

Oracle® Enterprise Communications Broker

Administrator's Essentials Guide
Release P-CZ1.0.0

November 2014

Notices

Copyright ©2013, 2013, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

1 Applicable Platforms.....	9
Software Packaging.....	9
Cabling the Netra Server X3-2 for Acme Packet.....	10
Available Connections.....	11
Local Console Cabling Procedure.....	12
ILOM Cabling Procedure.....	13
Network Management Ports Cabling Procedure.....	13
Media and Signaling Network Interfaces.....	14
Cabling for HA Deployments.....	15
HA Cabling.....	15
BIOS Setting Configuration.....	16
Virtual Systems.....	18
 2 Getting the System Operational.....	 19
Appliance Installation and Start-Up.....	19
Hardware Installation Summary.....	19
Connecting to Your Oracle ECB.....	19
System Boot.....	23
Format Hard Drive.....	25
System Image Filename.....	26
Running Setup.....	26
Adding a License with the Setup Wizard.....	29
Setting Up System Basics.....	30
New User and Superuser Passwords.....	30
New System Prompt.....	30
 3 Initial Configuration.....	 31
Overview.....	31
System Administration.....	31
Configuration Icons.....	32
Save and Activate.....	34
General Settings.....	35
System Settings.....	35
NTP Servers.....	35
Logging (Syslog).....	36
SNMP.....	36
Communications Monitoring Probe settings.....	37
Denial of Service Settings.....	38
High Availability Settings.....	38
Network Interface.....	40
Network Interface Configuration.....	40
Enable ICMP.....	40
Network Interface High Availability Configuration.....	40
SIP Interface Settings.....	41
SIP Interface Configuration.....	41
Accounting Settings.....	42
Configuring Accounting.....	42
FTP Push.....	43

FTP Push Configuration.....	43
Configuring a RADIUS Account Server.....	44
Security Settings.....	45
Certificate Record Configuration.....	45
TLS Profile Configuration.....	46
Generating a Certificate Request from the GUI.....	47
Importing Certificates.....	47
SNMP.....	48
Overview.....	48
Basic SNMP Parameters.....	48
SNMP Community.....	48
Trap Receivers.....	49
SNMP Community Settings.....	49
Trap Receiver Settings.....	49
Web Server Settings.....	49
 4 Oracle ECB Maintenance and Debugging.....	 51
Your Oracle ECB Image.....	51
Obtaining a New Image.....	52
Upgrade Software with the GUI.....	52

Preface

About this guide

The Oracle® Enterprise Communications Broker (ECB) is a purpose-built core communications controller designed to meet session management and other communications core requirements of enterprises.

Your Documentation Supplement

The Oracle® Enterprise Communications Broker Administrator's Essentials Guide Release Version P-CZ1.0.0 is augmented by documentation published for the Oracle Communications SBC and Oracle Enterprise SBC. This document covers the features and functions available with the Oracle ECB itself. As such, this document is dependent upon the larger body of documentation for those features and functions that are not specific to the Oracle ECB.

Product Name Notice

Although the product is named the Oracle Enterprise Communications Broker, there are multiple references to the product as an Acme Packet product within the software. Acme Packet is the name of a company recently acquired by Oracle. Please note that the naming within the software will change.

Related Documentation

The following table lists the members that comprise the documentation set for this release. There are multiple versions of these documents, based on software release. Please refer to documentation for enterprise software version E-C[xz]6.4.0 and service provider software version S-Cx6.3:

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide	Contains information about the components and installation of the Net-Net 4500 system.
Acme Packet 3800 Hardware Installation Guide	Contains information about the components and installation of the Net-Net 3800 system.
Acme Packet 3000 & 4000 Release Notes	Contains information about the current documentation set release, including new features and management changes.
Acme Packet 4000 ACLI Configuration Guide	Contains information about the administration and software configuration of the Oracle SBC.

Document Name	Document Description
Oracle Communications Session Border Controller ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide	Contains information about Oracle SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
Oracle Communications Session Border Controller 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.
Oracle Communications Session Border Controller Accounting Guide	Contains information about the Oracle SBC's accounting support, including details about RADIUS accounting.
Oracle Communications Session Border Controller HDR Resource Guide	Contains information about the Oracle SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Oracle Communications Session Border Controller Administrative Security Essentials	Contains information about the Oracle SBC's support for its Administrative Security license.

In addition to the above, refer to the following document as a supplement to this document.

Oracle® Communications Enterprise Session Border Controller-SE/VME Web GUI User Guide E-C[xz]6.4	Contains generic information about the Web GUI interface, including Monitoring and Tracing and System File management.
Oracle® Communications Enterprise Session Border Controller Configuration Guide Release Version E-C[xz]6.4	Contains a wide range on information on Oracle E-SBC product, including platform information.

Release Caveats

For high availability Oracle ECB deployments, session counts on the standby device are not accurate.

- The Oracle ECB runs in "session" mode, as opposed to "dialog" mode. In session mode, a standby can take over the active role and continue to process existing calls (as well as process new calls) without having existing call data synchronized by the high availability checkpointing process.

Known Issues

The table below lists known issues in the PCZ1.0.0 release of which the user should be aware. The information includes explanations of the impact of the issue and, if applicable, a workaround to the issue.

Issue	Workaround/Impact
The system can lose its tree view after importing dial plans via a CSV file.	Log in and out of the device to re-establish the desired tree view. Importing dial plans occurs infrequently. The scenario produces no negative impact on system operation and the impact on the user is low.

Issue	Workaround/Impact
The system exhibits various GUI function problems if it logs a user out of the "admin" account due to inactivity, and a user subsequently logs back in to the "user" account.	Ensure that users deliberately log out of the "admin" account without allowing the system to time out. Users infrequently change privilege levels. The impact on system operation and the user is low.
The system enables the dial pattern table's delete button even when no pattern is selected.	Be aware of the scenario. The impact is considered very low because the system does not perform any action if the user clicks the delete button.
The system does not perform accounting server configuration save procedures properly if the user does not click the OK button.	Be sure click the OK button to retain accounting server changes before moving to other dialogs. The impact is considered low because users do not often perform accounting configuration procedures.
The system does not perform enum server configuration save procedures properly if the user does not click the OK button.	Be sure to click the OK button to retain enum server changes before moving to other dialogs. The impact is considered low because users do not often perform accounting configuration procedures.
Changing case in GUI "name" fields does not enable the "OK" button.	If you find you need to change a field name to a different case, first change it to a temporary name and click OK. Then change the name back to the original name with the correct case. System configuration element names are case sensitive. Configurations for element names with incorrect case do not work.
The system allows the user to set route entry in the routing table to the wildcard character (*).	Do not set route entries to the wildcard character (*). These routes do not route the applicable traffic.
The "show support-info" ACLI command does not include software version.	When the user submits a defect, please include the output of the "show version" and "show running-config" commands, in addition to the output of the "show support-info" command.
<p>The Geographical dial plan data provided by default is currently incomplete.</p> <p>The Geographical dial plan data provided by default includes complete dial plan data for the following:</p> <ul style="list-style-type: none"> • Argentina • Brazil • Colombia • Mexico • Peru • France • Germany • Italy • Poland • Spain • United Kingdom 	Manually complete dial plan configuration for those countries with incomplete dial plan data.

Issue	Workaround/Impact
In addition, country codes for the largest 50 countries in the world is provided in the default dial plan, allowing outbound dialing to those countries.	
The system does not grey out "Network" High Availability (HA) settings even though HA is disabled globally within the system's "General" settings.	Be aware of the issue. There is no impact on system operation and the impact on the user is low because network HA settings have no effect when HA is disabled globally.
The system allows the user to set the Number Translation's "n-digit-dialing" setting to 0.	Do not set "n-digit-dialing" to 0. The valid range is 1-25 with a default of 1. Number translations with "n-digit-dialing" set to 0 do not work.
The file management function, under the System tab fails on backup configurations with names that include quotes, slashes, greater-than and less-than signs.	Do not configure backup configuration filenames with the characters listed. The impact includes error messages displayed by the GUI during applicable file management functions.
The system times out requests to download 0-length files from the System tab.	Click the Download button again. The system proceeds to download the file. There is no impact on the system and the impact on the user is considered low.
The system's Current Memory Usage pie graph does not display the usable memory for SUN Netra hardware. Instead, it displays the physical size of RAM.	Be aware of the issue. There is no impact on the system and the impact on the user is considered very low.

Revision History

Date	Revision Number	Description
October 30, 2013	Revision 1.00	Initial Release
November 11, 2013	Revision 1.10	Adds the Known Issues section to About this Guide
December 11, 2013	Revision 1.20	Adds minimum VM resource list
Sept 26, 2014	Revision 1.30	Removes references to wancom2 as being supported in HA configurations.
Nov 26, 2014	Revision 1.40	Corrects Communications monitoring probe default port as 4739.

Applicable Platforms

The Oracle ECB is available either as an appliance or as a application for operation on virtual machines. When running as an appliance, the Oracle ECB software is packaged with the Netra Server X3-2 for Acme Packet and delivered to the end customers. When running as a virtual application, the Oracle ECB software can be deployed on any third-party COTS hardware that meets the specified guidelines.

When delivered as an appliance, the application comes pre-installed on Oracle's Netra Server X3-2 for Acme Packet. Server cabling instructions, which also identifies key hardware elements, such as interfaces, are presented below. Instructions on installation and maintenance of the Netra Server X3-2 for Acme Packet are generic to SBC, Session Router and other appliance applications.

The generic Netra Server X3-2 for Acme Packet documentation herein identifies all hardware interfaces. With respect to cabling the Oracle ECB, the applicable interfaces, as named in the hardware documentation, include:


- s0p0—Service access
- wancom0—Management access
- wancom1—High Availability (HA) access
- SER MGT(COM1)—Serial management access

You run the application as a virtual machine over a VM system, such as Oracle VM Server. You use VM management software, such as Oracle VM Manager, to create and maintain your virtual machines.

Virtual machine installation instructions are available in the Platforms chapter of the *Oracle Enterprise Session Border Controller Configuration Guide*. Generic hardware information is provided in the applicable documentation provided by your hardware vendor.

Software Packaging

The Release P-Cz version 2 build image is labeled nnPCz200.bz. The image is compressed by the zlib software library and includes all software components needed to install and operate the Oracle ECB.

 **Note:** Note that you must obtain a license if you want to operate with TLS. The procedure to obtain this license is documented herein.

Oracle ECB software delivered for virtual machines includes the following packages:

Image Name	Description
nnPCz200.bz	Standalone compressed image - This .bz image package is primarily used to load and operate the Oracle ECB software as an appliance.

Applicable Platforms

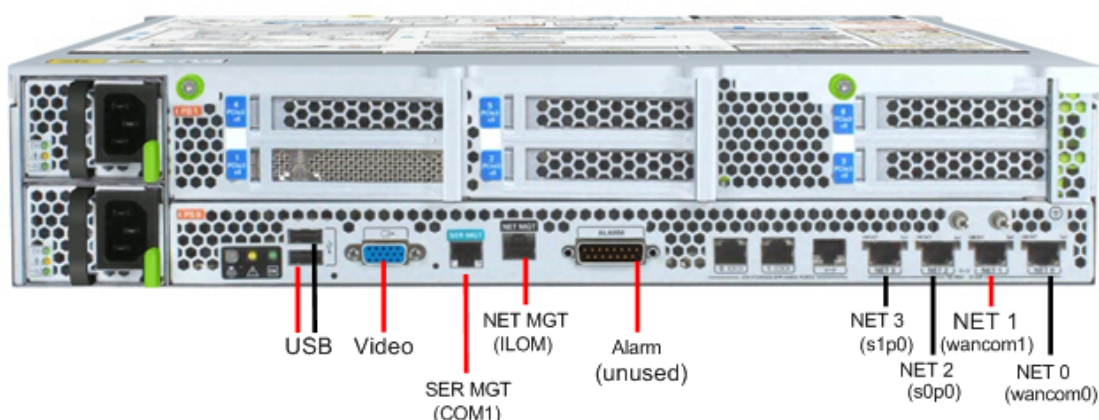
Image Name	Description
	You can also use the .bz image as a load image to existing virtual machines. Create your virtual machine according to specifications. Then copy this image to your machine (eg /code) and point your boot parameters to it.
nnPCz200-img-bin.ova	Virtual Machine Template - Import within virtual machine hypervisor to create the entire machine.

Cabling the Netra Server X3-2 for Acme Packet

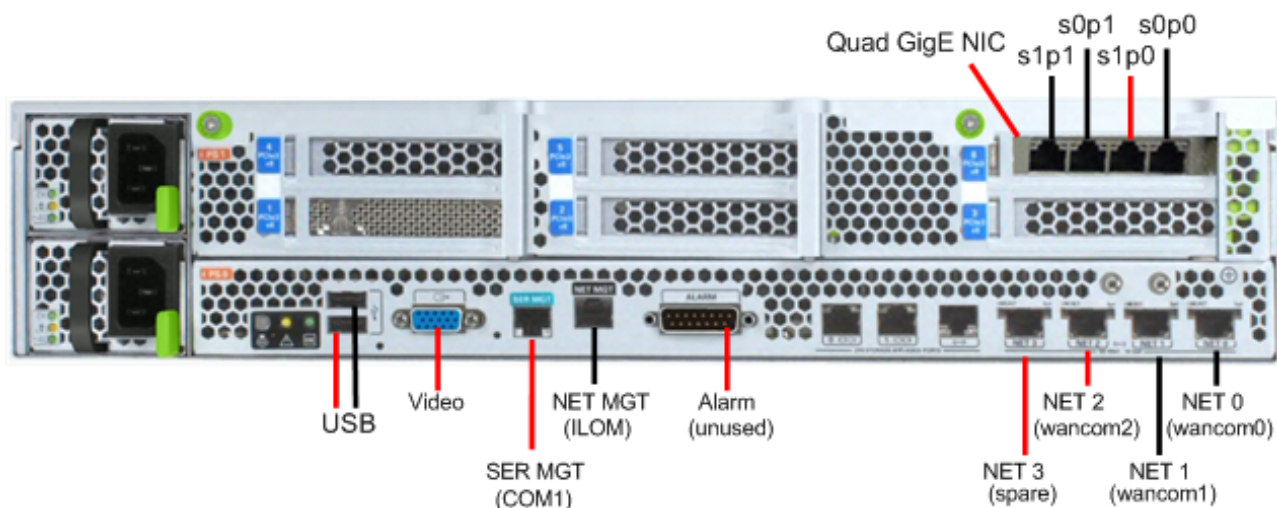
After mounting the Netra Server X3-2 for Acme Packet in an equipment rack and installing all components into it, connect all appropriate data cables to the ports before powering the system up and configuring it. This section describes how to make data cable connections.

Oracle supports the following configurations of the Netra Server X3-2 for Acme Packet (the onboard 10 GigE ports are configured for 1G operation):

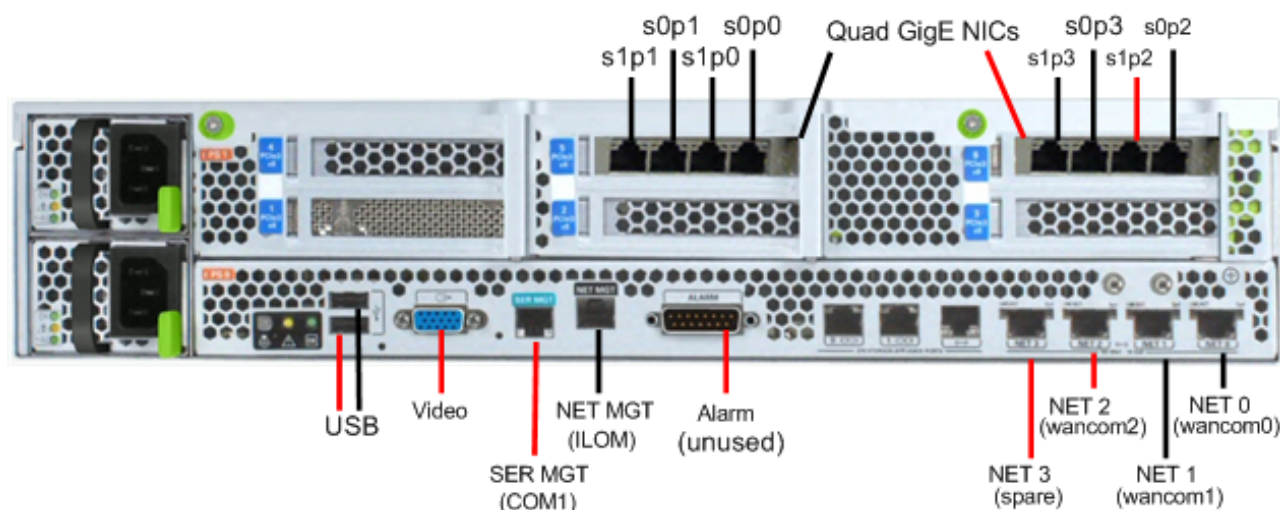
- Configuration A: Four onboard 10 GigE ports and no Quad GigE NIC
- Configuration B: Four onboard 10 GigE ports and 1 Quad GigE NIC
- Configuration C: Four onboard 10 GigE ports and 2 Quad GigE NICs



Netra Server X3-2 for Acme Packet Configuration A (4 Onboard 10 GigE Ports)



Netra Server X3-2 for Acme Packet Configuration B (4 Onboard 10 GigE Ports & 1 Quad GigE NIC)



Netra Server X3-2 for Acme Packet Configuration C (4 Onboard 10 GigE Ports & 2 Quad GigE NICs)

Oracle recommends using Category 6 (or better) for all Ethernet connections.

You can install and remove Ethernet and 1000BASE-T cables while the Netra Server X3-2 for Acme Packet is operational. Not every port needs to be utilized for proper operation. However, when a cable is disconnected and the link is lost, an alarm is generated.

Available Connections

Please read all of the information pertaining to each of the available connections prior to cabling the Netra Server X3-2 for Acme Packet.


Port	Description	You Need:
NET (0-3)	10 GigE ports - labeled Net 3, Net 2, Net 1 and Net 0 (left to right) - enable you to connect the Netra Server X3-2 for Net-Net to your network.	<p>A Category 6 (or better) Ethernet cable to connect to the NET 0 port to your network</p> <p>Network parameters such as an IP address (can be provided by DHCP services or assigned a static address in the OS)</p> <p>Additional Category 6 (or better) Ethernet cables and Ethernet addresses as needed for additional connections to NET 1 - 3</p>
NET MGT	Provides a 10/100BASE-T Ethernet connection to the SP through an RJ-45 connector. This port provides support connections to the SP using the Oracle ILOM CLI and Web interface. By default, this port is configured to use DHCP to automatically obtain an IP address. Alternatively, you can assign a static IP address to this port. To use this port, it must have its network settings configured. Once configured, use the NET MGT port IP address to log in to the SP using a browser or secure shell.	<p>Category 6 (or better) Ethernet cable to connect the NET MGT port to your network</p> <p>IP address for this port (required from DHCP or a static address)</p>
SER MGT (COM1)	Provides a TIA/EIA-232 serial Oracle/Cisco standard connection to the SP through an RJ-45 connector. Default settings for this port are: 8N1: eight data bits, no parity, one stop bit	A terminal device (e.g., terminal, connection to a terminal server, or computer such as a laptop running terminal emulation software)

Applicable Platforms

	115200 baud Disable hardware flow control (CTS/RTS) Disable software flow control (XON/XOFF)	A cable to connect the terminal device to the SER MGT (COM1) port
USB	Provides USB connections to the service processor (SP). The USB ports are hot pluggable, so you can connect/disconnect USB cables from these ports and peripheral devices without affecting server operations.	USB keyboard USB mouse Note: Maximum USB cable length: 5 meters
Video	Provides a temporary video connection to the SP.	VGA monitor HDB-15 video cable with a maximum cable length of 6 meters (19.7 feet)

Local Console Cabling Procedure

This section explains how to physically make a console connection to the Netra Server X3-2 for Acme Packet. Administration console may be connected to either the ILOM (NET MGT), the local VGA+USB console ports, or the local SER MGT (COM1) serial console port. When configuring bootloader parameters, set the console to VGA if ILOM or VGA+USB are used, or COM1 if SER MGT is used. The bootloader is accessible on all console ports, but only input from the active console port can be recognized by the Netra Server X3-2 for Acme Packet.


 **Note:** DO NOT configure COM2 in the bootparams menu! Configuring COM2 can cause the system to boot hang!

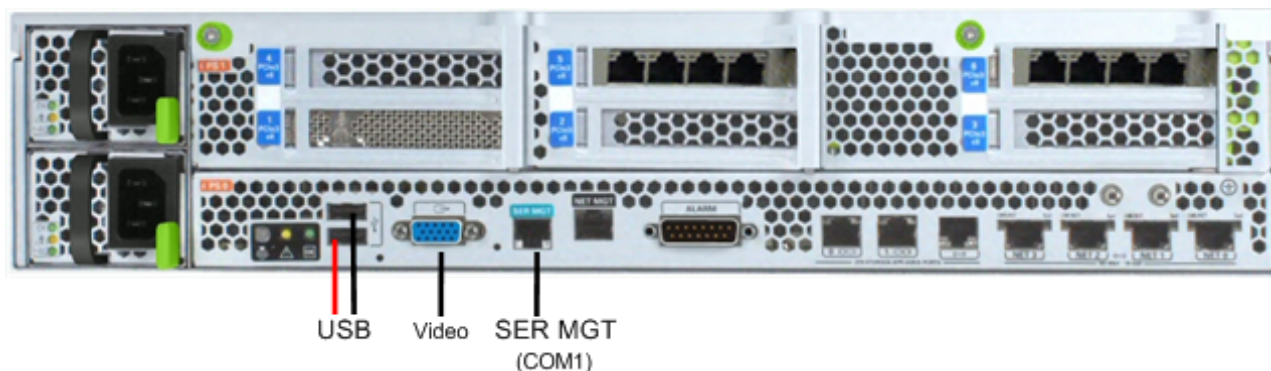
- To cable a serial console connection:
 - Serial console cable with an RJ-45 connector
- To cable a USB and Video Connection:
 - DB-15 video cable with a maximum cable length of 6 meters (19.7 feet)
 - USB cable with a maximum cable length of 6 meters (19.7 feet)
 - USB keyboard

In the following procedure, you have the option to either cable a serial connection or to cable a USB/Video connection.

To cable a local console connection:

1. Locate the appropriate cable(s) to connect to the Netra Server X3-2 for Acme Packet.
2. To cable a serial connection, insert the serial console cable into the SER MGT (COM1) port.

 **Note:** Refer to the Netra Server X3-2 hardware documentation for information on how to configure your terminal application to connect to the console, and how to establish communications with the Netra Server X3-2 for Acme Packet.



Connecting to USB, VGA and SER MGT (COM1) Ports

3. To cable a USB/Video connection, insert the 15-pin connector on the end of the video cable into the Video port. Then insert the USB cable from the mouse and keyboard into the USB ports.
4. Lead the cables neatly away from the rear panel.
5. Plug in the cables to their respective destination components.

ILOM Cabling Procedure

This section explains how to make a connection to the Netra Server X3-2 for Acme Packet ILOM port. For a remote permanent connection to the SP over the ILOM connection, use the rear panel NET MGT port.

Refer to the Netra Server X3-2 for Acme Packet hardware documentation for information on how to configure your Web browser application to connect to the console, and how to establish communications with the Netra Server X3-2 for Acme Packet.



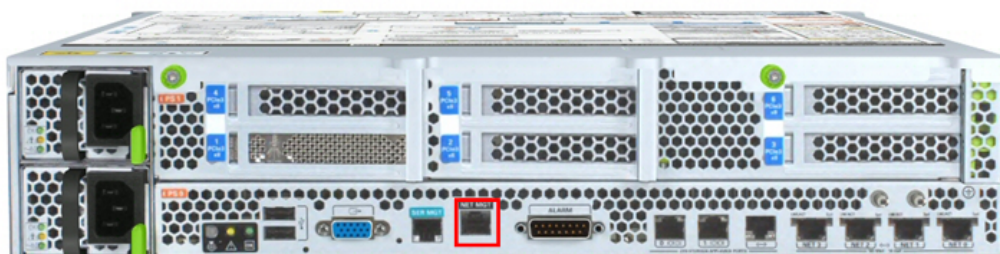
Note: Keep Ethernet cables separated from power cables by at least 60mm where possible and never run them in the same channel of the rack without segregation.

Prerequisites:

- Category 6 (or better) Ethernet cable with RJ-45 jacks

To cable an ILOM connection:

1. Locate the cable to connect to the Netra Server X3-2 for Acme Packet.
2. Insert the male end of the RJ-45 connector on the end of the Ethernet cable into the female RJ-45 receptacle. The release tab on the RJ-45 jack clicks into place when you insert it properly.



NET MGT (ILOM) Port

3. Lead the cable neatly away from the rear panel.
4. Connect the other end of the cable to the LAN.

Network Management Ports Cabling Procedure

This section describes how to connect cables to the network management ports. These ports support 10/100/1G/10G Mbps speeds.



Note: Keep Ethernet cables separated from power cables by at least 60mm where possible and never run them in the same channel of the rack without segregation.

Prerequisites:

- Category 6 (or better) Ethernet cable with RJ-45 jacks

To connect to the network management ports:

1. Locate the Ethernet cables you plan to connect to the Netra Server X3-2 for Acme Packet.
2. Insert the RJ-45 connector on the end of the Ethernet cable into one the NET0 Ethernet port (wancom0).



Note: The wancom0 and wancom1 ports are common to all supported Netra Server X3-2 for Acme Packet configurations. The wancom2 port is not used on the Oracle ECB.

The release tab on the RJ-45 jack will click into place when you insert it properly.



Network Management Ports

3. Route the cable away from the Netra Server X3-2 for Acme Packet, ensuring that the Ethernet cables are not stretched tightly or subjected to extreme stress.

Media and Signaling Network Interfaces

This section explains how to cable the media and signaling ports. These ports accept copper GigE connectors.



Note: Perform all cabling procedures according to the established standards for your organization.

Category 6 (or better) Ethernet cables with RJ-45 jacks are used for connecting to the Netra Server X3-2 for Acme Packet media and signaling ports to your production network.

Regardless of configuration, media ports support 10/100/1000BASE-T only. Do not attempt to connect 10GBASE-T equipment to the signaling and media ports.

Prerequisites:

- Category 6 (or better) Ethernet cables with RJ-45 jacks

To connect to the media and signaling ports:

1. Locate the Ethernet cables you plan to connect to the media and signaling ports of the Netra Server X3-2 for Acme Packet.
2. Insert the RJ-45 connector on the end of the Ethernet cable into one of the 1000BASE-T copper media and signaling ports. The available signaling and media ports depend on the chosen configuration:
 - For configurations with no Quad GigE NICs, two onboard Ethernet ports are available for use as signaling and media ports as shown in the following.



Supported Signaling/Media Ports (4 10 GigE Ports)

- When the configuration consists of four onboard 10 GigE ports and one Quad GigE NIC, the signaling and media ports include s1p1, s0p1, s1p0, and s0p0 as shown in the following. The release tab on the RJ-45 jack will click into place when you insert it properly.



Supported Signaling/Media Ports (4 OB 10 GigE Ports & 1 Quad GigE NIC)

- When the configuration consists of four onboard 10 GigE ports and two Quad GigE NICs, the signaling and media ports include s1p1, s0p1, s1p0, s0p0, s1p3, s0p3, s1p2 and s0p2 as shown in the following. The release tab on the RJ-45 jack will click into place when you insert it properly.



Supported Signaling/Media Ports (4 OB 10 GigE Ports & 2 Quad GigE NICs)

- Route the cable away from the Netra Server X3-2 for Acme Packet. Make sure that the Ethernet cables are not stretched tightly or subjected to extreme stress.
- Repeat Steps 1 through 2 for each additional Ethernet cable you connect to your Netra Server X3-2 for Acme Packet.

Cabling for HA Deployments

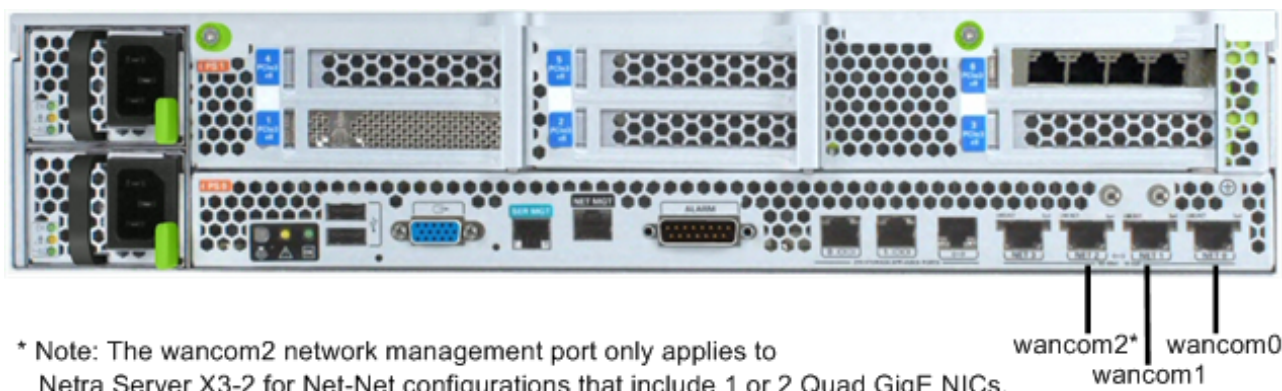
The information and instructions in this section explain how to cable a high availability (HA) node.

HA Cabling

Category 6 Ethernet cables are required for cabling two HA nodes together.

Rear Panel Cabling

You can use one connection for HA redundancy support between the two members of an HA node. As a rule, wancom0 should be reserved as the boot/maintenance interface. This leaves wancom1 available for sharing HA information.



4 Onboard 10 GigE Ports & 1 Quad GigE NIC

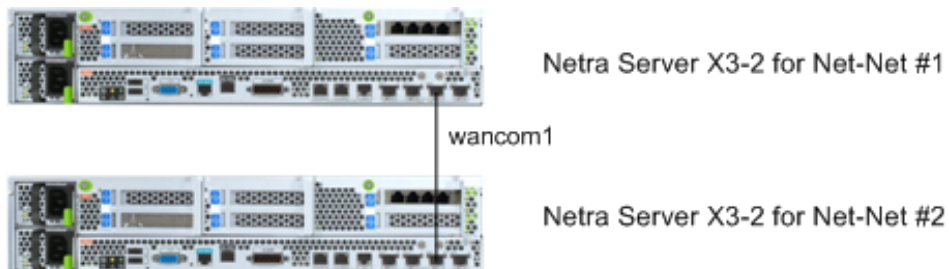
Prerequisites:

- Category 6 (or better) Ethernet cables with RJ-45 jacks

Single Rear Interface Support

To cable a Netra Server X3-2 for Acme Packet HA node using single rear interface support:

1. Insert one end of an Ethernet cable into wancom1 on the rear panel of Netra Server X3-2 for Acme Packet #1. The release tab on the RJ-45 jack clicks into place when you insert it properly.
2. Insert the other end of the Ethernet cable into the corresponding management interface on the rear panel of the Netra Server X3-2 for Acme Packet #2 as presented here. For example, If you use wancom1 on Netra Server X3-2 for Acme Packet #1, then you will connect it to wancom1 on Netra Server X3-2 for Acme Packet #2.



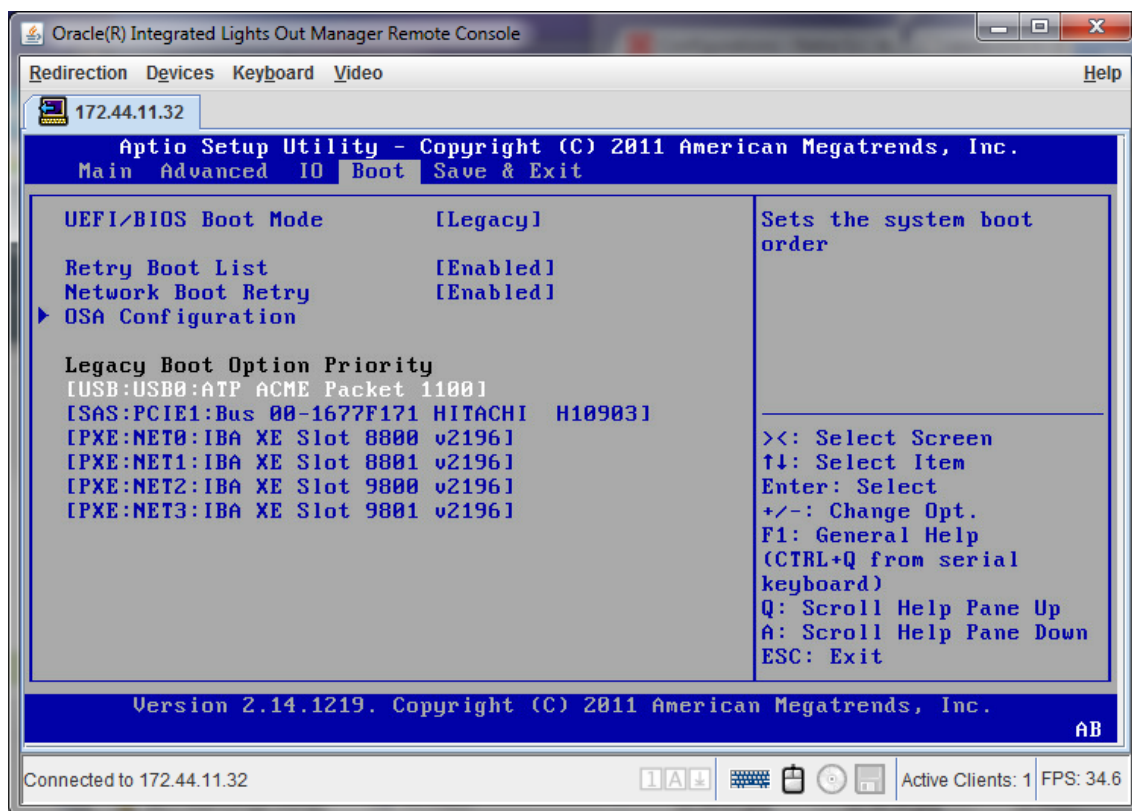
HA Node Using Single Rear Interface Support (No Quad GigE NIC)

3. Refer to the configuration procedures located in the HA Nodes information in this Configuration Guide.

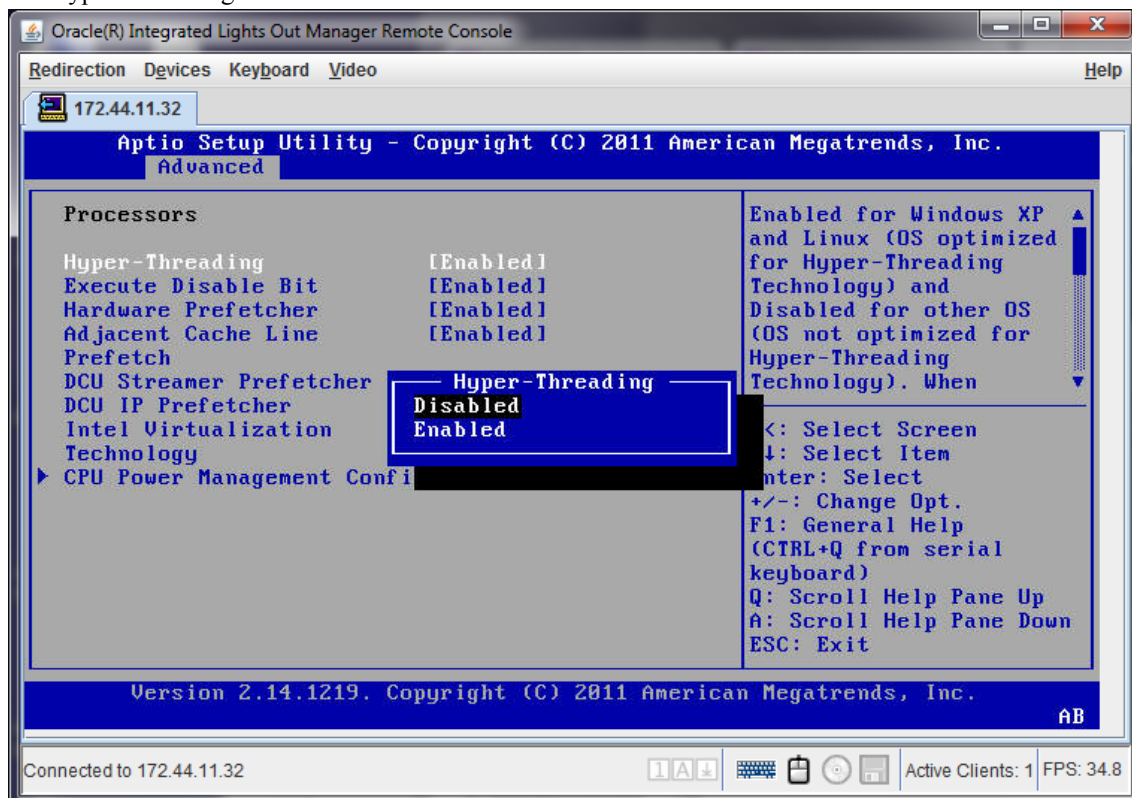
BIOS Setting Configuration

The following changes on the Netra Server X3-2 are required to run Oracle ECB. This procedure shows where to make changes in the BIOS setup utility.

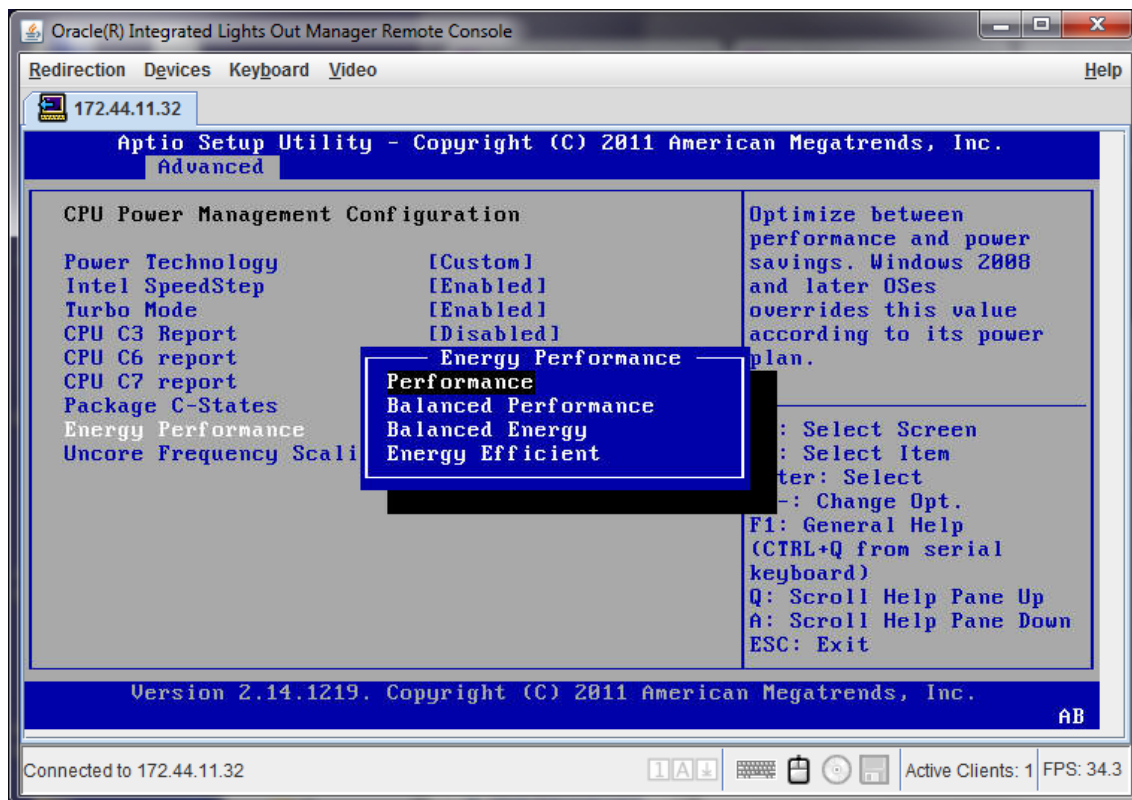
1. Set the USB slot to be the first boot device. The disk controller should be the second boot device.



2. Set Hyper-Threading to Disabled



3. Change Energy Performance to Performance



4. After setting Performance, press Escape to return to the main menu, then select Save & Exit to apply the changes. The system will reboot using the newly configured settings.

Virtual Systems

The Oracle ECB can operate on virtual machines running on generic, off-the-shelf servers. Specifications for virtual machines is available in the Platforms chapter of the *Oracle Enterprise Session Border Controller Configuration Guide*. This document also includes information about hardware components, including hard drive partitions created during install, interface mapping and high availability.

As its name indicates, the VM Edition software is designed for use within virtual environments. It provides support for a variety of hypervisors, including the Oracle hypervisor. Oracle recommends the use of Oracle Virtual Machine (OVM) hypervisor for running Oracle ECB virtual application.

The end-user installs the virtual machine software in hardware of the customer's choice. The number of VMs supported by a server is constrained only by the resources on your system.

Minimum VM Resources

Each VM instance requires the following minimum allocation or network resources.

- CPU cores: 2
- Memory: 2GB
- Hard drive storage: 40GB
- 32-bit application
- Interfaces: 8 recommended (less can be used)

Getting the System Operational

Appliance Installation and Start-Up

This section outlines hardware installation at a very high level and describes system power-on. It bridges hardware installation and application start-up, presenting information about what to expect from Oracle ECB software as the hardware powers up. Administrators need to know how to access the software while it boots, and what successful software startup looks like.

If running the Oracle ECB as a virtual application, refer to the hardware vendor's installation instructions for hardware to learn how to access the software while it boots. From a console connection, there is little difference to the way successful startup appears as an appliance versus a virtual machine.

Hardware Installation Summary

Installing your Oracle ECB in your rack requires the steps summarized here. This checklist is only an overview. It is not designed to substitute for following the detailed procedures in the hardware installation guides.

1. Unpacking the Oracle ECB
2. Installing the Oracle ECB into your rack
3. Installing power supplies
4. Installing fan modules
5. Installing physical interface cards
6. Cabling the Oracle ECB

Make sure you complete installation procedures fully and note the safety warnings to prevent physical harm to yourself and/or damage to your Oracle ECB.

After you have completed the hardware installation procedures, you are ready to establish a connection to your Oracle ECB. Then you can load the Oracle ECB software image you want to use and establish basic operating parameters.

Connecting to Your Oracle ECB

By default, the Oracle ECB is delivered with no management IP address. You must set this address the first time you start your system. Find instructions on configuring this address in the System Boot section below.

You can connect to your Oracle ECB either through a direct console connection, or by creating a remote Telnet or SSH session. Both of these access methods provide you with a wide range of configuration, monitoring, and

Getting the System Operational

management options. IP-based management access, including Telnet SSH and GUI, requires an IP address for your management port. This address is specified in boot parameter named "**ip address**".



Note: The **ip address** parameter is displayed using different names, depending on the context:

- The boot parameters wizard field name is also "**ip address**".
- The initial configuration wizard field name is "**Management interface ip address**".
- The ACLI **show interfaces** command field name is "**wancom0**".

By default, Telnet, sftp and web GUI connections to your Oracle ECB are enabled, but are only accessible via the "**ip address**" address. You cannot use telnet, sftp or the web GUI until you set this address.

Depending on platform, software installation may be required upon first startup. You perform/monitor software installation via the console connection. The Oracle ECB requires most configuration via the GUI. Procedures requiring the ACLI include:

- Change default management interface IP address
- Format hard drive
- Set/Change password
- Set/Change SIP Monitor and Trace filters
- Disable telnet

Local Connections and Time-outs

The ACLI is available via serial, telnet and SSH connections. Prior to software installation, you reach the ACLI via a local, serial connection.

If deploying the Oracle ECB on a virtual machine, the virtual machine manager provides console access via a virtual serial connection. See documentation on your virtual machine to learn how to access the console. Once you have accessed a virtual machine console, working within that console is the same as on dedicated hardware.

If deploying on dedicated hardware, you can connect your laptop or PC directly to the Oracle ECB using a serial connection. If you use a laptop, you must take appropriate steps to ensure grounding.

One end of the cable plugs into your terminal, and the other end plugs into the RJ-45 port, normally on the back of your server.

To set up a console connection to your Oracle ECB:

1. Set the connection parameters for your terminal to the default boot settings:
 - Baud rate: 115,200 bits/second
 - Data bits: 8
 - Parity: No
 - Stop bit: 1
 - Flow control: None
2. Use a serial cable to connect your PC to the Oracle ECB. Refer to your hardware documentation for the location of your server's serial port.
3. Power on your Oracle ECB.
The system boots. Upon successful boot, the system prompts you to log in.

Password:

4. Enter the appropriate password information when prompted to log into User mode of the ACLI. The default user mode password is acme.

The system displays the ACLI's user mode prompt :

ORACLE>

5. If necessary enter Superuser mode, by entering enable at the ACLI and pressing Enter.
The system ACLI prompts you for the superuser password:

```
ORACLE>enable
Password:
```

6. Enter the appropriate password information to log into Superuser mode of the ACLI. The default Superuser mode password is packet.
The system changes the ACLI prompt to:

```
ORACLE#
```

7. Proceed with system configuration or setup.

You can control the amount of time it takes for your console connection to time out by setting the console-timeout parameter in the system configuration. If your connection times out, the login sequence appears again and prompts you for your passwords. The default for this field is 0, which means that no time-out is being enforced.

Telnet Remote Connections and Time-outs

You can also Telnet to your Oracle ECB. Using remote Telnet access, you can provision the Oracle ECB remotely through the management interface over IP. You configure management interface IP during system setup, described below, or via the Oracle ECB boot parameters.

The Oracle ECB can support up to five concurrent Telnet sessions. However, only one user can carry out configuration tasks at one time.



Note: Telnet does not offer a secure method of sending passwords. Using Telnet, passwords are sent in clear text across the network.

To Telnet to your Oracle ECB, you need to know the IPv4 address of its administrative interface (wancom0). The wancom0 IPv4 address of your Oracle ECB can be found using the ACLI to display the boot parameter value named **IP Address**.

You can manage the Telnet connections to your Oracle ECB by setting certain ACLI parameters and by using certain commands:

- To set a time-out due to inactivity, use the telnet-timeout parameter in the system configuration. You can set the number of seconds that elapse before the Telnet connection or SSH connection is terminated. The default for this field is 0, which means that no time-out is being enforced.
- To view the users who are currently logged into the system, use the command, show users. You can see the ID, timestamp, connection source, and privilege level for active connections.
- From Superuser mode in the ACLI, you can terminate the connections of other users in order to free up connections. Use the command, kill user, with the corresponding connection ID.
- From Superuser mode in the ACLI, you can globally enable and disable Telnet connections to the Oracle ECB.
 - Telnet service is enabled by default on your Oracle ECB.
 - To disable Telnet, type the command, management disable telnet, at the ACLI Superuser prompt and reboot your system. The Oracle ECB then refuses any attempts at Telnet connections. If you want to restart Telnet service, type management enable telnet.
- If you reboot your Oracle ECB from a Telnet session, you lose IP access and therefore your connection.

SSH Remote Connections

For increased security, you can connect to your Oracle ECB using SSH. An SSH client is required for this type of connection.

The Oracle ECB supports five concurrent SSH and/or SFTP sessions.

There are two ways to use SSH to connect to your Oracle ECB. The first works the way a Telnet connection works, except that authentication takes place before the connection to the Oracle ECB is made. The second requires that you set an additional password

SSH without Username and Password

Many SSH clients allow you to initiate an SSH connection without specifying a username. To initiate an SSH connection to the Oracle ECB without specifying users and SSH user passwords:

1. Open your SSH client.
2. At the prompt in the SSH client, type the `ssh` command, a Space, the IPv4 address of your Oracle ECB, and then press Enter.

The SSH client prompts you for a password before connecting to the Oracle ECB. Enter the Oracle ECB's User mode password. After it is authenticated, an SSH session is initiated and you can continue with tasks in User mode or enable Superuser mode.

Bear in mind that some clients interpret SSH session initiation without a username as a means of logging in with your system login name. The procedure above does not work for these clients.



Note: You can also create connections to the Oracle ECB using additional username and password options.

SSH with Username and Password

To initiate an SSH connection to the Oracle ECB with an SSH username and password:

1. In the ACLI at the Superuser prompt, type the `ssh-password` and press Enter. Enter the name of the user you want to establish. Then enter a password for that user when prompted. Passwords do not appear on your screen.

```
SYSTEM# ssh-password
SSH username [saved]: MJones
Enter new password: 95X-SD
Enter new password again: 95X-SD
```



Note: After you configure `ssh-password`, the SSH login accepts the username and password you set, as well as the default SSH/SFTP usernames: User and admin.

2. Configure your SSH client to connect to your Oracle ECB's management IPv4 address using the username you just created. The standard version of this command would be:

```
ssh -l MJones 10.0.1.57
```

3. Enter the SSH password you set in the ACLI.

```
MJones@10.0.2.54 password: 95X-SD
```

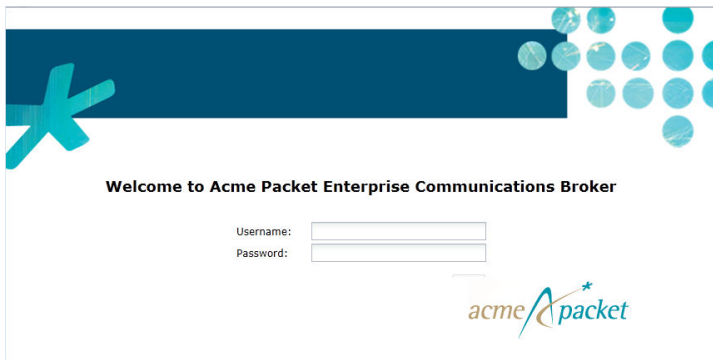
4. Enter your User password to work in User mode on the Oracle ECB. Enable Superuser mode and enter your password to work in Superuser mode.
5. An SSH session window opens and you can enter your password to use the ACLI.

GUI Access

Oracle requires the use of GUI for ongoing configuration and management of the Oracle ECB. Most user/provisioning procedures cannot be conducted via the ACLI. Important exceptions to this include setting the initial management IP address and changing GUI access passwords.

GUI access is available via HTTP at the configured management address. You must set this address before proceeding. You can configure HTTPS access, if desired. Disabling the GUI is not supported.

When you access the GUI via browser, you see the login screen, from which you login and then access System Administration and Service Provisioning controls.




System Boot

Whenever your Oracle ECB boots, the following information about the tasks and settings for the system appear in your terminal window.

- System boot parameters
- From what location the software image is being loaded: an external device or internal flash memory
- Requisite tasks that the system is starting
- Log information: established levels and where logs are being sent
- Any errors that might occur during the loading process

After the loading process is complete, the ACLI login prompt appears.

 **Note:** You can set boot parameters using the ACLI or the GUI. Boot parameter definitions, which help you understand what you should set them to, are provided below.

Oracle ECB Boot Parameters

Boot parameters specify the information that your Oracle ECB uses at boot time when it prepares to run applications. The Oracle ECB's boot parameters:


- Allow you to set the IP address for the management interface (wancom0).
- Allow you to set a system prompt. The target name parameter also specifies the title name displayed in your web browser and SNMP device name parameters.
- Determine the software image to boot and from where the system boots that image.
- Sets up the username and password for network booting from an external FTP server.

In addition to providing details about the Oracle ECB's boot parameters, this section explains how to view, edit, and implement them.

When displaying the boot parameters, your screen shows a help menu and the first boot parameter (boot device). Press Enter to continue down the list of boot parameters.

Boot Parameter Changes

You can access and edit boot parameters by using either the ACLI or by interrupting the system boot process.

 **Note:** Changes to boot parameters do not go into effect until you reboot the Oracle ECB.

Oracle recommends that you use management port 0 (wancom0) as the boot interface, and that your management network is either:

- directly a part of your LAN for management port 0
- accessible through management port 0

Otherwise, your management messages may use an incorrect source address.

Change Boot Parameters from the ACLI

To access and change boot parameters from the ACLI:

Getting the System Operational

1. In Superuser mode, type configure terminal, and press Enter.

```
ORACLE# configure terminal
```

2. Type bootparam, and press Enter. The boot device parameters display.

```
ORACLE(configure)# bootparam
'.' = clear field; '-' = go to previous field; ^D = quit
boot device      : eth0
```

To navigate through the boot parameters, press Enter and the next parameter appears on the following line.

You can navigate through the entire list this way. To go back to a previous line, type a hyphen (-) and press Enter. Any value that you enter entirely overwrites the existing value and does not append to it.

3. To change a boot parameter, type the new value that you want to use next to the old value. For example, if you want to change the image you are using, type the new filename next to the old one. You can clear the contents of a parameter by typing a period and then pressing Enter.

```
ORACLE(configure)# bootparam
'.' = clear field; '-' = go to previous field; ^D = quit
boot device      : eth0
processor number  : 0
host name        : goose
file name        : /boot/nnPCz100.gz /boot/nnPCz200.gz
```

When you have scrolled through all of the boot parameters, the system prompt for the configure terminal branch displays.

```
ORACLE(configure)#
```

4. Exit the configure terminal branch.
5. Reboot the Oracle ECB for the changes to take effect.

The ACLI reboot and reboot force commands initiate a reboot. With the reboot command, you must confirm that you want to reboot. With the reboot force command, you do not have make this confirmation.

```
ORACLE# reboot force
```

The Oracle ECB completes the full booting sequence. If necessary, you can stop the auto-boot at countdown to fix any boot parameters.

If you configured boot parameters correctly, the system prompt displays and you can go ahead with configuration, management, or monitoring tasks.



Note: If you configured the boot parameters incorrectly, the Oracle ECB goes into a booting loop and displays an error message.

```
Error loading file: errno = 0x226.
Can't load boot file!!
```

Press the space bar to stop the loop. Correct the error in the boot parameter, and reboot the system.

Change Boot Parameters by Interrupting a Boot in Progress

To access and change boot parameters by interrupting a boot in progress:

1. When the Oracle ECB is in the process of booting, you can press the space bar on your keyboard to interrupt when you see the following message appear:

```
Press the space bar to stop auto-boot...
```

2. After you stop the booting process, you can enter the letter p to display the current parameters, the letter c to change the boot parameters or the @ (at-sign) to continue booting.

```
[Acme Packet Boot]: c
'.' = clear field; '-' = go to previous field; ^D = quit
boot device      : wancom0
```

To navigate through the boot parameters, press Enter and the next parameter appears on the following line.

You can navigate through the entire list this way. To go back to a previous line, type a hyphen (-) and press Enter. Any value that you enter entirely overwrites the existing value and does not append to it.

3. To change a boot parameter, type the new value that you want to use next to the old value. For example, if you want to change the image you are using, type the new filename next to the old one.


```
ORACLE(configure)# bootparam
'.' = clear field; '-' = go to previous field; ^D = quit
boot device      : wancom0
processor number  : 0
host name        : goose
file name        : /code/nnPCz100.bz /code/nnPCz200.bz
```

4. After you have scrolled through the complete list of boot parameters, you return to the boot prompt. To reboot with your changes taking effect, type @ (the at-sign), and press Enter.

```
[Acme Packet Boot]: @
```

The Oracle ECB completes the full booting sequence, unless there is an error in the boot parameters.

If you have configured boot parameters correctly, the system prompt displays and you can go ahead with configuration, management, or monitoring tasks.

 **Note:** If you have configured the boot parameters incorrectly, the Oracle ECB goes into a booting loop and displays an error message.

```
Error loading file: errno = 0x226.
Can't load boot file!!
```

Press the space bar to stop the loop. Correct the error, and reboot your system.

Set Management IP Address

You must manually set your management IP address within the Oracle ECB's boot parameters.

To set your management interface IP, access the boot parameters using a serial console connection within the context of one of the methods described above.

1. Type the letter c (change) to start boot parameter editing.
2. Press Enter until you reach the parameter named **IP Address**.
3. Type in the desired IP address.
4. Press Enter until you reach the end of the boot parameter list.
5. Reboot your Oracle ECB.

After being set, the management interface IP address provides access to your system via telnet, ssh and web GUI.

You can verify the status of this interface using the following command to display the address and status of wancom0.

```
Oracle ECB# show interfaces brief
```

Slr Num	Prt Num	Vlan ID	Interface Name	IP Address	Gateway Address	Adm Stat	Oper Stat
-	-	-	lo	127.0.0.1	-	up	up
-	-	-	wancom0	122.30.204.127/16	-	up	up
0	0	0	M00	122.170.1.200/16	0.0.0.0	up	up

```
Oracle ECB#
```

Format Hard Drive

Manual software installation, performed on virtual and COTs machines, does not include formatting the hard drive automatically. After manual software installation and boot parameter configuration, the user must format the hard drive from the ACLI.

Generic installation documentation may not include the requirement to format the hard-disk. Run the command **format hard-disk** from the Oracle ECB ACLI to create a persistent partition for your /opt directory, within which you can store data needed after a reboot. Perform this procedure the FIRST time you start your Oracle ECB.

Getting the System Operational

Partial output is presented below. Be sure to accept all defaults presented during the format by typing the letter y when prompted.

```
ORACLE# format hard-disk
WARNING: Please ensure device is not currently in use by any applications
before proceeding
Continue [y/n]?: y
The following system partitions will now be created:
1: /opt 8000000 bytes
2: /crash 16218284032 bytes
Create the system partitions and filesystems as configured above [y/n]?: y
```

After the drive(s) are formatted, the system mounts the newly created partitions.

System Image Filename

The system image filename is a name you set for the image. This is also the filename the bootloader uses whenever booting your system. This filename must match the filename specified in the boot parameters. When your image is located on your Oracle ECB, the parameter should start with /boot/ to indicate that the Oracle ECB is booting from it's local /boot directory.

If the filename set in the boot parameters does not point to the image you want sent to the Oracle ECB via SFTP, then you could not only fail to load the appropriate image, but you could also load an image from a different directory or one that is obsolete for your purposes. This results in a boot loop condition that you can fix by stopping the countdown, entering the appropriate filename, and rebooting the Oracle ECB.

Running Setup

Use the Installation Wizard to enable the Web Server, set management access as well as configure high availability and service interface addressing.

To run the Installation Wizard:

1. In Superuser mode, enter run setup and press Enter.

```
ORACLE# run setup
```

The Installation Wizard can also be invoked by the run setup quiet command, which enables a less verbose presentation.

The following displays.

```
-----
Thank you for purchasing the Oracle ECB. The following
short wizard will guide you through the initial set-up.
-----
'?' = Help; '.' = Clear; 'q' = Exit
CONFIGURATION
WARNING: Proceeding with wizard will result in existing configuration
being erased.
Erase config and proceed (yes/no) [no] : yes
```

The wizard issues a Warning stating that using the wizard can overwrite the existing running configuration. While this is true, keep in mind that you can always use the 'q' key to escape the wizard during the initial set-up process. Using this escape mechanism returns you to the ACLI prompt, and makes no changes to the current running configuration. Note also that the installation wizard saves a backup copy of the current running configuration prior to making any configuration changes.

2. Enter yes and press Enter.

```
Configuration will be backed up as
bkup_setup_wizard_Apr__8_13_25_49_632.gz
'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit
HIGH AVAILABILITY
```

This ECB may be a standalone or part of a highly available redundant pair.

Oracle ECB mode

1 - standalone

2 - high availability

Enter choice [1 - standalone] : 1

3. Enter 1 for a standalone server or Enter 2 to configure an HA device, press Enter and go to Step 4 in Setting Up HA Mode - Primary Oracle ECB to complete the installation.

It is highly recommended that you configure high availability (HA) using this Installation Wizard.

Enter choice [1 - standalone] :1

The following displays.

ECB SETTINGS

Unique target name of this ECB [primary] :

4. Enter a unique target name for the NN-ECB (or keep the default in []), and press Enter.

Unique target name of this ECB [primary] :ecb01

The following displays.

IP address on management interface [172.30.200.111] :

5. Enter the IP address to be used for accessing the Web GUI (or keep the default in []), and press Enter.

IP address on management interface : 164.30.85.51

The following displays.

Subnet mask on management interface [255.255.0.0] :

6. Enter subnet mask to be used for accessing the Web GUI (or keep the default in []), and press Enter.

subnet mask on management interface [255.255.0.0] :

The following displays.

Gateway IP address on management interface [164.30.0.1] :

7. Enter the SIP interface IP address (or keep the default in []), and press Enter.

Gateway IP address on management interface [164.30.0.1] :

The following displays.

IP address on SIP interface [] :

8. Enter the IP address to be used for accessing the SIP interface, and press Enter. This step is required; the system does not allow you to proceed without making a setting.

IP address on SIP interface : 172.16.12.12

The following displays.

Subnet mask on SIP interface [255.255.0.0] :

9. Enter subnet mask to be used for accessing the SIP interface (or keep the default in []), and press Enter.

Subnet mask on SIP interface [255.255.0.0] :

The following displays.

Gateway IP address on SIP interface :

10. Enter the gateway IP address and press Enter.

Gateway IP address on SIP interface :172.16.0.1

The following displays.

SETUP TIMEZONE Setup system timezone (yes/no) [yes] :

11. Type your response (yes/no) (or keep the default in []), and press Enter.

SETUP TIMEZONE Setup system timezone (yes/no) [yes] : yes

Getting the System Operational

The following displays.

```
Enter 1-20 to modify, 'd' to display summary, 's' to save, 'q' to exit.[s]:
```

12. Type your response (or keep the default in []), and press Enter.

The following displays.

```
Saving changes and quitting wizard. Are you sure? [y/n]?:
```

13. Type your response (yes/no) (or keep the default in []), and press Enter.

```
SETUP TIMEZONE Setup system timezone (yes/no) [yes] : yes
```

The following displays.

```
=====
Deleting configuration
Erase-Cache received, processing.
waiting 1200 for request to finish
Request to 'ERASE-CACHE' has Finished,
Erase-Cache: Completed
Running timezone setup application
-----
Calling tzselect. Use ^D to cancel without save
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#?
=====
```

14. Type your response, 2 for example and press Enter.

```
=====
The system lists applicable countries, countries in the Americas for example.
=====
```

15. Type your response, 49 for example and press Enter.

The following displays.

```
=====
Enter 1 - 20 to modify, 'd' to display summary, 's' to save, 'q' to exit. [s]:
=====
```

The system lists applicable timezones.

16. Type your response, Eastern Time for example, and press Enter.

The following displays.

```
The following information has been given:
United States
Eastern Time
Therefore TZ='America/New_York' will be used.
```

```
Local time is now: Thu Apr 11 10:13:38 EDT 2013.
Universal Time is now: Thu Apr 11 14:13:38 UTC 2013.
Is the above information OK?
1) Yes
2) No
#?
```

17. Type your response, 1 for example, and press Enter.

The following displays.

```
Timezone=America/New_York

-- Summary view -----

HIGH AVAILABILITY
2 : ECB mode : standalone
3 : ECB role : N/A
4 : Redundancy interface address : N/A
5 : Redundancy subnet mask : N/A

AUTOMATIC CONFIGURATION
6: Acquire config from the Primary (yes/no) : N/A

ECB SETTINGS
7 : Unique target name of this ECB : ecb01
8 : IP address on management interface : 172.30.200.111
9 : Subnet mask on management interface : 255.255.0.0
10 : Gateway IP address on management interface : 172.30.0.1
11: IP address on SIP interface : 172.16.12.12
12: Subnet mask on SIP interface : 255.255.0.0
13: Gateway IP address on SIP interface : 172.16.0.1

PEER CONFIGURATION
14: Peer IP address : N/A
15: Peer target name : N/A

SETUP TIMEZONE
16: Setup system timezone (yes/no) : yes
You may access the GUI via http://172.30.200.111:80/ or continue
using the accli after reboot.
=====
You have completed the Installation Wizard
```

Adding a License with the Setup Wizard

You must obtain a license before you can add it. To obtain a license, you must present the correct system serial number to Oracle for your license to be generated. See the section on Obtaining a License for this information.

Systems that are not licensed run the setup wizard differently from those that are already licensed. Specifically, setup does not proceed unless a license is installed. In such cases, you may find you want to add a license using setup. The steps below provide that procedure. Setup procedures after licensing are documented in the ensuing sections.

1. In Superuser mode, enter run setup and press Enter.

```
ORACLE# run setup
```

If your system is not licensed, the following displays.

```
-----
Thank you for purchasing the
Oracle ECB. The following
short wizard will guide you through the initial set-up.
```

Getting the System Operational

```
-----  
'?' = Help; '.' = Clear; 'q' = Exit  
  
LICENSE  
  
This wizard needs a license to run.  
Enter license (XXX serial number is xxxxx42274873xxx):
```

2. Enter your license and press Enter.
The system checks the license and, if correct, installs it.

```
Attempting to install license ... 100%  
License installed successfully.
```

3. If the license is incorrect, the system tells you. Note the serial number displayed and obtain a working license.

```
Attempting to install license ... Failed to install license  
- 405 (Method Not Allowed) Bad serial number  
Try again, or 'q' to quit the wizard.  
  
Enter license (XXX serial number is xxxxx42274873xxx):
```

Setup skips the license check if it finds a valid license is already installed.

Setting Up System Basics

Before configuring and deploying your Oracle ECB, you might want to establish some basic attributes such as new User and Superuser passwords and system prompt.

New User and Superuser Passwords

ACLI passwords provide access for Telnet, SSH, SFTP and GUI sessions. Common security practices include changing these passwords from their defaults and at intervals defined by your organization. Refer to the ACLI's `secret` command, documented in the *Oracle Communications Session Border Controller ACLI Reference Guide* for information about changing user and superuser passwords.

New System Prompt

You can set the ACLI system prompt using **Configure system** or the **Set boot parameters** Wizard. Change the target name value to make it meaningful within your network. The target name may be up to 38 characters. A value that identifies the system in some way is often helpful.

Initial Configuration

Overview

This chapter provides information about the System Administration configuration procedures, performed with the GUI on the Oracle ECB. These procedures are rarely performed during day-to-day operations. Instead, the system administrator performs many of these procedures as a means of establishing static system operations for which few, if any, changes would be made once the system is deployed and providing service.

Icons grouped under System Administration, but not covered herein include:

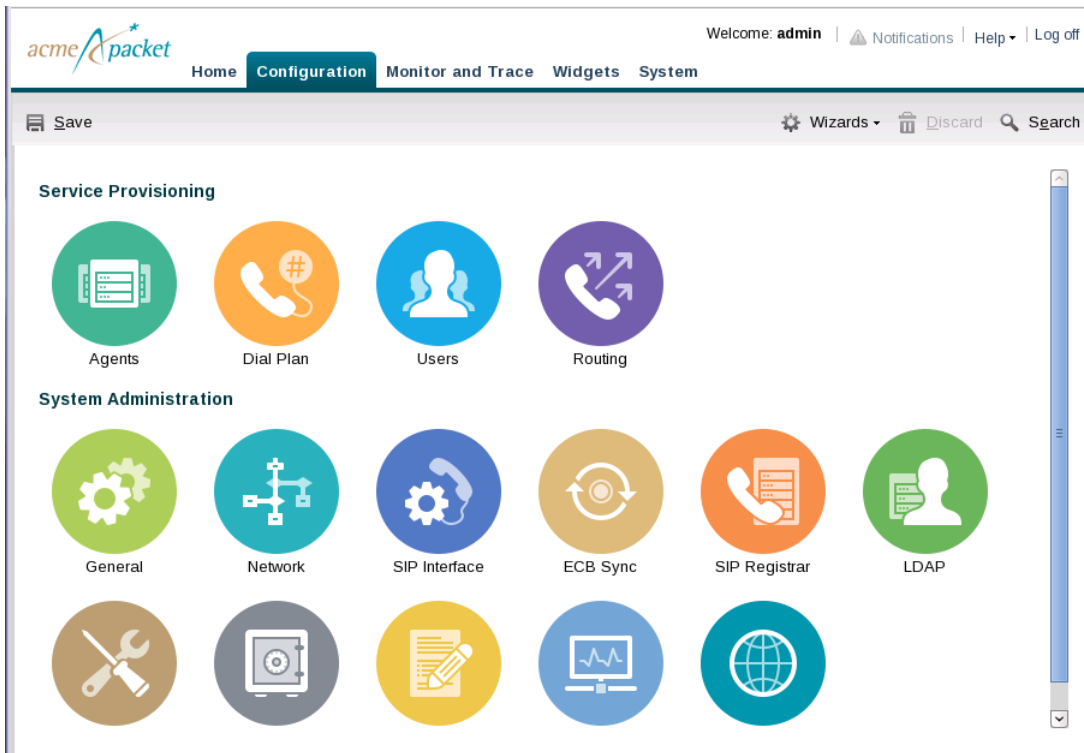
- SIP Registrar
- ECB Sync
- LDAP
- HMR

Although the above are not day-to-day procedures, they are integral to SIP service configuration and operation and require thorough understanding by the user. Refer to the *Oracle Enterprise Communications Broker User's Guide* for both conceptual and instructional information on how to work with these resources. Note that System File Management comprises another set of tasks that overlap between Administrator and User. These tasks are documented in the *Oracle Enterprise Communications Broker User's Guide*.

System Administration

The Oracle ECB GUI collects controls for administering your system under System Administration, which are covered herein. In contrast, The Oracle ECB GUI collects tools used by network architects and service provisioning technicians under Service Provisioning. Service provisioning is the focus of the *Oracle Enterprise Communications Broker User's Guide*.

Regardless, all icons are explained below for context.



Configuration Icons

The table below provides high-level descriptions of the Oracle ECB's Service Provisioning and System Administration controls. Service provisioning controls are shown to provide an overview of these items for system administrators.

Icon	Description
Service Provisioning	This set of icons provides access to the configuration required to deploy service.
Dial Plan	<p>Add multiple dialing-contexts and dial-patterns.</p> <p>Dialing-contexts define the system behavior for calls placed to and from either a corporate or geographic focus.</p> <p>Dialing-contexts include multiple dial-patterns, which define the normalization required to most effectively manage diverse signaling structures.</p>
Agents	<p>Agents - Add agents.</p> <p>An agent is usually a SIP-aware device that serves as a transit target and/or source for signaling managed by the Oracle ECB. Agents are often specified as next-hops for the purposes of routing.</p> <p>Indirect agents, Oracle ECB route termination points that require further routing to reach an end station are also configured here.</p> <p>In addition, configuration used to access ENUM servers is performed here.</p>
Users	Add user and other key phone numbers associated with the enterprise. The user database serves as a directory for phone numbers that need communications services.

Icon	Description
	This database can specify each entry's source context, which can provide a starting point for processing the logic behind a user's call treatment. It also can specify each user's home agent, providing a physical location for routing user's calls.
Routing	Add service routes. Route-entries specify strict paths for signaling traffic, allowing you to specify policy and cost for traffic based on source and/or destination.
System Administration	This set of icons provide access to configuration for which the System Administrator is responsible. This configuration is associated with system operation rather than service provisioning and management.
General	Specify standard system management information parameters. Information includes system identification information, system management information interfaces (SNMP and Syslog) and global service configurations, including Denial of Service and High Availability (system redundancy) configuration.
Network	Specify your service interface. Your signaling interface is separate from your management interface and carries all service traffic. There is only one network interface on the system.
SIP Interface	Add multiple service (SIP) ports. Service interfaces process SIP signaling. The system supports multiple SIP ports, allowing you to segregate traffic based on your own session network's architectural criteria.
Accounting	Configure connections to RADIUS servers to collect call detail records (CDRs) generated by the system. RADIUS provides a protocol for transferring CDRs for billing and troubleshooting purposes.
Security	Configure certificate records and TLS profiles, generate certificate requests, import certificates.
SNMP	Specify SNMP community for allowing access to READ functions and trap receivers.
Web Server	Specify desired web server functionality, including HTTP and/or HTTPS operation. In addition, controls for specifying the applicable TLS profile and inactivity timeout are available. Note that you cannot disable both HTTP and HTTPS operation.
ECB Sync	Provides control over multiple ECB synchronization processes, including defining applicable ECBs and initiating the synchronization.
LDAP	Define servers and server access rules for using an external LDAP database as a source for user authentication and routing procedures.
SIP Registrar	Creates and manages a SIP registrar object on the ECB to offload AOR registration processes from other network elements.

Initial Configuration

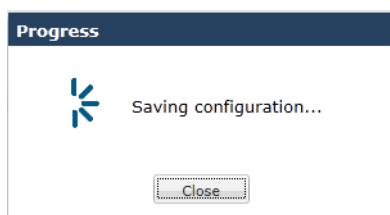
Icon	Description
HMR	Create header manipulation rules, to be assigned to specific agents, that change session service messages for interoperability, policy and other deployment purposes.

Save and Activate

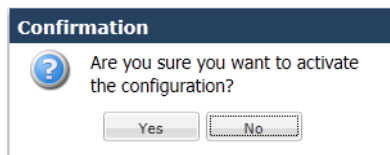
The Web GUI retains configuration changes until you send them to your device or discard them from the GUI. Configuration dialogs include an "OK" button that sends your changes to the device.

Bear in mind that you must also Save, then Activate your changes before your device actually uses your changes. The Save link, appearing as a disc icon towards the top left corner of each Web GUI page, initiates configuration Save and Activate procedures to your system.

When you click Save, the Web GUI either saves the configuration to your device or prevents you from saving invalid data. The system highlights any fields containing invalid data, allowing you to easily find and correct the mistake.



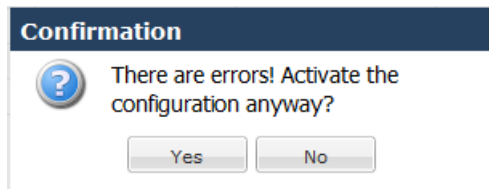
After the save is complete, the Web GUI provides you with a dialog box asking you if you wish to activate this configuration.



You are able to perform the save without activation, if desired. This would be common for configuration changes that need to be activated within a preferred window to avoid any service disruption.

The dialog above defaults to "No", which leaves your changes saved to your system, but not activated. Select No if you want to activate your configuration at a later time. Select Yes to activate. The Web GUI provides a final message box indicating success when it is finished.

The Web GUI also checks your configuration for errors every time you click the Save button, indicating when it finds them prior to activation. When it discovers configuration errors, the system displays the following dialog.



The system displays configuration errors in a list at the bottom of the Web GUI. You can hide and size this error list, an example of which is displayed below. The Web GUI allows you to navigate to the each object in the list by clicking the object in the Object column.

Configuration verify results: Critical:0, Errors:3, Warnings: 0					
Severity	Message	Object	Attribute Name	Other object	Form message
ERROR	tls-profile [SIPInt1] has reference to end-entity-certificate [LocalSer...	tls-profile [SIPInt1]	End entity certificate		ERROR: tls-pr...
ERROR	tls-profile [SIPInt1] has end-entity-certificate records without any en...	tls-profile [SIPInt1]	End entity certificate		ERROR: tls-pr...
ERROR	tls-profile [SIPInt1] has reference to trusted-ca-certificates [Cert1] ...	tls-profile [SIPInt1]	Trusted ca certificates		ERROR: tls-pr...

General Settings

This section explains the fields available for configuration in General Settings, accessed by clicking the General icon. The dialog under the General icon displays fields for configuration as well as collapsed drop down lists for setting the following:

- Logging settings
- SNMP settings
- Denial of service settings
- Communications monitoring probe settings
- High availability settings

Refer to the dialog and control descriptions below to set your system's general settings.

System Settings

The Oracle ECB allows you to specify identification and basic global parameters using the controls under the **General** icon.



Note: By default, clicking the **General** icon displays the Modify System settings dialog with a minimum of controls. This dialog, however, includes drop-down arrow controls below the initial controls that allow you to display and make settings to further categories of controls.

Set the following parameters to configure global system identification information:

1. **Hostname**—Set the primary hostname used to identify the Oracle ECB system. This parameter is used by the software for informational purposes.
2. **Description**—Enter a textual description of the Oracle ECB system. This parameter is used for informational purposes.
3. **Location**—Set a location description field for your Oracle ECB system. This parameter is used for informational purposes. For example, you could include the site name and address of the location where the system chassis is located.
4. **Default gateway IP address**—Set the default gateway for this Oracle ECB. This is the egress gateway for traffic without an explicit destination.
Changing this parameter can cause you to lose connectivity with the Oracle ECB GUI. Be prepared to access the Oracle ECB console if you lose connectivity. See the *Oracle Communications Session Border Controller ACLI Configuration Guide* for instructions on setting default gateway using the ACLI.
5. **Enable restart on critical failure**—When checked, the system attempts to restart after experiencing a failure.
6. **Enable SIP monitoring and tracing**—When checked, the system allows the SIP Monitoring and Tracing tool to collect traffic. Enabling this feature causes Monitor and Trace to capture and display all applicable traffic. See the chapter Oracle ECB User Guide for further information on the SIP Monitoring and Tracing tool.

NTP Servers

You configure NTP servers using the NTP Server listbox in the Modify System settings dialog. The procedure consists of simply clicking the listbox's Add link and entering the address or FQDN of each NTP server in the Add server dialog. The listbox provides you with the option of entering multiple NTP servers from the Add server listbox, as well as selecting existing entries to edit or delete them.

Logging (Syslog)

Logging events is a critical part of diagnosing mis-configurations and optimizing operations. Oracle ECBs can send both syslog and process log data to appropriate hosts for storage and analysis.

Overview

The Oracle ECB 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 per-task basis and are used mainly for debugging purposes. Because process logs are more data inclusive than syslogs, their contents encompass syslog log data when they are sent off box. A special application must be run on a remote server to receive process logs. Please contact your Oracle sales representative directly or calling Oracle Customer support for more information about the process log application.

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

Process Log Messages

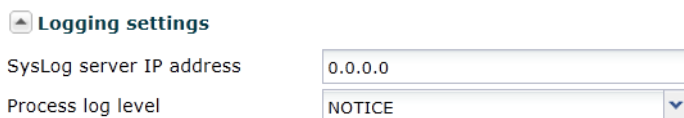
Process log messages are sent as UDP packets in the following format:

```
<file-name>:<log-message>
```

In this format, <file-name> indicates the log filename and <log-message> indicates the full text of the log message as it would appear if it were written to the normal log file.

Syslog Settings

Set the following parameters to configure system-wide Syslog functionality.



Logging settings

SysLog server IP address	0.0.0.0
Process log level	NOTICE

1. Syslog server IP address—Set the IP address of the server to which you are sending syslog messages from the Oracle ECB. Note that Syslog message log level is always **Warning**.
2. Process log level—Set the severity level of the process log messages. Debug is most verbose. Both Debug and Trace can adversely impact system performance; configure these levels temporarily and only when required.
 - Critical (2)
 - Minor (4)
 - Warning (5)
 - Notice (6)
 - Info (7)
 - Trace (8)
 - Debug (9)

SNMP

This section explains how to configure Simple Network Management Protocol (SNMP) basic parameters. 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 a Oracle ECB. These settings are system-wide configurations including MIB contact information, SNMP community settings, and trap receivers.


SNMP community and trap receiver configuration is performed via a separate icon on the GUI. Explanations of those fields is covered later in this document.

Basic SNMP Parameters

The Oracle ECB includes several parameters that control basic SNMP functionality. The MIB-related elements are for informational purposes, and are helpful if set. The remainder of the parameters determines if certain Oracle ECB events are reported to the SNMP system.

SNMP Settings

This section describes the system-wide SNMP parameters found in the System Configuration element. These parameters set global SNMP information.

 **SNMP settings**

MIB system contact	<input type="text"/>
MIB system name	<input type="text"/>
MIB system location	<input type="text"/>
Enable event SNMP traps:	<input type="checkbox"/>

Set the following parameters to configure system-wide SNMP functionality:

1. **MIB system contact**—Set the contact information used within the Oracle ECB's MIB transactions. The SNMP agent sends this information to an 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 Oracle ECB and/or information about how to contact that person.
2. **MIB system name**—Set the identification of this Oracle ECB presented within MIB transactions. This value, along with the target name of the system (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. 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 Oracle ECB returns SNMP communications in the following format:

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

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

3. **MIB system location**—Set the physical location of this Oracle ECB 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.
4. **Enable event SNMP traps**—When this parameter is enabled, the Oracle ECB generates traps with unique trap-IDs for each syslog event. If this parameter is disabled, a single trap-ID is used for all events, with different values in the description string. The default is disabled. The valid values are:
 - enabled | disabled

Communications Monitoring Probe settings

Configuring Communications Monitoring Probe settings allows you to make your Oracle ECB act as a probe, sending network traffic information to an Oracle Communications Session Monitor Mediation Engine.

The Communications Session Monitor is Oracle's Communication Experience Manager. The manager is powered by the Oracle Communications Session Monitor Mediation Engine, a platform that collects SIP, DNS, ENUM, and protocol message traffic received from Oracle Communications Session Monitor 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.

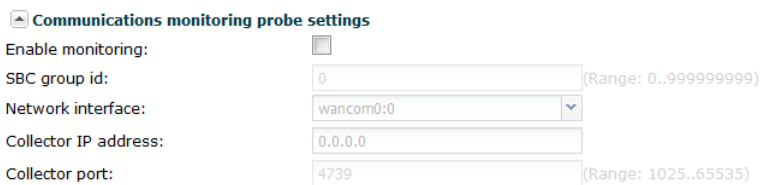
Acting as a Probe, or as an exporter, the Oracle ECB can:

- Establish an authenticated, persistent, reliable TCP connection between itself and one or more Oracle Communications Session Monitor Mediation Engines.

Initial Configuration

- Send UTC-timestamped, unencrypted copy of a protocol messages to the Palladian Engine(s).
- Accompany the copied message with related data to include: the port/vlan on which the message was sent/received, local and remote IP:port information, and the transport layer protocol.

Configure the probe setting fields as described below.



Communications monitoring probe settings

Enable monitoring: ☐

SBC group id: (Range: 0..999999999)

Network interface: ▼

Collector IP address:

Collector port: (Range: 1025..65535)

1. Enable the probe on your Oracle ECB by checking the Enable monitoring checkbox.
2. Set the SBC group id parameter to assign an integer value to the Oracle ECB, in its role as an information exporter.
The Oracle Communications Session Monitor mediation engine uses the SBC group id parameter to segregate probe traffic from multiple probes. Consult the administrators responsible for the Oracle Communications Session Monitor mediation engine to determine the desired setting. The default setting is zero.
3. Set the Network interface parameter to identify the network interface whose traffic will be exported to the Oracle Communications Session Monitor Mediation Engine.
In most cases, the setting should be to M00:0.
4. Set the Collector IP address parameter to specify the IP address of the target Oracle Communications Session Monitor Mediation Engine.
5. Set the Collector port parameter to specify the port number of the target Oracle Communications Session Monitor Mediation Engine.
The range is 1025 to 65535 with the default of 4739.

Denial of Service Settings

DoS protection on the Oracle ECB employs a means of measuring and limiting traffic based on whether the traffic is SIP signaling or ARP. This categorization aligns with queues that logically separate these traffic types, allowing a simple method of specifying limits. The means by which traffic is defined as trusted or untrusted is, in contrast, a complex set of rule that are not configurable via the GUI.

Denial of Service Configuration

Set the following parameters to configure system wide DoS functionality:

1. Click on Denial of service settings to expand the dialog box. The system expands the Modify System settings dialog to display the Denial of service settings.
2. Maximum SIP packet rate—Enter the maximum SIP packet rate, in packets per seconds. Valid values are 20 to 10,000. The default is 1000.
3. Maximum ARP packet rate—Enter the maximum ARP packet rate, in packets per seconds. Valid values are 20 to 10,000. The default is 1000.

High Availability Settings

High availability is best configured using the ACLI's SETUP wizard. If you use setup, you find the HA fields available from the GUI already configured by SETUP.

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

Two Oracle ECBs work together in an HA node, one in active mode and one in standby mode.

- The active Oracle ECB checks itself for internal process and IP connectivity issues. If it detects that it is experiencing certain faults, it hands over its role as the active system to the standby Oracle ECB in the node.

- The standby Oracle ECB is the backup system, fully synchronized with active Oracle ECB's session status. The standby Oracle ECB 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.

Refer to the *Oracle Enterprise Session Border Controller Configuration Guide* for more detail about High Availability operations, including:

- Synchronization
- Checkpointing

Overview

To produce seamless switchovers from one Oracle ECB 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). Sharing addresses eliminates the possibility that the MAC and IPv4 address set on one Oracle ECB in an HA node will be a single point of failure. The standby Oracle ECB sends ARP requests using a utility IPv4 address and its hard-coded MAC addresses to obtain Layer 2 bindings.

When there is a switchover, the standby Oracle ECB issues 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 Oracle ECBs 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 Oracle ECBs communicate with UDP messages sent out and received on the interfaces carrying "heartbeat" traffic between the active and standby devices.

The standby Oracle ECB assumes the active role when:

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

Establishing Active and Standby Roles

Oracle ECBs establish active and standby roles in the following ways.

- If a Oracle ECB boots up and is alone in the network, it is automatically the active system. If you then pair a second Oracle ECB with the first to form an HA node, then the second system to boot up will establish itself as the standby automatically.
- If both Oracle ECBs in the HA node boot up at the same time, they negotiate with each other for the active role. If both systems have perfect health, then the Oracle ECB with the lowest HA interface IPv4 address will become the active Oracle ECB. The Oracle ECB with the higher HA interface IPv4 address will become the standby Oracle ECB.

If the physical link between the two Oracle ECBs fails during boot up or operation, both will attempt to become the active Oracle ECB. In this case, processing will not work properly.

High Availability Configuration

Set the following parameters to configure system wide HA functionality:

1. Click on High availability settings to expand the dialog box. In the Enable high availability field, place a check mark in the box to enable HA on the Oracle ECB.

High availability settings

Enable high availability:



Name of primary peer

Name of secondary peer

Initial Configuration

2. In the Name of primary peer field, enter the name of the primary Oracle ECB peer. Valid values are alpha-numeric characters. Default is <primary peer name>.
3. 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.



Note: Both of these fields are automatically populated with the peer names that you entered when you ran the Installation Wizard.

Network Interface

The network interface element specifies a logical network interface. The Oracle ECB supports only one network interface. You configure a SIP interface and one or more application (SIP) ports over this network interface.

This section explains how to configure a network interface with the GUI. Note that the system initialization procedure creates a network interface. If desired, you can set or change this configuration using the GUI.

Network Interface Configuration

Set the following parameters to configure a network interface.

1. Click the Network icon. The system displays the Modify Network settings dialog.
2. vlan—Enter the identification of a specific virtual interface in a physical interface (e.g., a VLAN tab). If this network interface is not channelized, leave this field blank, and the value will correctly default to 0. The sub-port-id is only required if the operation type is Media. The valid range is:
 - Minimum—0
 - Maximum—4095
3. Network IP address—Enter the IPv4 address of this network interface.
4. Network IP subnet mask—Enter the netmask of this network interface in dotted decimal notation.
5. Network IP gateway address —Enter the gateway that this network interface uses to communicate with the next hop. You can set an additional, secondary gateway via the sec-gateway parameter.
6. DNS server ip address—Enter the IP address of the targeted DNS server.
7. DNS domain—Enter the default domain name.
8. Enable ICMP—See the ensuing section on Enabling ICMP.
9. Enable gateway heartbeat—Within the context of high availability, check this checkbox to allow the network interface to continually confirm that its gateway is reachable.

Enable ICMP

To configure ICMP functionality on a media interface, you define the IPv4 address on your Oracle ECB network interface and enable ICMP. Enabling ICMP entries automatically opens the well-known port associated with a service.

Set the following parameters to enable ICMP functionality on a network interface:

Enable icmp—Check the checkbox to enable ICMP on this network interface.

For security and by default, if ICMP is not enabled, the Oracle ECB discards ICMP requests or responses for the address. It is recommended that you only enable ICMP temporarily on a network interface.

Network Interface High Availability Configuration

Having configured the first parameters on the Modify Network Settings dialog, the high availability setting fields allow you to manually specify addressing to be used by this interface for high availability operation. It is recommended, however, that you use run setup to configure high availability.

1. Click the arrow next to High Availability settings. The system adds the following fields to the Modify Network Settings dialog.

High availability settings

Primary utility IP address	<input type="text"/>
Secondary utility IP address	<input type="text"/>
Interface virtual MAC	<input type="text" value="02:50:56:a6:21:55"/>

2. Primary utility IP address—Enter the utility IPv4 address for the primary HA peer in an HA architecture. This address can be any unused IPv4 address within the subnet defined for the network interface. For example, given a network interface with the IPv4 address 168.0.4.15/24 (identifying the host associated with the network interface), the possible range of unused IPv4 addresses is 168.0.4.1 to 168.0.4.254. Your network administrator will know which IPv4 addresses are available for use.
3. Secondary utility IP address—Enter the utility IPv4 address for the secondary Oracle ECB peer in an HA architecture. Usually, this IPv4 address is the next in the sequence up from the primary utility address. It is also generated from the range of unused IPv4 addresses within the subnet defined for the network interface.

Virtual MAC Addresses

To create an HA node, you create virtual MAC addresses for the media interfaces. You enter these addresses in virtual MAC address parameters for physical interface configurations.

This field is automatically populated with a valid virtual MAC address during run setup. It is recommended that you retain this configuration.

The HA node uses shared virtual MAC (media access control) and virtual IP addresses for the interfaces. When there is a switchover, the standby Oracle ECB sends out an ARP message using the virtual MAC address, establishing that MAC on another physical port within the Ethernet switch.

A MAC address is a hardware address that uniquely identifies Oracle ECB components. Given that, the virtual MAC address you configure allows the HA node to appear as a single system from the perspective of other network devices. To the upstream router, the MAC and IP are still alive, meaning that existing sessions continue uninterrupted through the standby Oracle ECB.

To configure a virtual MAC, enter the virtual MAC address in the Interface virtual MAC field.

SIP Interface Settings

A SIP Interface is an application layer interface logically residing "over" a network interface. The SIP interface defines the transport addresses (IP address and port) upon which the Oracle ECB receives and sends SIP messages. You can define a SIP interface for each network to which the Oracle ECB is connected. Note that these networks must be within the Oracle ECB's Network Interface subnet. SIP interfaces support UDP, TCP and TLS transport.

In addition to defining a SIP interface's network participation (**Port**), you can also define forking and other functionality (**Interface settings**).

SIP Interface Configuration

The Oracle ECB setup program allows you to configure a SIP interface address. You should find that address listed when you open the SIP Interface icon.

1. Maximum SIP message length—The system can constrain outgoing SIP messages to a maximum size in bytes in order to support fraud prevention techniques. If a message does exceed the configured size, it is dropped. Set the maximum SIP message length from 0 to 65535 bytes, with a default value of 4096 bytes.
2. SIP options—The system supports a wide range of optional configuration settings you would enter here. Simply click the Add link, enter the option syntax into the dialog and click the OK or, if you wish to configure multiple options, the Apply/Add Another button.
3. Enable Parallel Forking—Check the checkbox to cause the system to fork all sessions to all of an AOR's contacts.

Initial Configuration

4. Default source context—Set the default source context for this Oracle ECB. This is the context the system uses as source context for a given call if it cannot identify source context via any other method.
5. Click the **Port** link on the left control bar to display the **SIP Ports** list.
6. From the SIP Port list, click the Add link. The system displays the **Add SIP Port Settings** dialog.
7. IP address—Enter the IP address of the host associated with the sip-port entry on which to listen.
8. port—Enter the port number you want to use for this sip-port. The default is 5060. The valid range is:
 - Minimum: 0
 - Maximum: 65535
9. Transport Protocol—Indicate the transport protocol you want to associate with the SIP interface. The default is UDP. The valid values are:
 - TCP—Provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgment with the retransmission of packets when necessary.
 - UDP—Provides a simple message service for transaction-oriented services. Each UDP header carries both a source port identifier and destination port identifier, allowing high-level protocols to target specific applications and services among hosts.
 - TLS—Provides a reliable and encrypted stream delivery.
10. TLS Profile—Select a pre-configured TLS profile from the drop-down list.
11. Save and activate you configuration.

Accounting Settings

The Oracle ECB offers support for RADIUS, an accounting, authentication, and authorization (AAA) system. In general, 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 Oracle ECB to send call accounting information to one or more RADIUS servers. This information can help you to see usage and QoS metrics, monitor traffic, and even troubleshoot your system.

Configuring Accounting

Set the Accounting Configuration parameters in this dialog to indicate where and when you want the system to produce accounting messages.

1. Click the accounting icon. The system displays the Modify Accounting Settings dialog.
2. Enabled—Enable the generation of accounting records by clicking the checkbox or retain the default of disabled.
 - enabled | disabled
3. Generate Start—Retain the default value ok if you want the CDR Start record to be generated once the system receives an OK message in response to an INVITE. (A CDR Start record informs the accounting server that a SIP session has started.) Other values include:
 - None—Start message should not be generated.
 - Invite—Start message should be generated once the Oracle ECB receives a SIP session INVITE.
4. Generate Interim—Retain the default value, Re-invite Response, to cause the Oracle ECB to transmit an Interim message. (An Interim message indicates to the accounting server that the SIP session parameters have changed.) Other values include:
 - OK—Start message is generated when the Oracle ECB receives an OK message in response to an INVITE.
 - Re-invite—Interim message is generated when the Oracle ECB receives a SIP session reINVITE message.
 - Re-invite Cancel—Interim message is generated when the Oracle ECB receives a SIP session reINVITE, and the Reinvite is cancelled before the Oracle ECB responds to it.
 - Unsuccessful-Attempt—Interim message is generated when a SIP session set-up attempt from a preference-ordered list of next-hop destinations is unsuccessful. The interim message contains: the destination IP address, the disconnect reason, a timestamp for the failure, and the number that was called.

5. Enable file output—Enable the system to generate local files containing accounting records by clicking the checkbox or retain the default of disabled.
 - enabled | disabled
6. File Path—Specify where, on the system, you want the system to store accounting record files by typing in a valid path.
7. File rotate time—Set how often in minutes you want to rotate the stored files; the Oracle ECB overwrites the oldest file first. The minimum rotation time is 2 minutes; the default is 60 minutes. This parameter defaults to 0, and leaving it set to the default means that the Oracle ECB does not rotate (or push) the files.
8. Max files—Set the maximum number of files to be stored on the Oracle ECB at one time. You can configure the Oracle ECB to store as few as one file or as many as 4096. The default is 5.

Configure a RADIUS server to send accounting records (optional).

FTP Push

In addition to local and RADIUS server storage, the Oracle ECB provides you with the ability to send accounting files to an FTP server. The information sent to the FTP server is the same as is stored locally.

The FTP push feature is used to copy local CDR files to a remote FTP server on a periodic basis. This feature is configured by defining push receivers which contain standard login and FTP server credentials of the remote machine. At the time interval (file rotate time), the Oracle ECB closes the current file and pushes the files that are complete and have not yet been pushed, including the just-closed file to the FTP server.

Push receiver configurations must include:

- The server's IP address and port
- Remote path of where to upload the accounting files
- Account login credentials

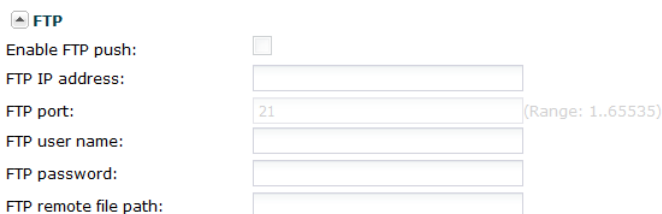
The FTP push configuration creates and pushes accounting files using the following criteria:

- The maximum accounting file size, after which the system creates a new file, is 1000000 bytes.
- The number of files the system creates before it begins to overwrite files (oldest file first) is 5.
- The amount of time between system file push to the FTP server is 60 minutes.

FTP Push Configuration

This configuration assumes a reachable, operating FTP server.

A push receiver configuration includes all the credentials that the Oracle ECB needs to log into an FTP server and upload any recent local CDR files. To configure an FTP push server, click the FTP arrow on the Accounting configuration dialog to display the FTP push fields.



FTP

Enable FTP push: ☐

FTP IP address:

FTP port: (Range: 1..65535)

FTP user name:

FTP password:

FTP remote file path:

1. Enable FTP push —Check the checkbox to enable FTP push.
2. FTP-address—Set the IP address of this STP server.
3. FTP-port—Set the port of this service:
 - Minimum: 0
 - Maximum: 65535
 - Default: 21

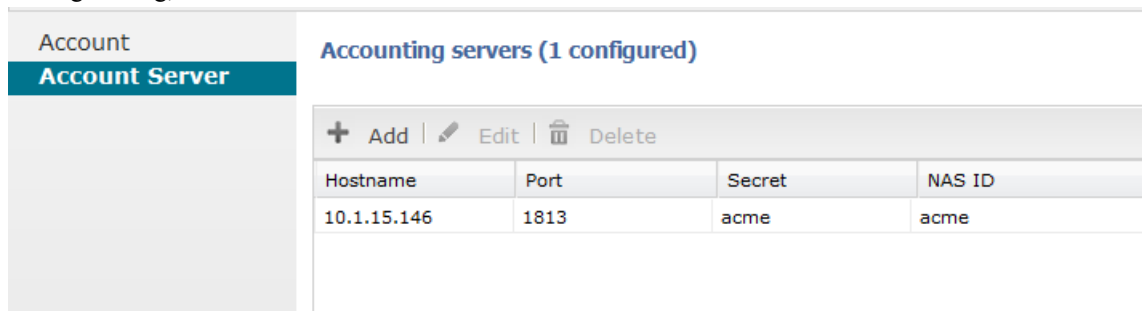
Initial Configuration

4. FTP-user—Set the username you must use to login to this FTP server.
5. FTP-password—Set the password you must use to login to this FTP server.
6. FTP-remote-path—Set the path on this FTP server on which you want to save your accounting files.

Configuring a RADIUS Account Server

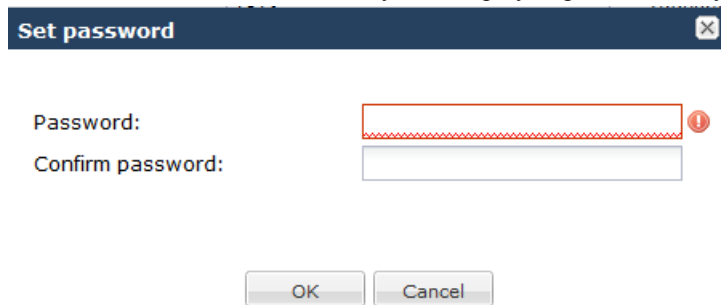
The following procedure is required to provide accounting detail to a RADIUS server.

1. Click the Accounting tab, followed by the Account Server link. The system displays the Add Accounting Server Settings dialog, shown below.



Accounting servers (1 configured)			
+ Add Edit Delete			
Hostname	Port	Secret	NAS ID
10.1.15.146	1813	acme	acme

2. Click the Add link to add a new server to your list. You can also edit and delete existing servers from links on this dialog.
3. Hostname—Name of the host associated with the account server in hostname format (FQDN) or as an IP address.
4. Port—Retain the default 1813 or enter the number of the UDP port associated with the account server to which RADIUS messages are sent.
 - Minimum: 1025
 - Maximum: 65535
5. Secret—Click the set button. The system displays a password entry and confirm dialog, shown below.



Enter and then confirm the secret passed from the account server to the client in text format. Transactions between the client and the RADIUS server are authenticated by the shared secret; which is determined by the source IPv4 address of the received packet. You can set or cancel this setting from this dialog using the OK and Cancel buttons respectively.

6. NAS ID—Enter the NAS ID in text format (FQDN allowed). The account server uses this value to identify the Oracle ECB for the transmittal of accounting messages. (Optional)
The remote server to which the account configuration sends messages uses at least one of two potential pieces of information for purposes of identification. The Oracle ECB accounting messages always includes in the first of these:
 - Network Access Server (NAS) IP address (the IP address of the Oracle ECB's SIP proxy)
 - NAS ID (the second piece of information) provided by this value. If you enter a value here, the NAS ID is sent to the remote server.

If you have more than one Oracle ECB pointing to the same account server, the NAS ID can be used to identify which Oracle ECB generated the record.

Security Settings

Security configuration from the GUI consists of creating the building blocks you can use to establish TLS-secured paths for your signaling traffic. The overall process includes generating certificate requests and certificate import.

The TLS configuration procedures that you can perform from the GUI includes:

- Configure Certificate Records.
- Generate Certificate Request for your CA.
- Import Certificates.
- Upload certificate files.
- Download certificate files.
- Configure TLS Profiles, which utilize your certificate records.
- Apply TLS Profiles to SIP Interfaces, agents and the web-server-config.

The dialogs available from the Security icon allow you to perform all procedures with the exception of applying a TLS profile to a configuration element. You apply TLS profiles to configuration elements using controls within their respective dialogs.

Certificate Record Configuration

A certificate record configuration represents either the end-entity or the Certificate Authority (CA) certificate on the Oracle ECB. If it is used to present an end-entity certificate, a private key should be associated with this certificate record configuration using a certificate request. No private key should be associated with the certificate record configuration if it was issued to hold a CA certificate.

A certificate can be imported to a certificate record configuration using the GUI as described below.



Note: There is no need to create a certificate record when importing a CA certificate or certificate in pkcs12 format.

Follow the steps below to create a certificate record.

1. Access certificate configuration controls via the Security link.
2. Click the link indicating **Certificate** configuration. The system displays the list of certificate records already configured on this system.
3. Click the **Add** link. The system displays the Add Certificates dialog. Note that this dialog is truncated for presentation purposes here.
4. name—Enter the name of the certificate record. This parameter is required; you cannot leave it empty.
In the case of establishing a certificate for the Oracle ECB, this name must be the same as the name you use to generate a certificate request.
If configuring for an end stations CA certificate (mutual authentication), this name must be the same name used during the import procedure. When performing an import procedure that creates the record automatically, this name will be derived from the certificate itself.
5. country—Enter the name of the country. The default is US.
6. state—Enter the name of the state. The default is MA.
7. locality—Enter the name of the locality for the state. The default is Burlington.
8. organization—Enter the name of the organization holding the certificate. The default is engineering.
9. unit—Enter the name of the unit within the organization holding the certificate.
10. common-name—Enter the common name for the certificate record.
11. key-size—Enter the size of the key for the certificate. Use the default of 1024, or change it to one of the other supported values: 512, 2048, or 4096.
12. alternate-name—Enter the alternate name of the certificate holder.
13. key-usage-list—Enter the usage extensions you want to use with this certificate record. This parameter can be configured with multiple values, and it defaults to the combination of digitalSignature and keyEncipherment. For

Initial Configuration

a list of possible values and their descriptions, see the section “Key Usage Control” in the *Oracle Communications Session Border Controller Configuration Guide*.

14. **extended-key-usage-list**—Enter the extended key usage extensions you want to use with this certificate record. The default is `serverAuth`. For a list of possible values and their descriptions, see the section “Key Usage Control” in the *Oracle Communications Session Border Controller Configuration Guide*.

Create TLS profiles, using your certificate records to further define the encryption behavior and provide an entity that you can apply to a SIP interface.

TLS Profile Configuration

Certificate records must exist prior to this configuration.

Configure a TLS profile to further define the encryption behavior you want between these systems and to establish an entity that you can apply to SIP Interfaces. Steps required follow.

1. Click the TLS Profile link. The system displays the TLS profile list.
2. Click the Add link. The system displays the dialog below, which is truncated for the purpose of presentation here.
3. **Name**—Enter the name of the TLS profile. This parameter is required.
4. **end-entity-certificate**—Enter the name of the Certificate Record for the applicable entity.
5. **trusted-ca-certificates**—Enter the names of the trusted CA certificate records.
6. **cipher-list**—The following cipher-lists are supported for the GUI only:
 - AES256-SHA (TLS_RSA_WITH_AES_256_CBC_SHA) - Firefox (version 12) and Chrome (version 19.0.1084.46m)
 - AES128-SHA (TLS_RSA_WITH_AES_128_CBC_SHA) - Firefox (version 12) and Chrome (version 19.0.1084.46m)
 - DES-CBC-SHA (SSL_RSA_WITH_DES_CBC_SHA or TLS_RSA_WITH_DES_CBC_SHA) - Internet Explorer (Version 9)
7. **verify-depth**—Specify the maximum depth of the certificate chain that will be verified. The default value is 10. The valid range is:
 - Minimum-0
 - Maximum-10
8. **mutual-authenticate**—Define whether or not you want the Oracle ECB to mutually authenticate the client. The default value is disabled. The valid values are:
 - enabled-disabled (default)
9. **tls-version**—Enter the TLS version you want to use with this TLS profile. Default is compatibility. Valid values are:
 - TLSv1
 - SSLv3
 - compatibility (default)
10. **cert-status-check**—Enables OCSP in conjunction with an existing TLS profile.
11. **cert-status-profile-list**—Assigns one or more cert-status-profiles to the current TLS profile. Each assigned cert-status-profile provides the information needed to access a single OCSP responder.
12. **ignore-dead-responder**—Enables your device to establish a client connection even if the OCSP responder is unavailable, assuming the associated certificate was signed by a trusted certificate authority.
 - enabled-disabled (default)
13. **allow-self-signed-cert**—Enables your device to establish client connections to clients that present self-signed certificates.
 - enabled-disabled (default)

Apply your TLS profile to a SIP Interface by selecting it from the SIP Interface's TLS Profile drop-down.

Generating a Certificate Request from the GUI

To operate with a certificate authorized by a CA, you provide a certificate request to that CA. To do this, you create a certificate record and generate the request from this record.

You can generate a certificate request using the CLI or the GUI. This procedure provides the steps you use on the GUI.

1. Highlight the certificate record you created for the purposes of containing your device's certificate.

certificate-record (1 configured)

Add	Edit	Copy	Delete	Generate certificate	Import certificate
Name	Country	State	Locality	Organization	Unit
test	US	MA	Burlington	Engineering	

2. Click the Generate certificate link.

The system creates the request and presents it to you in a dialog.



3. Copy the information from the dialog and send to your CA as a text file.

When the CA replies with the certificate for your device, import this certificate to the device against the same certificate record. This allows end stations to establish TLS paths within either server or mutual authentication scenarios.

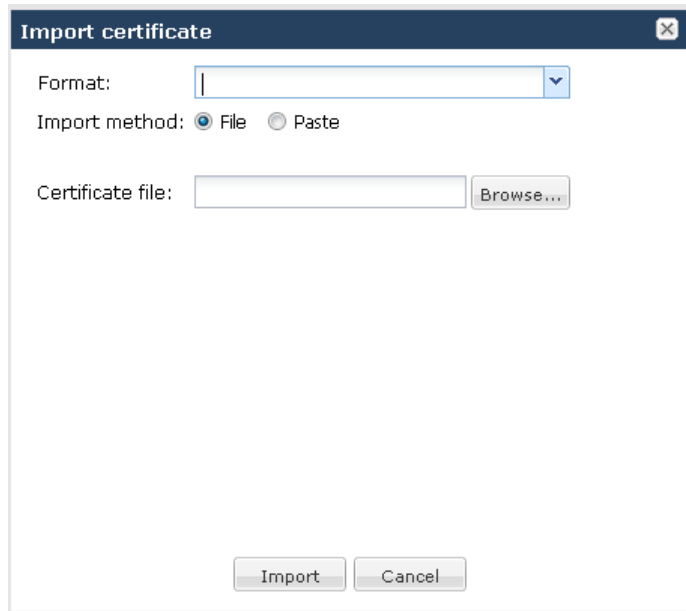
Importing Certificates

Use this procedure to import both your device certificate and end station CA certificates for mutual authentication scenarios. Recall that you must import your Oracle ECB certificate against the certificate record you created for your Oracle ECB. End station CA certificates may or may not need to be imported against a pre-configured certificate record.

1. If applicable, highlight the certificate record for which this certificate applies.
2. Click the Import certificate link.
The system responds with a dialog from which you can either import the certificate file directly or paste the contents of the certificate.
3. Select the Format of the certificate from the drop down list. Options include:
 - pkcs7
 - x509
 - Try-all, which attempts to import via all possible formats until it is able to import the certificate.

Initial Configuration

4. Either browse to and select the certificate file, or click the paste button to change the dialog to its "paste format". This "paste format" provides a text field into which you paste your certificate information

A screenshot of a software dialog box titled "Import certificate". The dialog has a dark blue header bar with a close button (X) in the top right corner. Below the header, there are three main sections. The first section is labeled "Format:" and contains a dropdown menu. The second section is labeled "Import method:" and contains two radio buttons: "File" (which is selected) and "Paste". The third section is labeled "Certificate file:" and contains a text input field followed by a "Browse..." button. At the bottom of the dialog, there are two buttons: "Import" and "Cancel".

5. Click the Import button.
The system completes the procedure by importing the certificate.
Apply the operational certificate record to the intended SIP interface.

SNMP

This section explains how to configure Simple Network Management Protocol (SNMP) communities and trap receivers. These features are not essential for baseline Oracle ECB service, but they are necessary to use an element management system to manage Oracle ECBs. They provide important monitoring and system health information that contribute to a robust deployment of the Oracle ECB.

Overview

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 a Oracle ECB. These settings are system-wide configurations including MIB contact information, SNMP community settings, and trap receivers.

Basic SNMP Parameters

The Oracle ECB includes several parameters that control basic SNMP functionality. The MIB-related elements are for informational purposes, and are helpful if set. The remainder of the parameters determines if certain Oracle ECB events are reported to the SNMP system.

SNMP Community

An SNMP community is a grouping of network devices and management stations used to define where information is sent and accepted. An SNMP device or agent might belong to more than one SNMP community. SNMP communities provide a type of password protection for viewing and setting management information within a community.

SNMP communities also include access level settings. They are used to define the access rights associated with a specific SNMP community. The Oracle ECB lets you define two types of access levels: read-only and read-write. You can define multiple SNMP communities on a Oracle ECB to segregate access modes per community and NMS host.

Trap Receivers

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

Each server that an element management system is installed on should be configured as a trap receiver on all Oracle ECB's managed by that element management system.

SNMP Community Settings

Follow the steps below to configure an SNMP community on your device.

1. Community name—Enter an SNMP community name of an active community where this Oracle ECB 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 Oracle ECB. 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.
2. From the SNMP community list, click the Add link. The system displays the Add dialog.
3. IP addresses—Enter an IPv4 address that is valid within this SNMP community. This IPv4 address corresponds with the IPv4 address of the NMS application that monitors or configures this Oracle ECB. You can enter multiple addresses, if desired.
4. Click OK to close the Add dialog.

Trap Receiver Settings

Follow the steps below to configure trap receivers on your device.

1. From the Trap receiver list, click the Add link. The system displays the Add SNMP Trap Settings dialog.

2. Community name—Enter the SNMP community name to which this trap receiver belongs. For example, Public. Valid values are alpha-numeric characters. Default is blank.
3. IP address—Enter the IPv4 address of an authorized NMS. This value is the IPv4 address of an NMS where traps are sent. Enter the IP address in dotted decimal format.
4. IP Port—Enter the port number of an authorized NMS. If you do not specify a port number, the default SNMP trap port of 162 is used.

Web Server Settings

Configure your preferences for the Oracle ECB's web server using the Modify web-server-config dialog, available from the Web Server icon. Configuration field descriptions are provided below.

1. Inactivity timeout—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 Oracle ECB. You can edit these parameters if required.

Initial Configuration

2. HTTP state—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.
3. HTTPS state—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.
4. TLS profile—Enter the Transport Layer Security (TLS) Protocol profile name to use with HTTPS. Valid values are alpha-numeric characters. Default is blank.



Note: If you specify a TLS profile, and HTTP is enabled, the Oracle ECB checks against the TLS profile table for a match. If there is no match, the applicable errors display during the verification of the configuration.

5. Click OK.

Oracle ECB Maintenance and Debugging

Oracle ECB software closely aligns with Oracle SBC software. As such, the vast majority of reference and debugging processes, procedures and information is common across Oracle SBC product.

This chapter documents maintenance and debugging information that is specific to the Oracle ECB as well as points to other members of the documentation set that provide applicable reference and debugging information.

Generic Maintenance and Debugging Documentation

The following table directs you to other Oracle documentation that provides generic monitoring and debugging information.

Information Type	Documentation
Log File Definition and Descriptions Fault Information Management Manual Configuration Management Process and Procedures	Oracle SBC Maintenance and Troubleshooting Guide
MIB Descriptions MIB Definition and Identification (OID Reference) SNMP GETs SNMP Trap Definition and Descriptions	Oracle SBC MIB Reference Guide
Manual HDR Management HDR Group Definition and Descriptions	Oracle SBC Historical Data Recording (HDR) Resource Guide

Your Oracle ECB Image

Your Oracle ECB arrives with the most recent, manufacturing-approved run-time image installed on the flash memory. If you want to use this image, you can install your Oracle ECB, establish a connection to the Oracle ECB, and then begin to configure it. On boot up, your system displays information about certain configurations not being present. You can dismiss these displays and begin configuring your Oracle ECB.

If you want to use an image other than the one installed on your Oracle ECB when it arrives, you can use the information in this section to obtain and install it.

Obtaining a New Image

You can download software images onto the platform of your Oracle ECB from various sources. You can take any one of the following actions:

- Obtain an image from where the Oracle Software Delivery Cloud.
- Obtain an image from your Oracle customer support representative, who will transfer it to your system.

Regardless of how you obtain the image, you need to use Secure File Transfer Protocol (SFTP) to copy it from its source to your Oracle ECB.

Upgrade Software with the GUI

Previously, software upgrade was a manual process consisting of file transfer tools and ACLI procedures. Release E-C[xz]6.4.0 M2 now allows you to upgrade software directly from the GUI.

You can upgrade (or downgrade) the software on your system from the GUI's System tab. The function is found via the Upgrade Software link. It performs the following tasks for you:

For standalone system upgrade:

- System Health Score Display
- System Disk Space Check
- Display Current CFG Version
- Display Current Running Version
- File Transfer from Local System
- Change Boot Parameters
- System Reboot

For High Availability configuration upgrade, the system displays the synchronization health.

This procedure assumes SFTP access between your device the source of your new software. Follow the steps below to perform a software upgrade:

1. Click the System tab.
The system opens the System dialog.
2. Click the Upgrade Software link.
The system displays the upgrade software dialog.
3. Open the Verification menu.

The system displays the current system health and links from which you can assess synchronization health, current configuration version and disk usage.

4. Verify that system health, synchronization health, current configuration version and disk usage are appropriate and adequate for you to proceed with your upgrade.
5. Select the Upload method from the drop-down box. Options include.
 - Local - Allows you to select a file from your system for transfer.
 - Flash - Allows you to select a file already on the device.
 - Network - Allows you to specify parameters for network boot via file transfer. These parameters initially display the current boot parameters.

The system updates the Upgrade Software dialog with the fields you need for your selection.

6. Complete the fields, specific to your current upgrade.
 - Software file to upload - (Local) Use the Browse button to locate the file on your local system.
 - Software file - (Flash) the location and name of the file on the device.
 - Boot file - (Network) The complete name of the boot file.
 - Host IP - (Network) The IP address of the FTP server.
 - FTP username - (Network) The username to log into the FTP server.
 - FTP password - (Network) The password to log into the FTP server.
7. Click the Reboot after upload checkbox, if desired.
8. Click the Complete button.

If you did not check the Reboot after upload checkbox, the system displays an information dialog indicating that the it needs to reboot for changes to take effect. If you did check the Reboot after upload checkbox, the system displays an information dialog indicating that it is about to reboot.
9. Click OK.

The system performs the file transfer or boot parameter change and, if selected, reboots.

