Oracle® Communications Session Delivery Manager

Core Functionality
Release 7.4
Formerly Net-Net Central

May 2014

ORACLE

Notices

Contents

About this Guide – NNC73 – Core Functionality

The Oracle Communications Session Delivery Manager Core Functionality Guide contains an overview of the Session Element Manager graphical user interface (GUI), and describes device management.

Related Session Delivery Manager Documentation

The following table lists related documents for the Session Delivery Manager

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

Revision History

Date	Description
May 2014	• Initial release

1

Getting Started

Overview

Session Delivery Manager provides a centralized framework for working with Net-Net SBCs (devices). It lets you add the devices deployed in your network, configure those devices, view device information, perform administrative functions, and supports additional licensed applications.

Session Delivery Manager delivers:

- Scalability: User sessions are load balanced across a cluster of servers
- On-demand configuration data: Load configurations on-demand to provision locally and then push your changes back to the device
- High availability: With the clustering of NNC servers any single point of failure is minimized
- Rich thin client: Client interface is delivered through your browser

Net-Net Central Applications

Session Delivery Manager provides a flexible, centralized framework for you to license applications based on the needs or your organization.

For example, with Session Delivery Manager's core framework and an Element Manager license, you can:

- Add and manage devices and device groups
- View device status, memory usage, CPU usage, including key performance indicators and alarm counts from the dashboard summary view
- Load a configuration copy of the device, on-demand, to Session Delivery Manager for editing
- View your own modifications made to a device via a local configuration view, which details your configuration changes
- Customize your configuration by choosing from three distinct configuration view styles. Top-level elements are grouped by:
  - Default: Displayed logically, according to the type of configuration required
  - ACLI: Displayed as they would appear in the ACLI: by media-manager, session-router, system, or security
  - List: Displayed in an alphabetically-ordered list
- Conduct view-to-view navigation: Switch from one configuration view to another configuration view, with the content area automatically refreshing to the last attribute displayed from the previous view

Net-Net Central's Base System

Session Delivery Manager's base system includes Device Manager, Security Manager, and Health Monitor. With Device Manager you add and manage devices and device groups. With Security Manager, you control user-access and group-access to devices by setting and granting permissions. With Health Monitor, you can monitor heartbeat and disk usage.

Element Manager

With the appropriate license, Element Manager is an application that enhances the core system by providing provisioning capabilities, along with fault management and performance statistics for your managed devices. Configuration Manager lets you load and provision devices. You view events, alarms, and trap summary data with Fault Manager. And, Performance Manager lets you view performance statistics collected from the Net-Net SBC, such as system, SNMP, IP, environmental, and so on. Another key feature of Element Manager is Dashboard Manager, which provides a dashboard summary view with at-a-glance device status and key performance indicators for your managed devices.

Route Manager

With the appropriate license, Route Manager lets you import routing data from an external source and update local route table (LRT) data on a single device or on multiple devices.

About Managed Devices

Session Delivery Manager's Element Manager application allows for the loading, configuring, and managing of devices, (Net-Net SBC). This release of Session Delivery Manager can manage the following devices:

- C-Series—Also known as the Net-Net 4000 series and Net-Net 3000 series. The Net-Net 4000 series contains two systems: the Net-Net 4250 and Net-Net 4500. The Net-Net 3000 series contains two systems: the Net-Net 3800 (Sku 3810) and Net-Net 3820.
- D-Series—Also known as the Net-Net 9000 series, it contains one system: the Net-Net 9200.
- E-Series—Also known as the Net-Net 2000 series, it contains one system: the Net-Net 2600.

Minimum Net-Net SBC Configuration

The Net-Net SBC configurations you plan to manage using Session Delivery Manager must have the following information configured in order to be properly loaded into Configuration Manager. To verify the minimum configuration for Net-Net SBCs you plan to manage, see the following documentation:

- Session Delivery Manager Configuration Guide for details about configuring a Net-Net SBC using the Acme Command Line Interface (ACLI)
- Net-Net ACLI Reference Guide to refer to all ACLI commands

Boot Parameters

Boot parameters specify the information your Net-Net SBC system uses at boot time when it prepares to run applications. The Net-Net SBC system's boot parameters include the Net-Net SBC system's IP address for the management interface (wancom0) and the target name.

Session Delivery Manager uses the target name to uniquely identify a Net-Net SBC from among the list of Net-Net SBCs in the content area. You need to ensure that all Net-Net SBCs you plan to manage, thus load, with Session Delivery Manager have unique target names. Otherwise, a list of Net-Net SBCs, all with the default name acmesystem would appear in the list.

Ensure the following boot parameters have been configured:

- wancom0 IP address and mask
- target name is set to a unique name (do not use the default name acmesystem)

System Configuration Element

You need to ensure the system-config element has been configured. This element establishes general system information and settings, for example:

- Contact information for this Net-Net SBC system for SNMP purposes
- Identification of the Net-Net SBC system for SNMP purposes
- Physical location of the Net-Net SBC system for SNMP purposes
- Whether SNMP is enabled on the system
- Whether traps are enabled
- default gateway

For complete details about system configuration, see the Net-Net 4000 Configuration Guide and the Net-Net ACLI Reference Guide.

SNMP Community Element

You need to ensure the snmp-community element is configured. This element defines the Session Delivery Manager server from which the Net-Net SBC system will accept SNMP requests. Specifically, you need to ensure:

- IP address list contains the address of the host upon which Session Delivery Manager server is running. IP address(es) for SNMP communities for authentication purposes.
- Access mode is read-only

Note: If configuring the snmp-community element for a cluster, you must add both server IP addresses in the cluster.

Note: Adding a device in Session Delivery Manager will fail if SNMP is not configured properly.

Trap Receiver Element

You need to ensure the trap-receiver element is configured. This element defines the Session Delivery Manager server to which the Net-Net SBC system sends SNMP traps for event reporting. Specifically, you need to ensure:

- IP address is that of the Session Delivery Manager server
- Filter level is set to All
- Community name matches the name in the SNMP community element

Accessing Session Delivery Manager

You can access the Session Delivery Manager server by using two address formats (as shown in step 2.)

To access Session Delivery Manager:

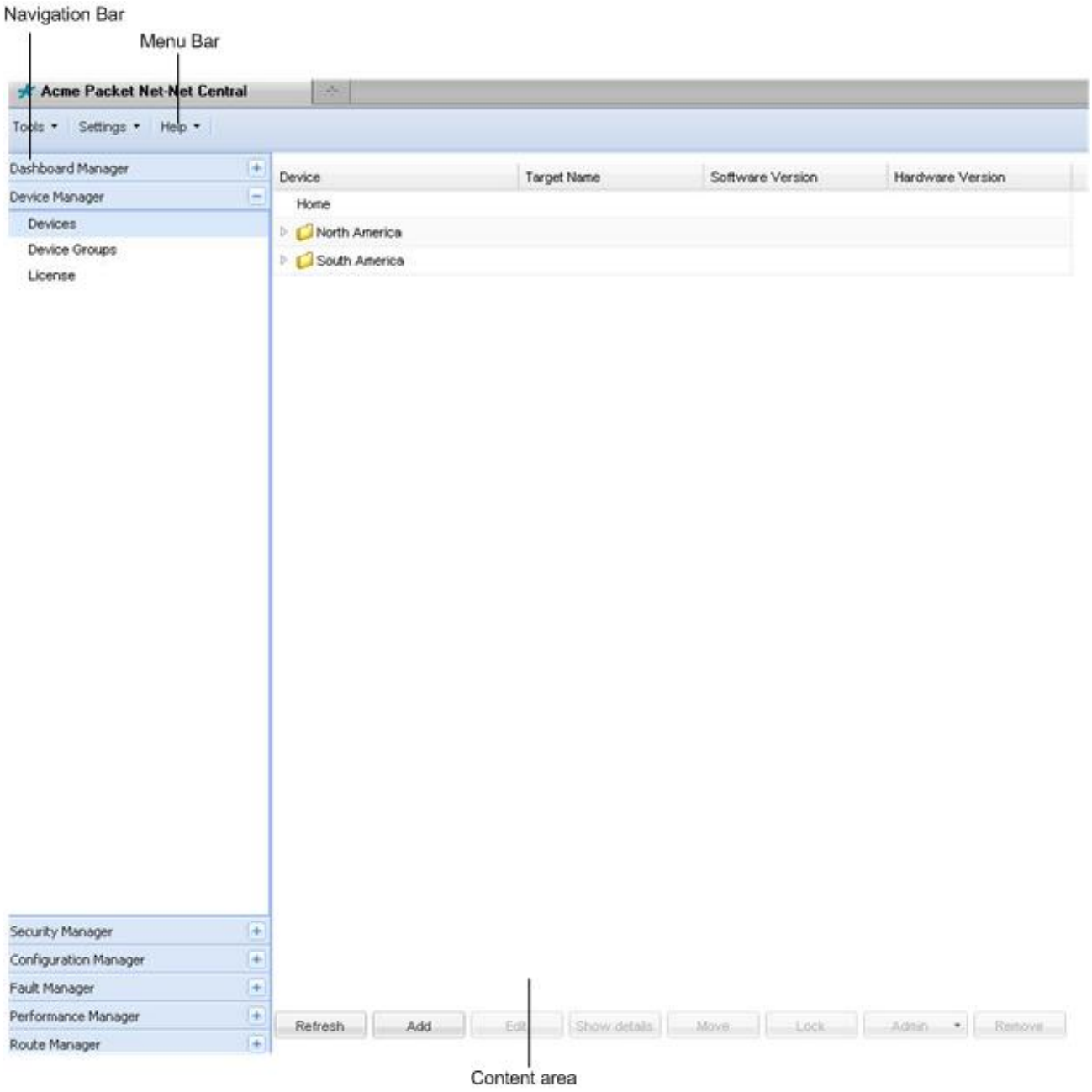
1. Open a Web browser.
2. Connect to the Session Delivery Manager server using one of the following address formats:

```
http://<Session Delivery Manager server IP address>:8080
https://<Session Delivery Manager server IP address>:8443
```

   The Login screen appears.

3. Enter your user name and password and click Login. (The default username is admin, with a default password of admin.)

   You have now accessed Session Delivery Manager.



Note: When you login to Session Delivery Manager, your display will differ based on your licensed applications.

Changing Your Password

When your Session Delivery Manager login password falls within a pre-determined expiration window, a notification dialog box will pop up with a message indicating your password will expire in x number of days. The dialog box provides a mechanism to change your password. Clicking Yes will launch the Change password dialog box.

To change your password during an expiration window:

An Info dialog box appears alerting you that your password will expire in x number of days.

1. Click Yes to the question, Do you want to change your password? The Change password dialog box appears.
2. Current login user password:—Enter your current Session Delivery Manager login password.
3. New password:—Enter your new Net-Net Central login password.

4. Confirm new password:—Re-enter your new Session Delivery Manager login password to confirm.

5. Click OK. Your new password is in effect.

   For more information about password rules, see the Session Delivery Manager Administration Guide.

User Interaction

There are several ways to enter user input and configure parameters. For more information about user-interaction scenarios, see the Session Delivery Manager Element Manager Guide, Using Element Manager.

2

GUI Overview

Introduction

This chapter explains how to use the Session Delivery Manager Graphical User Interface (GUI). It explains how to login to Session Delivery Manager and contains descriptions of the GUI itself.

The top-level screen is divided into the following areas:

- Menu bar across the top of the window, which houses the drop down lists for administration, help, and monitoring tools
- Navigation bar in the left pane of the window, which contains sliders: Device Manager, Security Manager, and with appropriate licenses, Dashboard Manager, Configuration Manager, Fault Manager, Performance Manager, and Route Manager
- Content area on the right side of the window, where information pertaining to each slider in the navigation bar is displayed
- Status bar across the top of the content area

Menu Bar

The menu bar across the top of the screen contains sets of functions you can perform organized into different categories (menus). You click a menu to access a list of options, from which you then select the function you want to perform.

The following table lists the menus and their options; including a brief description.

Menu	Menu Option	Description
Tools	Change password	Change the password used to login to Session Delivery Manager
	Health Monitor	View heartbeat summary data and disk usage summary data
Settings	Fault configuration	Configure purging period for fault events and alarms
	Trap receivers	Configure trap receivers and/or edit trap receivers

Menu	Menu Option	Description
	Fault email notifications	Add and/or edit recipient information for fault email notifications
	Edit the login banner	Edit the information that appears in the banner at login
	Alarm colors	Configure the alarm colors for each alarm severity level
Help	Help topics	Access Help topic
	License Information	Access the Session Delivery Manager license information
	About	Access Session Delivery Manager version information

Navigation Bar

The left pane is called the Navigation bar. The Navigation bar is divided into categories, represented by sliders. Each slider contains information specific to its slider category.

Note: The navigation sliders shown in your Session Delivery Manager framework will vary based on your licensed applications, for example, Element Manager or Route Manager. For more information, contact your Oracle sales representative.

Session Delivery Manager Base System

The navigation sliders included with your Session Delivery Manager framework are:

- Device Manger
- Security Manager

Element Manager

Element Manager is a licensed application and includes:

- Dashboard Manager
- Configuration Manager
- Fault Manager
- Performance Manager

Route Manager

Route Manager is a licensed application and includes:

- Route Manager

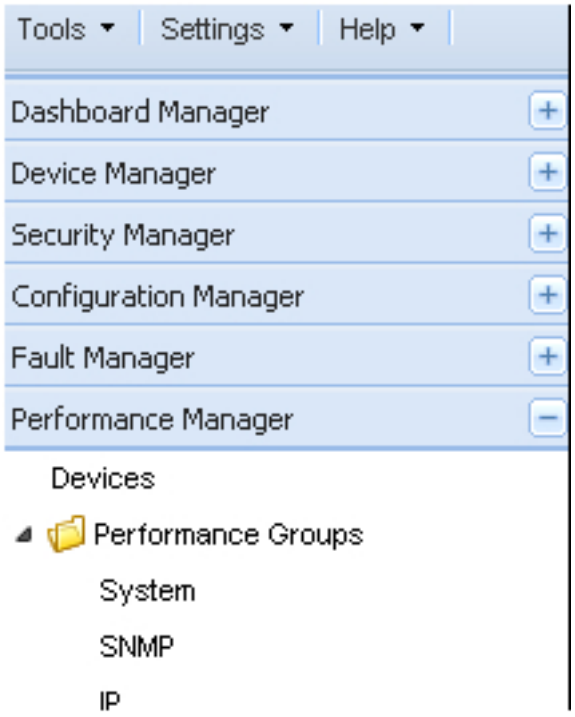
Session Delivery Manager Navigation Sliders

The left pane is called the Navigation bar. The Navigation bar is divided into categories, represented by sliders. Each slider contains information specific to its slider category.

The following sections describe each of the navigation sliders.; those included with the base Session Delivery Manager system and those accompanying licensed Session Delivery Manager applications.

Session Delivery Manager Base Framework

Below is an example of the navigation bar with the Session Delivery Manager base framework:



The following sections describe the sliders included with the Net-Net Central framework.

Device Manager

Device Manager lets you add and manage the device groups and devices you work with in Session Delivery Manager. Device Manager displays the device groups and devices you work with. License, the third item under Device Manager, displays the license data for all licensed Session Delivery Manager applications, as well as how many managed devices are in use with each license(s)

Note: You may add an unlimited number of devices into Device Manager. However, the licensed applications (Element Manager and Route Manager) may only manage a subset of those devices based on the number of nodes allowed in your license.

Security Manager

Security Manager contains the user management and audit log functionalities. User management lets you create groups of users, users, set password rules, configure the inactivity timer, and configure the password interval. The audit log functionality lets you view the audit log, save it to a file, and set an automatic purge interval or manually purge the log. Refer to the Session Delivery Manager Administration Guide for more information about Session Delivery Manager privileges.

Element Manager

With the appropriate license, Element Manager lets you configure and manage your devices and view fault and performance data. Below are the navigation sliders for Element Manger.

The following sections describe the sliders included with Element Manager.

Dashboard Manager

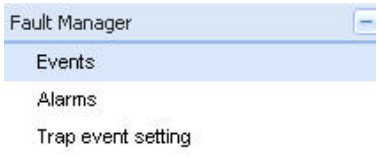
Dashboard Manager contains the summary view where you view a dashboard summary of critical alarm counts, health scores, CPU usage statistics, and other data for your devices.

Configuration Manager

Configuration Manager lets you load and configure your devices. Once you finish making your configuration changes, you apply them and perform an update to save the changes to the Net-Net SBC.

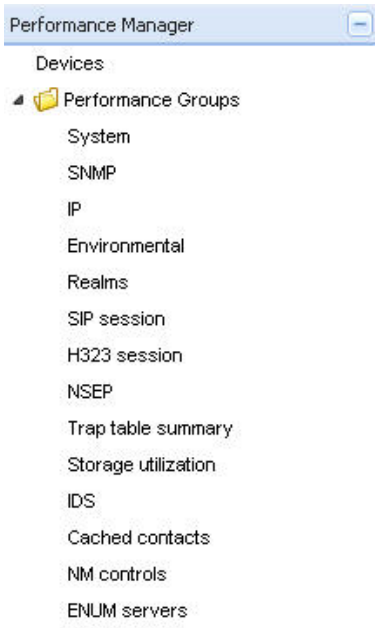
Fault Manager

Fault Manager contains information pertaining to events (caused by actions that generate alarms, entries in a log file, or SNMP traps), alarms, and trap event settings for your devices. You can monitor events, alarms, or trap data and save the data to a file. You also clear alarms within Fault Manager.



Performance Manager

Performance Manager displays real-time, on-demand performance statistics for monitoring performance and utilization. You can view this data or save it to a file.

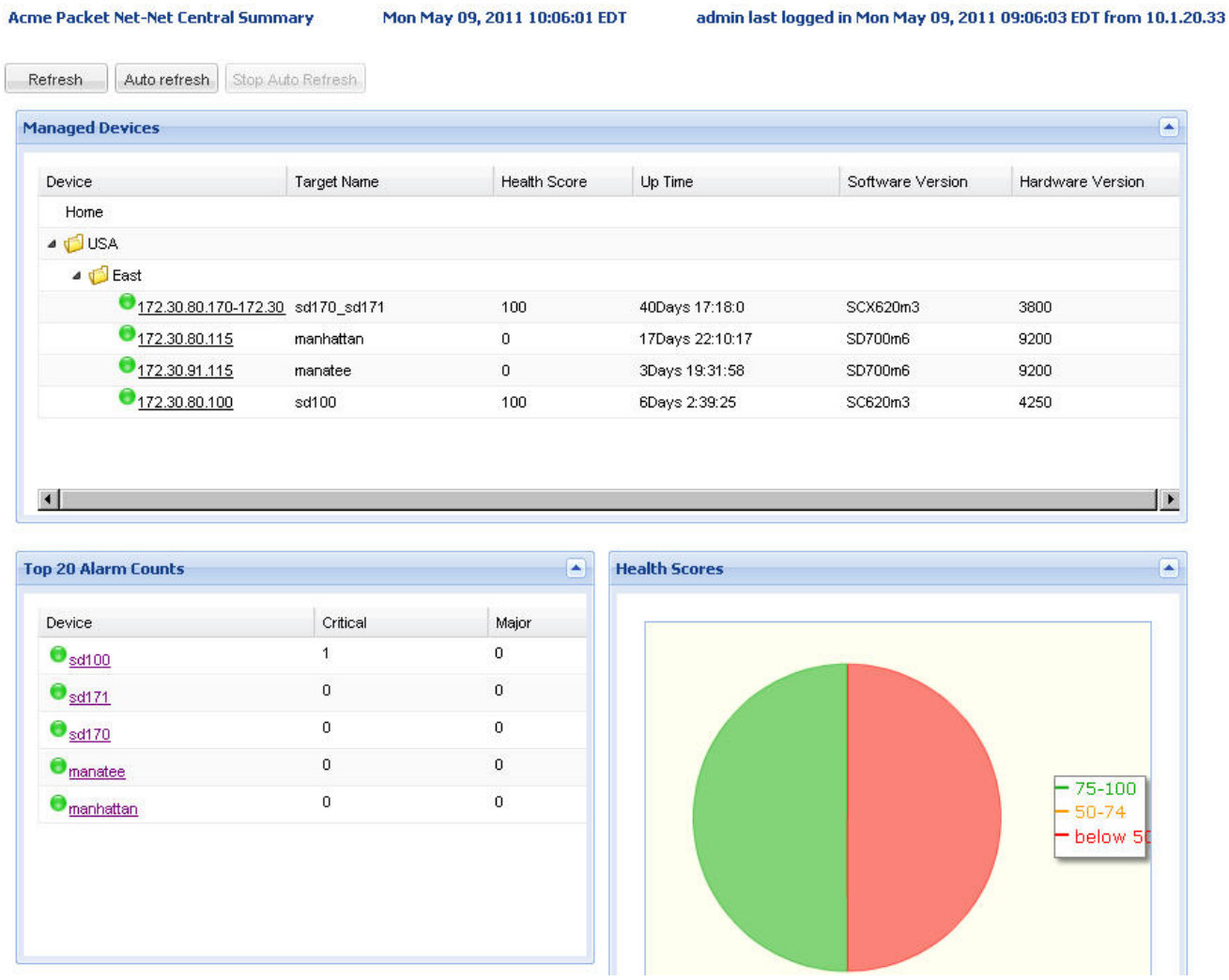


Route Manager

With the appropriate license, Route Manager lets you update local route table (LRT) data on a single device or on multiple devices. You can provision large LRTs across multiple Net-Net SBCs and Net-Net Session Routes for numeric-based routing. For more information about Route Manager, see the Net-Net Route Manager Guide.

Content Area

The content area is your work area. You can also view fault and real-time performance data in the content area. The information that appears depends on which navigation slider you select. The following example shows Dashboard Manager, summary view that appears with Element Manager (this image is a portion of this screen).



Note: When you login to Session Delivery Manager, your display will differ based on your licensed applications.

Status Bar

The Status Bar is located at the top of the content area in Dashboard Manager, Summary view. It displays a window title, date and time for this current Session Delivery Manager session, and the date and time you logged into this Session Delivery Manager session, including your client's IP address location.

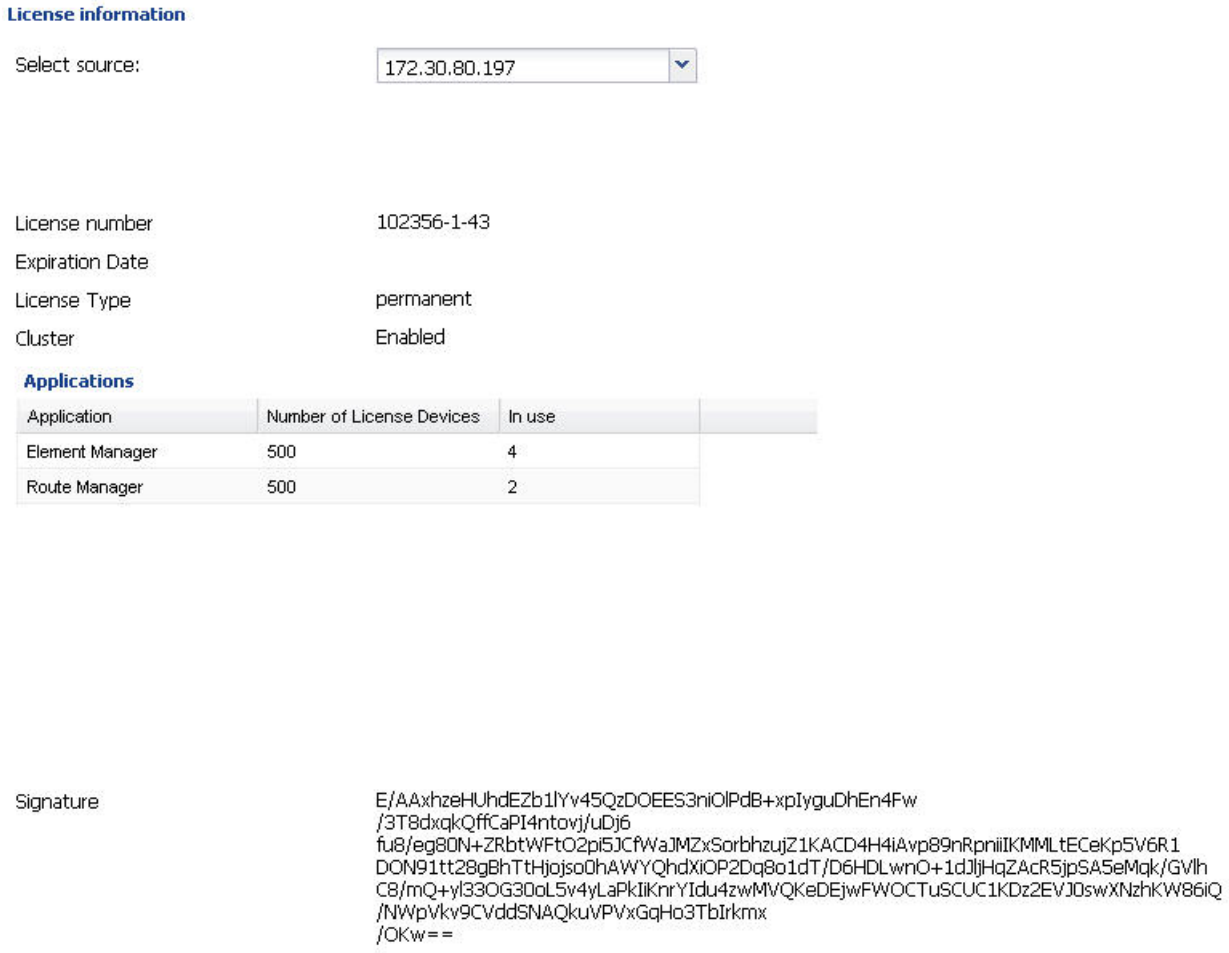
The example below shows the type of status information displayed from Summary View of Dashboard Manager.

Viewing Session Delivery Manager License Information

Session Delivery Manager License information displays the license data for each Session Delivery Manager server. The information includes:

- Licensed applications installed
- Number of licensed devices for each application
- Number of licensed devices in use for each application

For example, on the following Licence information screen there are two licensed applications, Element Manager and Route Manager. Each application has 500 devices licensed, with Element Manager having 4 devices in use and Route Manager having 2 devices in use.



The value in the Number Of License Devices column changes only when you update the Session Delivery Manager license. The value in the In use column fluctuates on the running Session Delivery Manager server depending on the number of devices in use at a particular time.

The number of devices in-use is important since it cannot exceed the number of licensed devices. For example, if you are licensed for 500 devices and have 498 devices in use, you can consider adding devices to your license. For more information, contact your Oracle sales representative.

There are two ways to access license information for your Session Delivery Manager servers:

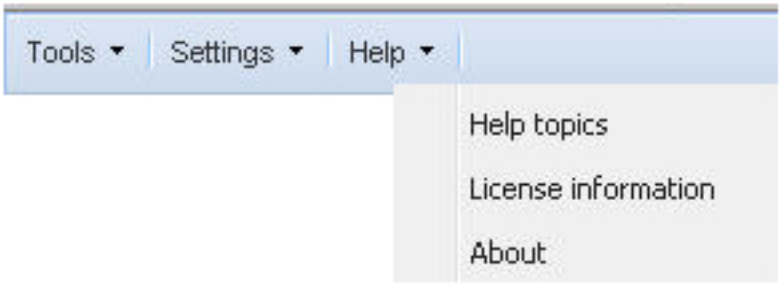
- Select License information from the Help menu in the top tool bar (shown below)
- Select License from the Device Manager navigation slider

Note: No privilege is required to view license information.

Accessing License Information

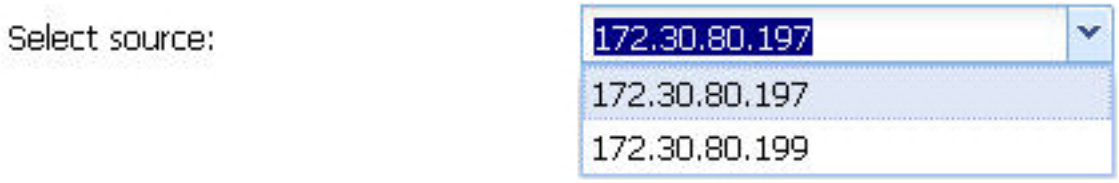
To access license information:

1. Click Help in the top tool bar. A drop-down menu appears.
2. Click License information.



The license information window appears.

3. Select source:—Click the source IP address of the Session Delivery Manager server in the cluster you want to view license information for in the drop-down list.



The license information for this Session Delivery Manager server appears.

The license information data is explained below.

Data	Description
Select source	IP address of the Session Delivery Manager server for which you want to view license information
License number	Unique number for this Session Delivery Manager license
Expiration Date	Expiration date for this Session Delivery Manager license. If left blank, there is no expiration date
License Type	License types for the Session Delivery Manager server are temporary or permanent. If temporary, the Expiration Date field displays the expiration date for this temporary license. If permanent, the Expiration Date field is left blank
Cluster	Specifies whether clustering is enabled or disabled with this Session Delivery Manager license. If enabled, clustering is permitted. If disabled, clustering is not permitted
Application	Name(s) of the licensed applications
Number of Licensed Devices	Number of licensed Net-Net SBCs for each application
In use	Number of Net-Net SBCs in use for each licensed application
Signature	A mathematical scheme, usually encrypted, that provides authenticity to a digital message or document. A valid digital signature gives a recipient validation that a message was created by a known sender, and that it was not altered in transit.

Note: For more information on clustering, see the Net-Net Central High Availability Guide.

3

Managing Devices

Overview

The Device Manager slider is where you manage the devices deployed in your network. First, you add the devices to Session Delivery Manager via Device Manager. Once added to Session Delivery Manager, you can view device information and, if properly licensed, can configure the devices.

After you add a managed device, you assign it to a device group. A device group is a logical grouping of devices managed by Session Delivery Manager. Device groups can be set up in a hierarchy that can contain an arbitrary number of levels. Devices can be maintained at any level in the device-group hierarchy. With the appropriate permissions, you can add, rename, or delete device groups.

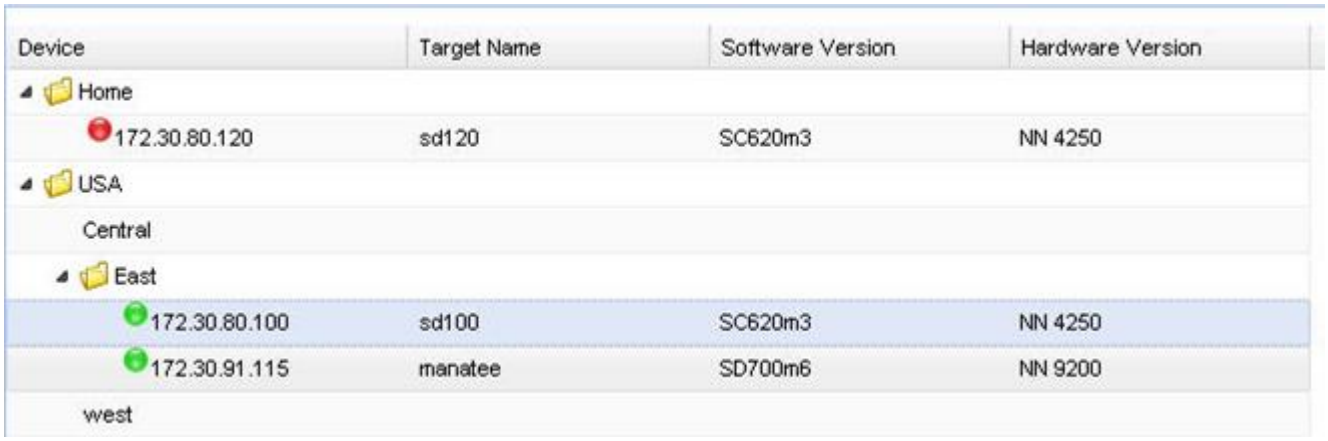
Device Manager is divided into three sections:

- Devices: Allows you to add, manage, and remove managed devices (Net-Net SBCs)
- Device Groups: Allows you to add, manage, and remove device groups
- License: Displays the license data for all licensed Session Delivery Manager applications, as well as how many managed devices are in use with each license(s)

About the Device Manager Display

Below is an example of a device group hierarchy, with one device in the device group, Home, and two devices in device group, East. The East device group is contained within the device group, USA. East is a child group of the parent group, USA.

A folder icon will appear next to the device group if it contains devices.



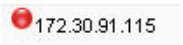
About Device Icons

A round, colored icon will appear to the left of your device in the Managed Devices table. This indicates whether or not the device is reachable by Session Delivery Manager. If the icon is:

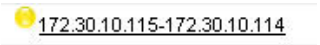
- Green: The device (or both devices in a cluster) is reachable by Session Delivery Manager and information for this device can be retrieved through SNMP.

- Red: Session Delivery Manager cannot currently contact the device (or cannot contact both devices in a cluster).

- Yellow: The standby device in the cluster is not reachable by Session Delivery Manager.

The Device table includes the following information for each device:

Device Information	Description
Device	IP address of the standalone device or each device in a cluster
Target Name	User-defined name for each device
Software Version	Full release version, including patch number, of software on device
Hardware Version	Full hardware platform identification

Performing Device-Related Tasks

At the bottom of the devices content area is a set of action buttons. For example:

The following table describes the actions.

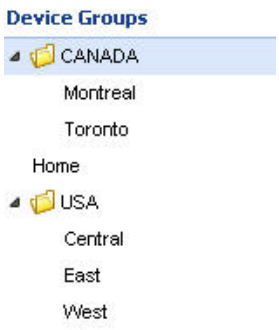
Action	Description
Refresh	Refreshes the data displayed on the screen for this device
Add	Launches the Add device dialog box where you add a device(s)
Edit	Launches the Edit Device dialog box where you can edit your device.
Show details	Displays the following details pertaining to this device: hardware, software, and license information. You can export this data to a file

Action	Description
Move	Launches the Move Device dialog box where you move your device from one device group to another device group
Lock	Launches the Confirm dialog box where you confirm that you want to lock this device. Locking a device will prevent another user from configuring this device. When you lock a device, a padlock icon appears next to the IP address of the device and the lock button toggles to Unlock
Admin	Launches a drop down menu with the following operations: Reboot: Reboots the device Synchronize alarms: Synchronizes alarms for this device Override lock: With the appropriate permissions assigned, allows you to break another user's lock on a device
Remove	Launches the Remove device dialog box where you confirm you want to remove this device from the Devices list. Once removed, you cannot access this device via Session Delivery Manager When removing a device, you cannot: Remove a device in the middle of a configuration update. If you try to remove a device during the update process, you will get an error message Remove a locked device, unless you are the owner of the lock, or an administrator removes the lock using the Override lock option

Working with Device Groups

Device Groups is the second option under Device Manager. You add and manage device groups here. Ideally, you create your device groups prior to adding your devices. Subsequently, when adding a device, you select the device group you want this device to belong to.

The hierarchy of the device groups is listed in the content area, for example:



A folder icon will appear next to a device group if it contains device groups. In the above example, Central, East, and West are child device groups of USA. Montreal and Toronto are child device groups of CANADA. Home, Central, East, West, Montreal, and Toronto are not parent device groups, or they currently do not contain device groups.

Using the Home Device Group

Device Groups includes a default device group called Home. You can add your devices to this default device group if no other device groups are created.

Note: You must have admin privileges assigned to view this device group. If you cannot view the Home default group in the Device Groups list, you do not have the appropriate privileges.

With the Home device group:

- You cannot rename this device group
- You cannot delete this device group
- When adding a device, the Home device group will display in the Add Device Group dialog only if you have not targeted a previous device group from the table
- Will appear in Device Groups, under Device Manager when a user with admin privileges logs in

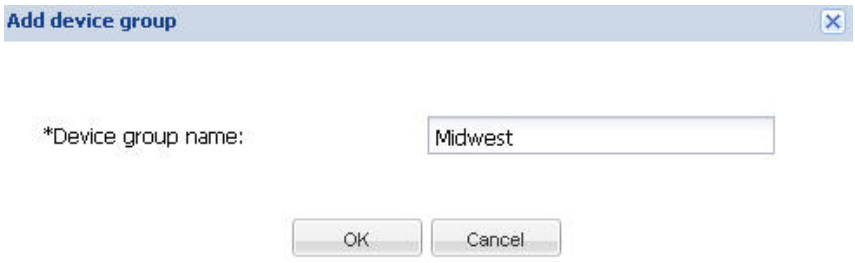
Adding a Device Group

When you add a new device group, the name you choose:

- Must start with an alphabetic character
- Can contain a minimum of three characters and a maximum of 50 characters
- Can contain the following characters: alphabetic, numeric, hyphens (-), and underscores (_)
- Can be a mix of upper-case and lower-case characters
- Cannot contain symbols
- Cannot be the same name as an existing group name within the same level in the hierarchy (sibling)

To add a device group:

1. Expand the Device Manager slider and click Device Groups. The Device Groups appear in the content area.
2. Click Add. The Add device group dialog box appears.
3. *Device group name:—Enter the name for this device group.



4. Click OK. The device group, Midwest, appears in the device groups.

Once you create a device group, you can move devices into the device group by:

- Specifying a device group when adding this device to be managed in Session Delivery Manager
- Moving devices or device groups from one device group to another device group by clicking the Move button

Moving a Device Group

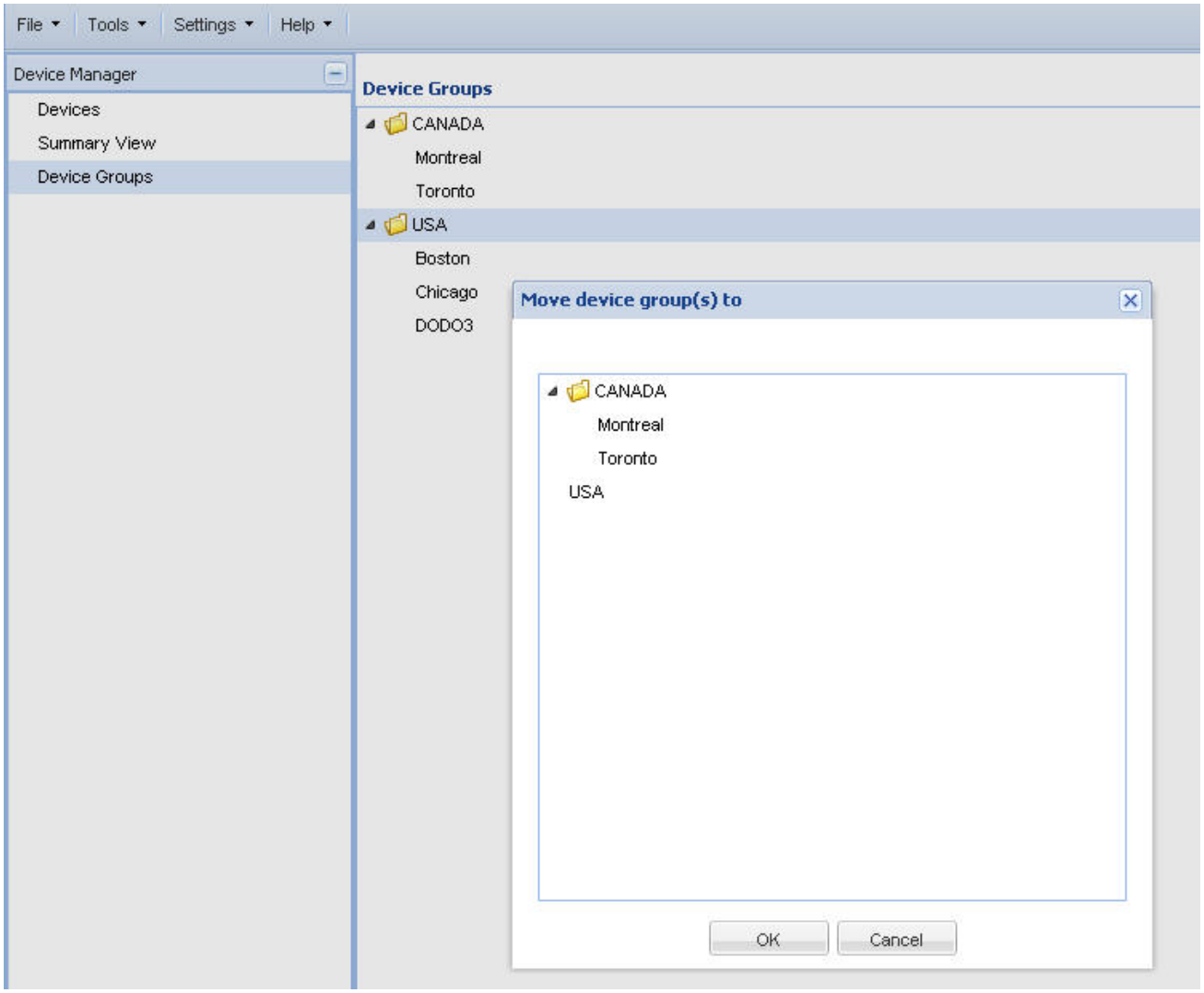
You can move device groups from one group to another. When you move a device group, you also move all devices within that device group.

Note: You cannot move a device group into one of its child groups. In the example below, CANADA could not be moved into Montreal or Toronto, but could be moved into Home or USA.

To move one device group to another device group:

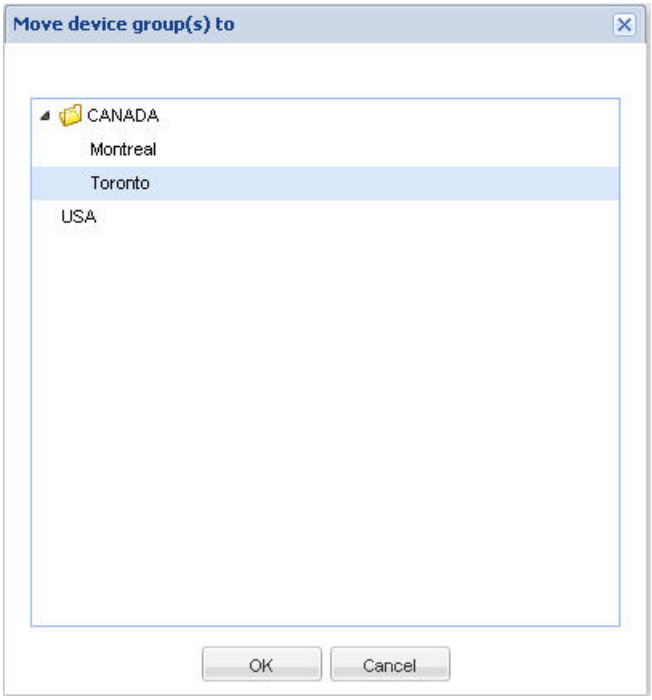
1. Expand the Device Manager slider and click Device Groups. The device groups appear in the content area.
2. Click the device group you want to move to select it and click Move.

   To select multiple device groups at one time, press Ctrl + click to select multiple groups. The Move device group(s) to dialog box appears.



Note: In the example above, device group USA is selected for a move. As a result, The Move device group(s) to list excludes the child device groups under USA, since USA cannot be moved into one of its child groups.

3. Click the device group you want to move your device group to. In the example below, USA is moving to Toronto.
4. Click OK.



The Move device group(s) to dialog box appears.

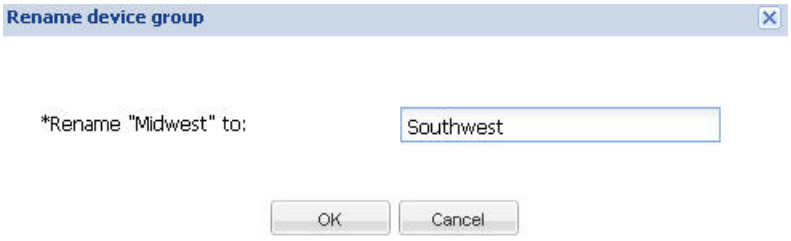
5. Click Ok.

Renaming a Device Group

You can rename a device group as long as the name does not belong to another device group within the same level of the hierarchy. For example, a device group cannot share the same name as one of it's siblings, but can share the same name with a device group on a different level of the device group hierarchy.

To rename a device group:

1. Expand the Device Manager slider and click Device Groups. The Device Groups appear in the content area.
2. Click the device group you want to rename to select it and click Rename. The Rename device group dialog box appears.
3. *Rename to:—Enter the new name for this device group.



4. Click OK. The Rename device group dialog box appears.

5. Click OK. The new name appears in Device Groups.

Deleting a Device Group

With appropriate permissions assigned, you can delete a device group from the Device Groups list.

There are two instances when you cannot delete a device group. You cannot delete a device group if the device group:

- Contains devices. If you attempt to delete a device group with devices, Session Delivery Manager will return the following error message, Failed to delete device group. Cannot remove device group. Device group contains one or more devices. You must first move these devices to another device group.
- Being deleted causes a duplicate path name within the same hierarchy. You can not have device groups with the same name at the same child level. For example, if you have a hierarchy such as: USA-->Mass-->East-->Boston

  And another hierarchy such as: USA-->Mass-->Boston, you cannot delete East or you will cause two duplicate paths, USA-->Mass-->Boston.

  In this example, Session Delivery Manager will return the following error message, Failed to delete device group. Device group Boston already exists.

  To delete a device group:

1. Expand the Device Manager slider and click Device Groups. The Device Groups appear in the content area.
2. Click the device group you want to delete.
3. Click Delete. The Delete device group dialog box appears.

4. Click Yes. The Delete device group dialog box appears.

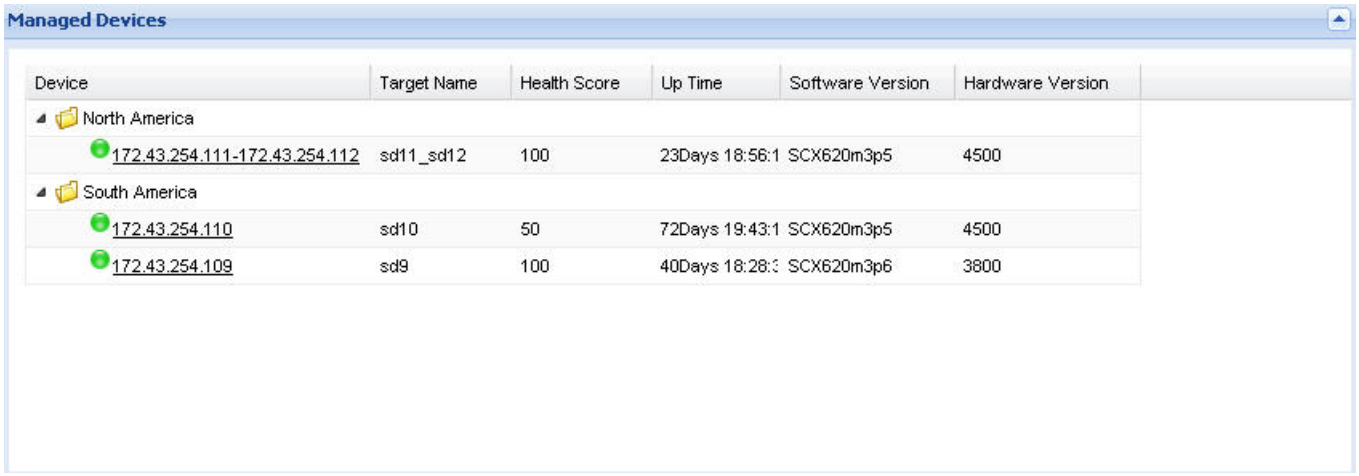
5. Click OK.

Working with Devices

Managed devices are the Net-Net SBCs that you manage using Session Delivery Manager. You create your device group, add your device, and then select the device group this device will belong to.

Identifying Net-Net SBC Versions

You can identify the specific type of Net-Net SBC you are managing by viewing the Managed Devices table under Dashboard Manager, Summary view. The software version and hardware version are listed, as in the example below.



Adding a Single Device

When adding devices in Session Delivery Manager, you have the ability to add a single device, or to add more than one device in a row. To add one device only, complete the required parameters in the Add Device dialog box and click the OK button at the bottom of the window.

To add a single device:

1. Expand the **Device Manager** slider.
2. Click **Devices**.

   The Device table appears in the content area.
3. Click Add. The Add Device dialog box appears.
4. IP address 1:—Enter the IP address for this device.
5. IP address 2:—Enter the IP address for the second device, if this device is part of a cluster.
6. SNMP community name:—Enter the SNMP community name for this device. The SNMP community name is the name of an active community where this SBC can send or receive SNMP information (performance and fault).

   Note: The SNMP community must be configured on the SBC before adding the device to the Session Delivery Manager. This is done on the SBC in the **ip-addresses** parameter found in the **configure terminal** > **system** > **snmp-community** element. For more information, see the "SNMP Community Configuration" section in the System Configuration chapter of the ACLI Configuration Guide.
7. SNMP port:—Enter the SNMP port number for this device, or retain the default value of 161.
8. Device Group—Click Set device group. The Set device group dialog box appears.
9. Click the device group you want this device to belong to.
10. Click OK to add the device group.
11. Click OK to add this single device. Your device appears in the device group and the dialog box closes.

Adding Multiple Devices

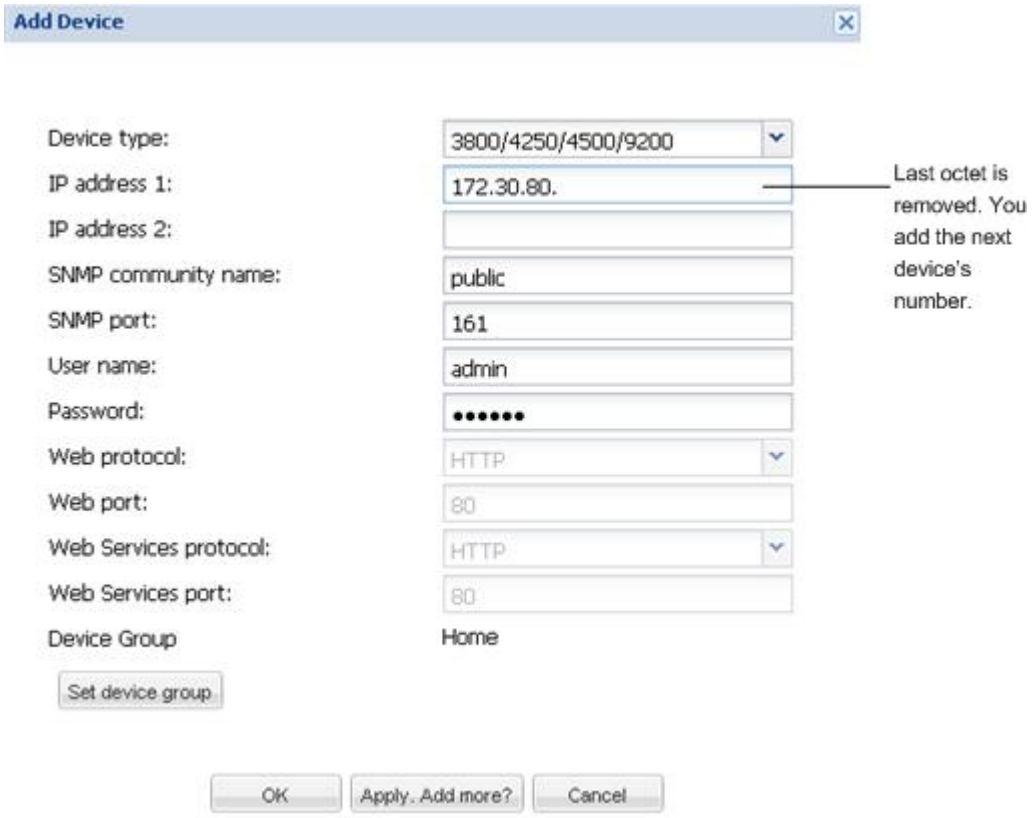
To add multiple devices, once you complete the required parameters in the Add Device dialog box for the first device, you retain most of the original information you entered by clicking the Apply. Add more? button.

When you click Apply. Add more?, the Add Device dialog box remains open with your originally-entered values, but the last octet of the management IP address is deleted so you can rapidly add another device, for example, 172.30.80.112, 172.30.80.125, and so on.

To add multiple devices:

1. Perform steps 1 through 17 in Adding a Single Device above.
2. Click Apply. Add More? to add this device. A Success box appears.
3. Click OK. Your device is added to the device group.

   The Add Device dialog box remains open with the same values, except for the IP address 1 field. The last octet in the IP address 1 field is removed.



4. IP address 1—Enter the last octet of the IP address.

   If required, revise other fields in the Add Device dialog box.
5. Click OK to add this device and no more.
6. Click Apply. Add more? to add this device and keep this Add Device dialog box open to add additional devices.

Adding Administrative Users

When adding a device in the NNC GUI, you are asked to input a User name for the device. It is possible that the user name you supply does not have administrative privilieges, and therefore, certain operations are restricted. In this event, a warning message is sent:

```
Warning: the user XXX is not known by NNC to be an administrator on the
device. Would you like to proceed? (Yes/No):
```

By default, each device has one administrative user to begin: admin. In order to add more user names to this admin list, you must modify the sbcAdmins.conf file. The file is located in the following directory within NNC installation:

```
<NNC folder>/conf/device/sbcAdmins.conf
```

Once you modify this file by adding an Administrative user, you must restart NNC in order for the changes to be applied.

Adding Administrative User List

To add users to the administrative user list:

1. In Superuser mode, navigate to the file <NNC folder>/conf/device/sbcAdmins.conf.
2. Edit the sbcAdmins.conf file using any text editor.
3. Type the name to append to the admins list.
4. Save the file.

   For example:

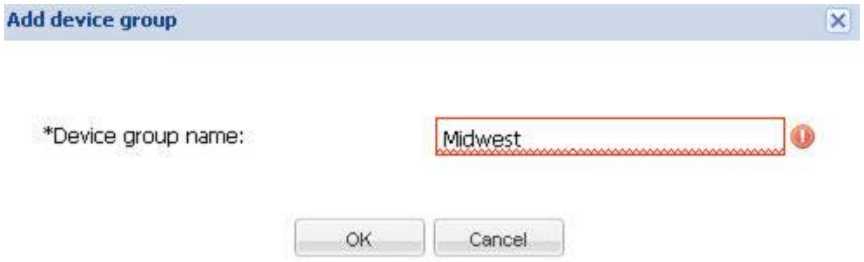
```
# This file contains a listing of all SBC usernames NNC will consider as
admins.
# By default, this file contains just the admin username.
# To add a new username, simply append a new line containing just the
username.
admin
Robert
```

Adding a Device Group

If while adding a device, you notice that the device group you want is not in the list, you can add it from the Set Device Group dialog box.

1. From the Set device group dialog box, click Add. The Add Device group dialog box appears.
2. *Device group name:—Enter the name for this device group.

   For more information about naming criteria, see Adding a Device Group



3. Click OK. A dialog box appears.

4. Click OK.

Moving Devices

You can move devices from one device group to another.

To move a device to another device group:

1. Expand the Device Manager slider and click Devices. The Device table appears in the content area.
2. Click the device group to expand the list of devices within the group.
3. Click the device you want to move from one device group to another to select it.
4. Click Move. The Move Device dialog box appears.

5. Click on the device group you want the device to belong to select it.
6. Click OK. A Success dialog box appears.

7. Click OK.

Locking Devices

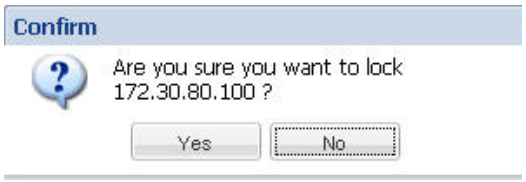
With the appropriate admin permissions, you can lock a device. When locked, other users cannot perform operations on this device. For example:

- Rebooting a device
- Updating a configuration
- Updating the device for route sets
- Pushing configuration changes to the Net-Net SBC

Note: Only users with override lock permissions granted can override your lock. Otherwise, the device must be unlocked by you.

To lock a device for configuration:

1. Expand the Device Manager slider and click Devices. The Device table appears in the content area.
2. Click the device you want to lock in the device content area.
3. Click Lock. A Confirm dialog box appears.



4. Click Yes.

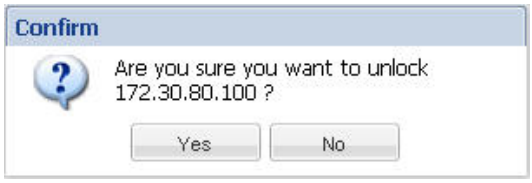
The lock icon appears next to the locked device and Lock toggles to Unlock.

Unlocking Devices

You can unlock a device if you are the owner of the lock, or if you have the appropriate admin permissions to override another user's lock on a device.

To unlock a device:

1. Click the locked device to select it.
2. Click Unlock. A Confirm dialog box appears.



3. Click Yes.
4. Click Refresh. The lock icon is removed. Unlock toggles to Lock.

Device	Target Name	Software Version	Hardware Version
CANADA			
USA			
DODO3			
172.30.80.100	sd100	SC620m3	NN 4250
172.30.91.115	manatee	SD700m6	NN 9200

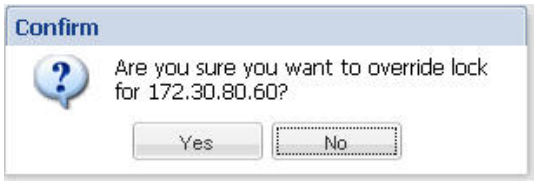
Overriding a Device Lock

With the appropriate admin permissions assigned, you can override another user's lock on a device.

To override another user's lock on a device:

1. Expand the Device Manager slider and click Devices. The Device table appears in the content area.
2. Click the device whose lock you want to override in the device content area.
3. Click Admin to open a pop-up menu.
4. Click Override lock.

A Confirm dialog box appears.



5. Click Yes.
6. Click Refresh. The lock icon is removed from the device.

Rebooting a Device

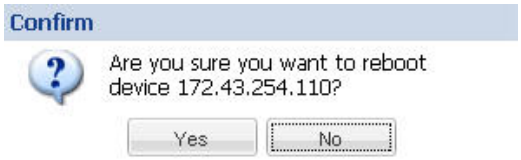
With the appropriate admin permissions assigned, you can reboot a device.

To reboot a device:

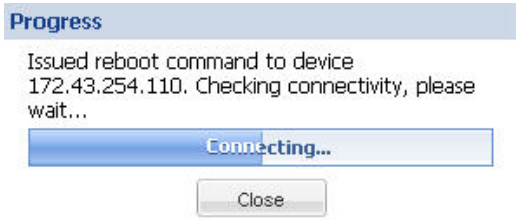
1. Expand the Device Manager slider and click Devices. The Device table appears in the content area.
2. Click the device you want to reboot in the device content area.
3. Click Admin to open a pop-up menu.

4. Click Reboot.

A Confirm dialog box appears.



5. Click Yes. A Progress dialog box appears.



6. Click Close.

A Reboot Device message appears when the reboot process completes:

7. Click OK.

Hardware Information

This section explains the inventory data displayed by the Session Delivery Manager for the following hardware components:

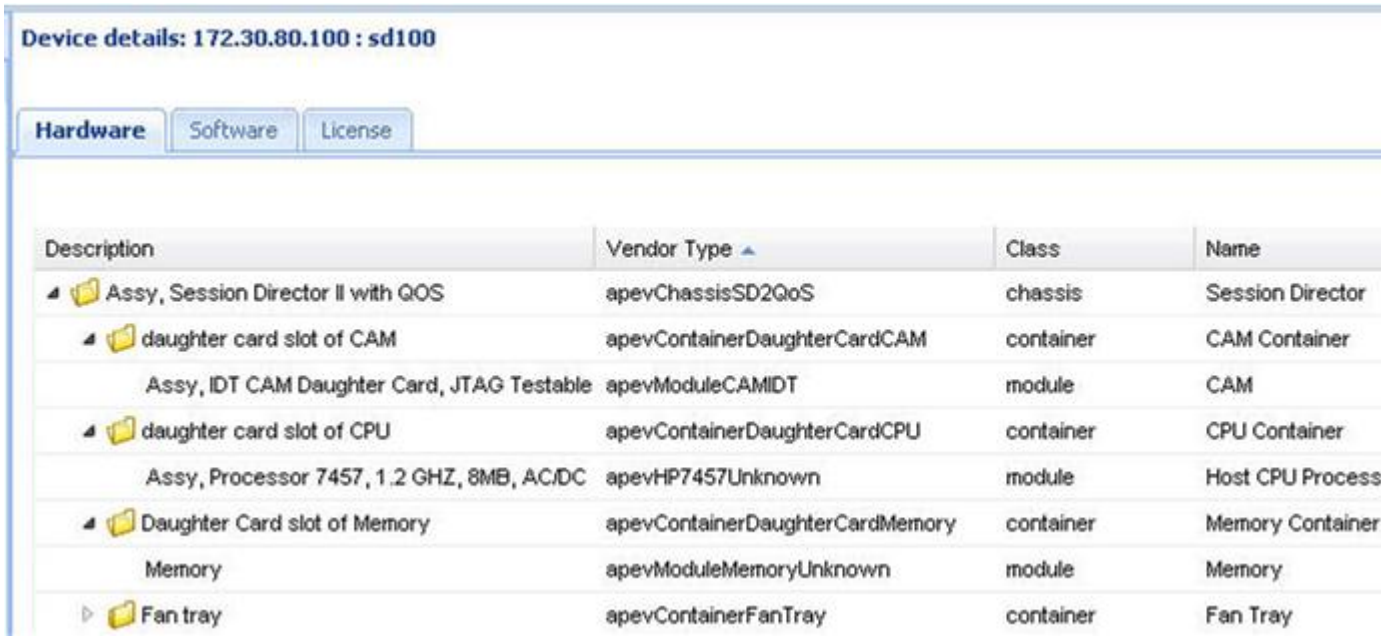
- chassis (main system board)
- CPU
- memory
- network processor
- fans
- packet-processing CAM
- environmental sensors
- network interface
- physical interface cards
- power supplies

Accessing Hardware Details

To access hardware details for a device:

1. Expand the Device Manager slider and click Devices. The Device table appears in the content area.
2. Click the device group to expand the list of devices within the group.
3. Click the device you want to view hardware details for.
4. Click Show Details. Three tabs appear: Hardware, Software, and License.
5. Click the Hardware tab.
6. Click the following buttons to perform tasks:
   - Back: Go back to the Devices main page
   - Refresh: Refresh the data on the page
   - Save to file: Export all or part of the data to a file

Below is an example of the Hardware display.



The folder icon next to an item indicates additional data related to this item.

The following table describes the hardware data displayed by Session Delivery Manager for a standalone device or for devices that belong to a cluster.

Data	Description
Description	Textual description of the physical entity
Vendor type	Vendor-specific hardware type of the physical entity. (This value is different from the definition of MIB-II's sysObjectID.)
Class	Enumerated value that indicates the general hardware type of this physical entity
Name	Textual name of this physical entity. Name of the component as assigned by the local device.
Hardware Rev	Vendor-specific hardware revision string for the physical entity
Firmware Rev	Vendor-specific firmware revision string for the physical entity
Manufacturer	Name of the manufacturer of this physical entity

Data	Description
Model Name	Vendor-specific model name identifier string associated with this physical entity
Is FRU	Whether this physical entity is considered a field replace unit (FRU) by the vendor

Customizing the Display

You can customize the table display by changing the columns that are displayed and/or the order of the table entries.

Note: You can customize most tables found in Session Delivery Manager by following the steps outlined below.

To customize the hardware data:

1. Position the cursor over a column heading. An arrow appears 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 ascending order or Sort Descending to sort the data in descending order.
4. Click Columns to access a list of column names. For example:

5. Click a marked checkbox to hide that column or click an empty checkbox to display that column. The display view automatically updates.
6. Click elsewhere in the display to clear the menus.

Software Information

This section explains how to view the inventory data for the following software components:

- Software images: current software image as well as other loaded images, including the version
- Configuration files: current file as well as other loaded files

Accessing Software Details

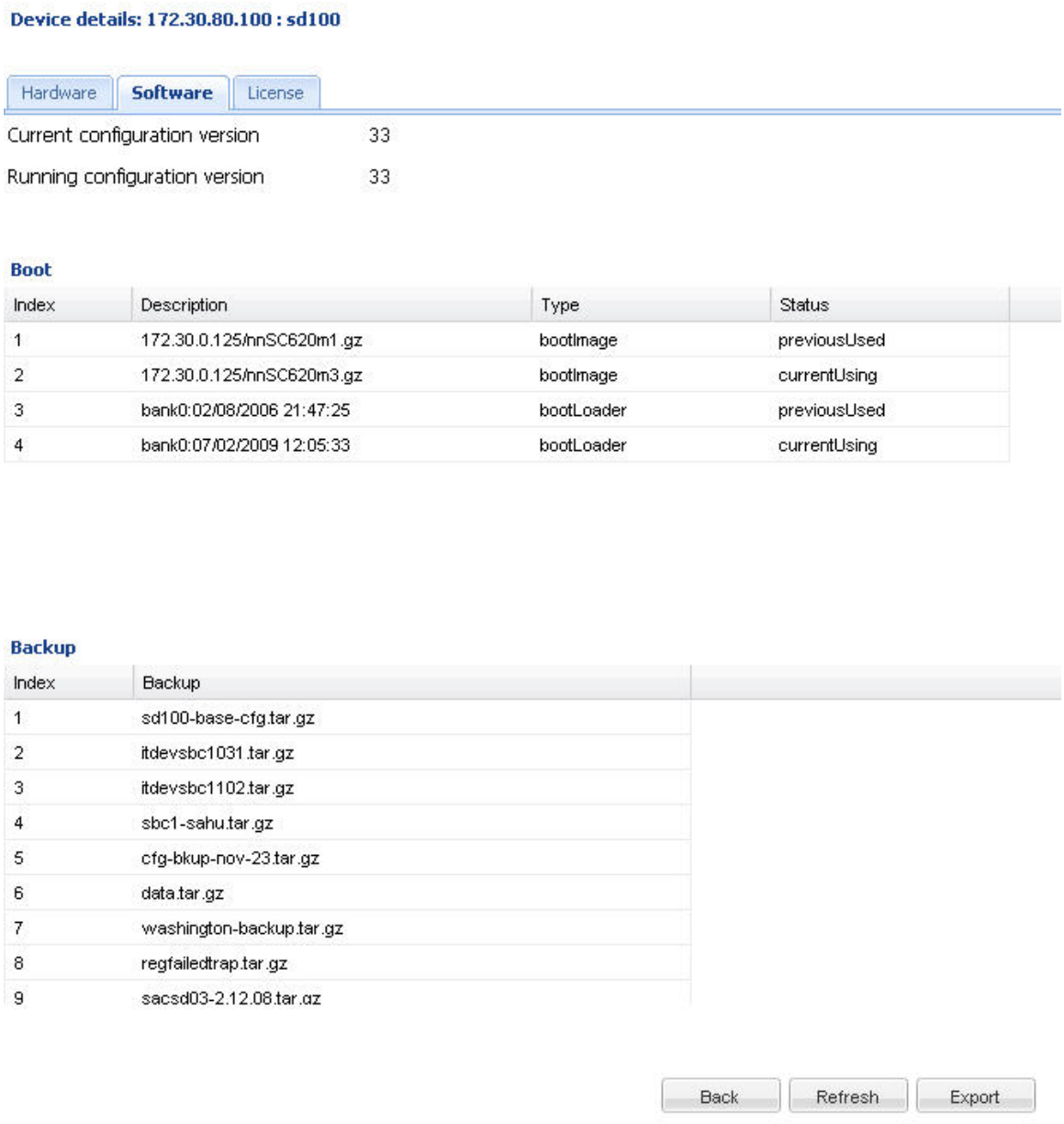
To access software details for a device:

1. Expand the Device Manager slider and click Devices. The Device table appears in the content area.

2. Click the device group to expand the list of devices within the group.
3. Click the device you want to view software details for to select it.
4. Click Show Details. Three tabs appear: Hardware, Software, and License.
5. Click the Software tab.
6. Click the following buttons to perform tasks:

   - Back: Go back to the Devices main page
   - Refresh: Refresh the data on the page
   - Save to file: Export all or part of the data to a file

   The following tables describe the software data displayed by Session Delivery Manager for a standalone device or for the devices that belong to a cluster.



Device details: 172.30.80.100 : sd100

Hardware | **Software** | License

Current configuration version	33
Running configuration version	33

Boot

Index	Description	Type	Status
1	172.30.0.125/nnSC620m1.gz	bootImage	previousUsed
2	172.30.0.125/nnSC620m3.gz	bootImage	currentUsing
3	bank0:02/08/2006 21:47:25	bootLoader	previousUsed
4	bank0:07/02/2009 12:05:33	bootLoader	currentUsing

Backup

Index	Backup
1	sd100-base-cfg.tar.gz
2	itdevsbc1031.tar.gz
3	itdevsbc1102.tar.gz
4	sbc1-sahu.tar.gz
5	cfg-bkup-nov-23.tar.gz
6	data.tar.gz
7	washington-backup.tar.gz
8	regfailedtrap.tar.gz
9	sacsd03-2.12.08.tar.gz

Back | Refresh | Export

About Configuration Versions

The top section of the screen displays both the current configuration version and the running configuration version.

- Current configuration version: Saved version number of the current configuration

- Running configuration version: Saved version number of the configuration currently running on the Net-Net SBC

About the Boot Table

Boot parameters specify what information your Net-Net system uses at boot time when it prepares to run applications. The Net-Net system's boot parameters:

- Determine what software image the Net-Net SBC is using and from where it boots that image: an external device or internal flash memory
- Type of software entity being booted
- Status of that software entity

The following table defines the boot data and backup data displayed by Session Delivery Manager for a standalone Net-Net SBC or for Net-Net SBCs that belong to a cluster.

Data	Description
Boot	
Index	Number that represents the physical entity
Description	Textual description that uniquely identifies the software image. Filename, date and time image was built, or other unique identifiers can be used. For example: host address/image name (boot image) 10.0.1.12/sd121p3.gz boot from flash0/image name (boot image) /tffs0/sd121p3.gz bank0:date time (boot loader) bank0:06/13/2005 10:58:25
Type	Software entity type. Values are: bootImage bootLoader
Status	Software entity status. Values are: previousUsed currentUsing
Backup	
Index	Number that represents the physical entity
Backup	The Net-Net SBC can save an existing configuration into a single backup file. Backups are created as gzipped tar files in a .tar.gz format. They are stored in the /code/bkups directory on the Net-Net SBC.

License Information

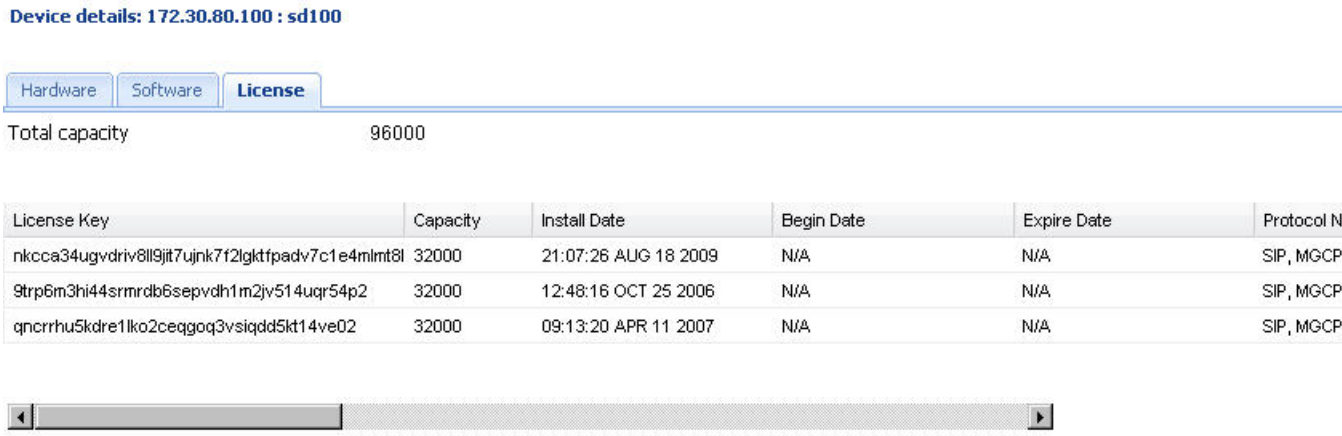
This section explains how to view inventory data for licenses. All components of the Net-Net system software are licensed by Oracle, Inc. (In order to use these components and deploy their related applications in your network, you must have a valid license for each of them.)

Accessing License Details

To access license details for a device:

1. Expand the Device Manager slider and click Devices. The Device table appears in the content area.
2. Click the device group to expand the list of devices within the group.
3. Click the device you want to view license details for to select it.
4. Click Show Details. Three tabs appear: Hardware, Software, and License.
5. Click the License tab.
6. Click the following buttons to perform tasks:
   - Back: Go back to the Devices main page
   - Refresh: Refresh the data on the page
   - Save to file: Export all or part of the data to a file

   Below is an example of the License display.



Total Capacity

The top section of the screen displays the total capacity for the Net-Net SBC, which comprises the maximum number of simultaneous sessions allowed by a Net-Net system for all combined protocols. If the Net-Net SBC had undergone several license upgrades, the value of each capacity row adds up to the total capacity value.

The following table describes the license data displayed by Session Delivery Manager:

Data	Description
License Key	License number
Capacity	Maximum number of simultaneous sessions allowed by the Net-Net system for all combined protocols
Install Date	Installation time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled
Begin Date	Installation time and date in the following format: hh:mm:ss month day year. Displays N/A if a license is not enabled
Expire Date	Expiration time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled
Protocol Names	All protocols licensed for this Net-Net SBC. Values are: SIP MGCP

Data	Description
	H.323
Feature Names	All features licensed for this Net-Net SBC. Values are: Interworking (IWF) Quality of Service (QoS) Acme Control Protocol (ACP) Local Policy (LP) Session Agent Group (SAG) ACC (allows the Net-Net system to create connections and send CDRs to one or more RADIUS servers) High Availability (HA)