Installing Avaya Session Border Controller for Enterprise

Release 6.2
Issue 3
June 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information

regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

About this book

This book documents how to physically install the equipment chassis for Avaya Session Border Controller for Enterprise (Avaya SBCE) into a Session Initiation Protocol (SIP) enterprise VoIP network and run the preliminary provisioning processes.

Note:

This document contains hardware-related installation information only. See the Avaya SBCE Administration Guide for information and procedures related to the configuration and administration of Avaya SBCE security products using the Element Management System (EMS).

Note:

Before proceeding with the installation or maintenance of this equipment, please refer to important information included in the accompanying End-User License Agreement.

Note:

This note applies only to the new platform for Avaya SBCE.

Any reference to ports A1, A2, B1, or B2 in the documentation or in the software application graphical user interface (GUI) screens used for configuration or administration correlate to Data Ports 1,2,3, and 4, respectively. And any reference to ports M1 or M2 correlate to Management Ports 1 and 2, respectively.

Intended audience

This document is intended for enterprise network personnel who are responsible for maintaining the VoIP network hardware and the installation and integration of new equipment.

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Title	Description	Audience
Avaya Session Border Controller for Enterprise Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBCE.	Sales Engineers, Solution Architects and Implementation Engineers
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading: • software only from Sipera 4.0.5 to Avaya SBCE 6.2 • Avaya Aura® Session Border Controller6.0 to Avaya SBCE 6.2	Implementation Engineers
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation Engineers, Administrators

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Hardware overview

About the servers

The Avaya SBCE servers are fully–integrated, user-installable chassis.

- The Portwell CAD-0208 is a compact server that is configured as a standalone SBCE.
- The standard Dell R210–ii server is configured as an SBCE core.
- The Dell R210–ii XL server has two configurations, one as an EMS and one as an SBCE core.
- The AMAX EMS server is equipped with an Intel™-based Supermicro™ PDSMI+ motherboard, two Gigabit Ethernet (GbE) network interfaces, a high-speed serial port, four (4) hard disk drive (HDD) bays, and one (1) CD-ROM bay.

Panel descriptions

Front panel (Dell R210–ii, Dell R210–ii XL)

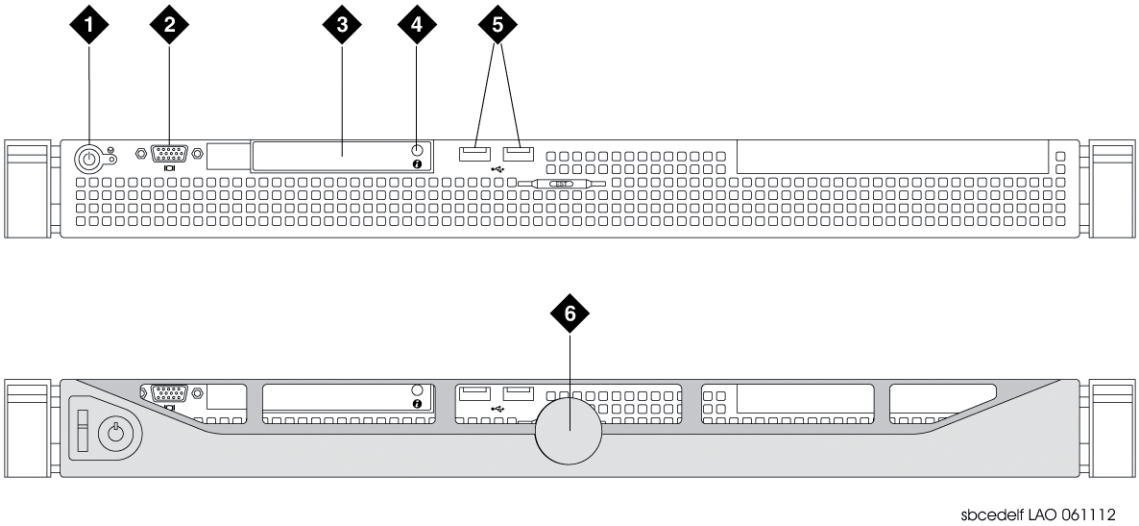


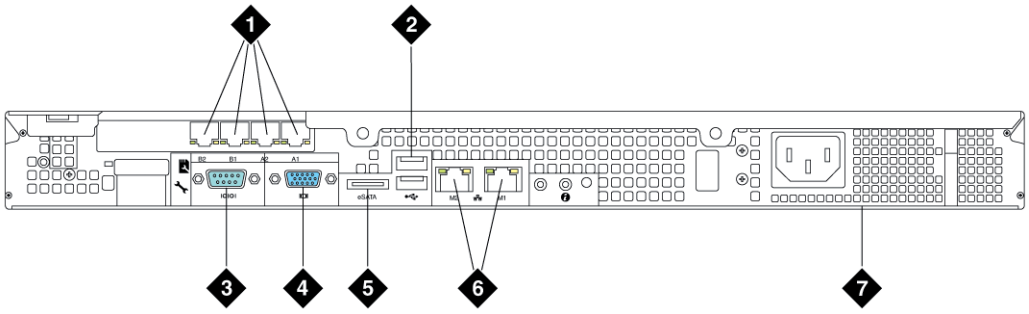
Figure 1:

Component	Number / Icon	Description
Power-on indicator, power button	1 ⏻	The power button turns system power off and on. **Note:** If you turn off the system using the power button and the system is running an ACPI-compliant operating system, the system can perform an orderly shutdown before power is turned off. If the power button is pressed for more than 4 seconds, the system power will turn off regardless of the current operating system state. If the system is not running an ACPI-

Component	Number / Icon	Description
		compliant operating system, power is turned off immediately after the power button is pressed. The power button is enabled in the System Setup program. When disabled, the button can only turn the system power on. The power-on indicator lights or blinks to indicate the status of power to the system. The power-on indicator lights when the system is on. The indicator is off when the system is off and power is disconnected from the system. The indicator blinks when the system is on but in standby state, or when the system is off but is still connected to the power source. Briefly pressing the power button exits the standby state.
NMI Button		The NMI button is used to troubleshoot software and device driver errors when using certain operating systems. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel or by the operating system's documentation.
Video connector	2	Connects a monitor to the system.
Diagnostic indicators (4)	3	The diagnostic indicators aid in diagnosing and troubleshooting the system.
Hard-drive activity indicator		The green hard-drive activity indicator flashes when the hard drives are in use.

Component	Number / Icon	Description
System status indicator	4	The blue system status indicator lights up during normal system operation. The amber system status indicator flashes when the system needs attention due to a system problem.
System identification button		You can use the system identification buttons on the front and back panels to locate a particular system within a rack. When one of these buttons is pushed, the blue system status indicators on the front and back panels blink until one of the buttons is pushed again. You can also use the systems management software to cause the indicators to flash to identify a particular system.
USB connectors (2)	5	Connect USB 2.0-compliant devices to the system
Bezel (panel cover)	6	Protects front panel.

Rear panel (Dell R210–ii, Dell R210–ii XL)



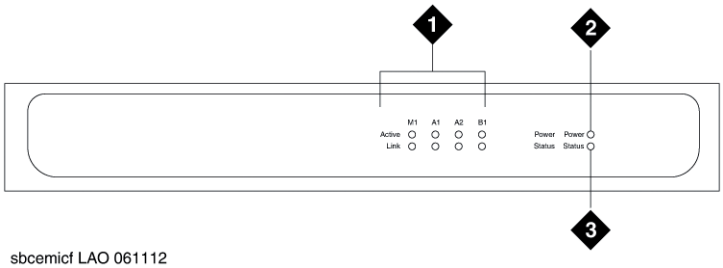
sbcedelb LAO 061112

Figure 2:

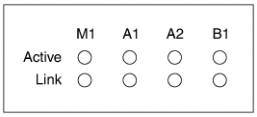
Number	Description
1	4X 100/1000 Ethernet Ports (PCI Card) Used for data network

	Note: A blank plate is in the place of these ports on the EMS configuration of the Dell R210–ii XL.
2	Two (2) USB ports, used for installation only
3	Serial Port used for Command Line Interface
4	VGA Port (not used)
5	E-SATA Port (not used)
6	Two (2) 100/1000 Ethernet ports, used for management interface
7	Non-Redundant Power Supply

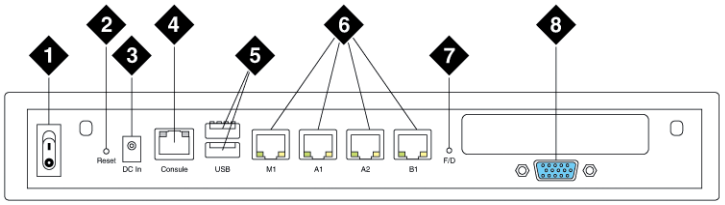
Front panel (Portwell CAD-0208)



sbcemicf LAO 061112

Number	Component	Description
1	Power LED (D2) power indicator and hard-disk-drive (HDD) activity indicator	This is the By-Pass indicator LED. **Note:** This feature is currently not supported.
2	Status LED (D2)	This LED is illuminated when power to the unit is turned on and it flashes to indicate hard-disk-drive activity.
3	Network Activity LEDs (D7, D6, D5, and D4)	These are the four pairs of Active/Link LEDs (labeled M1, A1, A2, and B1 for D7, D6, D5, and D4, respectively). 

Rear panel (Portwell CAD-0208)

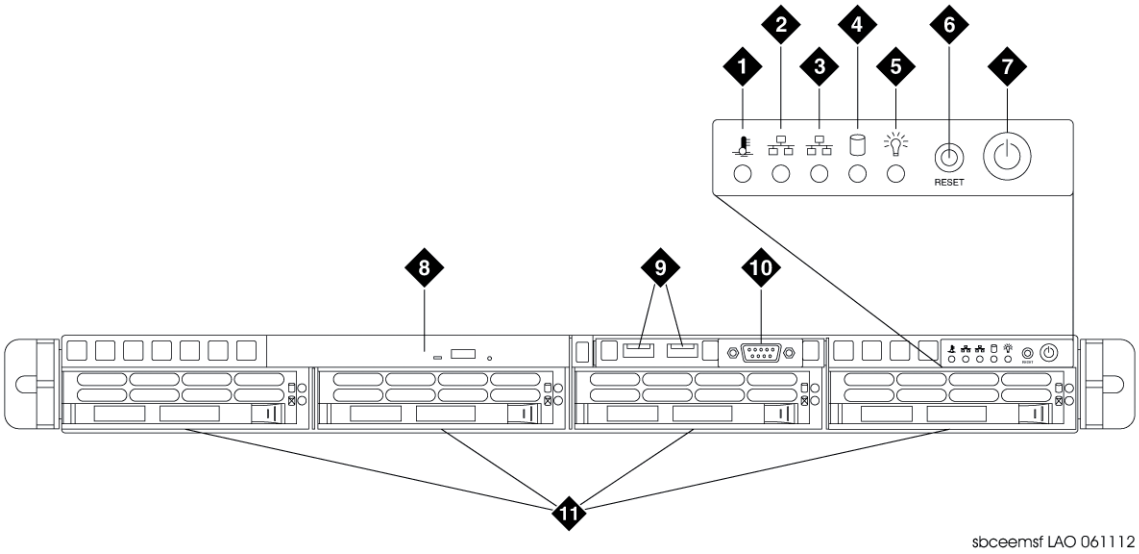


sbcemicr LAO 061112

Number	Component	Description
1	Power On/Off Switch	The Power On/Off switch turns system power on and off, and doubles as a hard disk activity indicator. The Power LED (D2, Feature 9) is illuminated when the system is on. The Power-On indicator is not illuminated when the system is turned off and the power is disconnected from the system. The Power-On indicator also blinks when there is hard disk drive activity. **Note:** If you turn off the system using the Power On/Off switch and the system is running an ACPI-compliant operating system, the system can perform an orderly shutdown before power is turned off. If the system is not running an ACPI-compliant operating system, power is turned off immediately after the Power On/Off switch is moved to the Off position. The Power On/Off switch is enabled in the System Setup program. When disabled, the switch can only turn the system power on. Moving the Power On/Off switch to the On position illuminates the Power LED (D2, Feature 9) to indicate that power is applied to the system. The Power LED is located on the Front Panel in the right-most position above the Status indicator (D3).
2	Reset Button (SW2)	This is the system reset button. This button is recessed, and can be pressed using the end of a paper clip. Use

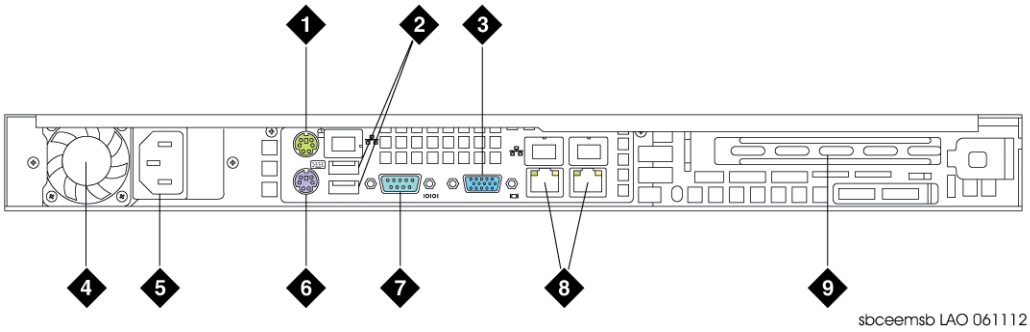
		this button only if directed to do so by qualified support personnel or by the product documentation.
3	DC In Jack (J18)	This is the DC Power Jack (15V).
4	Console Port (J17)	This is a standard Ethernet RJ-45 connector jack for use in connecting a system console.
5	USB connectors (2 ea., J12A and J12B)	Connects USB 2.0-compliant devices to the system.
6	Network Ports (4 ea., J13, J14, J15, and J16)	These are standard Ethernet RJ-45 connector jacks (labeled M1, A1, A2, and B1 for J13, J14, J15, and J16, respectively) for use in connecting to the network.
7	F/D Button (SW1)	This is the Factory Defaults (F/D) reset button that is normally used to reset the device to its original factory default settings. **Note:** This feature is currently not supported.
8	VGA Connector (J2)	This is a standard 15-pin female video graphics adapter (VGA) connector used for connecting a monitor to the system.

Front panel (AMAX EMS)



Number	Description
1	Over Temperature Indicator
2	LAN 2 Indicator
3	LAN 1 Indicator
4	Hard Disk Drive Access Indicator
5	Power On Indicator
6	Hardware Reset Switch
7	Power On Switch
8	CD ROM Drive (Optional)
9	USB Ports
10	Serial Port (not used)
11	Four (4) Hot-Swappable SCA Hard Disk Drive Slots

Rear panel (AMAX EMS)



Number	Description
1	PS2 Mouse
2	USB Ports (2)
3	VGA Output
4	Cooling Fan
5	Power Receptacle
6	Keyboard Port
7	Serial COM Port
8	32–bit GbE Ports (LAN 1 left, LAN 2 right)
9	PCI Slot Plate (PCI not used)

Specifications

Processors

Server	Processors
Dell R210–ii XL (core)	Intel Xeon E3-1220 3.10 GHz Quad Core/4T
Dell R210–ii (core)	Intel Xeon E3-1230 3.20 GHz Quad Core/4T
Dell R210–ii XL (EMS)	Intel Pentium G850 2.90 GHz – Dual Core/2T

AMAX (EMS)	Intel Core 2 Duo E6400 2.13 GHz – Dual Core
Portwell CAD-0208 (core)	Intel® Atom D510 1.66GHz - Dual Core

System memory

Server	System Memory
Dell R210–ii XL (core)	4 GB (DDR3 1333MHz)
Dell R210–ii (core)	4 GB (DDR3 1333MHz)
Dell R210–ii XL (EMS)	2 GB (DDR3 1333MHz)
AMAX (EMS)	2 GB (DDR2 667MHz)
Portwell CAD-0208 (core)	2GB (SO-DIMM DDR2 667MHz)

On-board storage

Server	On-board Storage
Dell R210–ii XL (core)	500 GB (3.5-in SATA 3Gb/s – 7.2K)
Dell R210–ii (core)	500 GB (3.5-in SATA 3Gb/s – 7.2K)
Dell R210–ii XL (EMS)	2 x 500 GB (3.5-in SATA 3Gb/s – 7.2K) Hardware RAID 1 (always active)
AMAX (EMS)	2 x 160 GB (3.5-in SATA 3Gb/s – 7.2K)
Portwell CAD-0208 (core)	320GB (2.5-in SATA 3Gb/s – 7.2K)

Interfaces

Dell R210–ii (core) & Dell R210–ii XL (core)

- Rear-accessible PCI-Express Gigabit Ethernet (GbE) ports (RJ-45 connectors)

Port	Interface
A1	(eth3)
A2	(eth2)

Port	Interface
B1	(eth1)
B2	(eth0)

Note:

A1 ports are used for internal and B1 ports are used for external.

- Rear-accessible 32-bit GbE ports

Port	Interface
M1	(eth5) Management
M2	(eth4) HA link

Note:

To prevent possible routing problems, the Management interfaces (M1) and (M2) should be configured on different subnets than the subnets assigned to the Data interfaces (A1/A2) and (B1/B2).

- One rear-accessible DB9 serial port for system console
- One rear-accessible eSATA port (not supported with this model)
- One front and rear-accessible VGA for system monitor (not supported with this model)
- Two front-accessible USB 2.0 ports
- Two rear-accessible USB 2.0 ports

Dell R210–ii XL (EMS)

- Rear-accessible 32-bit GbE

Port	Interface
Gb1 (left)	(eth0) Management
Gb2 (right)	(eth1) Not used

- One rear-accessible DB9 serial port for system console
- One rear-accessible eSATA port (not supported with this model)
- One front and rear-accessible VGA for system monitor (not supported with this model)
- One rear-accessible eSATA port (not supported with this model)
- Two front-accessible USB 2.0 ports
- Two rear-accessible USB 2.0 ports

AMAX (EMS)

- Rear-accessible 32-bit GbE

Port	Interface
left port	(eth0) Management
right port	(eth1) Not used

- One rear-accessible DB9 serial port for system console (not supported with this model)
- One front-accessible DB9 serial port (not supported with this model)
- One rear-accessible VGA for system monitor
- One rear-accessible PS2 for Keyboard
- One rear-accessible PS2 for Mouse
- Two front-accessible USB 2.0 ports
- Two rear-accessible USB 2.0 ports

Portwell CAD-0208 (Core)

- Rear-accessible 32–bit GbE ports (RJ-45 connectors)

Port	Interface
M1	(eth3) Management
A1	(eth2)
A2	(eth1)
B1	(eth0)

Note:

A1 ports are used for internal and B1 ports are used for external. To prevent possible routing problems, the Management interfaces (M1) and (M2) should be configured on different subnets than the subnets assigned to the Data interfaces (A1/A2) and (B1/B2).

- One rear-accessible RJ45 serial port for system console
- One rear-accessible VGA for system monitor (not supported with this model)
- Two rear-accessible USB 2.0 ports

Status LEDs

Dell R210–ii (core) & Dell R210–ii XL (core)

- Internal HDD access and system power status
- 12 LED indicators (two on each GbE interface) for link status and data activity

Dell R210–ii XL (EMS)

- Internal HDD access and system power status
- Four (4) LED indicators (two on each GbE interface) for link status and data activity

AMAX (EMS)

- Five (5) LED indicators across the front panel for over temperature indication, network (LAN) activity, internal HDD access, and system power status
- Four (4) LED indicators on the rear side (two on each GbE interface) for link status and data activity.

Portwell CAD-0208 (core)

- Six (6) LED indicators across the front panel for Power, HDD and network (LAN) activity
- Four (4) LED indicators on the rear side (two on each GbE interface) for link status and data activity

Chapter 3: Preparing for installation

In this chapter

This chapter presents the recommended placement, installation options, and preparations required for proper physical installation of the equipment chassis.

Note:

Throughout this document, when referring to Avaya SBCE devices, the terms *Primary* and *Secondary* are used interchangeably with the terms *Active* and *Stand-by*, respectively.

Important:

If Release Notes were shipped with your equipment chassis and they contain information that differs from the information in this document, follow the Release Notes.

Note:

The requirements described in this document are intended for system administrators, network managers, or other qualified network equipment technicians and maintenance personnel. It assumes a working knowledge of general communications equipment protocols and network security requirements. Installation, maintenance, and removal of the Avaya SBCE 1U equipment chassis should only be done by qualified service personnel only.

Important:

The Avaya SBCE 1U equipment chassis does not contain user-serviceable subsystems or components. Opening the chassis voids the product warranty.

Hardware safety

The following general safety precautions must be observed during all phases of operation, service, and repair of this equipment. Failure to comply with these precautions or with specific warnings elsewhere in this manual could result in personal injury, network outage, or damage to the equipment.

The safety precautions listed below represent warnings of certain dangers of which Avaya is aware. You, as the user of the product, should follow these warnings and all other safety

precautions necessary for the safe operation of the equipment in your operating environment.

Ground the equipment

To minimize shock hazard, the equipment chassis and enclosure must be connected to an electrical ground. If the equipment is supplied with a three-conductor AC power cable, the power cable must be plugged into an approved three-contact electrical outlet, with the grounding wire reliably connected to an electrical ground (safety ground) at the power outlet. The power jack and mating plug of the power cable meet International Electrotechnical Commission (IEC) safety standards and local electrical regulatory codes.

Do not operate in an explosive atmosphere

Do not operate the equipment in any explosive atmosphere such as in the presence of flammable gases or fumes. Operation of any electrical equipment in such an environment could result in an explosion and cause injury or damage.

Keep away from live circuits inside the equipment

Operations and maintenance personnel are *not* authorized to remove chassis equipment covers. Only Factory Authorized Service Personnel or other qualified service personnel designated by Avaya may remove equipment covers for internal subassembly or component replacement or any internal adjustment. Service personnel should not replace components with power cable connected unless explicitly directed to do so (such as when replacing a disk drive or power supply). Under certain conditions, dangerous voltages may exist even with the power cable removed. To avoid injuries, such personnel should always disconnect power and discharge circuits before touching components.

Observe all cautions and warnings in manual

Warnings, such as the following example, precede potentially dangerous procedures throughout this manual. Instructions contained in the warnings must be followed. You should also employ all other safety precautions which you deem necessary for the operation of the equipment in your operating environment.

Warning:

To prevent serious injury or death from dangerous voltages, use extreme caution when handling, testing, and performing maintenance on this equipment and its components.

Flammability

All Avaya PCBs (printed circuit boards) are manufactured with a flammability rating of 94V-0 by UL-recognized manufacturers.

EMI caution

Caution:

The Avaya SBCE equipment chassis generates, uses, and can generate electromagnetic interference (EMI)

Lithium battery caution

The Avaya SBCE 1U equipment chassis contains a lithium battery to power the internal clock and calendar circuitry.

Caution:

A danger of an explosion exists is the lithium battery is replaced incorrectly. Currently, only authorized Avaya personnel or their agents may open the equipment chassis to replace the battery.

Equipment inventory

Each Avaya SBCE equipment chassis is packaged containing the items listed in the following table.

Item	Description
Avaya SBCE equipment chassis	• One (1) pre-configured Avaya SBCE equipment chassis • Product Information Guide
Rack installation kit	• Rack Installation Guide • Two (2) slide assemblies for mounting the equipment chassis.

Item	Description
	• Two (2) stop blocks • Eight (8) 10-32 x 0.5-inch flange-head Phillips screws
Cable binding	• Two (2) Cable Clips • Eight (8) Zip Ties
Cables	• One (1) power cable • **(Portwell only)** One (1) USB-to-Serial converter cable. Driver can be downloaded from PLDS.
Thumb drive	One (1) thumb drive The procedure for restoring a system from this drive can be found in the appendix of this book, and should only be used when directed to by Avaya support.

Meeting site requirements

Once the customer site survey has been completed and submitted to Avaya, check the physical location where the server will be installed. This location must meet several requirements for a safe and successful installation and are the customer's responsibility.

Building and electrical code requirements

Building codes

Three major building codes are:

- Uniform Building Code — produced by the International Conference of Building Officials (ICBO); 5360 South Workman Mill Road; Whittier, California 90601 USA.
- BOCA Basic Building Code — produced by the Building Officials and Code Administrators (BOCA) International, Inc.; 4051 West Flossmoor Road; Country Club Hills, Illinois 60478 USA. www.bocai.org
- Standard Building Code (SBC) — produced by the Southern Building Code Congress International, Inc.; 900 Montclair Road; Birmingham, Alabama 35213 USA. www.sbcci.org

Note:

It is the customer's responsibility to ensure that all relevant building codes have been complied with prior to installing this equipment.

Electrical codes

Five authorities on electrical codes are:

- National Electrical Code (NEC) Classification (USA only) — a recognized authority on safe electrical wiring. Federal, state, and local governments use NEC standards to establish their own laws, ordinances, and codes on wiring specifications. The NEC classification is published by the National Fire Protection Association (NFPA). The address is NFPA; 1 Batterymarch Park; Quincy, Massachusetts 02269 USA. www.nfpa.org
- Underwriters' Laboratory (UL) (USA only) — an independent research and testing laboratory. UL evaluates the performance and capability of electrical wiring and equipment to determine whether they meet certain safety standards when properly used. Acceptance is usually indicated by the words "UL Approved" or "UL Listed." The address is UL; 333 Pfingsten Road; Northbrook, Illinois 60062-2096 USA. www.ul.com
- National Electrical Manufacturing Association (NEMA) (USA only) — an organization of electrical product manufacturers. Members develop consensus standards for cables, wiring, and electrical components. The address is NEMA; 2101 L Street N.W.; Washington, D.C. 20037 USA. www.nema.org
- Electronics Industry Association (EIA) — a trade association that develops technical standards, disseminates marketing data, and maintains contact with government agencies in matters relating to the electronics industry. The address is EIA; 2001 Eye Street N.W.; Washington, D.C. 20006 USA. www.eia.org
- Federal Communications Commission (FCC) — a commission that regulates all interstate and foreign electrical communication systems that originate in the United States according to the Communications Act of 1934. The FCC regulates all U.S. telephone and cable systems. The address is FCC; 1919 M Street N.W.; Washington, D.C. 20554 USA.

Physical system protection requirements

The server is equipped with air vents on either side of the equipment chassis, and exhaust vents on the back. Be sure to follow these guidelines:

- Do not block these air vents.
- Do not place the server in a location where dirt or dust might clog the air vents or enter the chassis and damage internal components.
- Do not install the device in or near a source of heat (i.e. proximate high-current or high-power consuming equipment such as switch banks); excessive heat might cause the server to overheat and fail.

Note:

It is the customer's responsibility to ensure that no environmental hazards (i.e. excessive heat, excessive humidity, or improper ventilation) or electromagnetic interference from proximate equipment interfere with the operation of the Avaya SBCE server.

Rack requirements

Racks should conform to conventional standards:

- In the United States, use EIA Standard RS-310C: Racks, Panels, and Associated Equipment.
- In countries other than the United States, use IEC Standard 297.

In addition, verify that your rack meets the following basic mechanical and space requirements.

Mechanical requirements for the rack

Use distribution racks that meet the following mechanical recommendations:

- Use an open style, 19-inch (48.26 cm) rack to facilitate easy maintenance and to provide proper ventilation.
- The rack should use the universal mounting rail hole pattern that is identified in EIA Standard RS-310C (in countries other than the US, use IEC Standard 297).
- The mounting holes should be flush with the rails to accommodate the chassis.
- Use a rack made of steel or aluminum.
- The rack should be able to easily support an additional load of approximately 50 pounds.

Grounding requirements for the rack

Use a rack grounding kit and a ground conductor that is carried back to earth or to another suitable building ground.

All Extreme Networks switches are designed with mounting brackets that provide solid metal-to-metal connection to the rack. If you do not use equipment racks, you can attach wiring terminals directly to the mounting brackets for appropriate grounding. At minimum, follow these guidelines:

- Ground equipment racks to earth ground.
- CAD weld appropriate wire terminals to building I-beams or earth ground rods.
- Use #4 copper wire.
- Drill and tap wire terminals to equipment racks.

- Position the earth ground as close to the equipment rack as possible to maintain the shortest wiring distance possible.
- Properly test the quality of the earth ground.

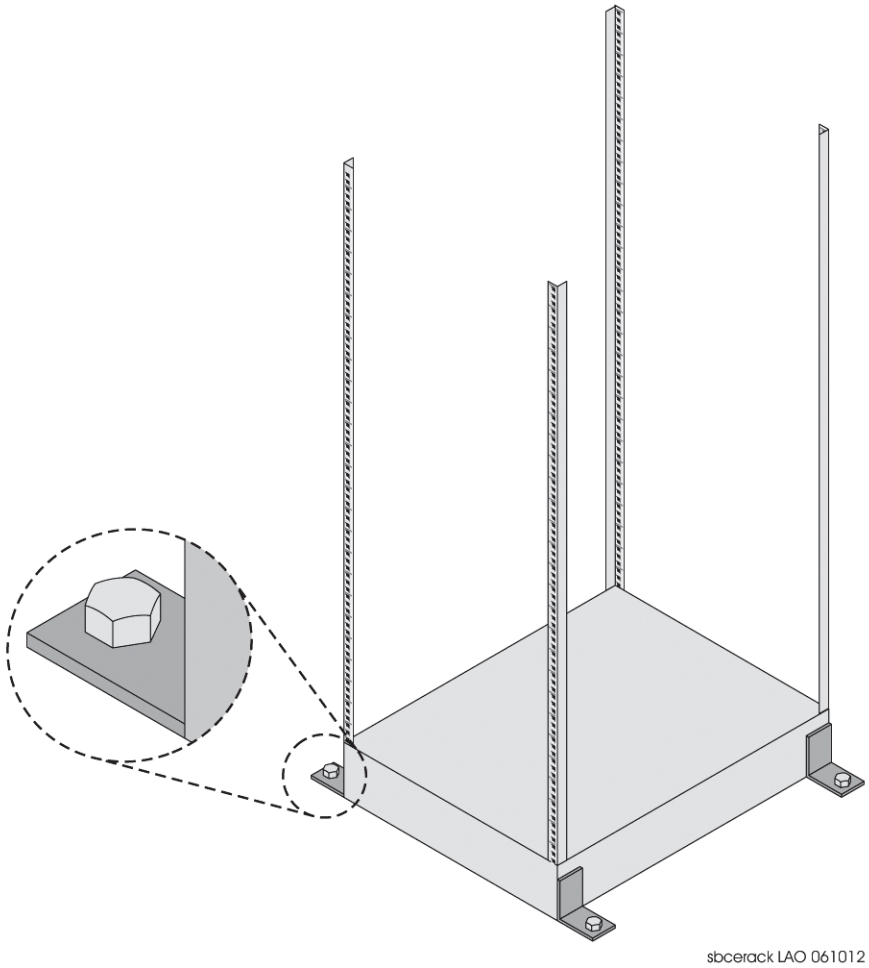
Space requirements for the rack

The following space requirements ensure adequate space to easily service the server.

- Minimum distance of 48 inches in front of the rack.
- Minimum of 24 inches behind the rack.
- Space on either side of the equipment rack is not a concern.

Securing the rack

Attach the equipment rack to the equipment room floor with 3/8- inch lag screws or equivalent hardware. The floor under the rack should be level within 3/16 inch. Use a floor-leveling cement compound if necessary or bolt the racks to the floor as shown in the following figure.



Meeting cabling requirements

Once the site survey has been completed and site requirements have been met, evaluate the existing cable plant to ensure that proper connections can be accommodated and maintained between the Avaya SBCE server and the VoIP network call server(s).

Cabling standards

Applicable cabling standards are those promulgated by BICSI (Building Industry Consulting Service International) and should be planned and installed by an RCDD (Registered Communications Distribution Designer).

Cable labeling and record keeping

A reliable cable labeling system is essential when planning and installing communications equipment into a network. Maintaining accurate records helps you:

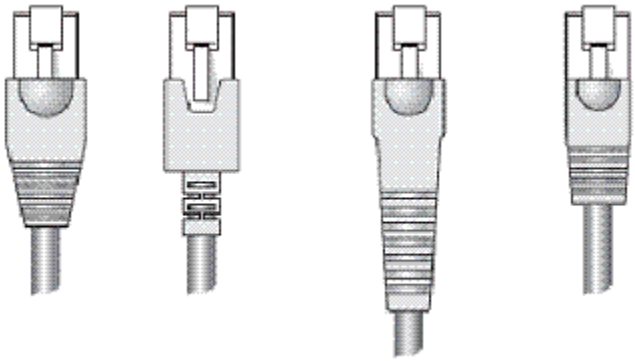
- Isolate faults and facilitate troubleshooting
- Easily relocate equipment
- Quickly and accurately make changes

RJ-45 connector jackets

Use RJ-45 cable with connector jackets that are flush with the connector or that have connectors with a ‘no-snag’ feature. Using cable with jackets that are wider than the connectors can cause:

- Connectors that are not properly aligned with the port.
- Crowded cable installation, which can cause connectors to pop out of the port.

The following figure shows examples of RJ-45 connector jacket types that are not recommended as well as those that are recommended. The two on the left are not recommended, the one that is second from the right is recommended, and the one on the far right has the highest recommendation.



Connecting cables to the server

About this task

Use only high-quality, shielded RJ-45 terminated cables to connect the server.

Procedure

1. Verify that you identified the correct cable for the port.
2. Use an alcohol wipe or other appropriate cleaning agent to clean the cable connectors; making sure they are free from all dust, oil, and other contaminants.
3. Press the cable connector into the port mating connector on the front panel of the server until the cable is securely seated.
4. Repeat steps 1 through 3 for each remaining cable.
5. Dress and secure the cable bundle to provide appropriate strain relief and protection against excessive bends and kinks.

Meeting power requirements

About this task

A back-up power supply is strongly recommended.

Caution:

Do not apply power to the server using extension cords or power strips.

Procedure

Ensure unobstructed access exists to an adequate power receptacle that provides AC 110V – 240V.

Chapter 4: Installation

About installation

Installation of the Avaya SBCE server is comprised of the following steps:

- Mounting the equipment chassis into an equipment rack or on an electrically grounded table-top.
- Interconnecting the equipment chassis into the existing network.
- Provisioning the equipment chassis.
- Configuring the equipment chassis for network operation using the Avaya EMS.

The Avaya SBCE server can be installed either in a standard 19” equipment rack or placed free-standing on an equipment tabletop.

Important:

Read through the information in this chapter thoroughly before attempting to install, provision, or remove the Avaya SBCE server.

Mounting the server

Procedure

For information on mounting the Avaya SBCE server, see the *Rack Installation Guide*.

Connecting the server to the VoIP network

Once the Avaya SBCE server has been properly installed, the network interface cables can be installed. The actual connection of the Avaya SBCE server to the network is determined by the particular configuration of the enterprise network and the desired location of the server with

that topology. The current release of the Avaya SBCE can be deployed in any of the following scenarios:

- **Deployment Option 1** Single Availability (SA) — A single Avaya SBCE server utilizing the internal EMS.
- **Deployment Option 2** - Two or more Avaya SBCE servers controlled by one or more Avaya Element Management Systems (EMS) devices.
- **Deployment Option 3** High Availability (HA) — Two Avaya SBCE servers deployed in HA (High-Availability) mode, both controlled by a separate single Avaya Element Management Systems (EMS) device.

Install scripts should be run on every box in the system, beginning with the EMS box. Then the install script is run in each of the multiple boxes one at a time (remotely) from the EMS GUI screen. If there are HA-pair boxes being managed by the EMS, run the script remotely on each of the HA boxes before running the install script remotely in each of the stand-alone boxes. When installing a single availability server (Deployment Option 1), install script using the options for “EMS + SBCE.”

Note:

When Avaya devices are all in the same subnet, you may use a one-wire deployment (for example, using only interface A1 instead of interfaces A1 and B1). When Avaya devices are all within the DMZ, the use of internal or external firewalls is optional, depending upon the deployment.

Caution:

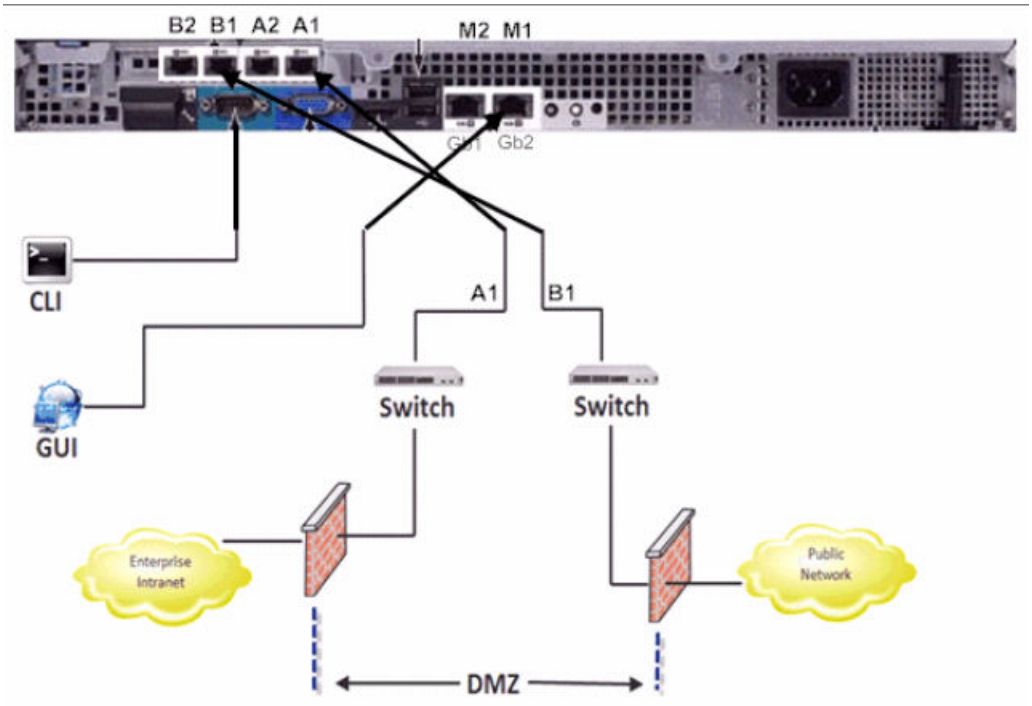
Do not interrupt existing network connections without being thoroughly certain of how Avaya SBCE will be integrated into existing operations. If you are uncertain how to proceed, call Avaya Customer Service for assistance.

Related topics:

Deployment option 1: Single Availability on page 34
Deployment option 2: 2+ servers on page 35
Deployment option 3: High Availability on page 35

Deployment option 1: Single Availability

Deployment option 1 is a single Avaya SBCE server deployed as shown in the following diagram utilizing internal EMS.



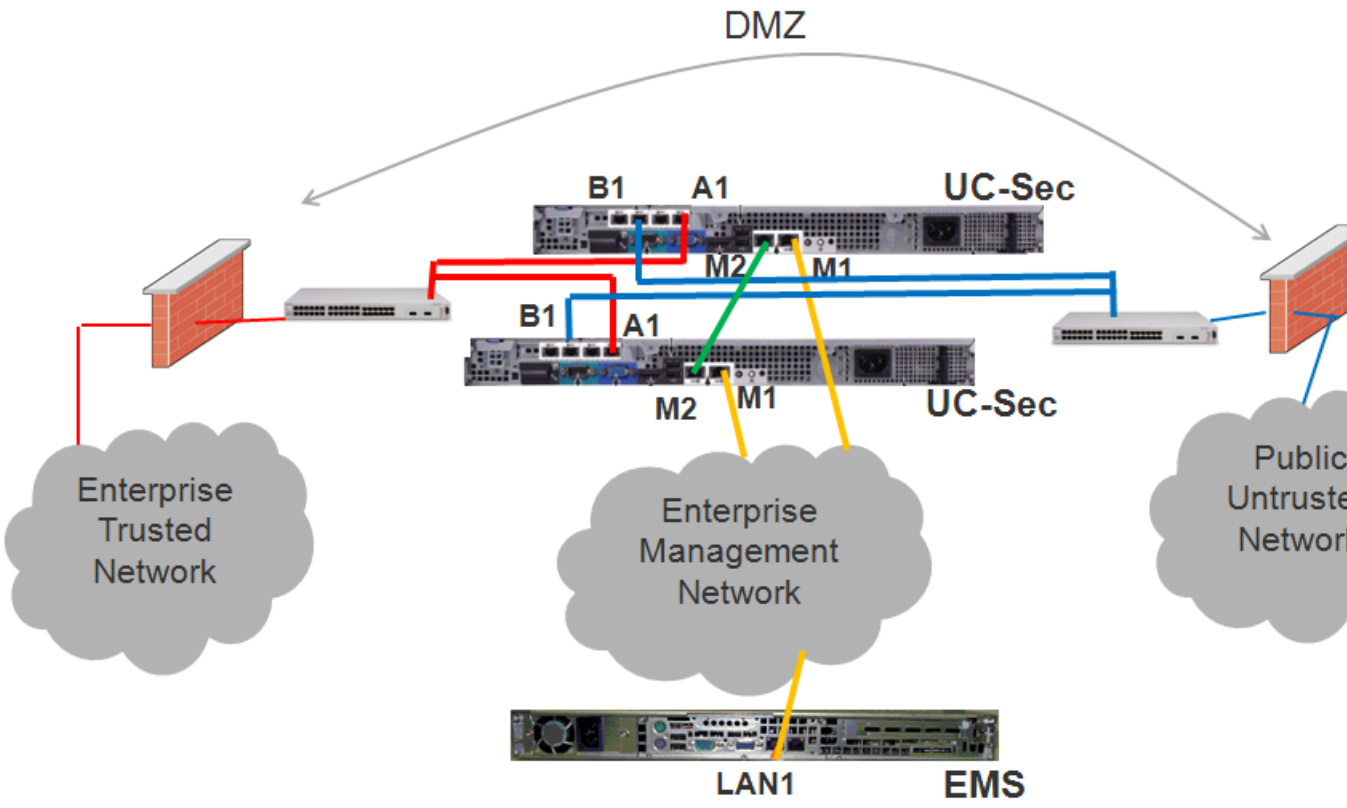
Deployment option 2: 2+ servers

Deployment option 2 is two or moreAvaya SBCE servers controlled by one or more Avaya Element Management Systems (EMS) devices.

There is a supported limit of 25 SBCs.

Deployment option 3: High Availability

Deployment option 3 is two Avaya SBCE servers deployed in HA (High-Availability) mode, both controlled by a separate single Avaya Element Management System (EMS) device. See the following figure.



Installing the EMS

About this task

Once the Avaya EMS is properly installed into the equipment rack and connected to the enterprise network, it is ready to be configured for operation. Perform the following steps to install and configure the Avaya EMS.

Procedure

1. Connect a video monitor to the PS2 **VGA Output** port and a standard computer keyboard to the PS2 **Keyboard** port on the rear panel of the Avaya EMS equipment chassis.
2. Power-on the video monitor according to the manufacturer's instructions.
3. Press the **Power On** switch located on the front panel of the Avaya EMS equipment chassis.
   The **Power On** indicator LED will be illuminated and the EMS installation scripts will run, providing a series of outputs to the video display. When the configuration script

is ready for user input, the video display will present a prompt telling you to press the **Enter** key on the keyboard to begin the configuration process.

4. Press **Enter**.
   The Device Type window is displayed.
5. Select device type (only choice is EMS) and press **Enter**.
   A message appears instructing user to choose yes to proceed or no to exit.
6. Choose **yes** to proceed.
   An installing as a EMS device notification screen appears.
7. Press **Enter**.
   A device configuration screen is displayed, containing two (2) options: EMS Configurations and EMS Operations.
8. The EMS Configuration screen should default to the EMS Configuration option. If it does not, press the **Tab** key until the **EMS Configuration** option is highlighted and press **Enter**.
   The top-level EMS Configuration screen is displayed.

   Caution:

   The **EMS Operations** option is used to reset the EMS operating software to the factory default state. It permanently deletes all system configuration information and cannot be undone. DO NOT select this option unless that is the operation you want to perform.
9. Choose **EMS Configurations**
10. If not already selected by default, use the arrow keys to select the **Installation Type** option and click **Enter**.
    Another configuration screen is displayed, containing two (2) options: Primary and Secondary.
11. Select **Primary** and click **Enter**.
    The top-level configuration screen is displayed.
12. Use the arrow keys to select the **EMS Appliance Configuration** option and click **Enter**.
    The Configure EMS Appliance screen is displayed.
13. Enter the requested information into the appropriate fields. (See EMS Appliance Configuration screen Field Descriptions table.)
14. Click **Enter**.
    The top-level configuration screen is displayed.
15. Use the arrow keys to select the **Management Interface Setup** option and click **Enter**.
    The Management Interface Setup EMS screen is displayed.

16. Enter the requested information into the appropriate fields and click **OK**. (See Management Interface Setup screen Field Descriptions table.)
17. Use the arrow keys to select the **Time Zone** option.
    The Configure Time Zone screen is displayed
18. Provide the requested information and click **OK**.
19. (Optional) Custom Routes are optional. Contact support if you need to configure Custom Routes.
20. (Optional) Use the arrow keys to select the **Self-Signed Certificate** option.
    The Configure Self-Signed Certificate screen is displayed

    The self-signed certificate is used to enforce Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) access for the Graphical User Interface (GUI).
21. Provide the requested information and click **OK**.
    The top-level provisioning screen is displayed.
22. Use the arrow keys to select **Back**.
    The top-level configuration screen is displayed.
23. Use the arrow keys to select **Done**.
    A script is automatically activated which configures the Avaya EMS with the information provided in the previous steps.
24. Set the Time manually (if prompted)
25. Set the Date manually (if prompted)
26. When prompted, provide the password to be used by the root user and press **Enter**.
27. When prompted, provide the same password for the ipcs user and press **Enter**. This password will be used for secure shell (ssh) access to the EMS.
    A series of scripts automatically run, which configure the EMS with the information you input. As these scripts run a series of outputs are provided to the video display informing you of the progress of the configuration. The configuration is successfully completed when the following prompt is displayed: `EMS login:`

Next steps

Verifying EMS Operation on page 40

Installing EMS + SBCE

About this task

Installing an EMS + SBCE is the same basic process as installing an EMS, with a few minor changes.

Procedure

1. Connect a video monitor to the **Serial Connection** port and a standard computer keyboard to the PS2 **Keyboard** port on the rear panel of the Avaya EMS equipment chassis.
2. Power-on the video monitor according to the manufacturer's instructions.
3. Press the **Power On** switch located on the front panel of the equipment chassis. The **Power On** indicator LED will be illuminated and the EMS installation scripts will run, providing a series of outputs to the video display. When the configuration script is ready for user input, the video display will present a prompt telling you to press the **Enter** key on the keyboard to begin the configuration process.
4. Press **Enter**.
   The Device Type screen comes up with two (2) choices: SBCE and EMS+SBCE.
5. Select EMS+SBCE and press **Enter**.
   A screen is displayed with the message "Please Choose Yes to proceed or No to Exit."
6. Select Yes and press **Enter**.
   A screen is displayed with the message "Installing as a EMS+SBCE device"
7. Press **Enter**.
   A device configuration screen is displayed, containing two (2) options: Configuration and Operation.
8. Choose **Configurations**
   The top-level configuration screen is displayed.
9. Use the arrow keys to select the **Appliance Configuration** option and click **Enter**.
   The Configure Appliance screen is displayed.
10. Enter the requested information into the appropriate fields. (See EMS Appliance Configuration screen Field Descriptions table.)
11. Click **Enter**.
    The top-level configuration screen is displayed.
12. Use the arrow keys to select the **Management Interface Setup** option and click **Enter**.
    The Management Interface Setup EMS screen is displayed.
13. Enter the requested information into the appropriate fields and click **OK**. (See Management Interface Setup screen Field Descriptions table.)
14. Use the arrow keys to select the **Time Zone** option.
    The Configure Time Zone screen is displayed
15. Provide the requested information and click **OK**.
16. (Optional) Custom Routes are optional. Contact support if you need to configure Custom Routes.

17. (Optional) Use the arrow keys to select the **Self-Signed Certificate** option.
    The Configure Self-Signed Certificate screen is displayed

    The self-signed certificate is used to enforce Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) access for the Avaya Control Center Graphical User Interface (GUI).
18. Provide the requested information and click **OK**.
    The top-level provisioning screen is displayed.
19. Use the arrow keys to select **Back**.
    The top-level configuration screen is displayed.
20. Use the arrow keys to select **Done** and press **Enter**.
    A script is automatically activated which configures the Avaya EMS with the information provided in the previous steps.
21. Set the Time manually (if prompted)
22. Set the Date manually (if prompted)
23. When prompted, provide the password to be used by the root user and press **Enter**.
24. When prompted, provide the same password for the ipcs user and press **Enter**. This password will be used for secure shell (ssh) access to the EMS.
    A series of scripts automatically run, which configure the EMS with the information you input. As these scripts run a series of outputs are provided to the video display informing you of the progress of the configuration. The configuration is successfully completed when the following prompt is displayed: `EMS login:`

Next steps

Verifying EMS Operation on page 40

Verifying EMS Operation

The operational status of the EMS can be verified by either attempting to access the Avaya SBCE Control Center using the GUI interface or by establishing a CLI session via a secure shell session (SSH) and manually checking the status of various internal processes. Each of these methods is described in the following sections.

Related topics:

Logging in to the EMS GUI on page 41
Establishing a communications session on page 41

Logging in to the EMS GUI

Procedure

1. Using Mozilla Firefox™ or Windows® Internet Explorer, open a new browser tab or window.
2. Enter the following URL: `https://<M1_Management_IP_Address>` replacing the bracketed text with the Avaya EMS equipment chassis IP address.
3. Press **Enter**.
   If the Welcome screen is displayed, the EMS is operating normally and available for use. You can log-in to the EMS and perform normal administrative and operational tasks. Refer to the *Administering Avaya Session Border Controller for Enterprise* document for more information.

Establishing a communications session

Procedure

1. Configure the communications parameters of your terminal program to the settings in the following table.

Parameter	Value
Baud rate	19200
Parity	None
Data bits	8
Stop bits	1
Connection Setting	Direct to Com1

2. Press **Enter** to establish the communications session.
   A prompt asking for your User Name and Password will be displayed.
3. Provide the requested information and press **Enter**.

Chapter 5: Configuring SBC

Starting the provisioning process

About this task

When the server is turned on, a series of scripts are automatically run and then the Device Type screen is displayed.

Procedure

1. Use the arrow keys to select the appropriate option for your intended deployment and press **Enter**.
   - Select **EMS + SBCE** if the server will be deployed in the network as a stand-alone device and run the Element Management System (EMS) GUI as well as the Avaya SBCE security software.
   - Select **SBCE** if the server will be deployed in the network as part of a multi-box solution and will communicate with a separate Element Management System (EMS) GUI server.
2. Use the arrow keys to select **Configuration** and then press **Enter**.
   The Appliance Configuration screen is displayed.

Next steps

Configuring the appliance on page 43

Configuring the appliance

Before you begin

Starting the provisioning process on page 43

Procedure

1. Complete the fields on the Appliance Configuration screen, and then select OK.
   The SBCE Provisioning screen is redisplayed.
2. Use the arrow keys to select **Management Interface Setup** and press **Enter**.

The Management Interface Setup screen is displayed.

Next steps

Configuring the management interface on page 45

Related topics:

Appliance Configuration field descriptions on page 44

Appliance Configuration field descriptions

Name	Description
E-SBC Appliance Name	A descriptive name assigned to this Avaya SBCE server. This field is displayed only for Avaya SBCE only installations
EMS Appliance Name	A descriptive name assigned to the EMS component of this server. This field is displayed only for EMS + Avaya SBCE installations.
Domain Suffix (Optional)	The domain within which this server will be deployed.
List of DNS Servers	The IP address(es) of each Domain Name Server (DNS). **Note:** The list of DNS server names must be comma-separated, with no spaces.
NTP Server IP Address (ipv4)	The IP address of the Network Time Protocol (NTP) server. (If no NTP is present, configure manually.
Network Passphrase	A unique password that the EMS server and Avaya SBCE security devices deployed throughout the network will use for authentication. This field is displayed only for Avaya SBCE only installations **Important:** The same passphrase must be used when configuring each Avaya SBCE and EMS security device. Different

Name	Description
	passphrases will prevent the EMS and Avaya SBCE security devices from communicating with one another.

Related topics:

Configuring the appliance on page 43

Configuring the management interface

Before you begin

Configuring the appliance on page 43

Procedure

1. Complete the fields on the Management Interface Setup screen, and then select **OK**.
   The E-SBC Provisioning screen is redisplayed.
2. **(Optional)** Use the arrow keys to select **Custom Routes** and press **Enter**.

   Note:

   Custom Routes are not common. Please contact support if you would like to configure custom routes. Configuration of custom routes can be ignored and skipped entirely without affecting the operation of the device.

   The Custom Routes screen is displayed.
3. **(Optional)** If needed, use the arrow keys to select **Self-Signed Certificate** and press **Enter**.

   Note:

   Configuring the Self-Signed Certificate is optional. If this feature is not needed, skip this step.

   The Self-Signed Certificate screen is displayed.
4. Use the **Tab** key to select **Done** and press **Enter**.
   A script is automatically activated that provisions the Avaya SBCE server with the information provided in the previous steps.

Related topics:

Management Interface Setup field descriptions on page 46

Management Interface Setup field descriptions

Name	Description
Management Device	The logical port to which the network will be connected. M1 is the management interface. M2 is only used internally in HA deployments on SBCs.
Management IP Address (ipv4)	The IP address of the management network.
Management Network Mask	The network mask of the management network.
Management Gateway IP Address (ipv4)	The IP address of the gateway to the management network.
EMS Server IP Address (ipv4)	The IP address of the EMS server. This field is displayed only for Avaya SBCE only installations

Important:

When using SSL/VPN as configured on the M1 interface please be advised that the IP address associated with the M1 interface will need *outbound* internet access to initiate connectivity with the Avaya VPN Gateway (AVG) server (FQDN: plavg0(x).sal.avaya.com. M1 is the management interface is the required interface for SSL/VPN.

Note:

Security considerations for Voice Over IP (VoIP) systems recommend segmenting the data (or data management) network from the voice network. For SBCE deployments, this means configuring the Management Interface (M1) on a separate subnet from the subnet used for the Voice Interfaces (i.e., A1, A2, B1, and B2). Refer to the following documents for more information regarding this recommendation:

- Avaya: “Security Best Practices Checklist,” in the “Network” section — https://downloads.avaya.com/css/P8/documents/100070101
- Network Security Agency: “Recommended IP Telephony Architecture,” in the “IP Telephony Architecture” section — http://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf
- National Institute of Standards and Technology (NIST): “Security Considerations for Voice Over IP Systems,” in the “Overview of VoIP” section, in the “VoIP Security Issues” subsection — http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Related topics:

Configuring the management interface on page 45

Configuring Time Zone

Procedure

1. Select Configure TimeZone from the Avaya SBCE Runtime Options menu
   Time Zone screen comes up
2. Scroll through the Time Zone list until the one you want to select is highlighted.
3. Press Enter to choose the Select button
   Time Zone will be configured.

Note:

If TimeZone is not configured and the user presses **Skip**, “GMT” will be configured as the Current TimeZone.

Next steps

Note:

TimeZone can be reconfigured using the `ipcs-options` command. See *Administering Avaya Session Border Controller for Enterprise* chapter 1 for procedure.

Configuring a self-signed certificate

About this task

The self-signed certificate is used to enforce Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) access for the Avaya SBCE Graphical User Interface (GUI).

Note:

Entering all information on this screen is optional and can be skipped without affecting operation of Avaya SBCE. However, Avaya recommends that you complete the fields on this page because the values entered here are included in the HTTPS certificate for the GUI.

Procedure

1. Complete the fields on the Configure Self-Signed Certificate screen, and then select **OK**.

   The E-SBC Provisioning screen is redisplayed.

2. Use the **Tab** key to select **Back** and press **Enter**.
3. Use the **Tab** key to select **Done** and press **Enter**.
   A script is automatically activated that provisions the Avaya SBCE server with the information provided in the previous steps.

Next steps

Configuring date and time on page 48

Configuring date and time

About this task

In the event that the NTP server cannot be reached or a connection cannot be established, user will be prompted to input another NTP IP address that is reachable. The other option will be to click on **manual** and manually set the time and date. Once time and date have been input manually, user can return and set up NTP to make it work correctly. In a system utilizing HA, the NTP must be functioning in order to keep boxes synchronized.

Procedure

1. Set the time using the **tab** and **arrow** keys.
2. Set the date using the **tab** and **arrow** keys.

Next steps

Configuring passwords on page 48

Configuring passwords

Before you begin

Configuring date and time on page 48

Procedure

1. When prompted, enter the password to be used by the root user and press **Enter**.
2. When prompted, enter the same password for the ipcs and press **Enter**.
   This password will be used for secure shell (SSH) access to the Avaya SBCE.

As the server is being provisioned, the system displays a series of messages that inform you of the progress. The provisioning is successfully completed when the Avaya SBCE `login:` prompt is displayed.

Next steps

Configure Avaya SBCE for network operation by using the EMS. See Chapter 4, “Device Configuration” of the *Administering Avaya Session Border Controller for Enterprise* for more information.

Licensing information

PLDS

A license will need to be downloaded from PLDS for SBCE. Suggestions for the Host ID and License Host Name are listed below. Procedures for installing, viewing, and uninstalling license files can be found in the *Administering Avaya Session Border Controller for Enterprise* manual.

Host ID

Standalone non-HA SBCE licenses should use the management (M1–Eth5) mac address as the Host ID.

HA deployments should use the EMS management (Eth0) mac address as the Host ID.

License host name

Use `SBCE_(something descriptive for the site)` as the license host name on the license.

Remote access

Secure Access Link

Secure Access Link (SAL) is used for remote access for SBCE’s in non-IP Office environments. The Avaya SBCE needs to be registered for remote access with the customer SAL.

SSL VPN

Remote access to the Avaya SBCE when sold with IP Office is to SSL VPN into IP Office and then hops to the Avaya SBCE. IP Office and Avaya SBCEneed to be registered together and some configuration needs to be done. For details on this please see the job aid titled *ASBCE GRT Registration and Remote Connectivity via IP Office SSL/VPN NAPT*, which is available on http://support.avaya.com.

Note:

SSL VPN configured in the Avaya SBCEis not currently used or supported in 6.2

Appendix A: Recovering the system from USB drive

Before you begin

Set the BIOS settings to match the following table before performing the following procedure.

Item	Setting
BIOS Version	1.1.1
Date & Time	Verify/Set
CPU	E3–1220 3.1 GHz
Memory	4 GB ECC DDR3 1333 MHz
Hard Disk	> 80 GB

About this task

Only use the USB drive to recover a server when directed to by Avaya support.

Procedure

1. Connect a console cable to the serial port of the server and a computer with HyperTerminal.
2. Insert the Avaya SBCE USB thumb drive (with installer image) into the front USB port.
3. Reboot the server.

   Important:

   For Dell servers: Press `F11` to enter BIOS Boot Manager after rebooting the server. Then select **USB to boot > Flash Disk** to continue.
4. Verify boot-up dialog on console.
5. When “boot:” prompt displays, type `serial`, and then press **Enter**.
6. When prompted to “Choose image source”, type `1` and press **Enter**.
7. When prompted `“Do you wish to continue (y/n)?”`, Type `“y”` and press **Enter**.
   If disk is uninitialized, an error message will appear. Return to step one and repeat procedure to resolve this error. This should only occur one time on any server. A second error message indicates a true failure.
8. Monitor console output for exceptional errors as installation continues for about 10 minutes.
9. When prompted `“Please unplug installation media”`, remove USB thumb drive, and then press **Enter**.

After the server automatically restarts, the installer identifies the hardware such as `PowerEdge R210 II`.

10. Use the tab key to select **OK** and press **Enter**.
11. Enter IPCS serial number, then press **Enter**, then select OK, and then press **Enter**.
    The IPCS serial number is a 12 digit alphanumeric sequence with the format “IPCSxxxxxxxx”. The serial number is on a label on the server or in the luggage tag on some servers.
12. Use the tab key to select **OK** and press **Enter**.
    The installation takes about 10–15 minutes. When the process is complete, a prompt to restart the system displays.
13. When prompted `Enter Y to reboot or N to shutdown the machine`, type `Y` and press **Enter** to shut down the server. It takes a few minutes to shut down.

Next steps

Remove the keyboard, power, and console cables after server has turned off.

Appendix B: Acronyms and abbreviations

This appendix contains an alphabetical list of all the acronyms and abbreviations used in this manual.

Acronym	Definition
BICSI	Building Industry Consulting Service International
BOCA	Building Officials and Code Administrators
CE	Certification mark for the European Community
CLI	Command Line Interface
CM	Call Manager
CS	Call Server
CSA	Certification mark for the Canadian market
DDoS	Distributed Denial-of-Service
DIMM	Dual In-line Memory Module
DoS	Denial-of-Service
EIA	Electronics Industry Association
EMS	Element Management System
FCC	Certification mark of the Federal Communications Commission for the US market
FIPS	Federal Information Processing Standards
GbE	Gigabit Ethernet
GUI	Graphical User Interface
HA	High-Availability
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
ICBO	International Conference of Building Officials
IM	Instant Messaging
IP	Internet Protocol
IPCS	Internet Protocol Communications Security
LAN	Local Area Network
LED	Light-Emitting Diode

Acronym	Definition
NEC	National Electrical Code
NEMA	National Electrical Manufacturing Association
NFPA	National Fire Protection Association
NOC	Network Operations Center
POP	Point-of-Presence
RCDD	Registered Communications Distribution Designer
SBC	Standard Building Code
SIP	Session Initiation Protocol
UL	Certification mark of Underwriters Laboratories, Inc. for the US market
URL	Uniform Resource Locator
VoIP	Voice-over-Internet Protocol

Index

N

P

R

S

T

U

V