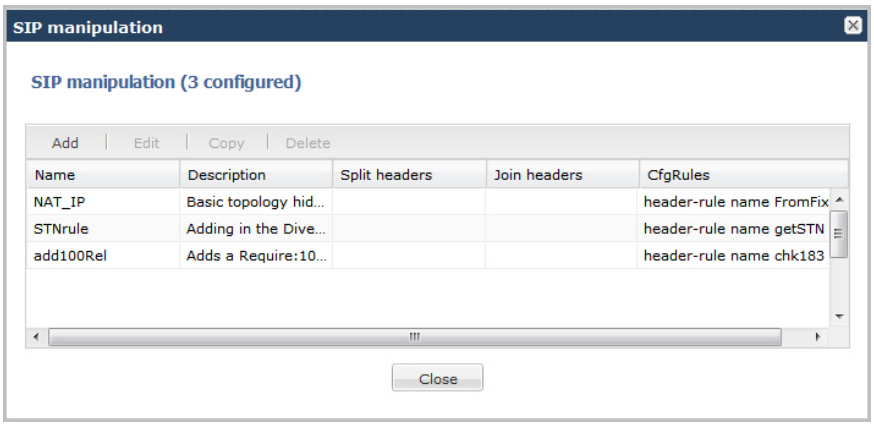
      Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
```

```
$ORIGINAL+"my name is \"john\""
$ORIGINAL-^781+^617
```

12. Click <OK>. The MIME Rule dialog box displays.

13. Click <OK>. The SIP Manipulation dialog box displays.



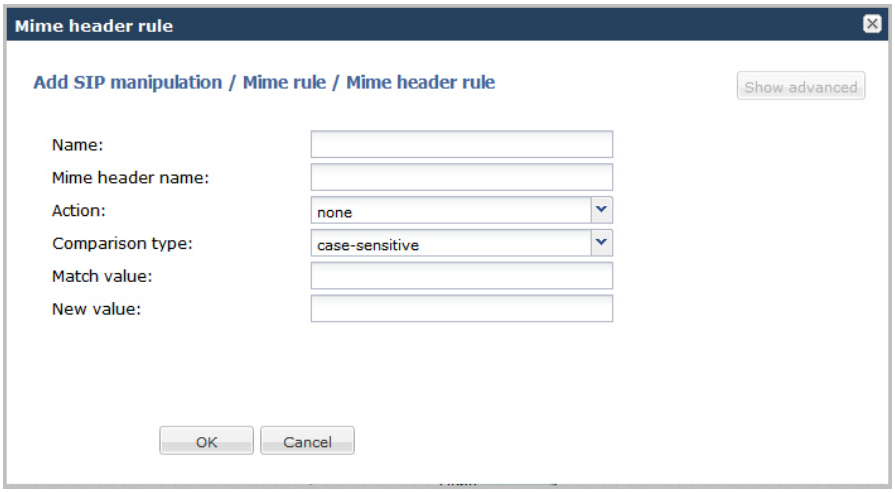
14. Click <Close>.

Configuring MIME Header Rule

You can configure MIME header rules within a MIME rule. Use the following procedure to configure a MIME header rule.

To configure a MIME header rule:

1. In the MIME rules dialog box, in the cfgRules field, click <Add>, and then select mime-header-rule from the drop-down list. This allows you to define the MIME rules you want to use to be performed on the elements of the header specified by the MIME rule. The following dialog box displays.



2. In the Name field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.

3. In the Mime header name field, enter the parameter name to which this rule applies. The parameter name depends on the element name you entered in step 2. For uri-param, uri-user-param, and header-param it is the parameter

name to be added, replaced, or deleted. For all other types, it serves to identify the element rule and any name can be used. Valid values are alpha-numeric characters. Default is blank.

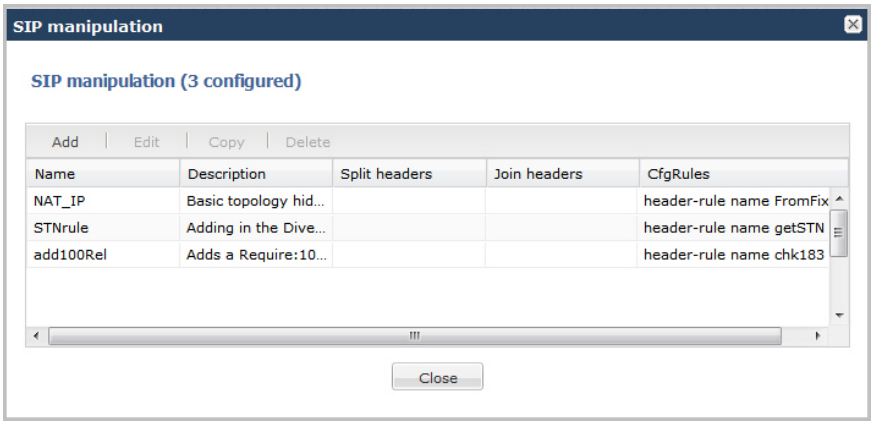
4. In the Action field, enter the action you want applied to the MIME rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete—Deletes the element, if it exists.
   - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
   - log—Logs the element.
   - monitor—Monitors the header for this element.
   - none—(default) No action is taken.
   - reject—Rejects the element.
   - replace—Replaces the element.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the element.
5. In the Comparison type field, select the way that you want the MIME to be compared with this MIME rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
   - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
   - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
   - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
   - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
6. In the Match value field, enter the value you want to match against the element value for an action to be performed.
7. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
   - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

     For example:

     sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
   - Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
   - Operators parameters - For valid values, see the Operators Table.

     Examples of entries for the new-value field.

     ```
     $ORIGINAL+acme
     $ORIGINAL+”my name is john”
     $ORIGINAL+”my name is \”john\””
     $ORIGINAL-^781+^617
     ```
8. Click <OK>. The MIME Rule dialog box displays.
9. Click <OK>. The SIP Manipulation dialog box displays.



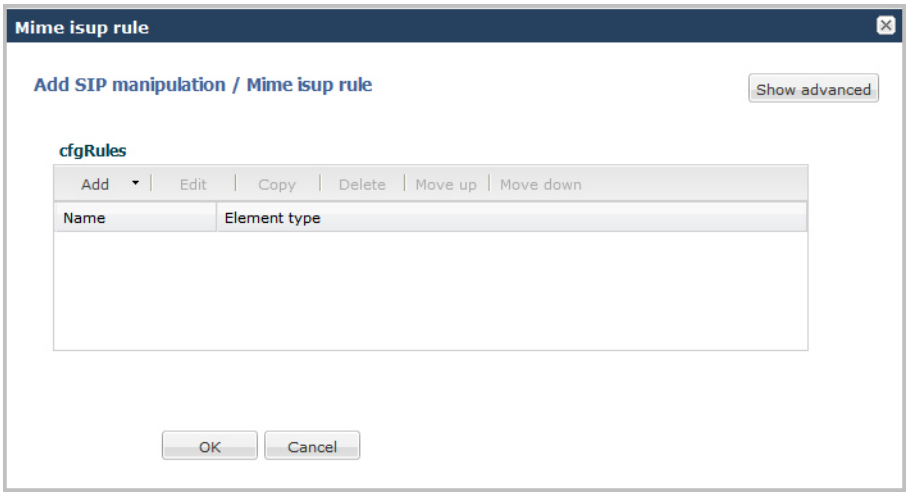
10. Click <Close>.

Configuring MIME ISUP Rule

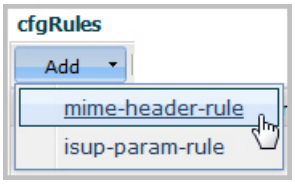
You can configure a MIME ISDN User Part (ISUP) rule for a SIP manipulatin rule. Use the following procedure to configure a MIME ISUP rule.

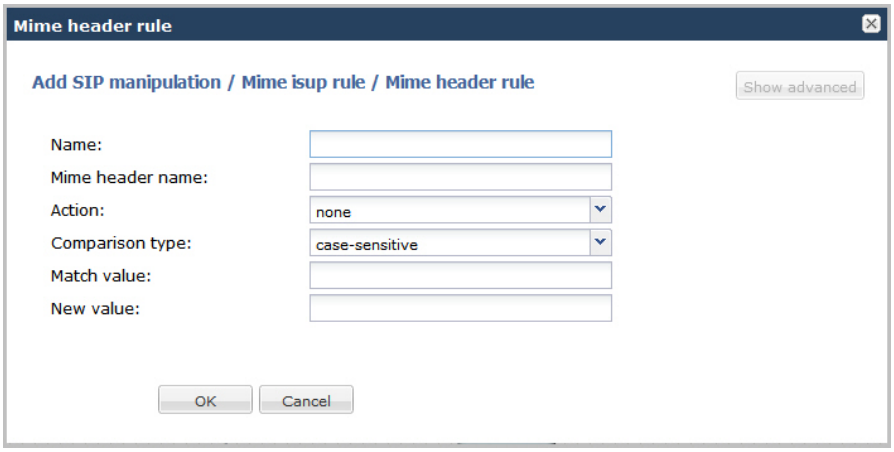
To configure a MIME ISUP rule:

1. In the SIP Manipulation dialog box, in the cfgRules field, click <Add>, and then select mime-isup-rule from the drop-down list. This allows you to define the MIME ISUP rules you want to use to be performed on the elements of the header specified by the MIME rule. The following dialog box displays.



2. In the cfgRules field, click <Add>, and then select mime-header-rule from the drop-down list. The following dialog box displays.





3. In the Name field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
4. In the Mime header name field, enter the parameter name to which this rule applies. The parameter name depends on the element name you entered in step 3. For uri-param, uri-user-param, and header-param it is the parameter name to be added, replaced, or deleted. For all other types, it serves to identify the element rule and any name can be used. Valid values are alpha-numeric characters. Default is blank.
5. In the Action field, enter the action you want applied to the MIME rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete—Deletes the element, if it exists.
   - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
   - log—Logs the element.
   - monitor—Monitors the header for this element.
   - none—(default) No action is taken.
   - reject—Rejects the element.
   - replace—Replaces the element.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the element.
6. In the Comparison type field, select the way that you want the MIME to be compared with this MIME rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
   - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
   - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
   - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
   - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
7. In the Match value field, enter the value you want to match against the element value for an action to be performed.

8. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
   - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

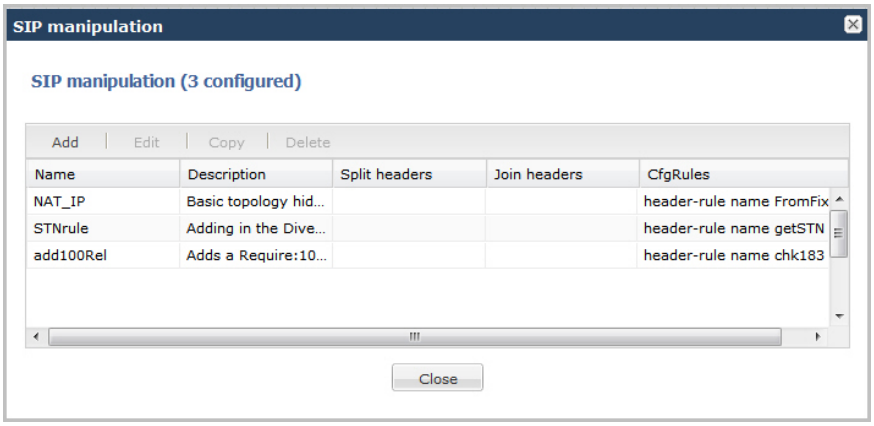
     For example:

     sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
   - Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
   - Operators parameters - For valid values, see the Operators Table.

     Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
$ORIGINAL+”my name is \”john\””
$ORIGINAL-^781+^617
```

9. Click <OK>. The MIME ISUP Rule dialog box displays.
10. Click <OK>. The SIP Manipulation dialog box displays.



11. Click <Close>.

Configuring ISUP Param Rules

The ISUP param rules are for advanced users only. This feature configures the following for the ISUP param rules:

- Name
- Type
- Format
- Action
- Comparison Type
- Match Value
- New Value

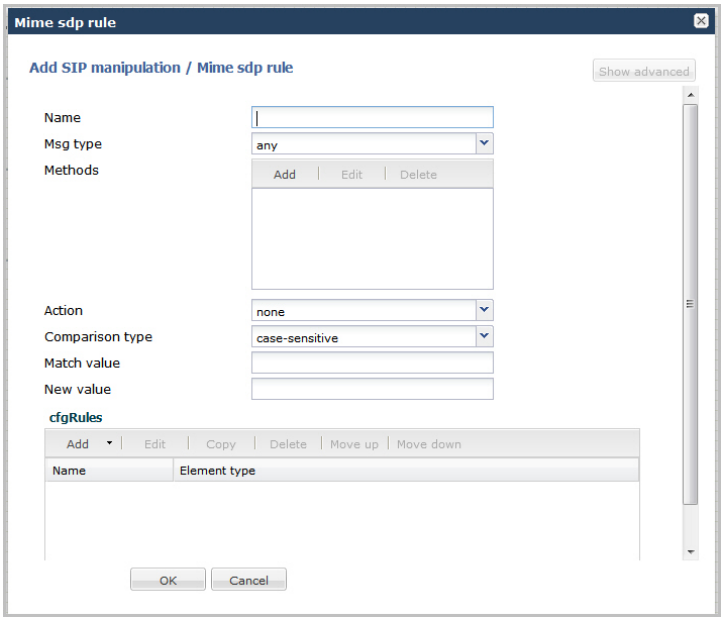
For more information about configuring ISUP Param Rules, see the section, Regular Experssions and Boolean Expressions in the *Net-Net® Enterprise Session Director Configuration Guide*.

Configuring MIME SDP Rules

You can configure MIME Session Description Protocol (SDP) rules for SIP Manipulation on the Enterprise Session Director if required. Use the following procedure to configure MIME SDP rules.

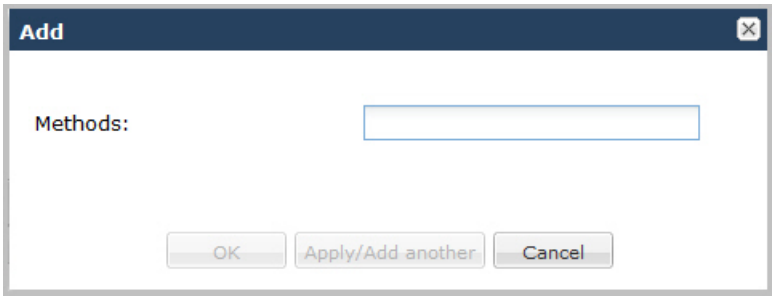
To configuration MIME SDP rules:

1. From the SIP Manipulation dialog box, in the cfgRules field, click <Add>, and then select mime-sdp-rule from the drop-down list. The following dialog box displays.



2. In the Name field, enter a name you want to use for this MIME SDP rule. Valid values are alpha-numeric characters. Default is blank.
3. In the Msg type field, specify the type of message to which this MIME SDP rule applies. Default is any. Valid values are:
   - any—Both Requests and Reply messages
   - out-of-dialog—Out of dialog messages only.
   - reply—Reply messages only
   - request—Request messages only
4. In the Methods field, specify the SIP method names to which you want to apply this MIME SDP rule.

   Click <Add>. The following diplays.

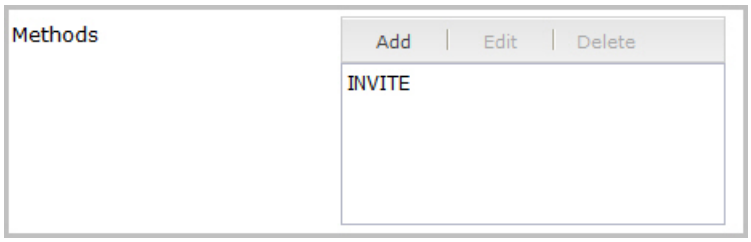


In the Methods field, enter SIP method names to which you want to apply this MIME SDP rule. For example, INVITE, ACK, BYE.

Note: This field is empty by default. If you leave the method field empty, the MIME rule applies to all methods.

To add the method to the list and apply another one, click <Apply/Add Another>.

When you have completed adding methods, click <OK>. The following displays.



5. In the Action field, enter the action you want applied to the MIME SDP rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete—Deletes the element, if it exists.
   - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
   - log—Logs the element.
   - manipulate—Manipulates the elements of this header to the element rules configured.
   - monitor—Monitors the header for this element.
   - none—(default) No action is taken.
   - reject—Rejects the element.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the element.
6. In the Comparison type field, select the way that you want the MIME to be compared with this MIME SDP rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
   - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
   - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
   - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
   - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
7. In the Match value field, enter the value you want to match against the element value for an action to be performed.
8. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
   - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

     For example:

     sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
   - Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
   - Operators parameters - For valid values, see the Operators Table.

     Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
$ORIGINAL+”my name is \”john\””
$ORIGINAL-^781+^617
```

Configuring MIME Header Rule for SDP

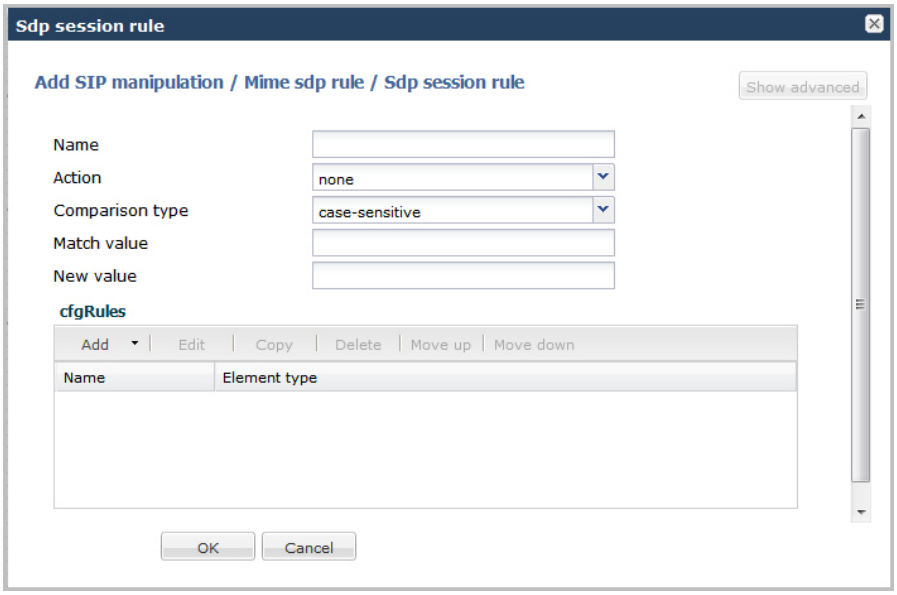
You can configure the MIME header rule for the MIME SDP rule if required. Use the procedures in Configuring MIME Header Rule to configure the MIME header rule fo SDP.

Configuring SDP Session Rule

You can configure the SDP session rules for the MIME SDP rules if required. Use the following procedure to configure SDP Session rules.

To configure SDP session rules:

1. In the MIME SDP Rules dialog box, in the cfgRules field, click <Add>, and then select sdp-session-rule from the drop-down list. This allows you to define the SDP session rules you want to use to be performed on the elements of the header specified by the MIME rule. The following dialog box displays.



2. In the Name field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the Action field, enter the action you want applied to the SDP session rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete—Deletes the element, if it exists.
   - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
   - log—Logs the element.
   - monitor—Monitors the header for this element.
   - none—(default) No action is taken.
   - reject—Rejects the element.
   - replace—Replaces the element.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the element.

4. In the Comparison type field, select the way that you want the MIME to be compared with this SDP session rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
   - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
   - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
   - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
   - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
5. In the Match value field, enter the value you want to match against the element value for an action to be performed.
6. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
   - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

     For example:

     sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
   - Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
   - Operators parameters - For valid values, see the Operators Table.

     Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
$ORIGINAL+”my name is \”john\””
$ORIGINAL-^781+^617
```

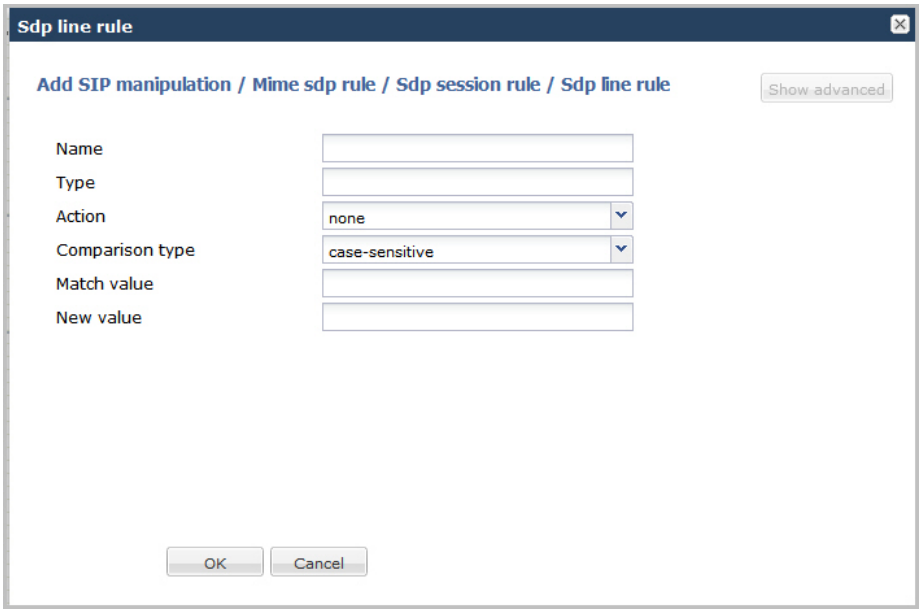
Configuring SDP Line Rules for Sessions

When configuring the SDP session rules, you can also configure the SDP line rules. For more information about configuring SDP line rules, see the section, sdp-line-rule in the *Net-Net® Enterprise Session Director Configuration Guide*.

Use the following procedure to configure the SDP line rules.

To configure SDP line rules:

1. From the SDP Session Rule dialog box, in the cfgRules field, click <Add>, and then select sdp-line-rules from the drop-down list. This allows you to define the SDP line rules you want to use to be performed on the elements of the header specified by the SDP session rule. The following dialog box displays.



2. In the Name field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the Type field, enter the applicable SDP descriptor for the SDP line rule. SDP descriptors are added to the SDP, adhering to the definitions in RFC 4566. Default is blank. Valid values are:

Session Description	
v	Protocol version
o	Originator and session identifier
s	Session name
i	Session information*
u	URI of description*
e	Email address*
p	Phone number*
c	Connection information - not required if included in all media*
b	Zero or more bandwidth information lines* One or more time descriptions (“t=” and r= lines; see below)
z	Time zone adjustments*
k	Encryption key*
a	Zero or more session attribute lines* Zero or more media descriptions (see below)
Time Description	
t	Time the session is active
r	Zero or more repeat times*

*Indicates an optional descriptor

4. In the Action field, enter the action you want applied to the SDP line rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.

- delete—Deletes the element, if it exists.
- find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
- log—Logs the element.
- monitor—Monitors the header for this element.
- none—(default) No action is taken.
- reject—Rejects the element.
- replace—Replaces the element.
- sip-manip—Manipulates the SIP elements of this header to the element rules configured.
- store—Stores the element.

5. In the Comparison type field, select the way that you want the MIME to be compared with this SDP line rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:

- boolean—Header is compared to MIME rule and must match exactly or it is rejected.
- case-insensitive—Header is compared to MIME rule regardless of the case of the header.
- case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
- pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
- refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
- refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.

6. In the Match value field, enter the value you want to match against the element value for an action to be performed.

7. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

  For example:

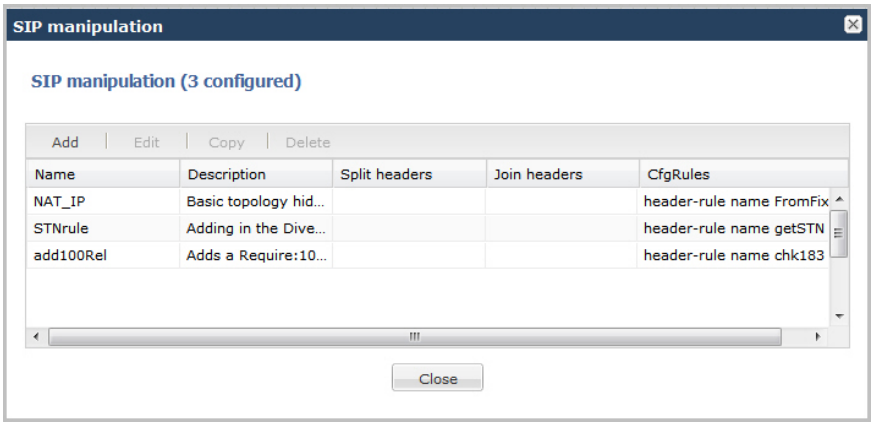
  sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
- Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
- Operators parameters - For valid values, see the Operators Table.

  Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
$ORIGINAL+”my name is \”john\””
$ORIGINAL-^781+^617
```

8. Click <OK>. The SDP Session Rule dialog box displays.

9. Click <OK>. The SIP Manipulation dialog box displays.



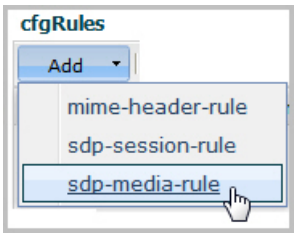
10. Click <Close>.

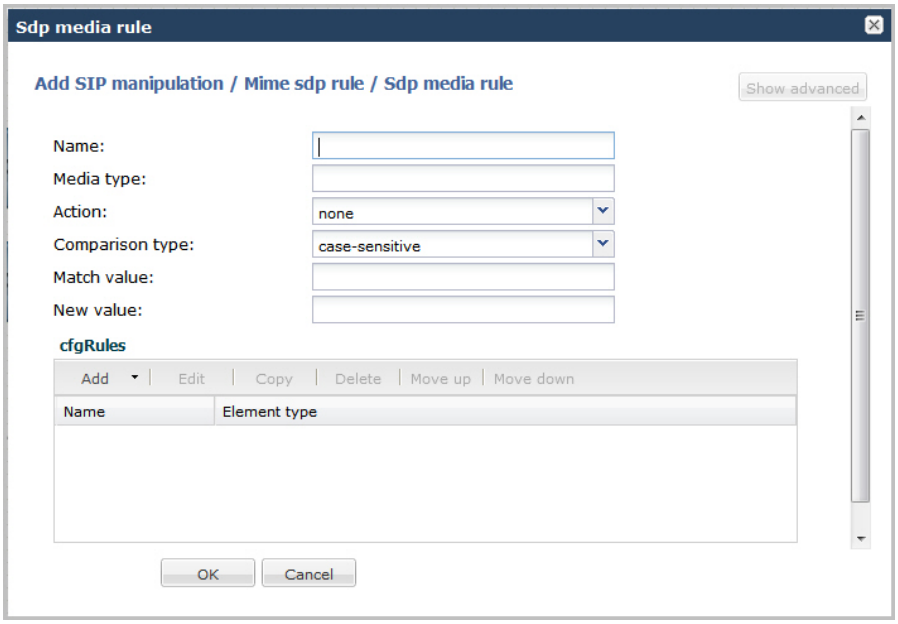
Configuring SDP Media Rules

When configuring the SDP session rules, you can also configure the SDP media rules. Use the following procedure to configure the SDP media rules.

To configure SDP media rules:

1. From the SDP Session Rule dialog box, in the cfgRules field, click <Add>, and then select sdp-media-rules from the drop-down list. This allows you to define the SDP media rules you want to use to be performed on the elements of the header specified by the SDP session rule. The following dialog box displays.





2. In the Name field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the Media Type field, enter the applicable SDP descriptor for the SDP media rule. SDP descriptors are added to the SDP, adhering to the definitions in RFC 4566. Default is blank. Valid values are:

Media Description (if present)	
m	Media name and transport address
i	Media title*
c	Connection information - optional if included at session level*
b	Zero or more bandwidth information lines*
k	Encryption key*
a	Zero or more media attribute lines*
Time Description	

t	Time the session is active
r	Zero or more repeat times*

*Indicates an optional descriptor

4. In the Action field, enter the action you want applied to the SDP media rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete—Deletes the element, if it exists.
   - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
   - log—Logs the element.
   - monitor—Monitors the header for this element.
   - none—(default) No action is taken.
   - reject—Rejects the element.
   - replace—Replaces the element.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the element.
5. In the Comparison type field, select the way that you want the MIME to be compared with this SDP media rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
   - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
   - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
   - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
   - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
6. In the Match value field, enter the value you want to match against the element value for an action to be performed.
7. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
   - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

     For example:

     sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
   - Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
   - Operators parameters - For valid values, see the Operators Table.

     Examples of entries for the new-value field.

```
$ORIGINAL+acme
$ORIGINAL+”my name is john”
$ORIGINAL+”my name is \”john\””
$ORIGINAL-^781+^617
```

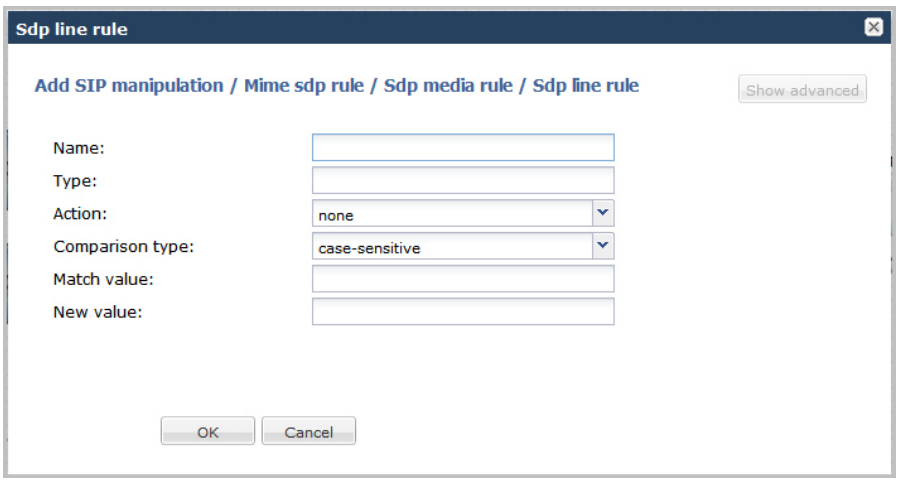
Configuring SDP Line Rules for Media

You can configure SDP Line Rules for Media if required. For more information about configuring SDP line rules, see the section, sdp-line-rule in the *Net-Net® Enterprise Session Director Configuration Guide*.

Use the following procedure to configure SDP line rules for media.

To configure SDP line rules for media:

1. From the SDP Media Rule dialog box, in the cfgRules field, click <Add>, and then select sdp-line-rules from the drop-down list. This allows you to define the SDP line rules you want to use to be performed on the elements of the header specified by the SDP media rule. The following dialog box displays.



2. In the Name field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the Type field, enter the applicable SDP descriptor for the SDP line rule. SDP descriptors are added to the SDP, adhering to the definitions in RFC 4566. Default is blank. Valid values are:

Session Description	
v	Protocol version
o	Originator and session identifier
s	Session name
i	Session information*
u	URI of description*
e	Email address*
p	Phone number*
c	Connection information - not required if included in all media*
b	Zero or more bandwidth information lines* One or more time descriptions (“t=” and r= lines; see below)
z	Time zone adjustments*
k	Encryption key*
a	Zero or more session attribute lines* Zero or more media descriptions (see below)
Time Description	
t	Time the session is active
r	Zero or more repeat times*

*Indicates an optional descriptor

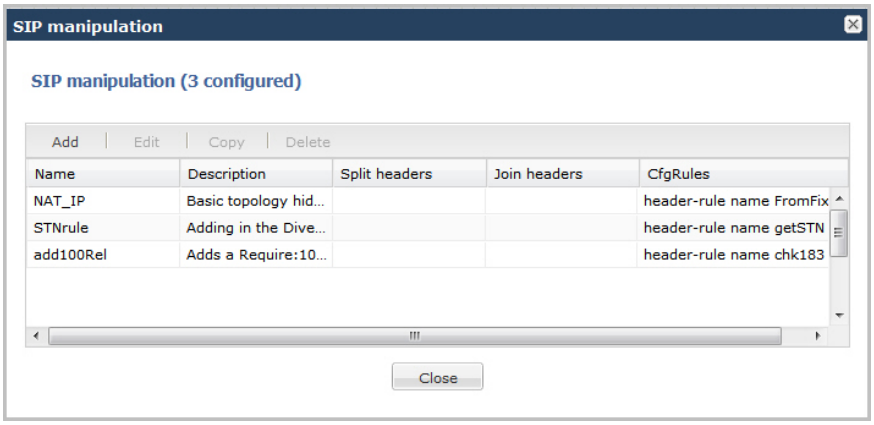
4. In the Action field, enter the action you want applied to the SDP line rule specified in the Name parameter, if there is a match value. Default is none. Valid values are:
   - add—Adds a new element, if that element does not already exist.
   - delete—Deletes the element, if it exists.
   - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
   - log—Logs the element.
   - monitor—Monitors the header for this element.
   - none—(default) No action is taken.
   - reject—Rejects the element.
   - replace—Replaces the element.
   - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
   - store—Stores the element.
5. In the Comparison type field, select the way that you want the MIME to be compared with this SDP line rule. This choice dictates how the Enterprise Session Director processes the match rules against the MIME. Default is case-sensitive. Valid values are:
   - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
   - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
   - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
   - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
   - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
   - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
6. In the Match value field, enter the value you want to match against the element value for an action to be performed.
7. In the New value field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
   - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

     For example:

     sip:”+$TRUNK_GROUP+”.$TRUNK_GROUP_CONTEXT
   - Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters Table.
   - Operators parameters - For valid values, see the Operators Table.

     Examples of entries for the new-value field.

     ```
     $ORIGINAL+acme
     $ORIGINAL+”my name is john”
     $ORIGINAL+”my name is \”john\””
     $ORIGINAL-^781+^617
     ```
8. Click <OK>. The SDP Media Rule dialog box displays.
9. Click <OK>. The MIME SDP Rule dialog box displays.
10. Click <OK>. The Modify SIP manipulation dialog box displays.
11. Click <OK>. The SIP Manipulation dialog box displays.



12. Click <Close>.

Adding an SPL

An SPL is an executable customized script created to implement a feature on the NN-ESD quick and easy. It is an Oracle signed plug-in that integrates with the NN-ESD operating system (OS). You can use an SPL to control signaling traffic (including persistent state maintenance). It augments running the software image on the NN-ESD, and provides new features when you need them by changing product behavior, but without having to upgrade your software. The SPL is there if you need it. If you don't use the SPL, your NN-ESD software performs as normal.

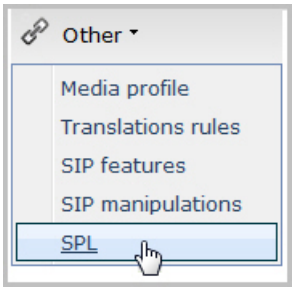
The Enterprise Session Director does not load unsigned SPLs or those with invalid signatures.

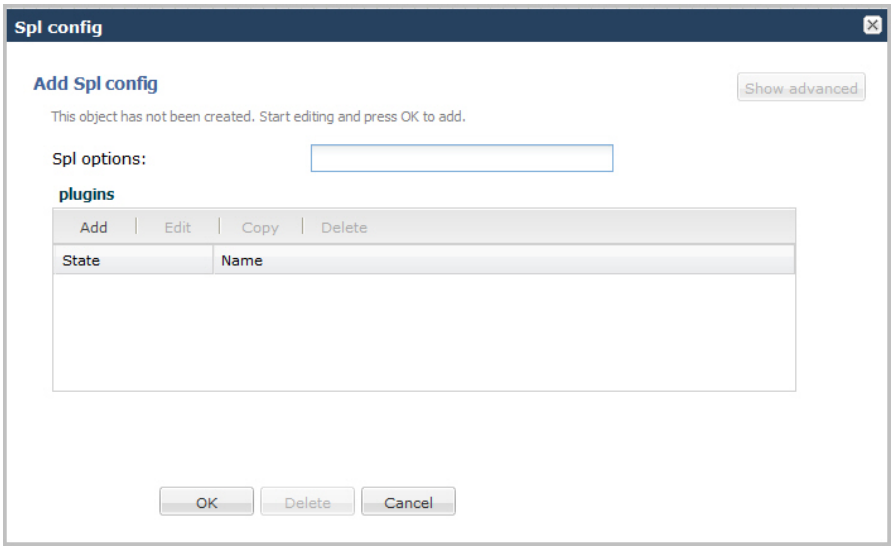
This SPL feature provides the customized solution for your requirement and provides accelerated deployment of your system in the network. It can run on any platform with an ANSI C compiler. You can use the SPL with Header Manipulation Rules (HMRs) via the Enterprise Session Director ACLI configuration.

For more information about an SPL, see Chapter 23, Session Plug-in Language, in the *Net-Net® Enterprise Session Director Configuration Guide*.

To add an SPL:

1. From the Main Menu, click **Other** > **SPL** . The following displays.

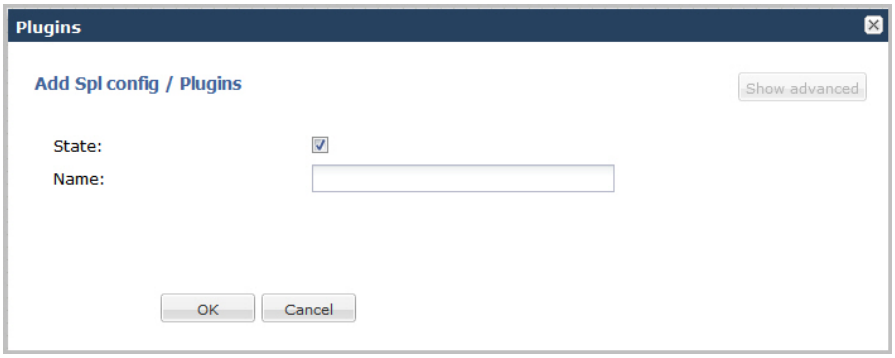




2. In the SPL options field, enter the playback options you want to use on the Enterprise Session Director if you are using the Local Media Playback SPL. Default is blank. Valid values are:
   - playback-on-183-to-originator—Playback enabled upon the receipt of a 183 Session Progress destined for the originator and stops when a either a (200-299 or 400-699) final response is sent.
   - playback-on-183-from-terminator—Playback enabled upon the receipt of a 183 Session Progress response is received from the terminator and stops when a (200-299 or 400-699) final response is received.
   - playback-on-refer—Playback enabled for the caller being transferred when the Enterprise Session Director receives a REFER message that is locally terminated (i.e., processed on the Enterprise Session Director on REFER completion).
   - playback-on-header—Starts or stops playback based on the presence of the P-Acme-Playback header and its definitions.

   Note: The Enterprise Session Director supports a maximum of 100 simultaneous playbacks.

3. In the plugins field, click <Add>. The following displays.



4. In the State field, enable the SPL plug-in on the Enterprise Session Director by placing a checkmark in the box. Disable the SPL plug-in by unchecking this box. Default is enabled.
5. In the Name field, enter the file name of the SPL plug-in. File names must be entered <filename.spl>. The following SPL plug-ins are applicable to Release E-C[xz]6.4.0, and are already installed and enabled:
   - MediaPlayback.1.0.spl
   - LyncEmergencyCall.1.0.spl
   - SipHeaderExtensionMetadata.1.2.spl
   - UniversalCallId.1.spl
   - ComfortNoiseGeneration.1.1.spl
6. Click <OK>. The Add SPL Config dialog box displays.

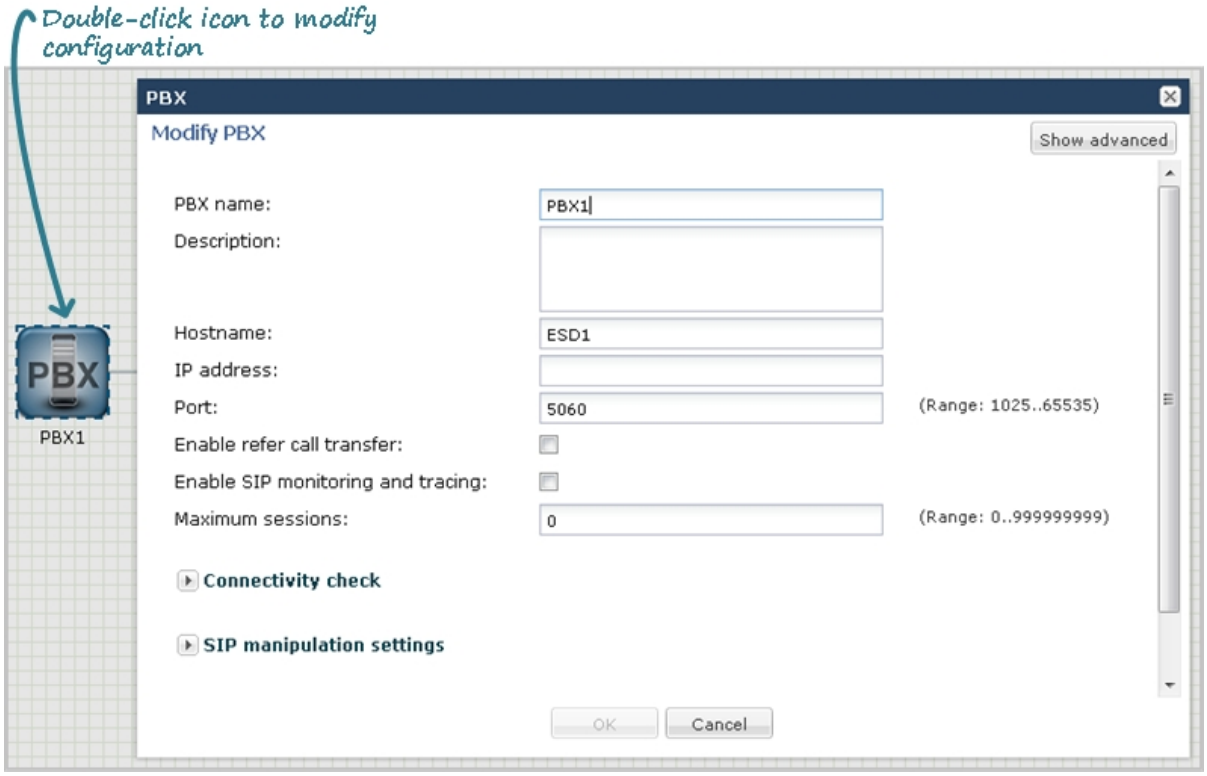
7. Click <OK>.

Editing a Configuration

In Basic Mode, you can edit any configuration if required. However, after editing a configuration, you must save and activate in order for the changes to take affect.

Editing Icon Configuration

For any device or interface that currently exists in your workspace, you can double-click the icon and edit the configuration, or right-click on the icon and select Edit from the drop-down menu. The following shows an example of editing the PBX configuration.

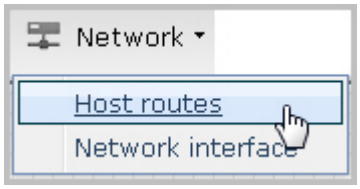


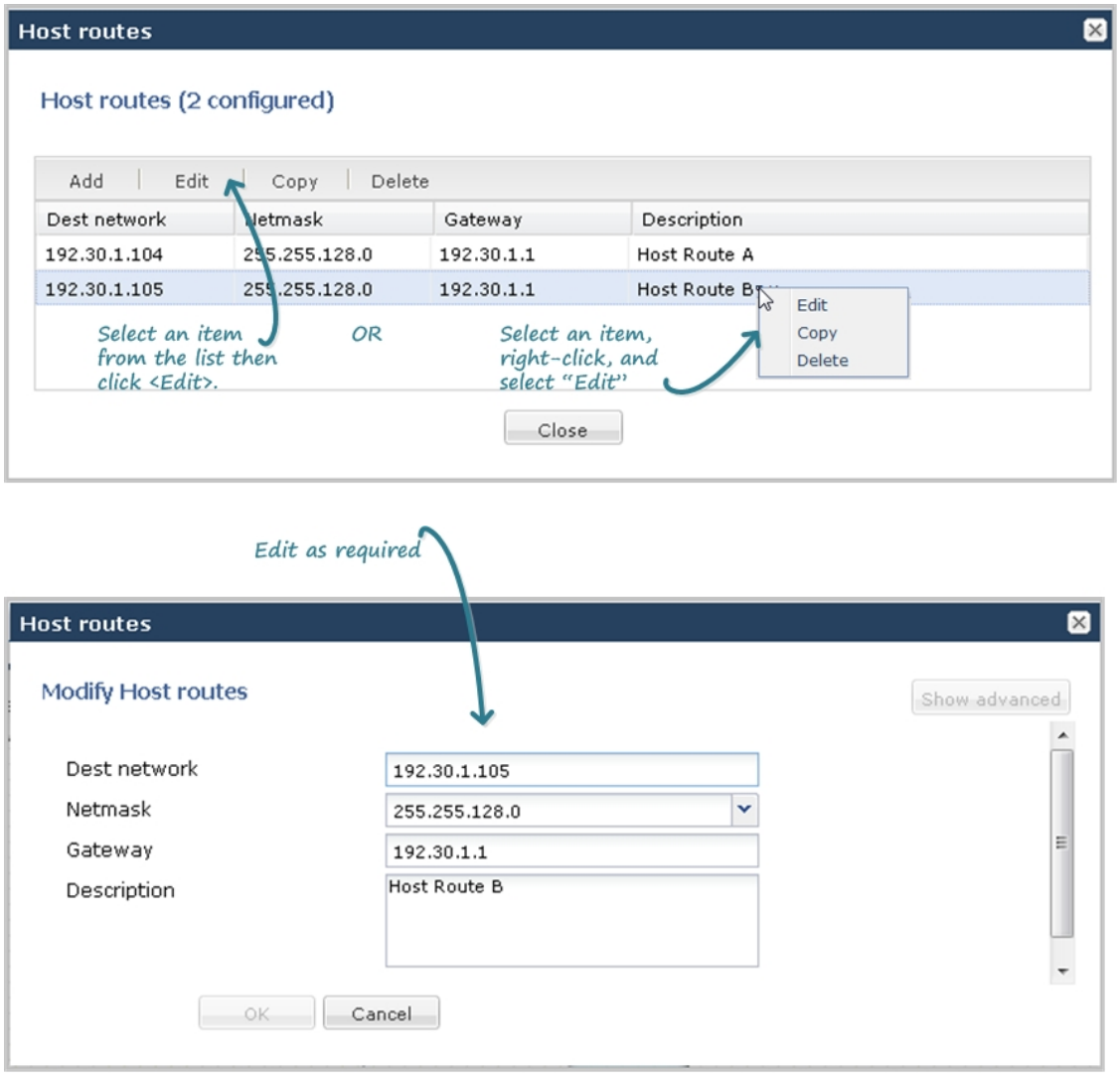
Editing Advanced Configuration

To edit more advanced configurations in your network, you can select the required configuration from the Main Menu, and edit the configuration item from the list that displays. You can edit an item using either of two methods:

- Selecting the item from the list and clicking the <Edit> button
- Selecting the item from the list, right clicking the mouse, and selecting Edit from the drop-down menu.

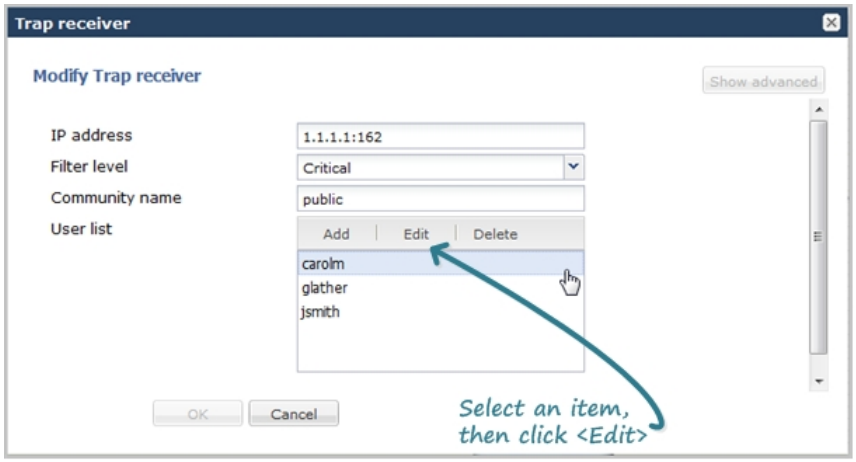
The following shows an example of editing a host route configuration.





Editing Parameter Fields

Some dialog boxes in a configuration provide the ability to edit within a parameter field. In the following example, a user list within the trap-receiver configuration is selected for editing.



Copying a Configuration

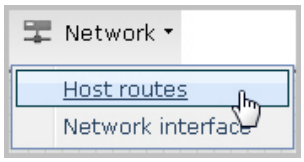
You can copy configurations , if required, when configuring your network.

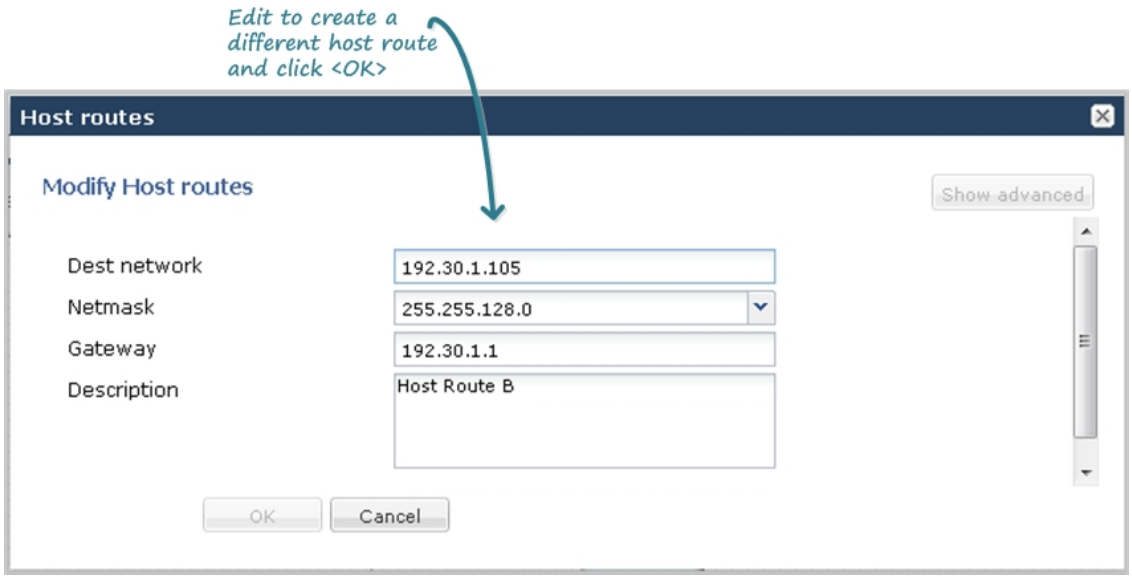
Copying Advanced Configuration

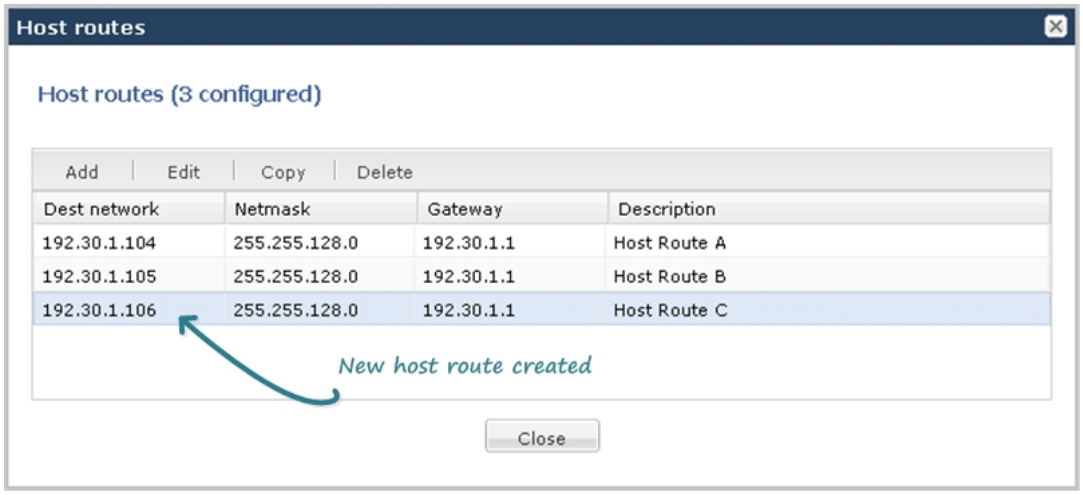
To copy more advanced configurations in your network, you can select the required configuration from a list that displays using either of two methods:

- Selecting the item from the list and clicking the <Copy> button
- Selecting the item from the list, right clicking the mouse, and selecting Copy from the drop-down menu.

The following shows host route 192.30.1.105 copied and edited as a new host route of 192.30.1.106.







Deleting a Configuration

In Basic Mode, you can delete configurations as required.

Deleting Icon Configuration

For any device or interface that currently exists in your workspace, you can right-click on the icon and select Delete from the drop-down menu. The following shows an example of deleting a PBX configuration.

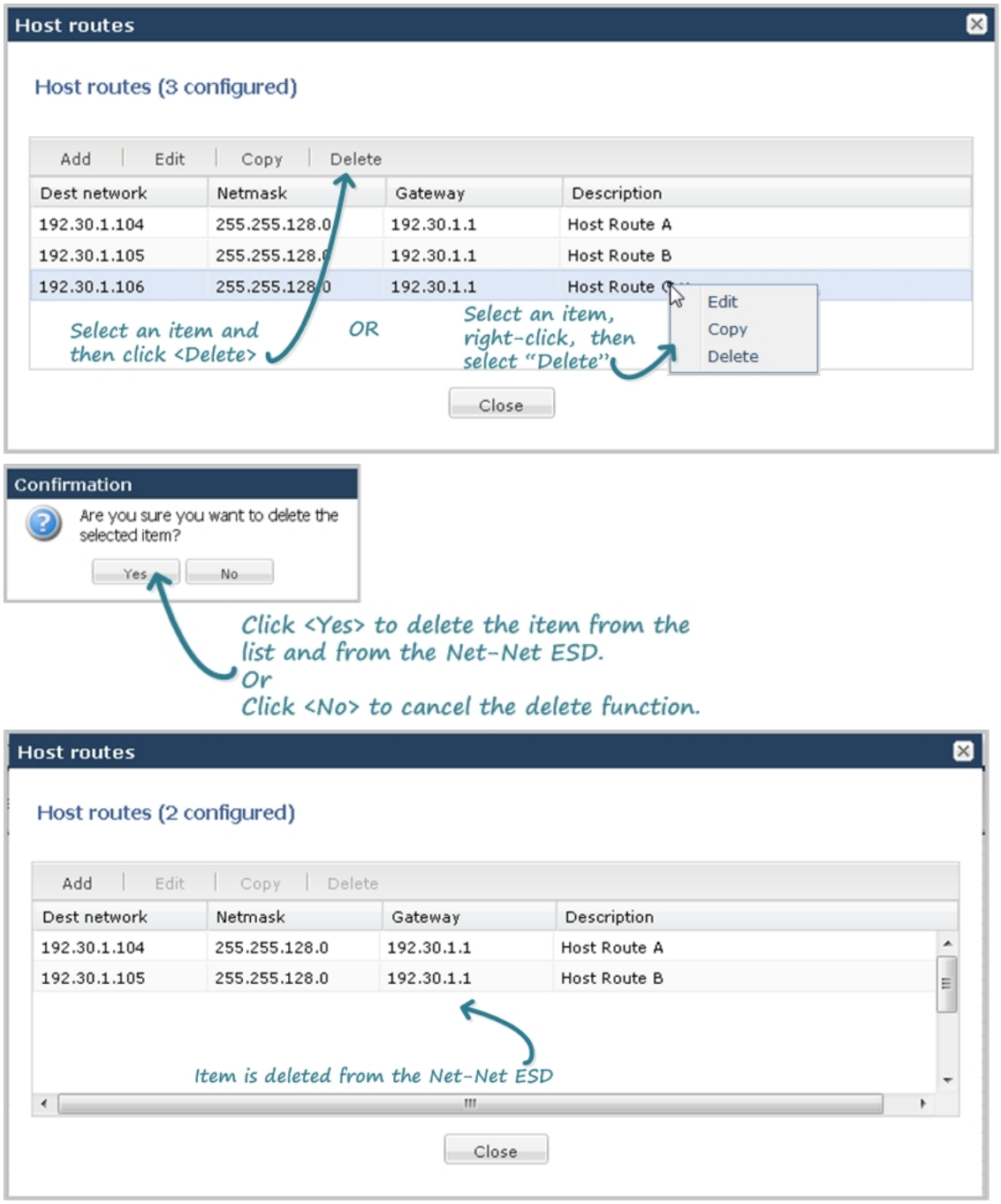
The configuration deletes from the workspace and from the Enterprise Session Director.

Deleting Advanced Configuration

To delete more advanced configurations in your network, you can select the required configuration from the Main Menu, and delete the configuration item from the list that displays. You can delete an item using either of two methods:

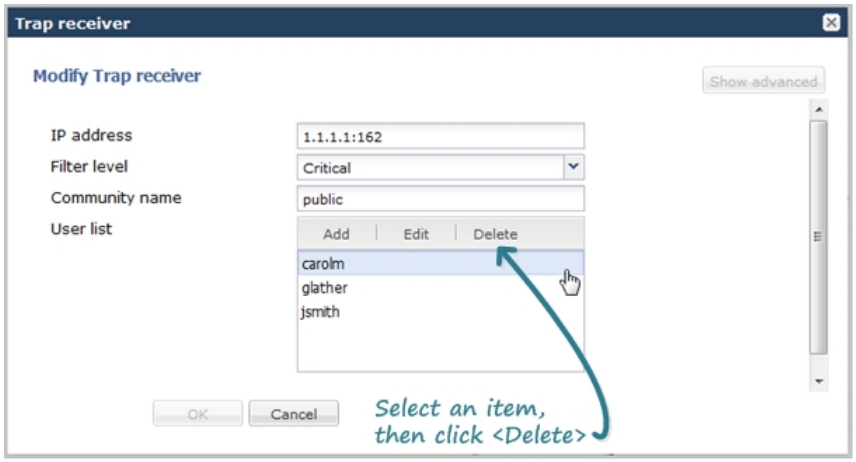
- Selecting the item from the list and clicking the <Delete> button
  or
- Selecting the item from the list, right clicking the mouse, and selecting Delete from the drop-down menu.

The following shows host route 192.30.1.106 being deleted from the Host route table.



Deleting Parameter Fields

Some dialog boxes in a configuration provide the ability to delete within a parameter field. In the following example, a user list within the trap-receiver configuration is selected for deleting.



Expert Mode

The Expert mode of configuring the NN-ESD allows you to set parameters by navigating through a tree structure of objects and attributes. This tree structure matches the Oracle Command Line Interface (ACLI)-view of the Enterprise Session Director.

Note: When configuring some advanced parameters, a field may be required but the Web GUI does not indicate it is required. You may be able to save the configuration even if you do not specify a value in the field. If you do not specify a field that is required, the Enterprise Session Director ignores the element in the configuration. No error message displays when you refrain from entering a required parameter.

Accessing Expert Mode

You can access the Expert mode of configuration by clicking the Configuration tab in the Web GUI.

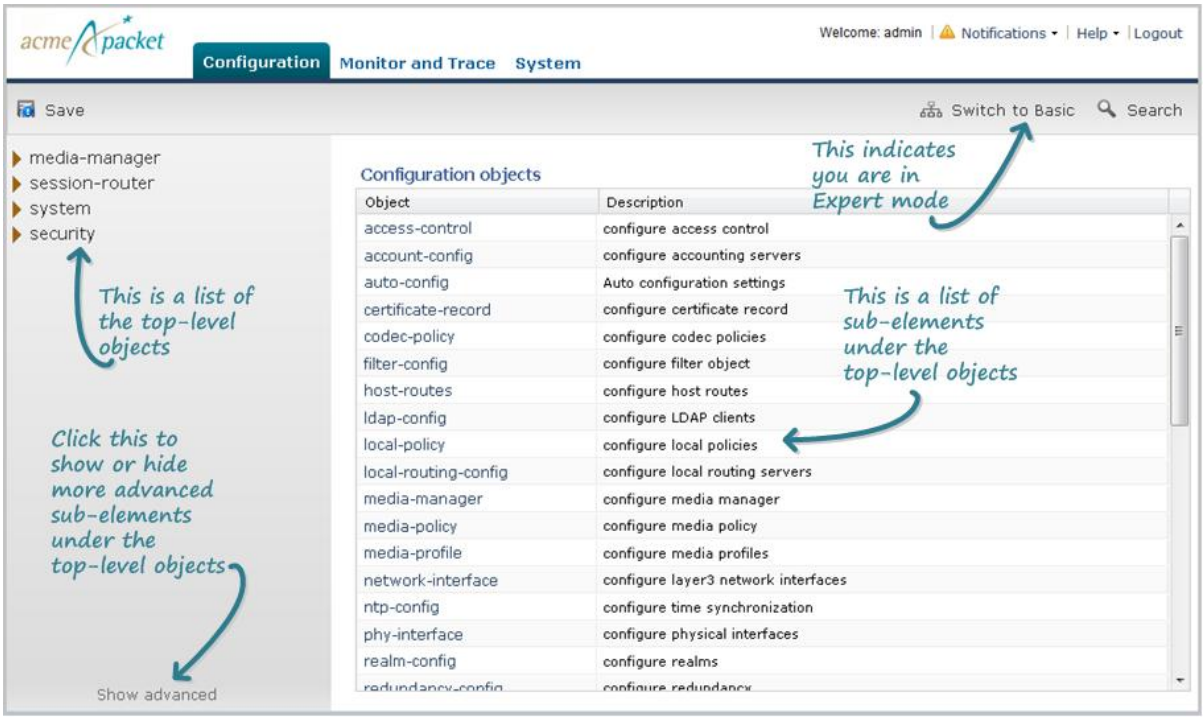
To access Expert mode:

1. After logging into the Web GUI, click on the Configuration tab. The following displays.

   Note: The “Expert Mode” displays only if your Administrator set this interface as default during the Installation Wizard setup. If “Basic Mode” is set as the default, click Switch to Expert in the upper right corner of the screen.

   The page displays the minimum objects you can set to configure the Enterprise Session Director. You can display additional objects to configure by clicking the Show Advanced link at the bottom of the left column.

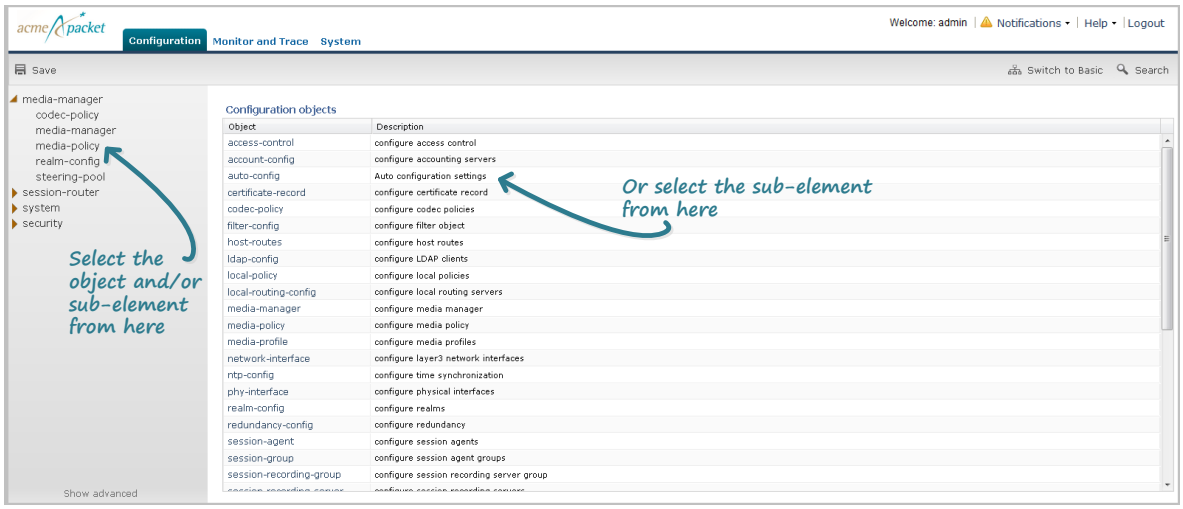
   Oracle recommends advanced parameters be configured by experienced administrators only.



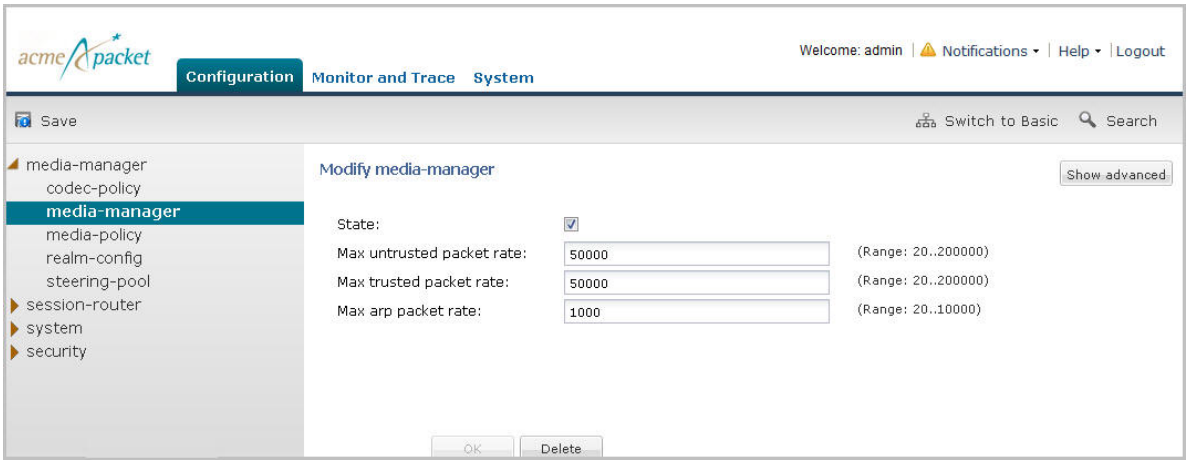
The list of sub-elements in the right column are all the sub-elements associated with the top-level element selected from the left column.

You can select the sub-element you want to configure from the right column if required; or you can expand a top-level object to show the sub-element of that object.

2. Expand a top-level object in the left column, and then click on a sub-element. Or click on the sub-element in the right column.



The page associated with the sub-element you select displays. The following illustration is an example of the media-manager page.



Some fields in the configuration windows of Expert Mode identify valid values for a field. For example, in the Modify media-manager window above, a range of values for each text box is provided.

Configuring in Expert Mode

In Expert Mode, you can add, modify, and delete configuration objects and attributes as required. Configuring more advanced parameters is for experienced Administrators only.

The top elements in Expert Mode are as follows:

- media manager
- session router
- system
- security

The following table lists the sub-elements of each top element in the Enterprise Session Director. The sub-elements in italics are advanced configuration parameters that display when you click the Show advanced link.

Media Manager	Session Router	System	Security
codec-policy	access-control	ntp-config	certificate-record
media-manager	account-config	auto-config	tls-global
media-policy	filter-config	host-routes	tls-profile
realm-config	ladp-config	network-interface	auth-params*
steering-pool	local-policy	phy-interface	authentication*
dns-config*	local-routing-config	redundancy-config	cert-status-profile*
playback-config*	media-profile	snmp-community	password-policy*
realm-group*	session-agent	spl-config	security-config*
static-flow*	session-group	system-config	media-security*
	sesson-recording group	trap-receiver	ipsec**
	session-recording-server	web-server-config	ike**
	session-translation	capture-receiver**	
	sip-config	network-parameters*	
	sip-feature	system-access-list*	
	sip-interface	timezone*	

Media Manager	Session Router	System	Security
	sip-manipulation		
	sip-monitoring		
	translation-rules		
	allowed-elements-profile*		
	call-recording-server*		
	enforcement-profile*		
	enum-config*		
	http-alg*		
	iwf-stack*		
	local-response-map		
	net-management-control		
	qos-constraints		
	response-map		
	session-constraints		
	surrogate-agent		
	class-profile		
	H323		

*These advanced parameters are applicable to Virtual Machines (VMs) and Session Director hardware.
**These parameters are applicable to Session Director hardware only.

Function Buttons

Expert Mode provides function buttons within each configuration page to perform actions such as add, edit, copy, and delete. These buttons in a window are enabled depending on your selection within a page. The following table describes each button.

Button	Description
Add | Edit | Copy | Delete	
Add	Allows you to add configuration information to the Enterprise Session Director.
Edit	Allows you to edit existing configuration information. Note: An item in a list must be selected to enable the <Edit> button.
Copy	Allows you to copy existing configuration information, and edit the information to create a new configuration. Note: An item in a list must be selected to enable the <Copy> button.
Delete	Allows you to delete existing configuration information. Note: An item in a list must be selected to enable the <Delete> button.

Note: The buttons in the table above can appear within sub-element tables as well and perform the same as described above.

The following sections provide examples you can use to configure the objects and elements of the Enterprise Session Director in Expert Mode. For a description and additional information on all the objects, attributes, and values in this mode, see the *Net-Net® Enterprise Session Director Configuration Guide*.

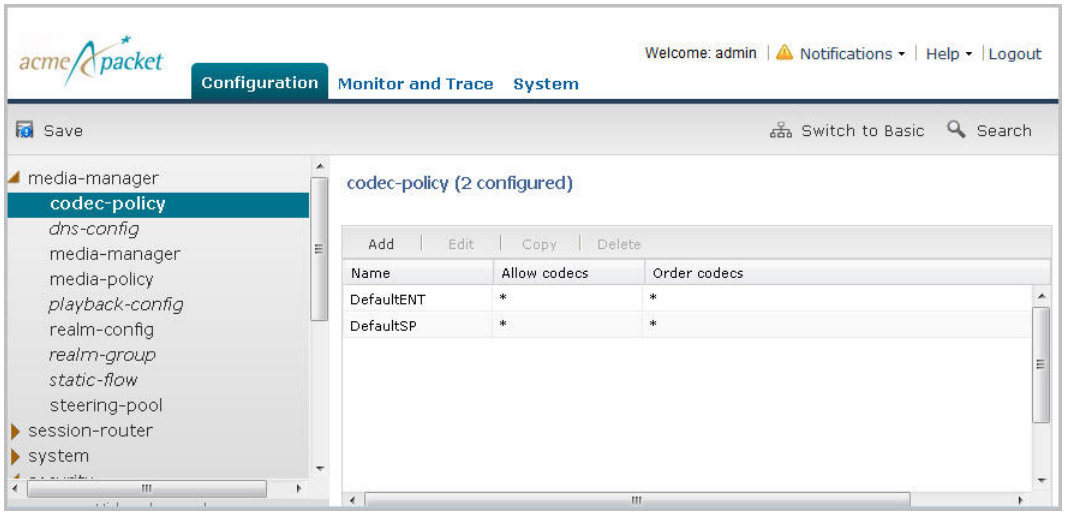
Adding a Configuration

The following is an example procedure for adding a configuration to the Enterprise Session Director.

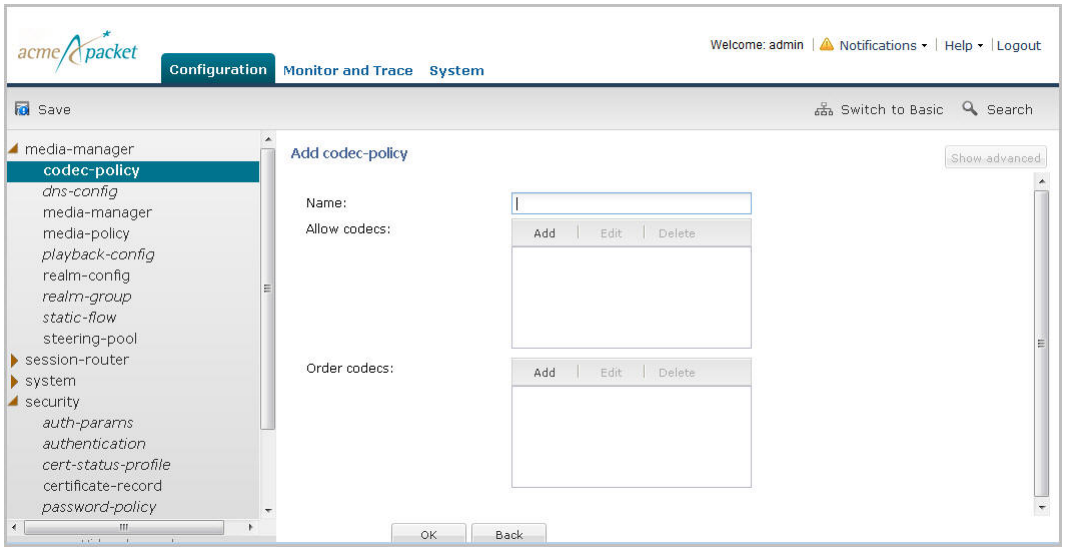
To add a configuration:

1. Under media-manager, click on codec-policy. The following displays.

   Note: In some tables, default information displays if applicable. In the example below, DefaultENT and DefaultSP are the default codec policies in the Enterprise Session Director.

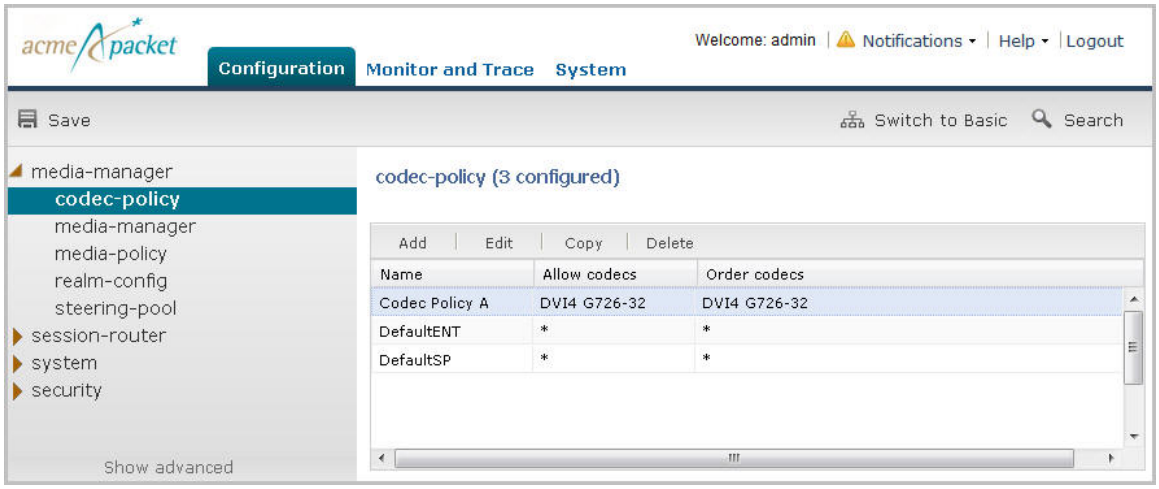


2. Click <Add>. The following displays.



3. Enter information in the text box and add information to the list boxes as required. Refer to the *Net-Net® Enterprise Session Director Configuration Guide* for valid values for each field.
4. Click <OK> to save the changes. Or click the <Back> button to discard any changes.

   The following is an example of a codec policy configuration.

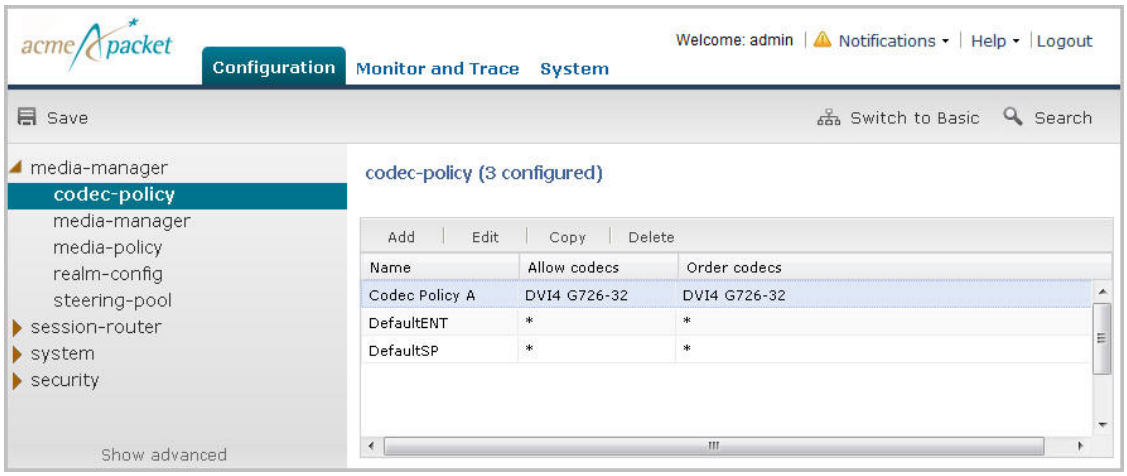


Editing a Configuration

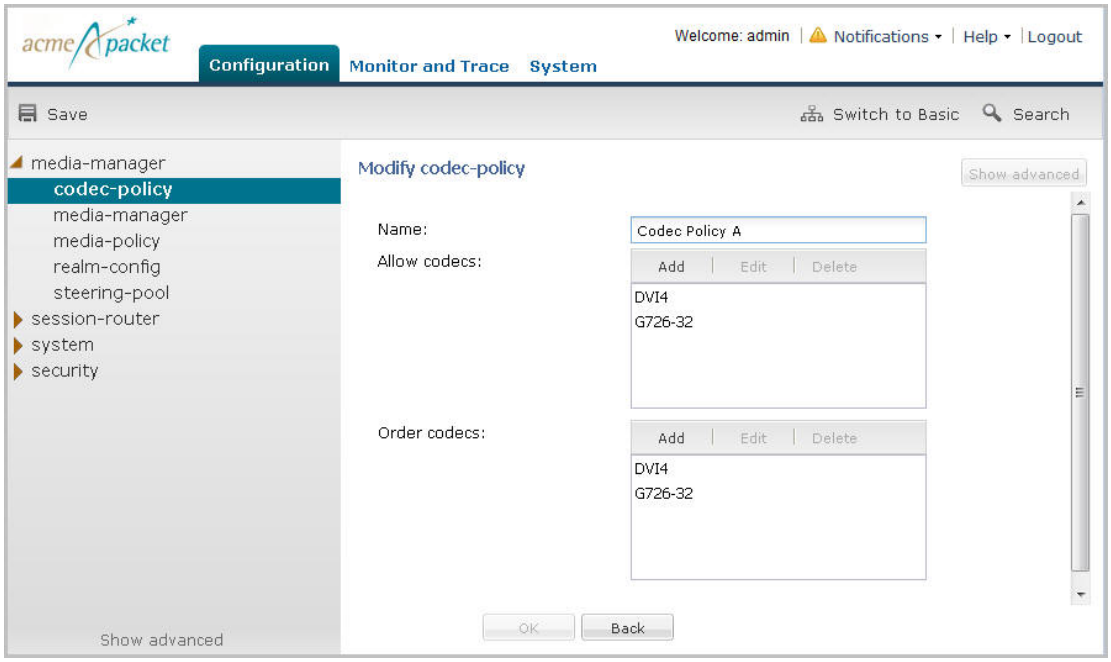
The following is an example procedure for editing a configuration in the Enterprise Session Director.

To edit a configuration:

1. Under media-manager, click on codec-policy. The following displays.



2. In the list box, select the item you want to edit and click <Edit>. The configuration you selected displays.



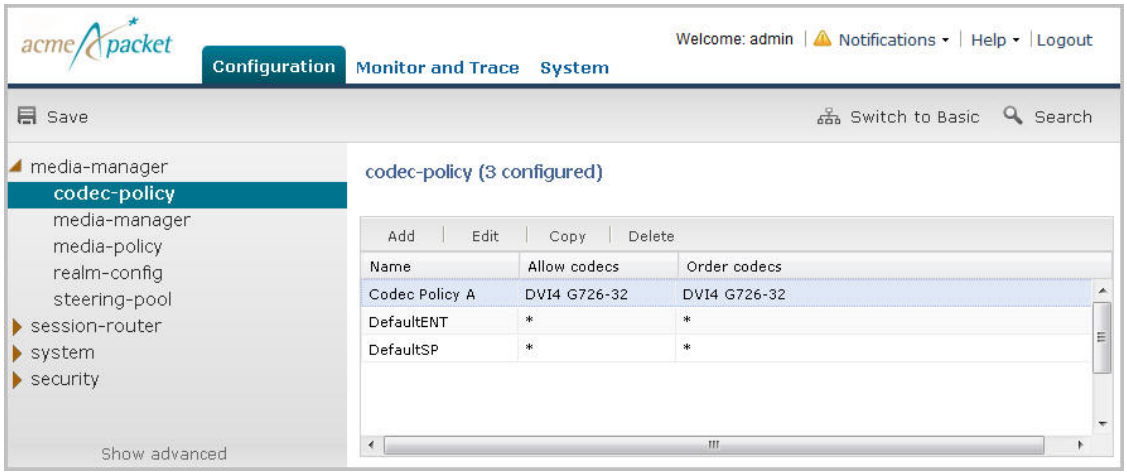
3. Edit the configuration as applicable and then click <OK>.

Deleting a Configuration

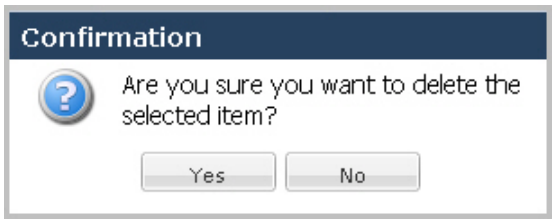
The following is an example procedure for deleting a configuration in the Enterprise Session Director.

To delete a configuration:

1. Under media-manager, click on codec-policy. The following displays.



2. In the list box, select the item you want to delete and click <Delete>. The following prompt displays.



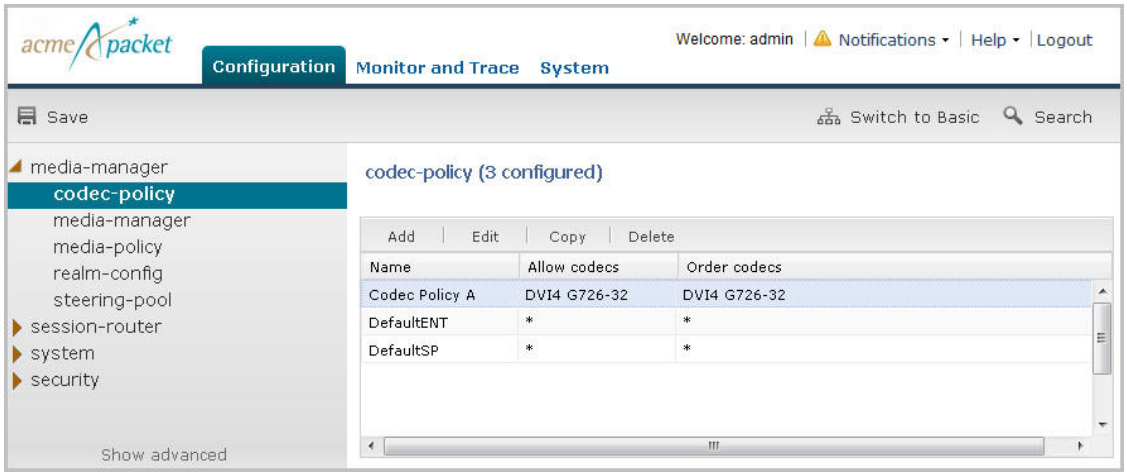
3. Click <Yes> to delete the item from the configuration. Or click <No> to cancel the delete function. If you delete the item, it no longer displays in the list box. You must save and activate the configuration for the change to take affect.

Copying a Configuration

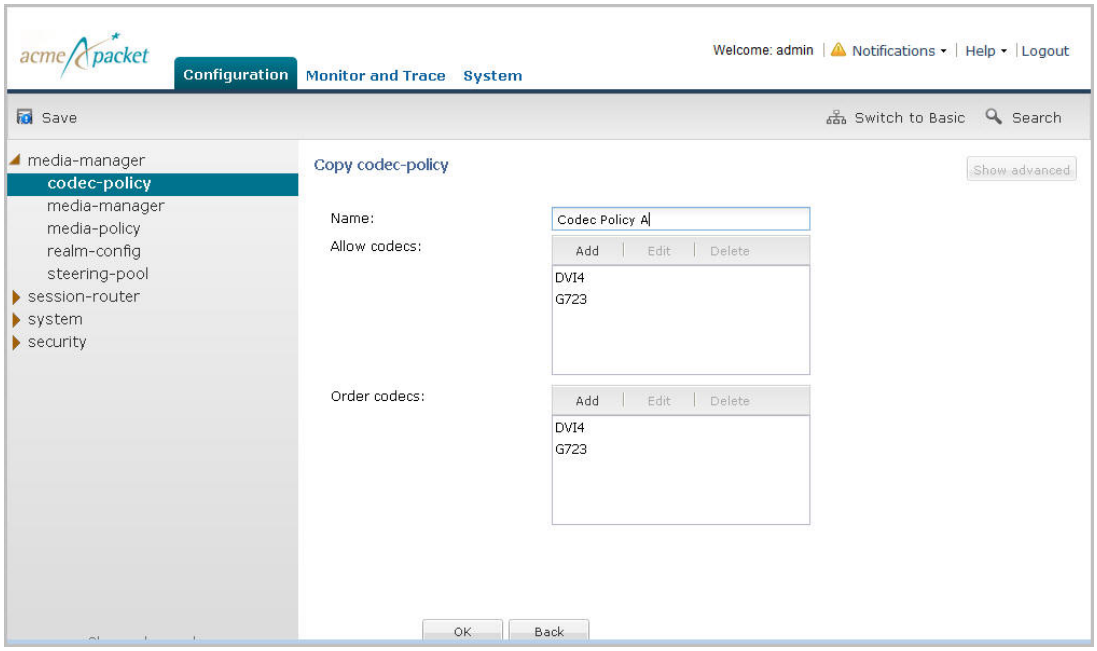
The following is an example procedure for copying a configuration in the Enterprise Session Director.

To copy a configuration:

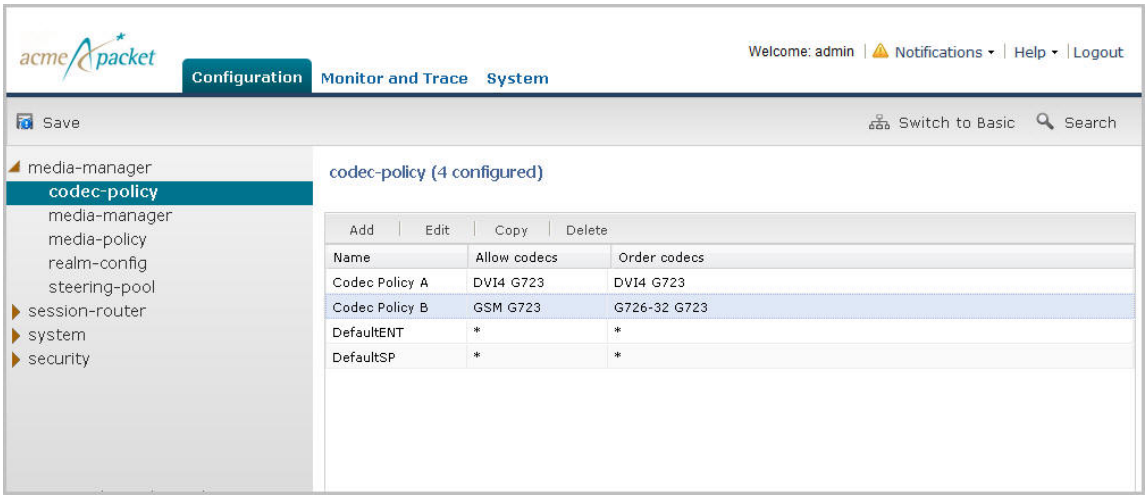
1. Under media-manager, click on codec-policy. The following displays.



2. In the list box, select the item you want to copy and click <Copy>. The configuration you selected displays.



3. Edit the configuration as applicable and then click <OK>. The new configuration displays in the list box, and the old configuration is retained. In the example, below, Codec Policy A is retained, and Codec Policy B is a new item in the list.



Save and Activate Network Configuration

When you have completed creating your network, the <Save> button allows you to verify, save, and activate the configuration on the Enterprise Session Director. Clicking <Save> verifies and saves the current configuration to the Enterprise Session Director's last-saved configuration, stored in flash memory. It also displays a prompt that allows you to activate the configurations the running configuration if required.

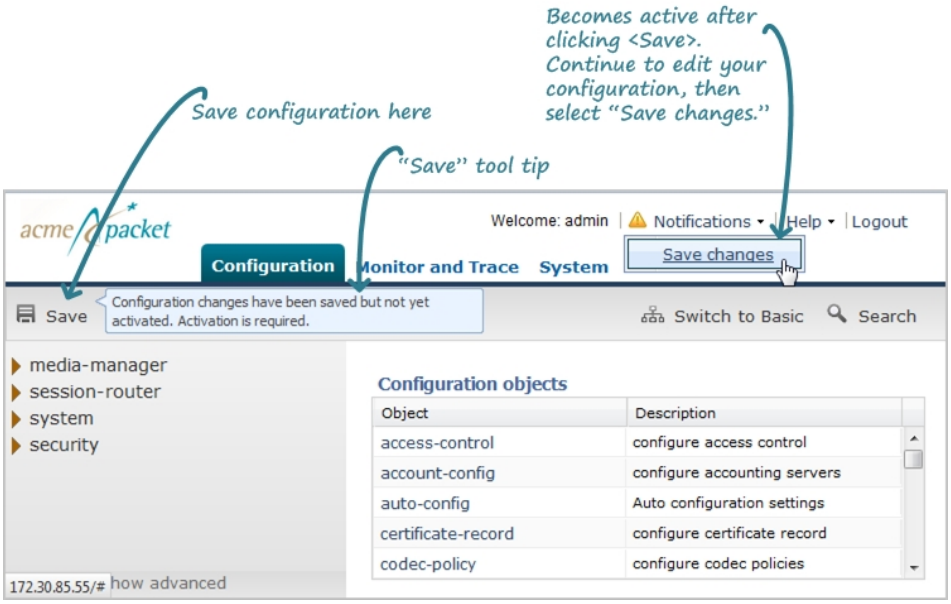
A notification icon displays grayed-out in the upper right corner of the screen. After clicking <Save>, the Notifications menu becomes active. This menu will remain active allowing you to continue making changes to the configuration, and when you are ready to save and activate the configuration, you can select **Notifications** > **Save Changes** and then choose to activate the configuration.

To save your Enterprise Session Director configuration:

1. Click Save to verify and save your configuration. This saves the current configuration to the Enterprise Session Director's last-saved configuration, stored in flash memory.

   Note: Placing the pointer over the <Save> button displays the following tool tip: Configuration changes have been made but not yet activated. Activation is required.

   The following prompt displays: Do you want to activate the configuration?
2. Click <Activate> to activate the current configuration in Basic Mode and make it the running configuration. Or click <Cancel> to cancel the activate function. The configuration is still saved in memory. If you click <Cancel>, you can continue to make changes to the configuration. After you clicked <Save> in Step 1, a notification icon became active in the upper right corner of the screen. When you complete your changes, you can then select **Notifications** > **Save changes** from this notification menu and then activate your configuration.

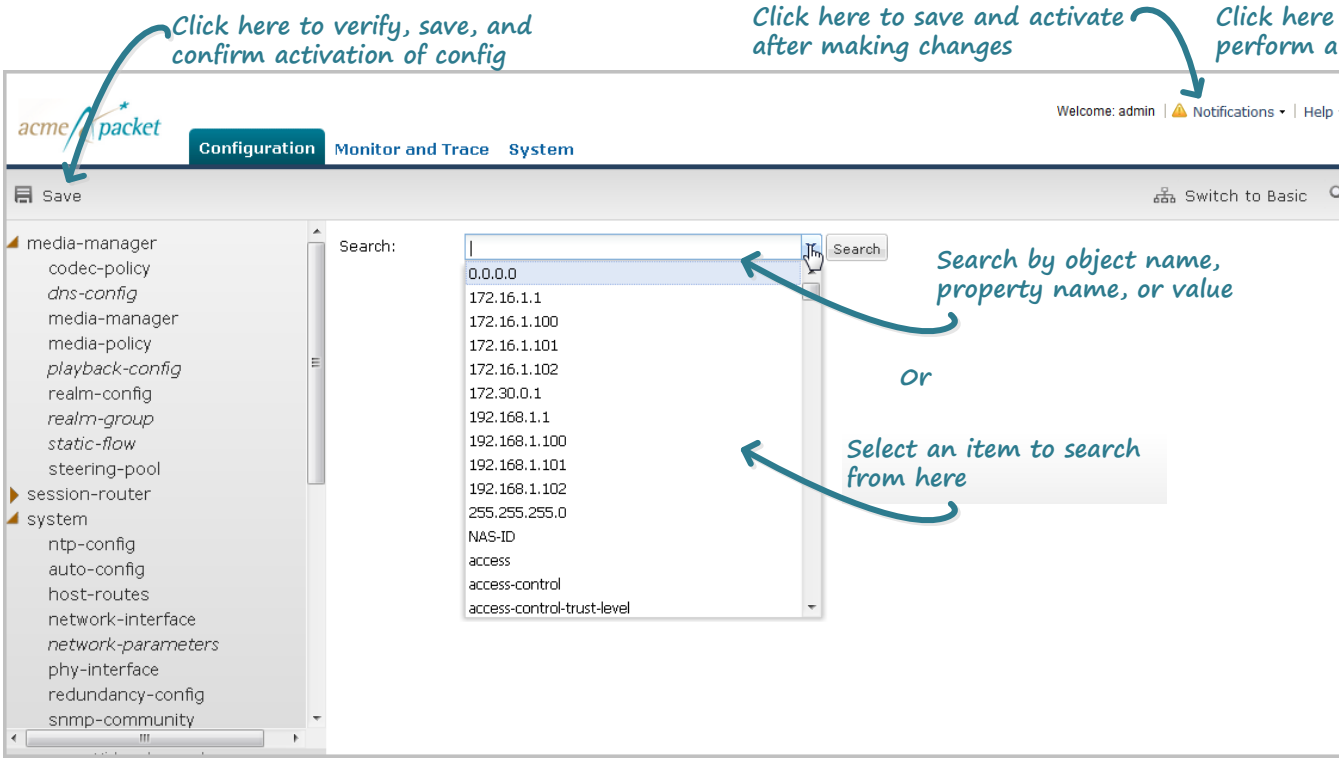


You have completed an expert Enterprise Session Director configuration. Your network is ready to use and you can begin sending/receiving calls.

Note: Once you save the configuration in Expert Mode, you cannot switch back to Basic Mode.

Search Functions

The Search link allows you to perform a search on an object name, property name, or a value in the Enterprise Session Director configuration. You can enter an item to find in the Search text box. A drop-down list also provides some items for which you can perform a search.

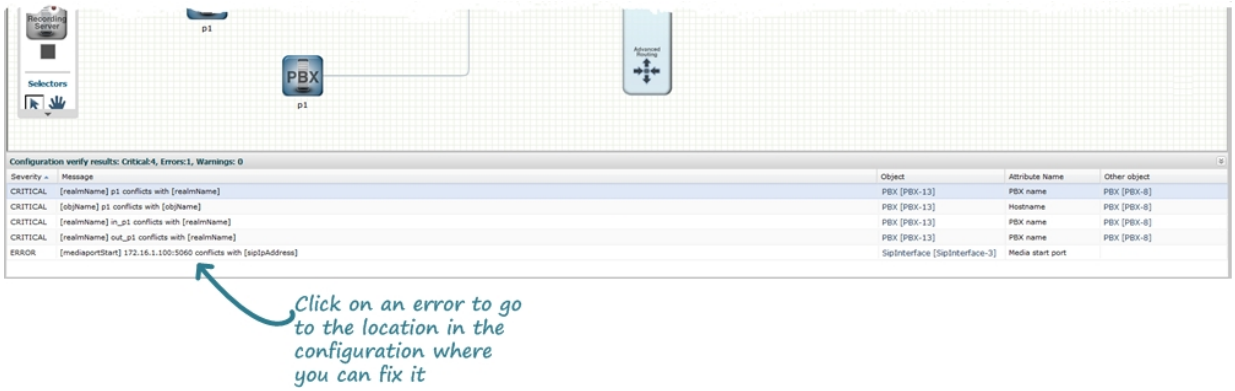


Error Messages

For both Basic and Expert Mode, if you save a configuration that contains errors, the errors display in a window at the bottom of the screen, and the following message displays:

There were errors! Are you sure you want to activate the configuration?

The following is an example of errors that display for a configuration in Basic Mode.



Click on an error to go to the location in the configuration where you can fix it

You can click on a specific error to go to the exact location in the configuration where the error exists, and then edit the configuration as applicable.

The following table identifies the columns in the error list.

Column	Description
Severity	Identifies the level of severity that the Enterprise Session Director assigns to the error. Valid values are: ERROR - Indicates the issue identified in the "Message" column was not correctly configured or it does not exist. You can still verify, save, and activate the configuration if this severity exists. WARNING - Indicates the configuration contains invalid information for the element field identified in the "Message" column. You can still verify, save, and activate the configuration if this severity exists. CRITICAL - Indicates a critical error has occurred in the configuration and you cannot verify, save, or activate until the error is corrected. The "Message" column indicates the element field where the error has occurred.
Message	Identifies the element field(s) where the error, warning, or critical error has occurred, and identifies the reason for the error.
Object	Identifies the element and the field for that element where the error occurred.
Attribute	Identifies the attribute within the element where the error occurred.
Other	Identifies any other pertinent information relating to the error.

3

Monitor and Trace

This chapter provides information and procedures for using the Monitor and Trace feature in the Net-Net ECB. Monitor and Trace allows you to display results of filtered SIP session data from one or multiple Net-Net ECBs, and provides traces in a common log format for local viewing or for exporting to your PC.

Topics include:

- Monitor and Trace
  - Session Reports
  - Registration Reports
  - Subscription Reports
  - Notable Event Reports
- Search for a Record
- Export Information to a Text File

Monitor and Trace SIP Messages

When the Net-Net ECB filters the data from SIP messages, it captures the message, applies the Header Manipulation Rules (HMR) configured on the Net-Net ECB, and applies the Session Plug-in Language (SPL) to that message. When the message is sent from the Net-Net ECB, it applies the SPL, applies the HMR, and sends the captured SIP message.

The Monitor and Trace tab on the GUI displays the results of filtered SIP session data from one or more Net-Net ECBs, and provides traces in a common log format for local viewing and for exporting. The monitor and trace function provides the following summary reports.

- Sessions
- Registrations
- Subscriptions
- Notable events

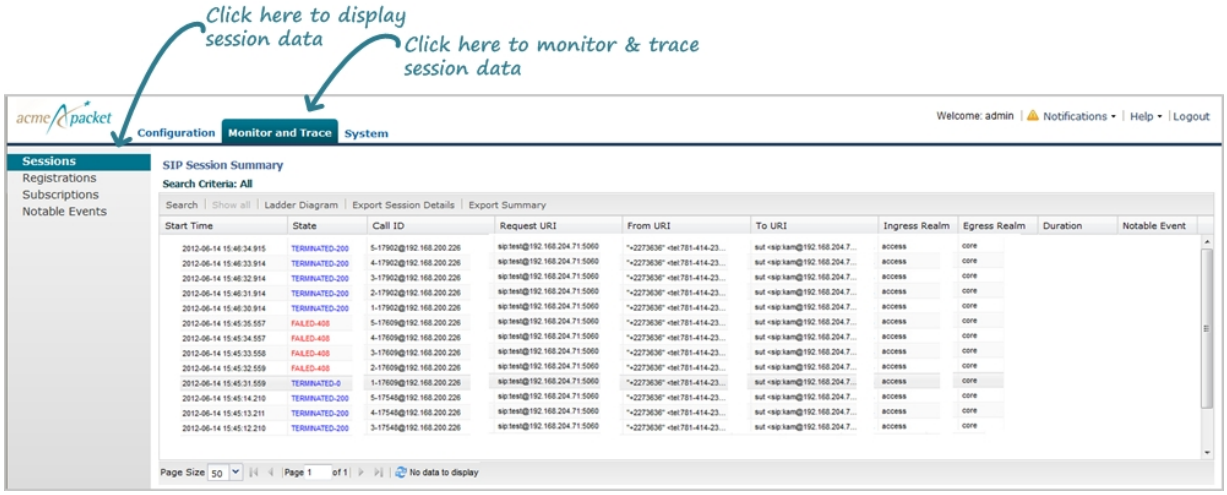
Each report summarizes the applicable information and displays it on a web page. From the web page, you can sort and customize the columns within each report, search for specific information in a report, and use the controls on the page to display additional information and perform a task.

The SIP Monitor and Trace function can store up to 2000 historical calls, which is a combined total from all of the summary report types. Once the 2000 call maximum is reached, the system removes the oldest call and adds the newest call. The call database is not persistent across reboots.

Session Reports

The Session Report is a SIP session summary of all logged call sessions on the Net-Net ECB. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net ECB. If Lightweight Directory Access Protocol (LDAP) is enabled on the Active Directory, LDAP session messages may also display.

The columns that display on the Session Report page are dependent on the columns you selected in the procedure, Customizing the Page Display.



The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
State	Status of the call or media session. Valid values are: INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. EARLY Session received the first provisional response (1xx other than 100). ESTABLISHED Session for which a success (2xx) response was received. TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or Early session. The session remains in the terminated state until all the resources for the session are freed up. FAILED Session that has failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net ECB in REQUEST headers.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Duration	Amount of time, in seconds, that the call or media event was active.
Notable Event	Indicates if a notable event has occurred on the call session. Valid values are:

Heading	Description
	short session - Sessions that don't meet a minimum configurable duration threshold; Session dialogue, captured media information and termination signalling; Any event flagged as a short session interesting event. local rejection - Sessions locally rejected at the Net-Net ECB for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event.
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Calling Pkts	Number of packets that occurred during outbound calling media traffic.
Called Pkts	Number of packets that occurred during inbound called media traffic.
Calling R Factor	Average Quality of Service (QoS) factor observed during the incoming call session. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This column defines the call or transmission quality expressed as an R factor.
Called R Factor	QoS factor observed during the outgoing call session. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This column defines the call or transmission quality expressed as an R factor.
Calling MOS	A measure of voice quality for an incoming media stream.
Called MOS	A measure of voice quality for an outgoing media stream.

The following table describes the buttons on this page.

Button	Description
Search | Show all | Ladder Diagram | Export Session Details | Export Summary	
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

Displaying Session Reports

To display a Session Report:

1. After logging into the GUI, click Sessions in the left column. The session summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

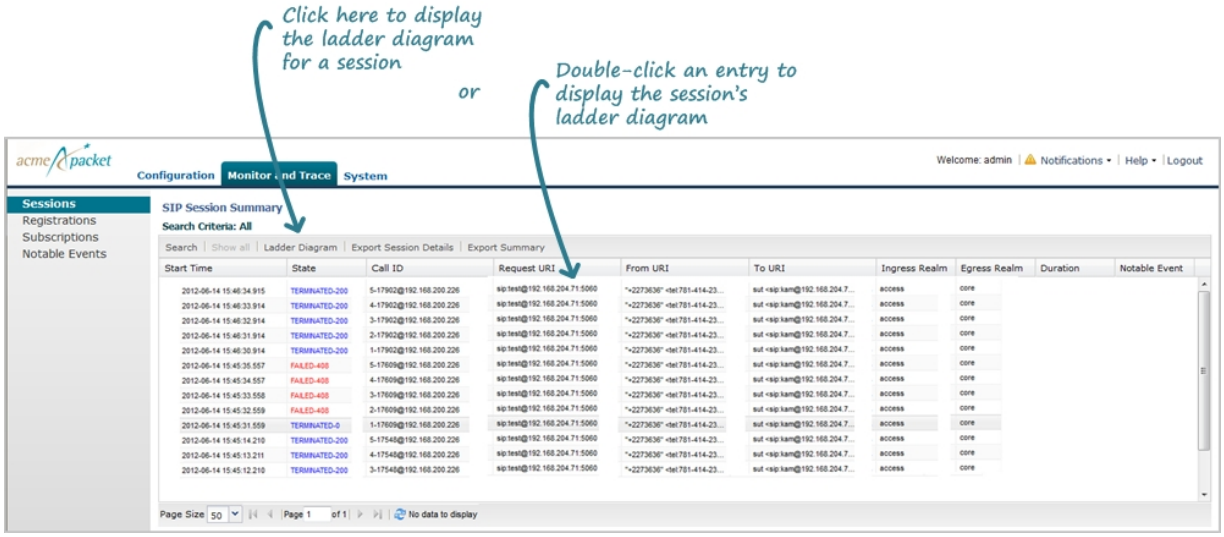
Ladder Diagram

Ladder diagrams in the GUI are logical schematics that show the call and media flow of packets on ingress and egress routes via the Net-Net ECB.

Ladder diagrams for the Session Report display the following session summary information:

- Quality of Service (QoS) statistics for call sessions
- SIP messages and media events in time sequence

To display a ladder diagram for a specific record in the Session Report, you can double-click a record in the summary table OR click <Ladder Diagram> on the Session Report page.

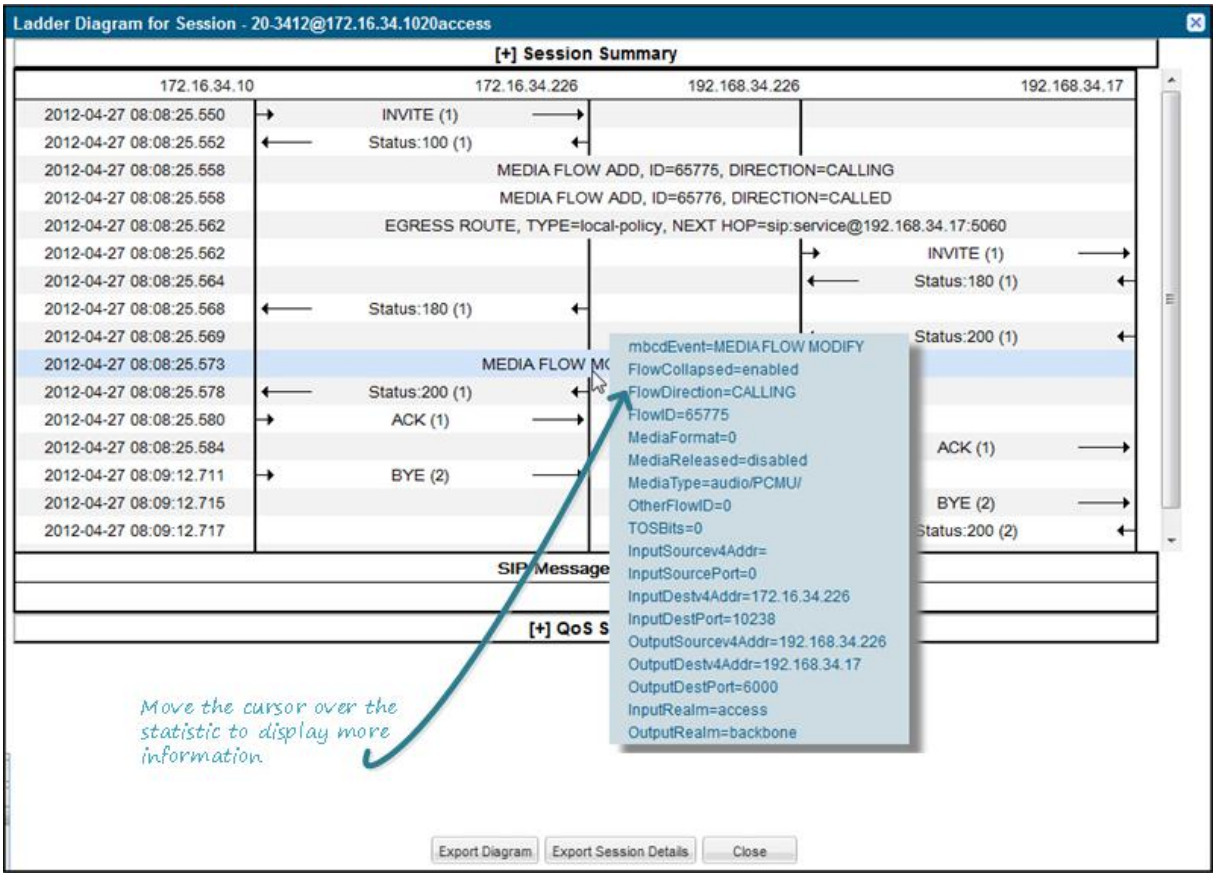


Displaying Ladder Diagrams

To display a ladder diagram:

On the Sessions Report page, click <Ladder Diagram>, or select a record in the table and double-click on that record. The following is an example of the ladder diagram that displays.

Note: The Net-Net SD captures SIP messages, applies the Header Manipulation Rules (HMR) configured on the Net-Net SD, and then applies the Session Plug-in Language (SPL) to that message. When the message is sent out from the Net-Net SD, it applies the SPL, the HMR, and then sends out the captured SIP message. Therefore, when viewing the session detail on a Ladder Diagram, the HMR and SPL information may be present.



The Session Record Ladder Diagram consists of the following information:

- Session Summary - summary information about the call or media session in focus.
- SIP Message Details - SIP message and call flow information about the call or media session in focus.
- QoS Statistics - Quality of Service (QoS) statistic information about the call or media session in focus.

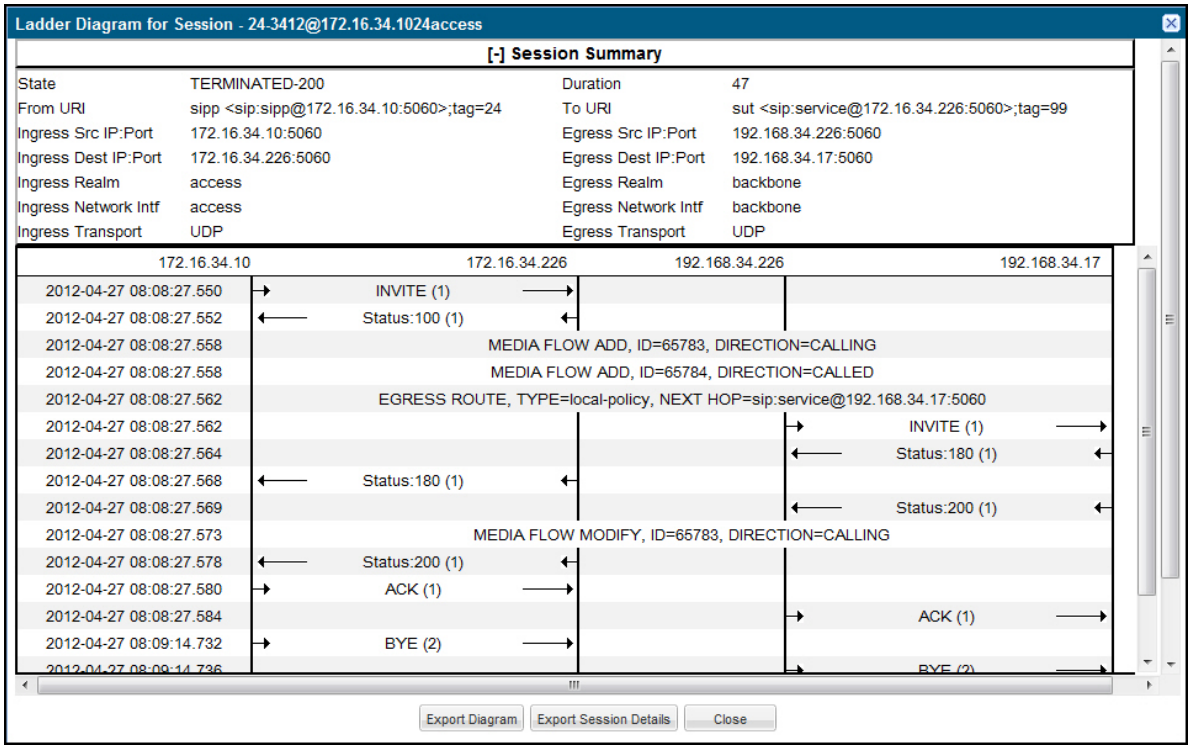
You can move your mouse over any statistic in the Ladder Diagram to view additional parameters and associated values for the statistic in a pop-up window.

The following table describes the buttons in this Ladder Diagram window.

Button	Description
Export Diagram	Exports all of the information in the Ladder Diagram (Session Summary, SIP Message Details, and QoS statistics), to a file in text format on the local machine.
Export Session Details	Exports detailed information about the SIP messages and media events associated with the session in focus, to a file in text format on the local machine.
Close	Closes the Ladder Diagram window.

Session Summary

The Session Summary window in the Ladder Diagram displays an overall summary of the call or media session in focus.



Displaying Session Summary

To display the Session Summary:

1. In the Ladder Diagram, click the [+] next to Session Summary at the top of the Ladder Diagram window. The Session Summary window expands. This window displays a summary of information about the call or media session in focus. The following table describes each field in the Session Summary window.

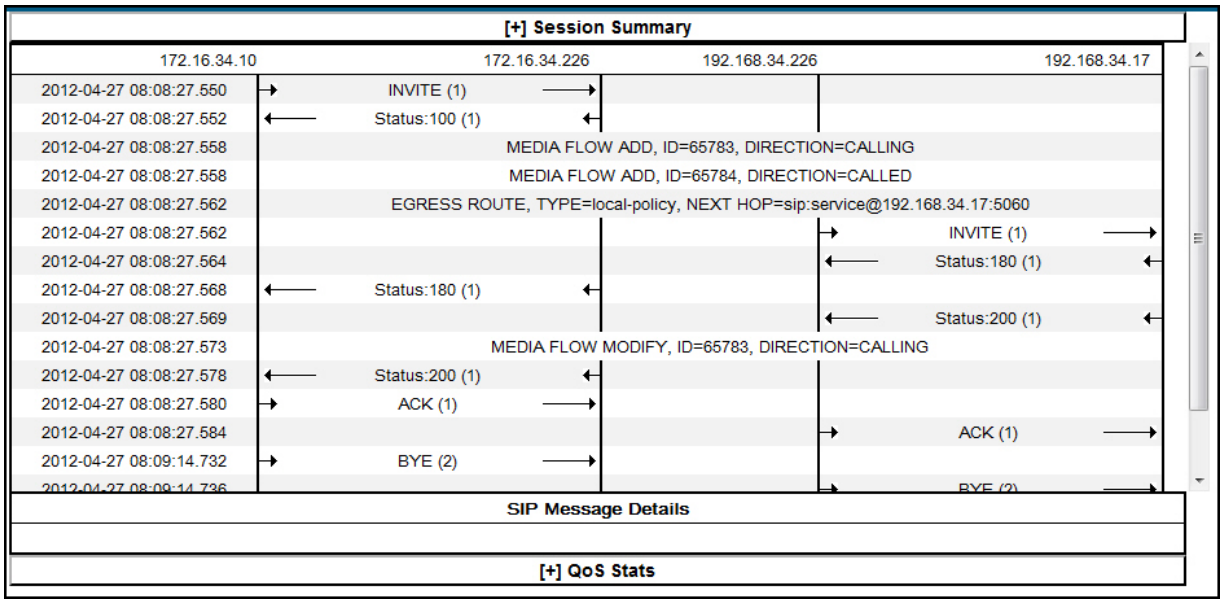
Heading	Description
State	Status of the call or media session. Valid values are: INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. EARLY Session received the first provisional response (1xx other than 100). ESTABLISHED Session for which a success (2xx) response was received. TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or Early session. The session remains in the terminated state until all the resources for the session are freed up. FAILED Session that has failed due to a 4xx or 5xx error code.
Duration	Amount of time, in seconds, that the call or media session was active.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Ingress Src IP:Port	Source IP address and port number of the incoming call or media session.
Egress Src IP: Port	Source IP address and port number of the outgoing call or media session.
Ingress Dest IP:Port	Destination IP address and port number of the incoming call or media session.
Egress Dest IP: Port	Destination IP address and port number of the outgoing call or media session.

Heading	Description
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Ingress Network Intf	Name of the incoming network interface on the Net-Net ECB.
Egress Network Intf	Name of the outgoing network interface on the Net-Net ECB.
Ingress Transport	Protocol type used on the incoming call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).
Egress Transport	Protocol type used on the outgoing call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).

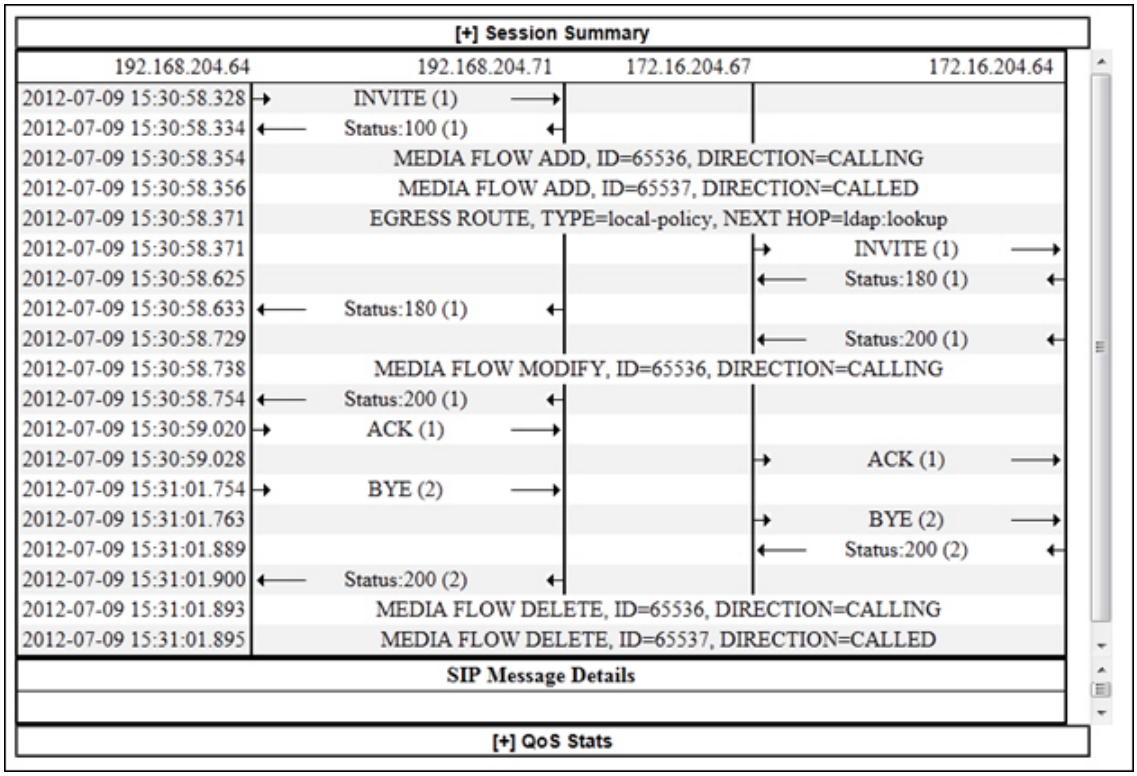
2. Click [-] to close the Session Summary window.

SIP Message Details

The SIP Message Detail window displays detailed information and data flow (ingress and egress) about the call or media event.



When a session is routed using the a Lightweight Directory Access Protocol (LDAP) configuration (Active Directory) for the local policy, the LDAP information displays in the Session Summary window. The next hop value containing "enum:…" or "dns:…" displays. Similarly, the next hop value "ldap:…" displays for LDAP queries.



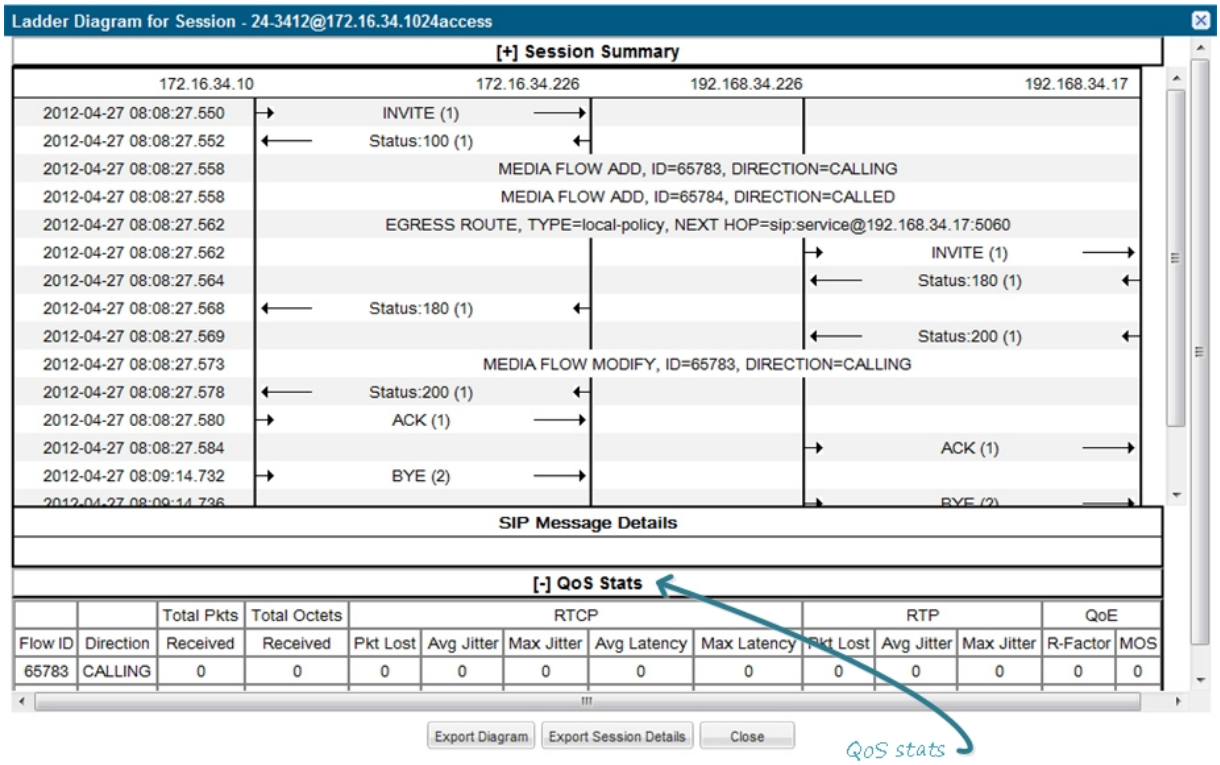
Displaying SIP Message Details

To display SIP Message Details:

On the Sessions Report page, click <Ladder Diagram>, or select a record in the table and double-click on that record. The SIP Message Details window displays. This window displays the messages and status codes that occurred during the active call session or media event. You can use the information to troubleshoot calls/media events that failed or timed out when trying to connect.

QoS Statistics

The Quality of Service (QoS) window displays information about the quality of the service used on the call session or media event when the call or event was active.



Displaying QoS Statistics

To display QoS Statistics:

1. In the Ladder Diagram, click the [+] next to QoS Stats at the bottom of the Ladder Diagram window. The QoS window expands. This window displays the QoS statistics for the call session or media event in focus. The following table describes each field in the QoS Statistics window.

Heading	Description
Flow ID	ID number assigned to the call session or media event flow of data.
Direction	The direction of the call or media event flow. Valid values are: CALLING (egress direction) CALLED (ingress direction)
Total Pkts Received	Total number of data packets received on the interface during the active call session or media event.
Total Octets Received	Total number of octets received on the interface during the active call session or media event. An octet is a unit of digital information that consists of eight bits.
RTCP	Real-time Transport Control Protocol - used to send control packets to participants in a call.
Pkts Lost	Number of RTCP data packets lost on the interface during the active call session or media event.
Avg Jitter	Average measure of the variability over time of the RTCP packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is referred to as Packet Delay Variation (PDV). It is the difference in the one-way end-to-end delay values for packets of a flow. Jitter is measured in terms of a time deviation from the nominal packet interarrival times for successive packets.

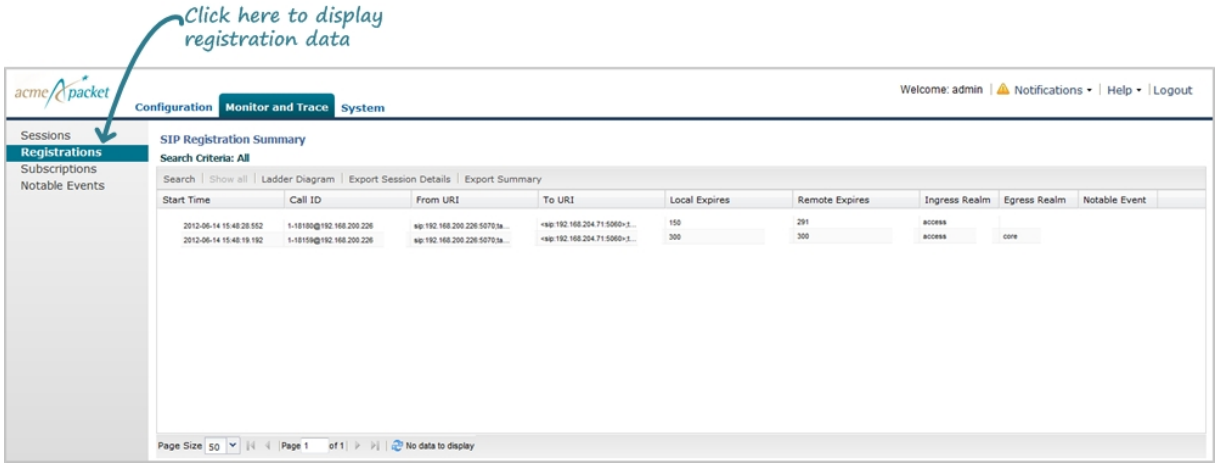
Heading	Description
Max Jitter	Maximum measure of the variability over time of the RTCP packet latency across a network. A network with constant latency has no variation (or jitter).
Avg Latency	Average observed one-way signaling latency during the active window period. This is the average amount of time the signaling travels in one direction.
Max Latency	Maximum observed one-way signaling latency during the sliding window period. This is the maximum amount of time the signaling travels in one direction.
RTP	Real-Time Transport Protocol - a standard packet format for delivering audio and video over the internet.
Pkts Lost	Number of RTP data packets lost on the interface during the active call session or media event.
Avg Jitter	Average measure of the variability over time of the RTP packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is referred to as Packet Delay Variation (PDV). It is the difference in the one-way end-to-end delay values for packets of a flow. Jitter is measured in terms of a time deviation from the nominal packet interarrival times for successive packets.
Max Jitter	Maximum measure of the variability over time of the RTP packet latency across a network. A network with constant latency has no variation (or jitter).
QoE	Quality of Experience - measurement used to determine how well the network is satisfying the end user's requirements.
R-Factor	Average Quality of Service (QoS) factor observed during the active window period. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This statistic defines the call or transmission quality expressed as an R factor.
MOS	Mean Opinion Score (MOS) score. MOS is a measure of voice quality. MOS gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using Codecs.

2. Click [-] to close the QoS Stats window.

Registration Reports

The Registration Report is a summary of all logged SIP registrations sessions on the Net-Net ECB. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net ECB.

The columns that display on the Registration Report page are dependent on the columns you selected in the procedure, Customizing the Page Display.



The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid value is: local rejection - Sessions locally rejected at the Net-Net ECB for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net ECB in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
Search | Show all | Ladder Diagram | Export Session Details | Export Summary	

Button	Description
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

Displaying Registration Reports

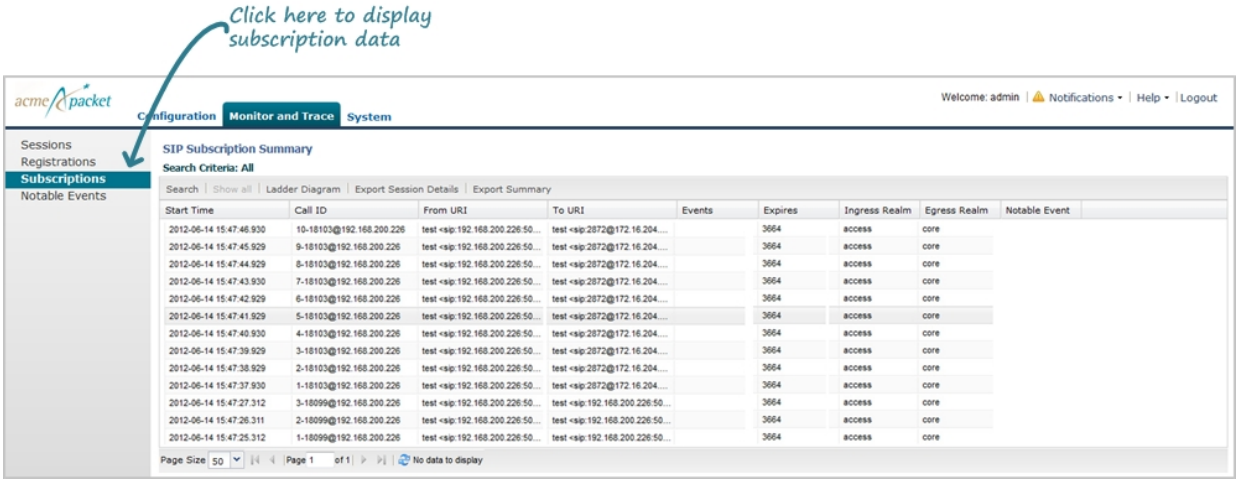
To display a Registrations Report:

1. After logging into the GUI, click Registrations in the left column. The registrations summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

Subscription Reports

The Subscription Report is a summary of all logged SIP subscription sessions on the Net-Net ECB. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net ECB.

The columns that display on the Subscription Report page are dependent on the columns you selected in the procedure, Customizing the Page Display (11).



The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Events	Specific subscribe event package that was sent from an endpoint to the destination endpoint. Applicable event packages can be:

Heading	Description
	conference - Event package that allows users to subscribe to a conference Uniform Resource Identifier (URI). consent-pending additions - Event package used by SIP relays to inform user agents about the consent-related status of the entries to be added to a resource list. dialog - Event package that allows users to subscribe to another user, and receive notifications about the changes in the state of the INVITE-initiated dialogs in which the user is involved. kpml - Event package that enables monitoring of dual-tone multi-frequency (DTMF) signals, and uses XML documents called Key Press Markup Language (KPML). message-summary - Event package that carries message-waiting status and message summaries from a messaging system to an interested User Agent (UA). presence - Event package that conveys the ability and willingness of a user to communicate across a set of devices. A presence protocol is a protocol for providing a presence service over the Internet or any IP network. reg - Event package that provides a way to monitor the status of *all* the registrations for a particular Address of Record (AoR). refer - Event package that provides a mechanism to allow the party sending the REFER to be notified of the outcome of a referenced request. .winfo - Event package for watcher information. It tracks the state of subscriptions to a resource in another package. vq-rtcpx - Event package that collects and reports the metrics that measure quality for RTP sessions.
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid value is: local rejection - Sessions locally rejected at the Net-Net ECB for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net ECB in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
Search | Show all | Ladder Diagram | Export Session Details | Export Summary	
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

Displaying Subscription Reports

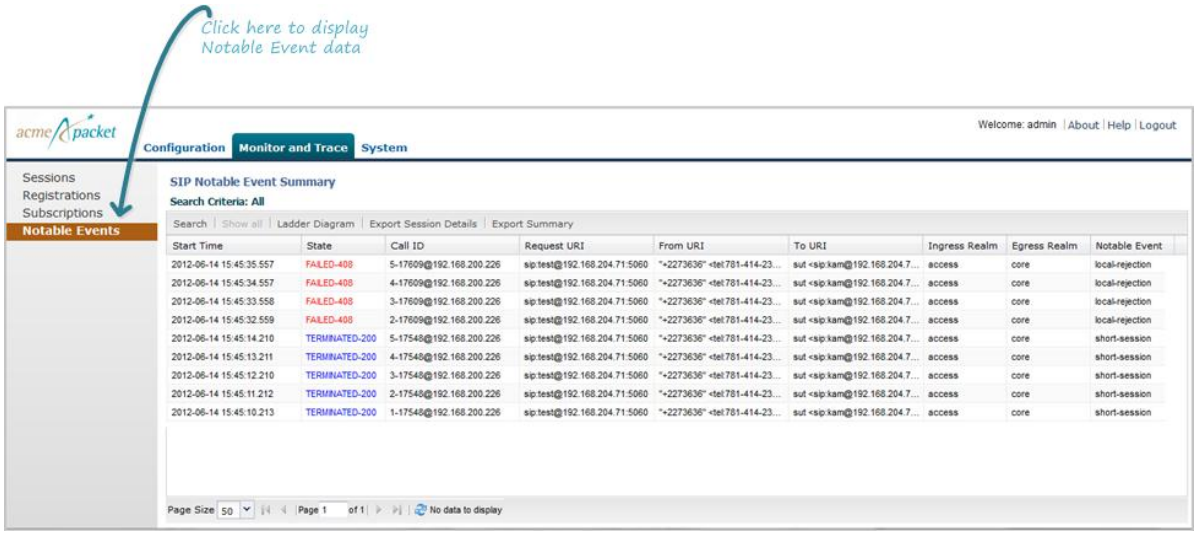
To display a Subscription Report:

1. After logging into the GUI, click Subscriptions in the left column. The subscriptions summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

Notable Event Reports

The Notable Events Report contains all logged sessions that have a notable event associated with the session on the Net-Net ECB. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net ECB.

The columns that display on the Notable Events Report page are dependent on the columns you selected in the procedure, Customizing the Page Display.



The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
State	Status of the call or media event session. Valid values are: INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. EARLY Session received the first provisional response (1xx other than 100).

Heading	Description
	ESTABLISHED Session for which a success (2xx) response was received. TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or Early session. The session remains in the terminated state until all the resources for the session are freed up. FAILED Session that has failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net ECB in REQUEST headers.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.
Events	Specific subscribe event package that was sent from an endpoint to the destination endpoint. Applicable event packages can be: conference - Event package that allows users to subscribe to a conference Uniform Resource Identifier (URI). consent-pending additions - Event package used by SIP relays to inform user agents about the consent-related status of the entries to be added to a resource list. dialog - Event package that allows users to subscribe to another user, and receive notifications about the changes in the state of the INVITE-initiated dialogs in which the user is involved. kpml - Event package that enables monitoring of dual-tone multi-frequency (DTMF) signals, and uses XML documents called Key Press Markup Language (KPML). message-summary - Event package that carries message-waiting status and message summaries from a messaging system to an interested User Agent (UA). presence - Event package that conveys the ability and willingness of a user to communicate across a set of devices. A presence protocol is a protocol for providing a presence service over the Internet or any IP network. reg - Event package that provides a way to monitor the status of *all* the registrations for a particular Address of Record (AoR). refer - Event package that provides a mechanism to allow the party sending the REFER to be notified of the outcome of a referenced request. .winfo - Event package for watcher information. It tracks the state of subscriptions to a resource in another package. vq-rtcpx - Event package that collects and reports the metrics that measure quality for RTP sessions.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid values are: short session - Sessions that don’t meet a minimum configurable duration threshold; Session dialogue, captured media information and termination signalling; Any event flagged as a short session interesting event.

Heading	Description
	local rejection - Sessions locally rejected at the Net-Net ECB for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event.
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.

The following table describes the buttons on this page.

Button	Description
Search | Show all | Ladder Diagram | Export Session Details | Export Summary	
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

Displaying Notable Events Reports

To display a Notable Events Report:

1. After logging into the GUI, click Notable Events in the left column. The notable events summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

Search for a Record

The <Search> button at the top of the report page allows you to perform a search to find a specific record(s) within a report (Sessions, Registrations, Subscriptions, Notable Events). It also allows you to specify criteria on which to perform the search.

After defining a search criteria in the Search Filter dialog box, clicking <Search>, automatically populates the report page with the records that match the criteria you specified. The search performs the filtering process of criteria dependent on the report page from which you are running the search.

For example, performing a search from the Sessions report page displays only the reports pertaining to call sessions. If you performed a search on the Registration report page, only the reports pertaining to call registrations displays on the report page. The search string containing the criteria on which you performed the search, displays in the top left corner of the page.

Note: A SIP Monitor and Trace global search can find items in the SIP headers as well.

The search criteria is saved until you click <Reset> in the dialog box, or until you log out of the HTTP session.

Performing Searches

To perform a search:

Note: You can specify a value for any or all of the fields in the Search box. The search process searches for records with all of the values you specify and displays only the records with these values. If you perform a “Global Search”, AND specify values in other fields, the search process searches the other specified fields first and then filters on the “Global Search” field.

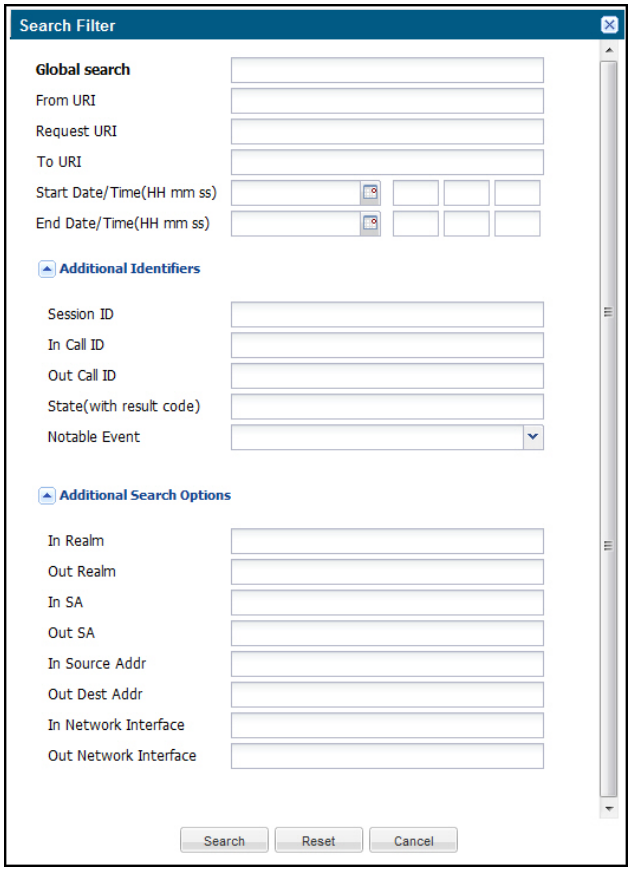
Note: If you specify a “*” in a search string, the search is performed on that exact string. For example, if you search for “123*45”, the search shows results for all strings containing “123*45”.

Note: You can use quotes (“ “) to specify a search. For example, you can enter Smith and the search finds all of the records that match Smith, such as:

John Smithfield<sip:sipp@192.168.1.70:5070>;tag=12260SIPpTag001

If you enter a space before or after a quotation mark, (for example, “Smith “), the search returns no data.

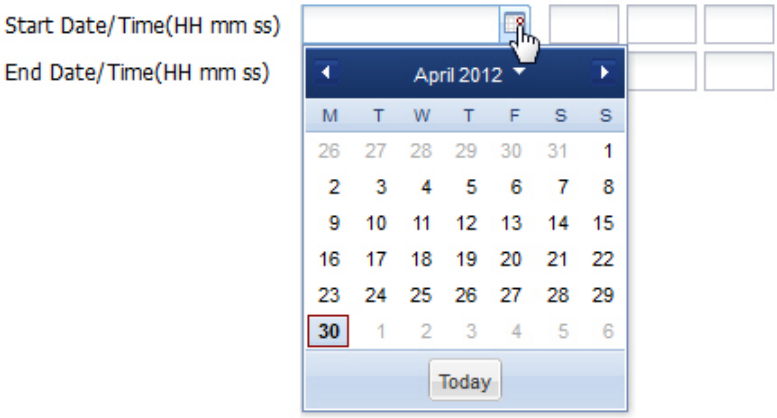
1. In any reports page, click <Search>.
2. The following dialog box displays.



3. In the Global Search field, specify a string to search all parameters in all records. Valid values are alpha-numeric characters.

   Note: The Global Search option searches all parameters in all the session records stored in memory. All values you specify in other fields are searched before the value specified in the Global Search field is used.

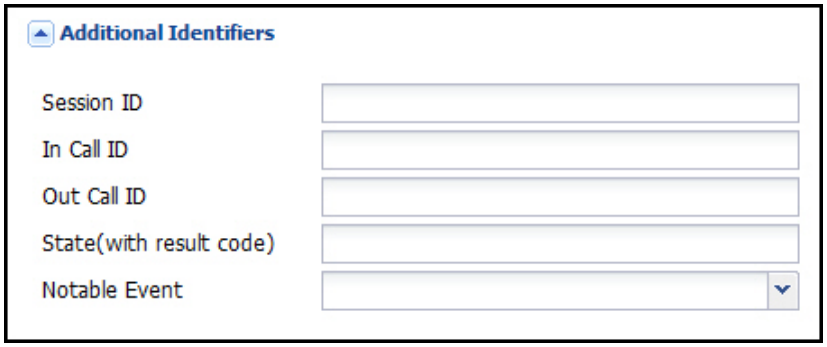
4. In the From URI field, enter the URI formatted string of the call source information you are searching. Valid values are alpha-numeric characters. For example, sipp<sip:sipp@172.16.34.10:5060;tag=24.
5. In the Requested URI field, enter the URI formatted string that contains a protocol, name, location, or any other applicable characteristic, that is sent by the Net-Net ECB in the REQUEST header. Valid values are alpha-numeric characters. For example, sip:service@172.16.34.226:5060.
6. In the To URI field, enter URI formatted string of the call destination information you are searching. Valid values are alpha-numeric characters. For example, sut<sip:service@172.16.34.226:5060;tag=99.
7. In the Start Date/Time (HH mm ss) field, enter a starting date to search on in the first text box in the format YYYY-MM-DD (where Y =year, M=month, and D=day). or Click on the calendar icon in this field to display a calendar from which you can select a date. Navigate the calendar to find the date you want and click on it to enter it into this field, or click <Today> to enter today's date. For example, 2012-04-15 would search for all records starting on April 15, 2012. Valid values are numeric characters only. Enter a start time to search on in the last three text boxes in the format HH mm ss (where H=hour, m=minutes, and s=seconds). For example, 01 30 45 would search for all records starting at 1:30 and 45 seconds. Valid value are numeric characters only.



8. In the End Date/Time (HH mm ss) field, repeat the process of entering a date and time as provided in Step 7.
9. To search on additional parameters, click on the Additional Identifiers down arrow to expand the dialog box.

Additional Identifiers

To specify additional identifiers:

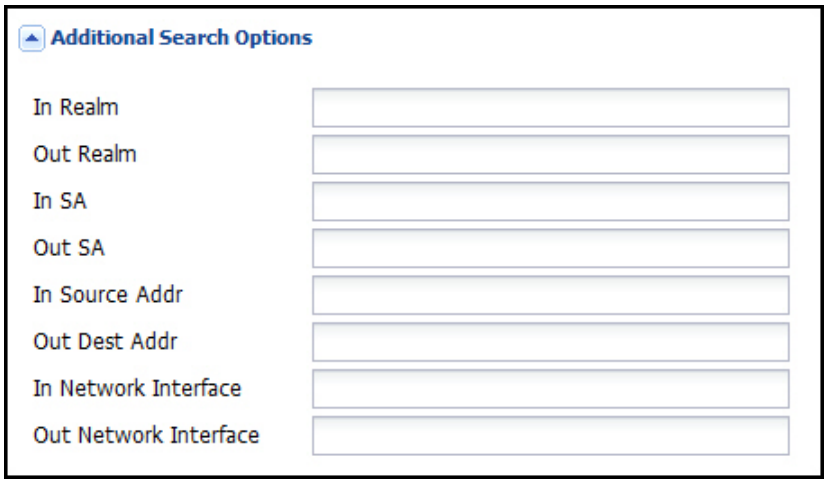


1. In the Session Id field, enter the ID of the call session you want to search. Valid values are alpha-numeric characters. For example, 22-3412@172.16.34.1.
2. In the In Call ID field, enter the ID of the incoming call (phone number and source IP address). Valid values are alpha-numeric characters. For example, 25-3412@172.16.34.10.
3. In the Out Call ID field, enter the ID of the outgoing call (phone number and IP address). Valid values are alpha-numeric characters. For example, 14-3412@172.14.54.6.
4. In the State (with result code) field, enter the status of the call session with the result code for which you want to search. Valid values are (case-sensitive):
   - INITIAL-<result code>
   - EARLY-<result code>
   - ESTABLISHED-<result code>
   - TERMINATED-<result code>
   - FAILED-<result code>

   Result codes can range from 1xx to 5xx. For example, terminated-200, or failed-400.
5. In the Notable Event field, select the notable event for which you want to search. Valid values are:
   - any-event - search displays any notable event that was stored in memory.
   - short-session - search displays only records that indicate a short-session duration has occurred.
   - local-rejection - search displays only records that indicate a local-rejection has occurred.
6. To search on additional parameters, click on the Additional Search Options down arrow to expand the dialog box.

Additional Search Options

To specify additional search options:



1. In the “In Realm” field, enter the name of the realm for which the incoming call belongs. Valid values are alpha-numeric characters. For example, access.
2. In the “Out Realm” field, enter the name of the realm for which the outgoing call belongs. Valid values are alpha-numeric characters. For example, backbone.
3. In the “In SA” field, enter the name of the session agent (SA) on the incoming call session. Valid values are alpha-numeric characters. For example, SA1.
4. In the “Out SA” field, enter the name of the session agent (SA) on the outgoing call session. Valid values are alpha-numeric characters. For example, SA2.
5. In the “In Source Addr” field, enter the source IP address of the SA that accepted the incoming call session. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 172.45.6.7.
6. In the “Out Dest Addr” field, enter the destination IP address of the SA that accepted the outgoing call session. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 172.64.56.7.
7. In the In Network Interface field, enter the incoming core network interface that connects the Net-Net ECB to your network. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 192.45.6.7.
8. In the Out Network Interface field, enter the outgoing network interface that connects your Net-Net ECB to the outside network. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 192.45.6.8.
9. Click <Search> to perform the search with the values you specified. A list of the records that the search process filtered, display in the window. The GUI saves the search specifications until you click <Reset> in the search dialog box, OR until you log out of the GUI.

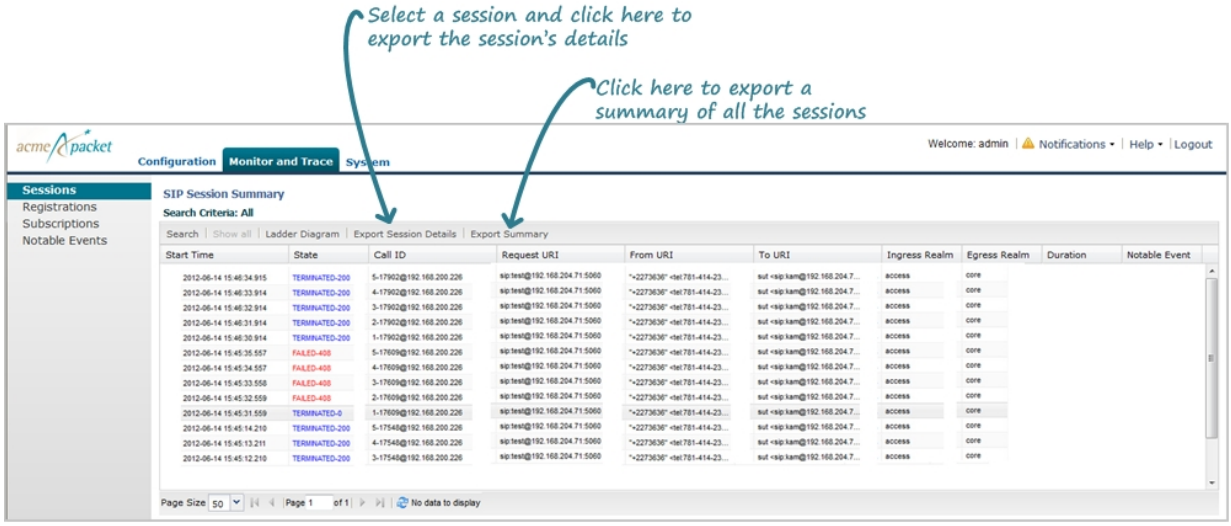
Export Information to a Text File

Monitor and Trace allows you to export information to a text file from the Sessions, Registrations, Subscriptions and Notable Events Reports, as well as from a specific ladder diagram, or from a page containing the results of a search. The data exports to a file that you can open and view as required.

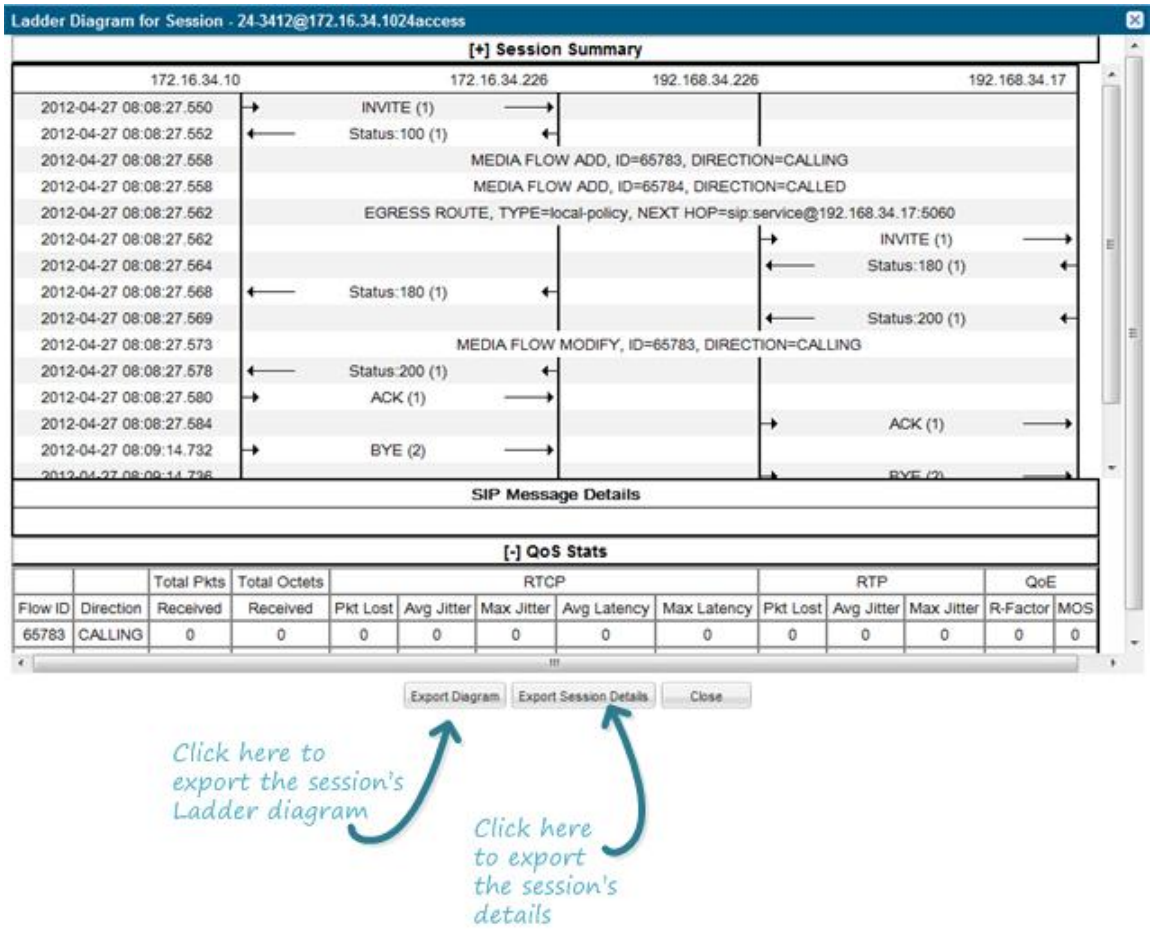
You can export any of the following:

- All information from each report
- Information from a specific record only
- Information from a search result
- Information from a Ladder Diagram

From the Sessions, Registrations, Subscriptions, and Notable Events Reports Page



From the Ladder Diagram Page



The following table identifies the buttons to use to export specific information from Monitor and Trace. All the export buttons in the GUI export to text files.

Button	Description
From the Sessions, Registrations, Subscriptions, and Notable Events Reports:	

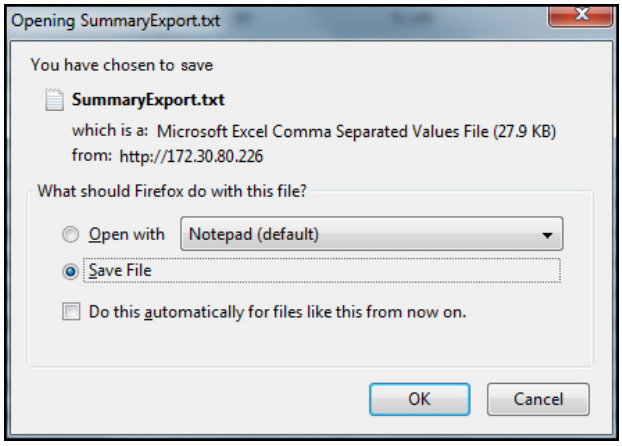
Button	Description
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine. Note: This button exports ALL call session summary records or the records that matched a search criteria to the file.
From the Ladder Diagram:	
Export Diagram	Exports all of the information in the Ladder Diagram (Session Summary, SIP Message Details, and QoS statistics), to an HTML file format on the local machine.
Export Session Details	Exports detailed information about the SIP messages and media events in the Ladder Diagram associated with the selected session, to a file in text format on the local machine.

The following procedure is an example of using the export buttons in Monitor and Trace:

Exporting Information to Text Files

To export information to a text file:

1. In the applicable Report window or Ladder Diagram window, click the appropriate Export button. The following example illustrates that the <Export Summary> button was clicked on a report page. The following prompt displays.\



The GUI assigns the file name for the text file (shown as SummaryExport.txt in the illustration above.)

Note: The GUI exports Ladder Diagrams as HTML files.

2. Click “Open with” and select the application for which to open the resulting text file. or Click Save File to save the text file to your local PC.
3. Click <OK> to export the session or media information to the text file.

   The following illustration shows a partial summary of the Sessions Report exported to a text file and opened using Microsoft Word™.

```
Export Summary:


----------Session Summary----------
Startup Time: 2012-04-26 08:40:44.624
State: TERMINATED-200
Duration: 9
From URI: sipp &lt;sip:sipp@172.16.34.10:5060&gt;;tag=25
To URI: sut &lt;sip:service@172.16.34.226:5060&gt;;tag=3453
Ingress Src Address:  172.16.34.10
Igress Src Port: 5060
Igress Dest Address: 172.16.34.226
Igress Dest Port: 5060
Egress Source Address: 192.168.34.226
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone

----------Session Summary----------
Startup Time: 2012-04-26 08:40:43.624
State: TERMINATED-200
Duration: 9
From URI: sipp &lt;sip:sipp@172.16.34.10:5060&gt;;tag=24
To URI: sut &lt;sip:service@172.16.34.226:5060&gt;;tag=3452
Ingress Src Address:  172.16.34.10
Igress Src Port: 5060
Igress Dest Address: 172.16.34.226
Igress Dest Port: 5060
Egress Source Address: 192.168.34.226
Egress Source Port: 5060
```

4

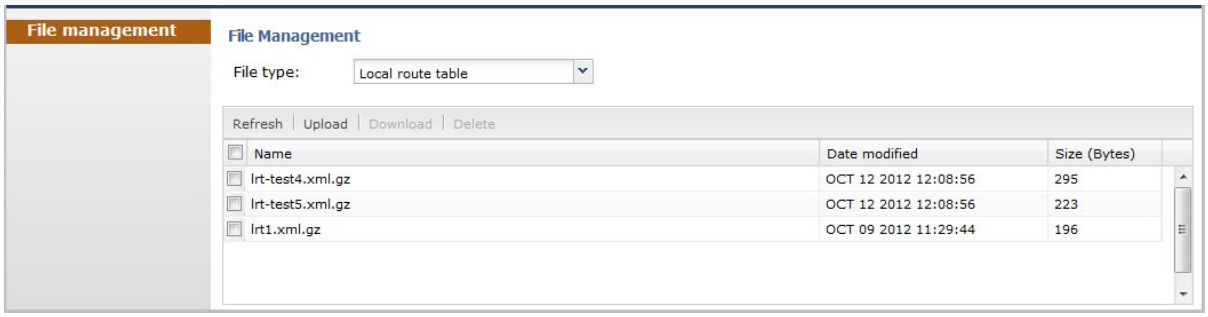
System File Management

Basic description of GUI file management dialogs.

The System tab within the GUI provides an easy and convenient means for managing your Net-Net ECB system files. It allows you to perform the following:

- Upload files
- Download files
- Delete files
- Restore files

The following is an example o the System tab window.



The following table identifies the files you can manage on the Net-Net ECB

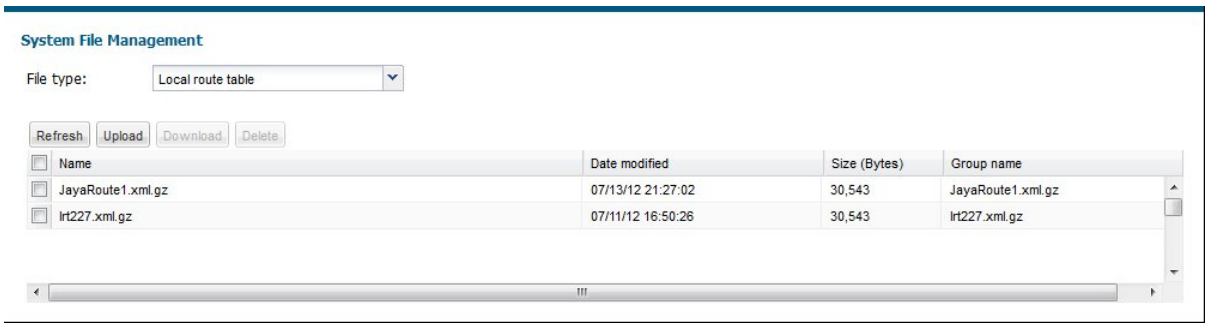
File Type	Format	Description
Local route table (LRT)	.xml.gz	Local routing table (LRT) file that you can apply to the Net-Net ECB. The LRT is an in-memory table that contains IP addresses that the local router recognizes. It calculates the destinations of messages it is responsible for forwarding.
SPL Plug-in	.lua	Session Plug-in Language (SPL) file that you can apply to the Net-Net ECB to incorporate additional functionality. The SPL file contains a programming language that is

File Type	Format	Description
		capable of performing various tasks by utilizing APIs and callbacks in the Net-Net ECB.
Backup configuration	.gz	File that contains a backup of the Net-Net ECB software configuration. You can apply this file to restore a previous configuration if required.
Playback media (Not applicable to the Net-Net ECB)	Any media format valid in an RTP audio stream	Call progress playback files. The Net-Net ESD can use these files in generated media streams if required. Note: The media files are raw binary files that contain data for the codec that a user wants to have played in the media stream. The Net-Net ESD plays the data on the first audio flow in the Session Description Protocol (SDP).
SIP Trunk Xpress bootstrap (Not applicable to the Net-Net ECB	.tar.gz	Service Provider or Enterprise file that contains the initial Net-Net ESD configuration to establish a SIP Trunk between a Service Provider SBC and an Enterprise SBC. You can download this file to your PC and then upload the file to the Net-Net ESD. Note: You must manually run the “load-bootstrap” command via the ACLI to apply the bootstrap to the Net-Net ESD. For more information on applying a bootstrap to a Net-Net ESD, see the SIP Trunk Xpress for Service Providers or the SIP Trunk Xpress for Enterprises documentation.
Log	Text	Log files that contain information about the various aspects of the Net-Net ESD. For example, information logged about the ACLI, SIP, or H323. Note: Only the Download and Delete functions are applicable to log files on the Net-Net ESD.

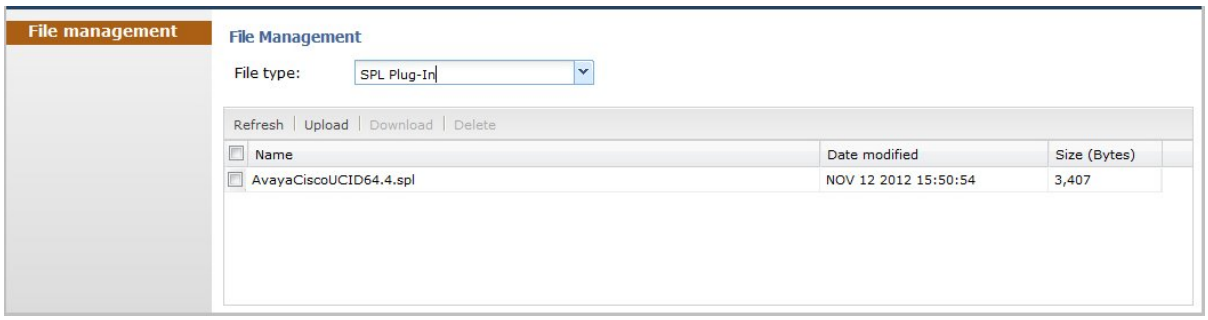
Note: You can activate an LRT file or an SPL file dynamically during an upload, if required. You can also immediately apply a backup configuration file during the upload process.

The following illustrations show an example of each file type screen.

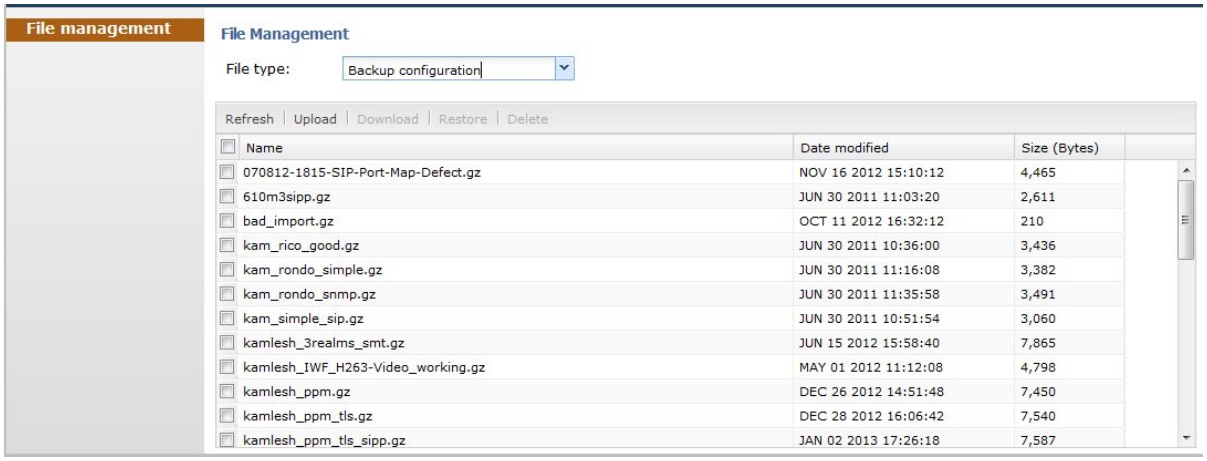
Local Route Table File Management



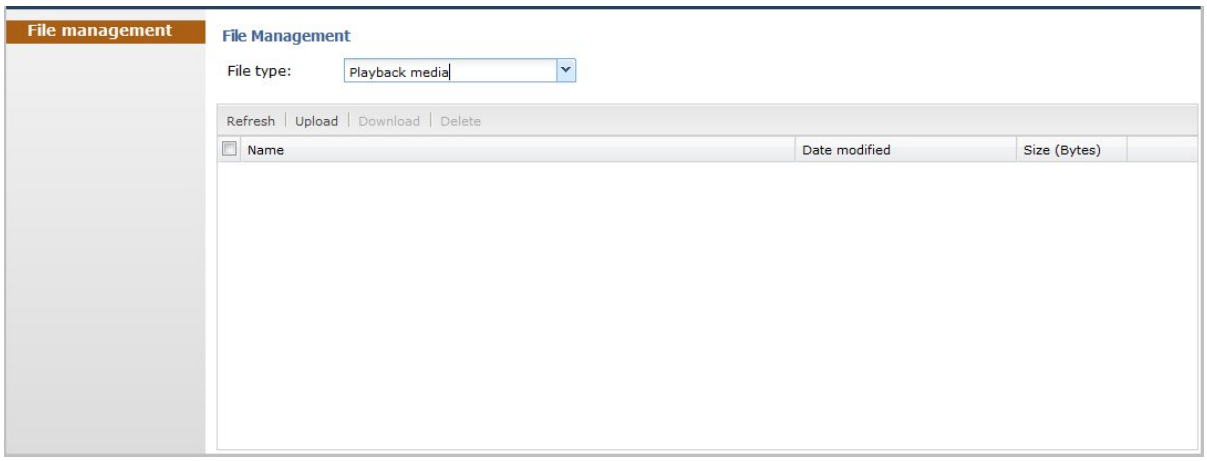
SPL Plugin File Management



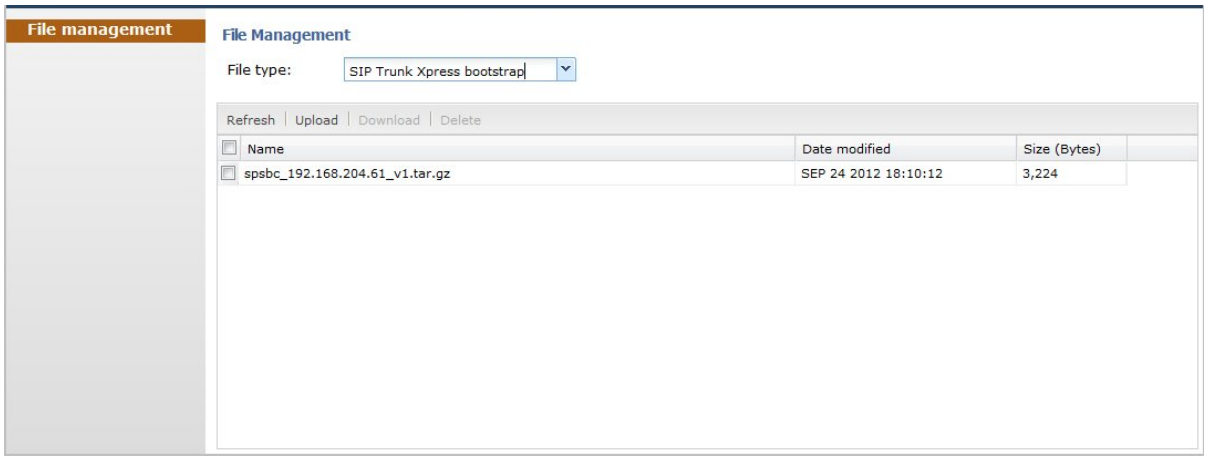
Backup Configuration File Management



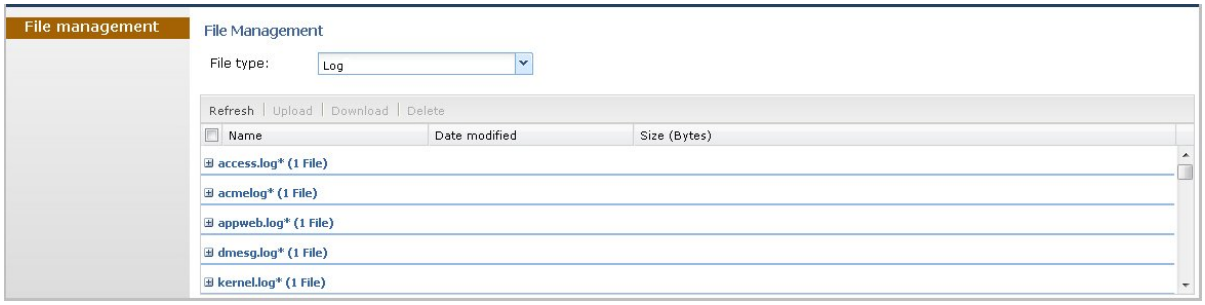
Playback Media File Management (Not relevant to ECB)



SIP Trunk Express Bootstrap File Management (Not relevant to ECB)

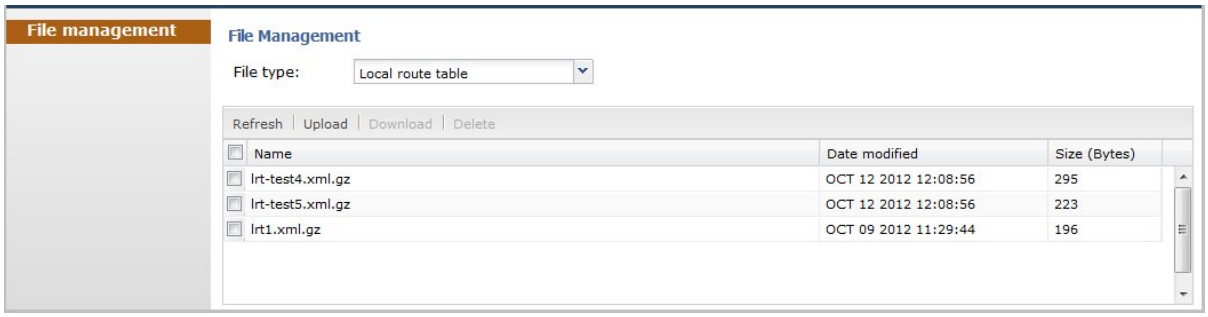


Log File Management



Accessing the System Tab

After logging into the GUI, click the “System” tab. The System files window displays.



This window shows the System files currently stored on the Net-Net ESD. The “Local route table” files display by default. The following table describes the columns on this page.

Column	Description
File Type	Lists the applicable System files you can select to display in the window. Valid values are: Local route table (LRT) SPL Plug-in (SPL) Backup configuration SIP Trunk Xpress bootstrap

Column	Description
	Playback media Log
Name	Name of the file(s) associated with the file type selected. All file names within a group have common file formats (for example, the local route table can consist of a group of files in the format “<filename>.xml.gz”.)
Date Modified	Month, day, year, and time that the file was last modified. Format is: <MM><DD><YYYY><HH><MM><SS>.
Size (Bytes)	Total size of this file (in bytes).
Group Name Note: This column is hidden by default. For more information about hidden columns, see Customizing the Page Display.	Name of the group to which this file belongs. For example, in the screen above, the file called “JayaRoute1.xml.gz”, belongs to the Group Name “JayaRoute1.xml.gz”, and the file called “lrt227.xml.gz” belongs to the Group Name “lrt227.xml.gz.”

The following table describes the buttons on this page

Button	Description
Refresh	Updates the screen to display the lastest data.
Upload	Uploads a file type from your server or PC to the Net-Net ECB. The LRT, SPL, and backup configuration upload process provide the option of dynamically applying these files to the Net-Net ECB.
Download	Downloads the file type from the Net-Net ECB to your local server or PC (typically to the download directory on your system).
Restore (Applicable to the “Backup configuration” file type only.)	Restores and applies a Backup configuration file to the Net-Net ECB.
Delete	Deletes the file type from the Net-Net ECB.

Uploading a File

Procedure and conditions around file upload on the Net-Net ECB.

You can upload any of the following file types from your local server or PC to the Net-Net ESD:

- Local route table (LRT)
- SPL Plug-in (SPL)
- Backup configuration
- SIP Trunk Xpress bootstrap
- Playback media

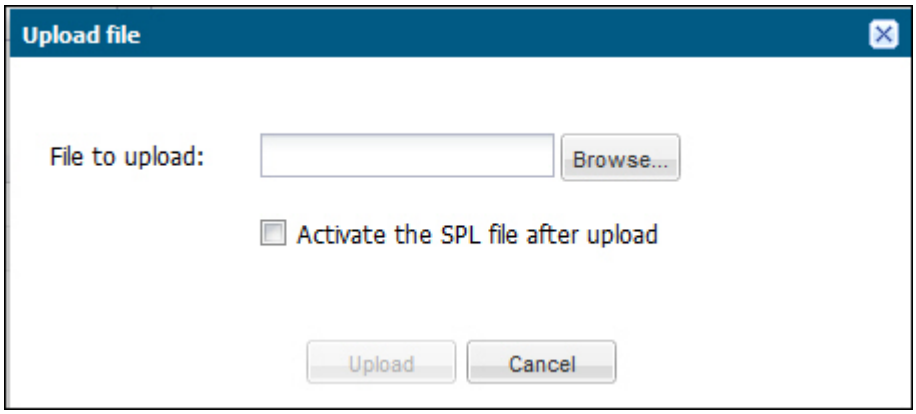
Note: You cannot upload log files.

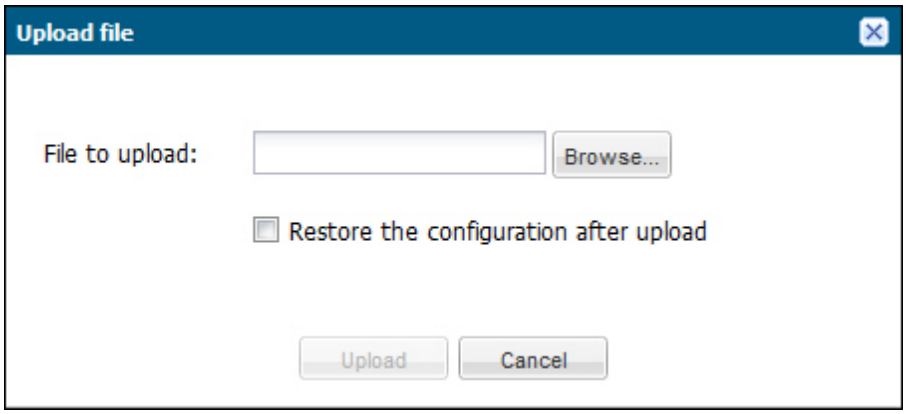
You can dynamically activate the “Local route table” and “SPL Plug-in”during the upload process, if required. You can also immediately restore a backup configuration file after an upload is complete.

1. (optional) In the “Select the file type” field, select the type of file you want to upload from your local server or PC to the Net-Net ECB. Valid types of files are:
   - Local route table (LRT)
   - SPL Plug-in (SPL)
   - Backup configuration
   - SIP Trunk Xpress bootstrap
   - Playback media

   Note: You can click the <Upload> button without selecting a file from the list of files that display

2. In the “Name” column, place a checkmark next to the file you want to upload.
3. Click <Upload>. The following are examples of the dialog box that display, dependant on which file type you chose.





4. In the “File to upload” field, click the <Browse> button, and navigate to the location on your server or PC where the file resides.

   Note: The file extension on the file must be applicable to the file type you select. For example, an SPL Plug-in file must have the file format of “<filename>.lua ”. The following table indicates the file formats required for each File Type, and the applicable directory to which the upload process stores the file on the Net-Net ECB.

File Type	File Format	Directory
Local route table (LRT)	.xml.gz	/code/gzConfig
SPL Plug-on (SPL)	.lua	/code/spl

File Type	File Format	Directory
Backup Configuuration	.gz	/code/bkups
SIP Trunk Xpress bootstrap	.tar.gz	/code/gzConfig
Playback media	Any media format valid in an RTP audio stream	/code/media

If you select a file with an incorrect file extension, the following message displays: “The file name extension doesn’t match the file type. The file should have the extension: <file type extension>” (For example, “.xml.gz).

5. Perform the following, based on your filetype.

   For the “Local route table” file type, place a checkmark in the “Activate the LRT file after upload” box, to immediately apply the LRT to the Net-Net ECB after upload is complete.

   or

   For the “SPL Plug-in” file type, place a checkmark in the “Activate the SPL file after upload” box, to immediately apply the SPL file to the Net-Net ECB after upload is complete.

   or

   For the “Backup configuration” file, place a checkmark in the “Restore the configuration after upload” box, to immediately apply a previous backed up configuration file to the Net-Net ECB after upload is complete. Uncheck the box to restore the backup configuration at a later time. You can use the <Restore> button to restore the configuration to the Net-Net ECB when required.

6. Click <Upload> or click <Cancel> to cancel the upload function.

   After clicking <Upload>, the Net-Net ESD checks if the file you are uploading already exists on the system. If the file exists, the following prompt displays:

   “Would you like to replace the current file?”

   Click <Yes> to replace the file.

   or

   Click <No> to cancel the upload function.

   If uploading a SIP Trunk Xpress bootstrap file, you must manually run the “load-bootstrap” command via the ACLI to apply the bootstrap to the Net-Net ESD. For more information on applying a bootstrap to a Net-Net ESD, see the SIP Trunk Xpress for Service Providers or the SIP Trunk Xpress for Enterprises documentation.

Enter the tasks the user should do after finishing this task (optional).

Downloading a File

Procedure and conditions around file download from the Net-Net ECB.

You can upload any of the following file types from your local server or PC to the Net-Net ESD:

- Local route table (LRT)
- SPL Plug-in (SPL)
- Backup configuration
- SIP Trunk Xpress bootstrap
- Playback media

1. In the “Select the file type” field, select the type of file you want to upload from your local server or PC to the Net-Net ECB. Valid types of files are:

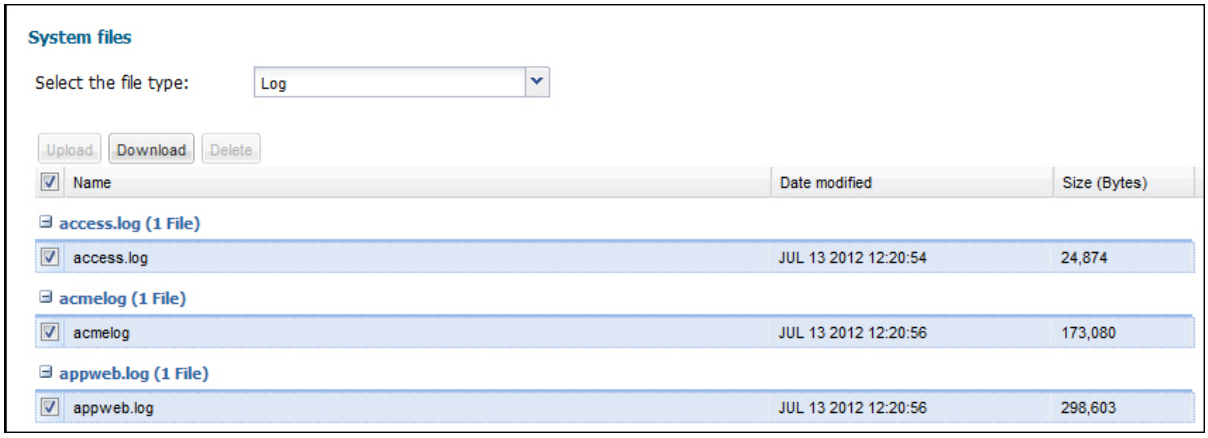
   - Local route table (LRT)
   - SPL Plug-in (SPL)

- Backup configuration
- SIP Trunk Xpress bootstrap
- Playback media

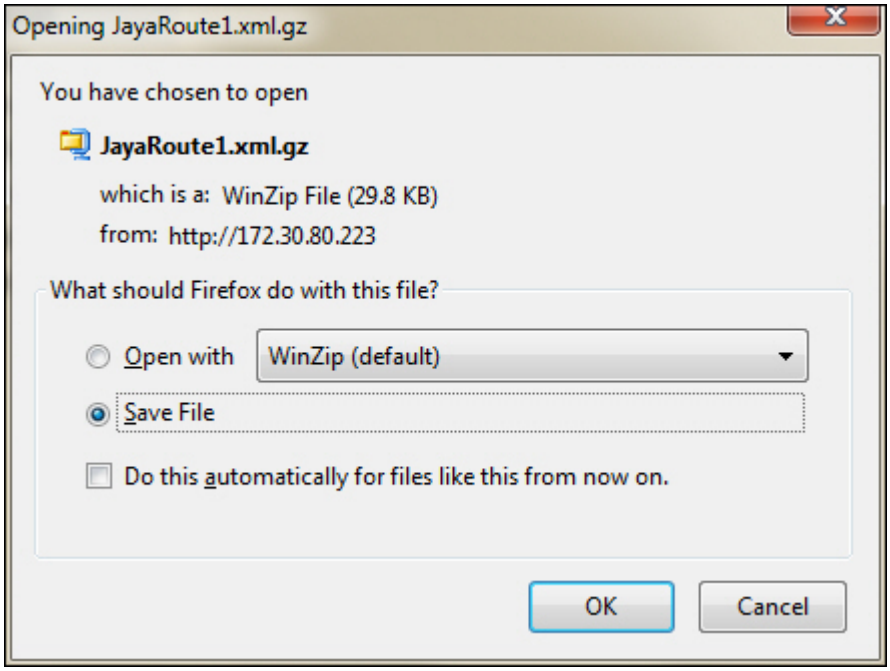
Note: You can click the <Upload> button without selecting a file from the list of files that display

2. In the “Name” column, place a checkmark next to the file you want to upload.

   For Log file types, you can select multiple log files to download, or place a checkmark in the box to the left of the “Name” column heading to select all log files to download. When downloading multiple log files, the File Management GUI compresses the files into one “.tar” file and downloads that file to your local server or PC.



3. Click <Download>. The following is an example dialog box that displays



4. Click “Open with” and select the application for which to open the file type for decompressing and/or editing. Or click “Save File” to save the file type to your local server or PC.
5. Click <OK>. The file type downloads to the folder on your local server or PC where your Browser sends all downloads (typically your “Download” folder) or opens (decompresses) the file type on your local server or PC (typically in the “Download” folder).

Deleting a File

Procedure and conditions around file delete from the Net-Net ECB.

You can upload any of the following file types from your local server or PC to the Net-Net ESD:

- Local route table (LRT)
- SPL Plug-in (SPL)
- Backup configuration
- SIP Trunk Xpress bootstrap
- Playback media

Note: You can select a single or multiple files to delete.

1. In the “Select the file type” field, select the type of file you want to upload from your local server or PC to the Net-Net ECB. Valid types of files are:
   - Local route table (LRT)
   - SPL Plug-in (SPL)
   - Backup configuration
   - SIP Trunk Xpress bootstrap
   - Playback media
2. In the “Name” column, place a checkmark next to the file(s) you want to delete.

   Note: For Log file types, place a checkmark in the box to the left of the “Name” column heading to select all log files to delete.
3. Click <Delete>. The following message displays.
   “Are you sure you want to delete the file?”
4. Click <Yes> to delete the file(s) from the Net-Net ECB.

   or

   Click <No> to cancel the delete function.

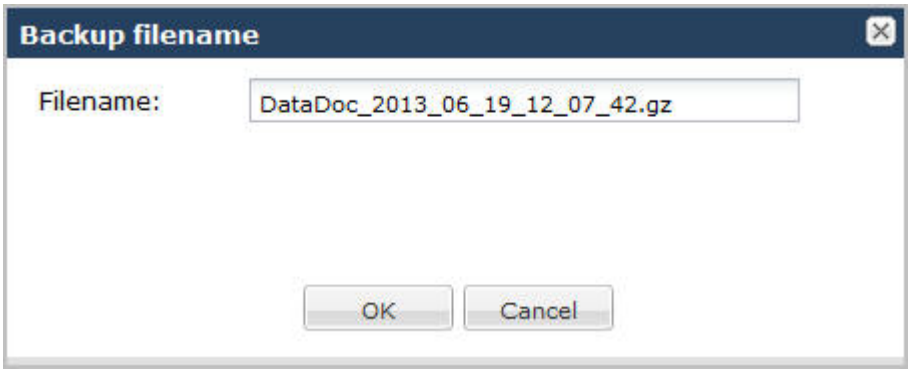
Backing up a File(s)

You can backup a configuration file from the Enterprise Session Director to your local server or PC if required. This allows you to save configurations that you can restore to your Enterprise Session Director at a later time.

To backup a configuration file:

1. In the “Select the file type” field, select “Backup configuration”.
2. Select a configuration file(s) to backup to your server or PC by placing a checkmark in the file’s checkbox.
3. Click Backup.

   The following dialog box displays:



4. Click OK to backup the configuration. Or click Cancel to cancel the backup function.

   If you click OK, the file downloads to your server or PC (typically into the download directory).

   You can restore the configuration at any time using the “Restore” function described in Restoring a File.

Restoring a File

Procedure and conditions around file restoration on the Net-Net ECB.

You can restore a backed up configuration file to the Net-Net ECB if required. When you select a file to restore, and click the <Restore> button, the backup configuration file downloads to the Net-Net ECB and the Net-Net ECB reboots.

1. In the “Select the file type” field, select “Backup configuration”.
2. Select a backup file to restore to the Net-Net ESD by placing a checkmark in the file’s checkbox.

   Note: The <Restore> button enables only if you select a backup file.

3. Click <Restore>. The following prompt displays:
   “Are you sure you want to restore the configuration? Note: The SBC will be rebooted. Connectivity may be lost between the browser and the SBC during this time.”
4. Click <Yes> to restore the backup configuration.

   or

   Click <No> to cancel the restore function.

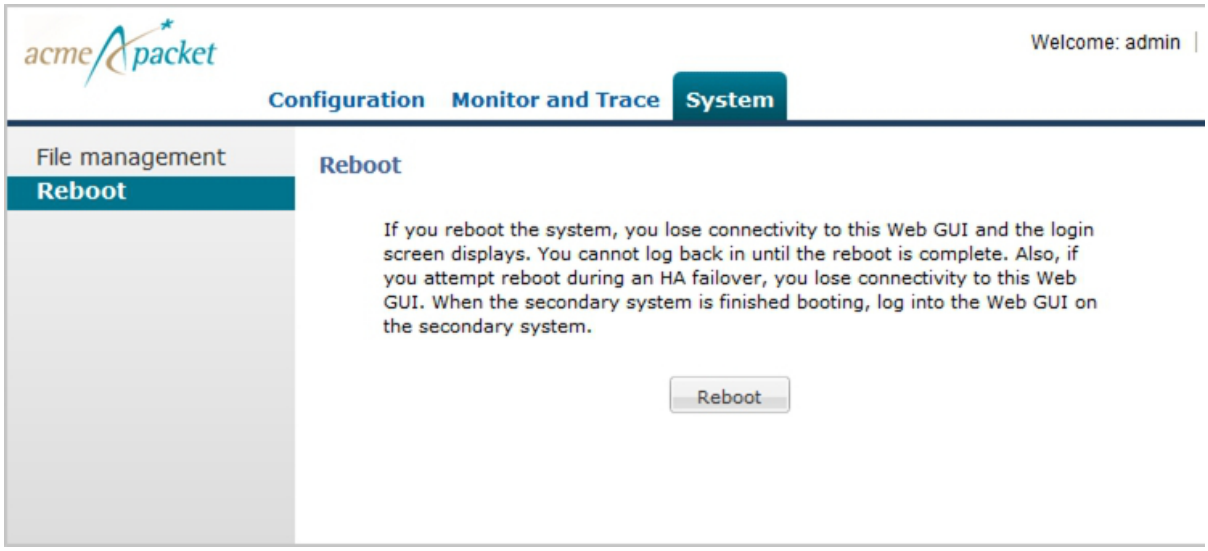
   If you click <Yes>, the backup file downloads to the Net-Net ESD and the Net-Net ESD reboots and restores the configuration from the backup file.

   Note: Connectivity between the Web GUI and the Net-Net ECB is temporarily lost during the reboot process.

Rebooting the System

If required, you can manually reboot the Enterprise Session Director. However, if you reboot the system, all connectivity is lost. If you have a High Availability setup, connectivity to the secondary (backup) Enterprise Session Director is lost as well.

When the reboot is complete, the login screen displays on both the primary and secondary systems. You must manually login to both systems.



IF	THEN
you perform a reboot from the Web GUI	the GUI session closes and displays the Login screen. You cannot login to the Web GUI until the reboot is complete on the Enterprise Session Director.
you perform a reboot from the Web GUI, and a reboot is already in progress	a message displays indicating that a reboot can not occur. The first reboot must complete before another reboot is initiated.
you perform a reboot from the Web GUI, and the primary system is currently failing over to the secondary system (HA environment)	a message displays indicating that a reboot can not occur. The HA failover is currently underway. The secondary system is updating and getting its configuration from the primary server. When the reboot is complete, you can no longer login to the primary system Web GUI. You need to login to the secondary system's Web GUI (which is now the primary system).

5

Format of Exported Text Files

Introduction

This Appendix provides a sample and format of each type of exported file from the Web-based GUI. Sample information in these files are provided as a reference for your convenience.

Exported file examples include:

- Session Summary exported file (text format)
- Session Details exported file (text format)
- Ladder Diagram exported file (HTML format)

Note: Acme Packet recommends you open an exported text file using an application that provides advanced text formating, such as Microsoft Word™. Opening the exported file using Notepad, or any other simple text editor can be difficult to read.

Exporting Files

The Web-based GUI allows you to export information to a text file from the Sessions, Registrations, Subscriptions and Notable Events Reports, as well as from a specific ladder diagram, or from a page containing the results of a search. The data exports to a file that you can open and view as required.

You can export any of the following to a file:

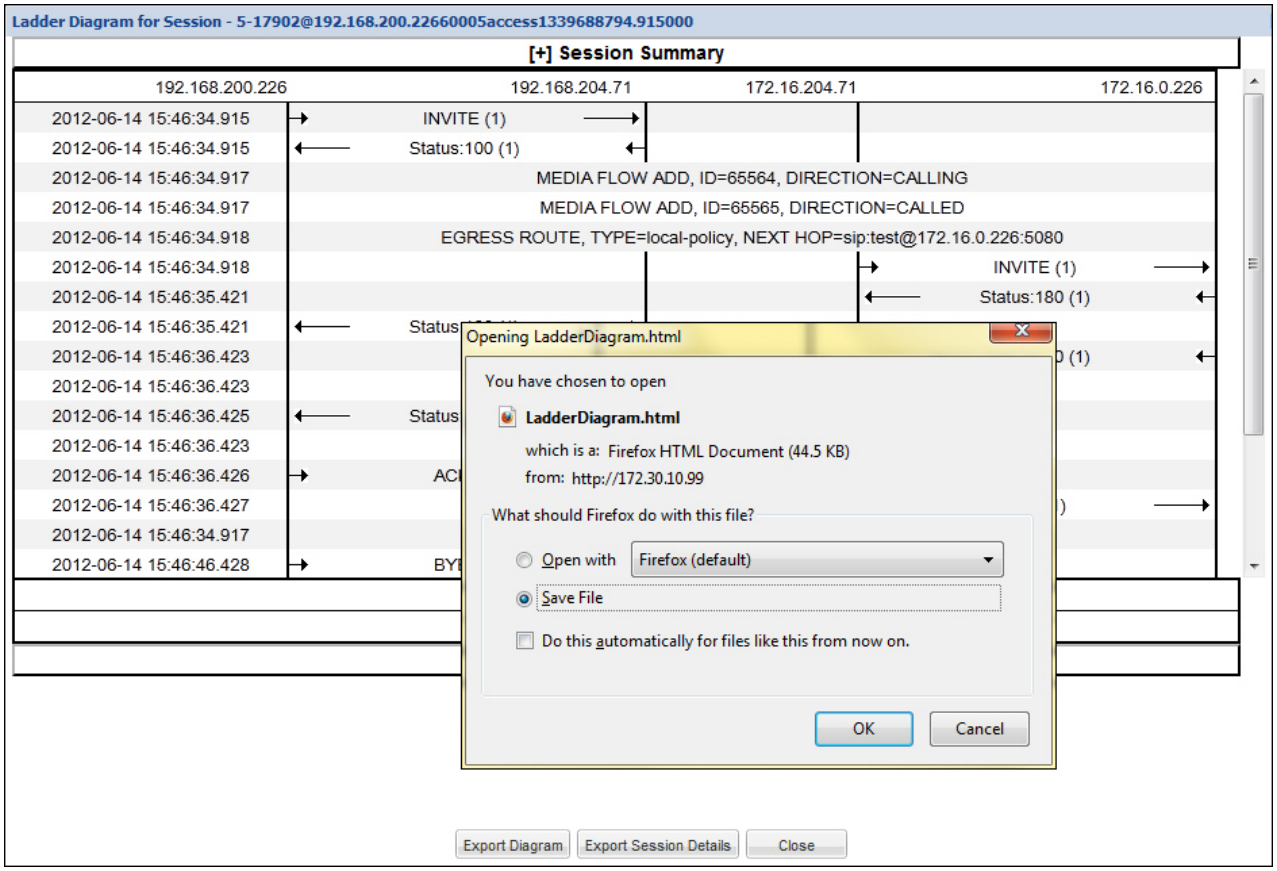
From the Sessions, Registrations, Subscriptions, and Notable Events Reports:

- Export session details - Exports the SIP messages and media events associated with the selected session, to a text file.
- Export summary - Exports all logged session summary records, to a text file. (Exports ALL call session summary records or the records that matched a search criteria).

From the Ladder Diagram:

- Export diagram - Exports all of the information in the Ladder Diagram to an HTML file (Session Summary, SIP Message Details, and QoS statistics).
- Export session details - Exports detailed information about the SIP messages and media events in the Ladder Diagram associated with the selected session, to a text file.

The following is an example that shows the export of a Ladder Diagram to a file called LadderDiagram.html.



The following paragraphs show examples of a:

- *Session Summary Exported File* (text format)
- *Session Details Exported File*(text format)
- *Ladder Diagram Exported File* (HTML format)

Session Summary Exported File

The following is an example of a Session Summary exported text file from the Web-based GUI.

Example

```
----------Session Summary----------

Startup Time: 2011-09-20 12:58:44.375

State: TERMINATED-200
Duration: 5
From URI: sipp &lt;sip:sipp@172.16.34.16:5060&gt;;tag=1
To URI: sut &lt;sip:service@172.16.34.225:5060&gt;;tag=13451
Ingress Src Address: 172.16.34.16
Igress Src Port: 5060
Igress Dest Address: 172.16.34.225
Igress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
```

```
Igress NetworkIf: access
Egress NetworkIf: backbone

----------Session Summary----------
Startup Time: 2011-09-20 12:58:05.340
State: TERMINATED-200
Duration: 5
From URI: sipp &lt;sip:sipp@172.16.34.16:5060&gt;;tag=1
To URI: sut &lt;sip:service@172.16.34.225:5060&gt;;tag=13450
Ingress Src Address: 172.16.34.16
Igress Src Port: 5060
Igress Dest Address: 172.16.34.225
Igress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone
```

Session Details Exported File

The following is an example of the a Session Details exported text file from the Web-based GUI.

Example

```
Session Details:

----------------------------------------
Nov 3 08:50:56.852 On [2:0]172.16.34.225:5060 received from 172.16.34.16:5060

INVITE sip:service@172.16.34.225:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: sip:sipp@172.16.34.16:5060
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 135

v=0
o=user1 53655765 2353687637 IN IP4 172.16.34.16
s=-
c=IN IP4 172.16.34.16
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000

----------------------------------------
Nov 3 08:50:56.855 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
```

```
CSeq: 1 INVITE

----MBCD Evt
Nov 3 08:50:56.862 On 127.0.0.1:2945 sent to 127.0.0.1:2944
mbcdEvent=FLOW ADD
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.225
InputDestPort=10004
OutputSourcev4Addr=192.168.34.225
OutputDestv4Addr=
OutputDestPort=0
InputRealm=access
OutputRealm=backbone
----MBCD Evt
Nov 3 08:50:56.862 On 127.0.0.1:2945 received from 127.0.0.1:2944

mbcdEvent=FLOW ADD
FlowCollapsed=enabled
FlowDirection=CALLED
FlowID=65542
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=192.168.34.225
InputDestPort=20004
OutputSourcev4Addr=172.16.34.225
OutputDestv4Addr=172.16.34.16
OutputDestPort=6000
InputRealm=backbone
OutputRealm=access

----------------------------------------
Nov 3 08:50:56.865 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

INVITE sip:service@192.168.34.17:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>
Max-Forwards: 69
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 140

v=0
o=user1 53655765 2353687637 IN IP4 192.168.34.225
s=-
c=IN IP4 192.168.34.225
t=0 0
```

```
m=audio 20004 RTP/AVP 0
a=rtpmap:0 PCMU/8000

----------------------------------------
Nov 3 08:50:56.868 On [1:0]192.168.34.225:5060 received from
192.168.34.17:5060

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Length: 0

----------------------------------------
Nov 3 08:50:56.872 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:service@172.16.34.225:5060;transport=udp>
Content-Length: 0

----------------------------------------
Nov 3 08:50:56.872 On [1:0]192.168.34.225:5060 received from
192.168.34.17:5060
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Type: application/sdp
Content-Length: 137
v=0
o=user1 53655765 2353687637 IN IP4 192.168.34.17
s=-
c=IN IP4 192.168.34.17
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000

----MBCD Evt
Nov 3 08:50:56.878 On 127.0.0.1:2945 sent to 127.0.0.1:2944

mbcdEvent=FLOW MODIFY
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.225
InputDestPort=10004
```

```
OutputSourcev4Addr=192.168.34.225
OutputDestv4Addr=192.168.34.17
OutputDestPort=6000
InputRealm=access
OutputRealm=backbone

----------------------------------------
Nov 3 08:50:56.881 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:service@172.16.34.225:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 138
v=0
o=user1 53655765 2353687637 IN IP4 172.16.34.225
s=-
c=IN IP4 172.16.34.225
t=0 0
m=audio 10004 RTP/AVP 0
a=rtpmap:0 PCMU/8000

----------------------------------------
Nov 3 08:50:56.883 On [2:0]172.16.34.225:5060 received from 172.16.34.16:5060

ACK sip:service@172.16.34.225:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-5
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 ACK
Contact: sip:sipp@172.16.34.16:5060
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0

----------------------------------------
Nov 3 08:50:56.887 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

ACK sip:192.168.34.17:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK48k3k1301ot00ssvf1v0.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 ACK
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>
Max-Forwards: 69
Subject: Performance Test
Content-Length: 0

----------------------------------------
Nov 3 08:51:01.883 On [2:0]172.16.34.225:5060 received from 172.16.34.16:5060
BYE sip:service@172.16.34.225:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-7
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: sip:sipp@172.16.34.16:5060
Max-Forwards: 70
```

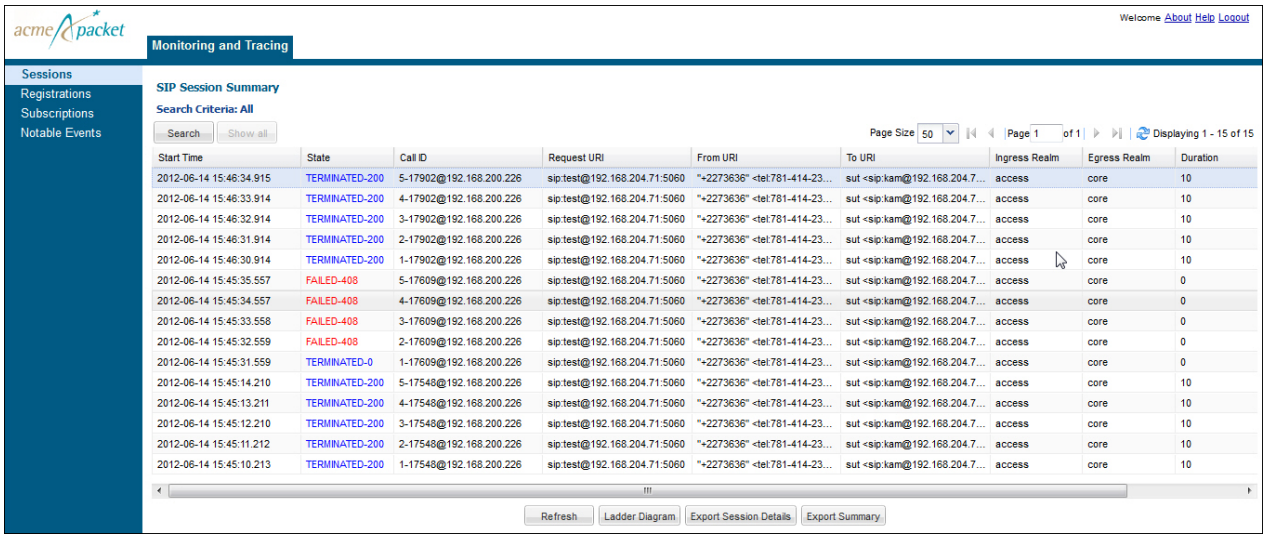
```
Subject: Performance Test
Content-Length: 0

----------------------------------------
Nov 3 08:51:01.887 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

BYE sip:192.168.34.17:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK5oq46d301gv0dus227f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>
Max-Forwards: 69
Subject: Performance Test
Content-Length: 0

----------------------------------------
Nov 3 08:51:01.889 On [1:0]192.168.34.225:5060 received from
192.168.34.17:5060

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK5oq46d301gv0dus227f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Length: 0

----------------------------------------
Nov 3 08:51:01.892 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-7
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: <sip:service@172.16.34.225:5060;transport=udp>
Content-Length: 0

----MBCD Evt
Nov 3 08:51:01.891 On 127.0.0.1:2945 sent to 127.0.0.1:2944

mbcdEvent=FLOW DELETE
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.225
InputDestPort=10004
OutputSourcev4Addr=192.168.34.225
OutputDestv4Addr=192.168.34.17
OutputDestPort=6000
InputRealm=access
OutputRealm=backbone

----MBCD Evt
```

```
mbcdEvent=FLOW DELETE
FlowCollapsed=enabled
FlowDirection=CALLED
FlowID=65542
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=65541
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=192.168.34.225
InputDestPort=20004
OutputSourcev4Addr=172.16.34.225
OutputDestv4Addr=172.16.34.16
OutputDestPort=6000
InputRealm=backbone
OutputRealm=access

----------Session Summary----------
Startup Time: 2012-01-25 10:28:30.394

State: TERMINATED-200
Duration: 5
From URI: sipp &lt;sip:sipp@172.16.34.16:5060&gt;;tag=1
To URI: sut &lt;sip:service@172.16.34.225:5060&gt;;tag=2578
Ingress Src Address: 172.16.34.16
Igress Src Port: 5060
Igress Dest Address: 172.16.34.225
Igress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone
```

Ladder Diagram Exported File

The following is an example of a Ladder Diagram for a session, exported to an HTML file from the Web-based GUI.

Example



Start Time	State	Call ID	Request URI	From URI	To URI	Ingress Realm	Egress Realm	Duration
2012-06-14 15:46:34.915	TERMINATED-200	5-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:33.914	TERMINATED-200	4-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:32.914	TERMINATED-200	3-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:31.914	TERMINATED-200	2-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:30.914	TERMINATED-200	1-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:35.557	FAILED-408	5-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:34.557	FAILED-408	4-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:33.558	FAILED-408	3-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:32.559	FAILED-408	2-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:31.559	TERMINATED-0	1-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:14.210	TERMINATED-200	5-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:13.211	TERMINATED-200	4-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:12.210	TERMINATED-200	3-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:11.212	TERMINATED-200	2-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:10.213	TERMINATED-200	1-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10

[-] Session Summary

State	TERMINATED-200	Duration	10
From URI	"+2273636" <tel:781-414-2345>;tag=60005	To URI	sut <sip:kam@192.168.204.71:5060>;tag=50004
Ingress Src IP:Port	192.168.200.226:5070	Egress Src IP:Port	172.16.204.71:5060
Ingress Dest IP:Port	192.168.204.71:5060	Egress Dest IP:Port	172.16.0.226:5070
Ingress Realm	access	Egress Realm	core
Ingress Network Intf	M00	Egress Network Intf	M10
Ingress Transport	UDP	Egress Transport	UDP

192.168.200.226		192.168.204.71	172.16.204.71	172.16.0.226
2012-06-14 15:46:34.915	→	INVITE (1) →		
2012-06-14 15:46:34.915	←	Status:100 (1) ←		
2012-06-14 15:46:34.917		MEDIA FLOW ADD, ID=65564, DIRECTION=CALLING		
2012-06-14 15:46:34.917		MEDIA FLOW ADD, ID=65565, DIRECTION=CALLED		
2012-06-14 15:46:34.918		EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:test@172.16.0.226:5080		
2012-06-14 15:46:34.918			→ INVITE (1)	→
2012-06-14 15:46:35.421			← Status:180 (1)	←
2012-06-14 15:46:35.421	←	Status:180 (1) ←		
2012-06-14 15:46:36.423			← Status:200 (1)	←
2012-06-14 15:46:36.423		MEDIA FLOW MODIFY, ID=65564, DIRECTION=CALLING		
2012-06-14 15:46:36.425	←	Status:200 (1) ←		
2012-06-14 15:46:36.423		MEDIA FLOW LATCH, ID=65564, DIRECTION=CALLING		
2012-06-14 15:46:36.426	→	ACK (1) →		
2012-06-14 15:46:36.427			→ ACK (1)	→
2012-06-14 15:46:34.917		MEDIA FLOW LATCH, ID=65565, DIRECTION=CALLED		
2012-06-14 15:46:46.428	→	BYE (2) →		
2012-06-14 15:46:46.428			→ BYE (2)	→
2012-06-14 15:46:46.430			← Status:200 (2)	←
2012-06-14 15:46:46.431	←	Status:200 (2) ←		
2012-06-14 15:46:46.430		MEDIA FLOW DELETE, ID=65564, DIRECTION=CALLING		
2012-06-14 15:46:46.430		MEDIA FLOW DELETE, ID=65565, DIRECTION=CALLED		

SIP Message Details

[-] QoS Stats

		Total Pkts	Total Octets	RTCP					RTP			QoE	
Flow ID	Direction	Received	Received	Pkt Lost	Avg Jitter	Max Jitter	Avg Latency	Max Latency	Pkt Lost	Avg Jitter	Max Jitter	R-Factor	MOS
65564	CALLING	0	0	0	0	0	0	0	0	0	0	0	0
65565	CALLED	0	0	0	0	0	0	0	0	0	0	0	0

Glossary