

# **Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise**

© 2014-2019, Avaya Inc. All Rights Reserved.

#### **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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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 Avaya hardware and software. 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: <a href="https://support.avaya.com/helpcenter/getGenericDetails?detailld=C20091120112456651010">https://support.avaya.com/helpcenter/getGenericDetails?detailld=C20091120112456651010</a> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. 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.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

#### **Hosted Service**

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

#### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN 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 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

#### License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, 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 or an Instance of the Software.

#### 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 is the software contained within the list of Heritage Nortel Products located at <a href="https://support.avaya.com/LicenseInfo">https://support.avaya.com/LicenseInfo</a> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. 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 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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.

#### Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

#### **Third Party Components**

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service 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"). As required, 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 products, Documentation or on Avaya's website at: https:// support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE http://www.mpegla.com/

#### Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN

WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP:// WWW.MPEGLA.COM.

#### **Compliance with Laws**

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

#### **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: <a href="https://support.avaya.com">https://support.avaya.com</a> or such successor site as designated by Avaya.

#### Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <a href="https://support.avaya.com/security">https://support.avaya.com/security</a>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<a href="https://support.avaya.com/css/P8/documents/100161515">https://support.avaya.com/css/P8/documents/100161515</a>).

### **Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: <a href="https://support.avaya.com">https://support.avaya.com</a>, or such successor site as designated by Avaya.

#### **Contact Avaya Support**

See the Avaya Support website: <a href="https://support.avaya.com">https://support.avaya.com</a> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <a href="https://support.avaya.com">https://support.avaya.com</a> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

#### Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) 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.

# **Contents**

Cł	napter 1: Introduction	8
	Purpose	8
	Change history	8
Cł	napter 2: Troubleshooting fundamentals	9
	Network configuration	
	Network configuration checklist	9
	Verifying integration configuration	10
	Ethernet port labels	12
	Loss of audio and active call drops during HA failover	17
	System Monitoring	. 17
	Dashboard	17
	Dashboard content descriptions	. 17
	Manage system alarms	18
	Viewing system incidents	
	Viewing system SIP statistics	20
	Viewing periodic statistics	
	Real Time SIP Server Status	
	Viewing system logs	
	Viewing audit logs	
	Viewing diagnostics results	
	Viewing administrative users	
	Managing Avaya SBCE logging level	
	Roll back to an earlier release	
	Enhanced Access Security Gateway	
	Checking EASG status	
	Enabling and disabling EASG using web interface	
	Enabling and disabling EASG using CLI	
	EASGManage	
	Loading and managing site certificate	
	Support contact checklist	
Cł	napter 3: Monitoring and analysis	
	Tools and utilities	
	traceSBC tool	
	Trace	
	showflow	
	Debugging logs	
	Enabling application debug logs	
	Disabling application debug logs	
	Enabling GUI debug logs	44

## Contents

	Disabling GUI Logs	
	Debug logs location	45
	Traps	46
	Incidents	47
	Logs collection	55
	Collecting and downloading logs	55
	Collect logs field descriptions	56
	Collect Archive field descriptions	57
	SNMP MIB	57
	MIB-II support	57
	SBCE OID Descriptions	57
	Avaya SBCE MIB	64
	System alarms	64
	System alarms list	64
	GUI and console alarm list	69
	New user-added alarm	69
	New Administrator-added alarm	70
	User privilege change alarm	70
	User deleted alarms	70
	Login failure alarm	71
Ch	apter 4: Maintenance procedures	
	Backup and restore	
	Designating a Snapshot Server	
	Creating system snapshots	
	Restoration of a system snapshot	
	Deleting a system snapshot	
	Handling duplicate hostnames in a multiserver deployment	
	Acquiring WebLM license on Avaya SBCE	
	Connecting Avaya SBCE with an external WebLM server	
	Swapping a Avaya SBCE device in single server deployment	
	Swapping Avaya SBCE devices in HA pair deployment	
	Swapping an EMS server in single server deployment	
	Swapping a primary EMS server in HA pair deployment	
	Swapping a secondary EMS server in HA pair deployment	
	Avaya SBCE reconfiguration script options	
	Changing management IP, gateway and network mask details for a single server	-
	deploymentdeployment	86
	Changing management IP for an HA deployment	
	Changing hostname	
	Changing network passphrase	
	Regenerating self-signed certificates	
	Changing DNS IP and FQDN	
	Enabling or disabling network interfaces using CLI	

	ipcs-options commands	89
	Determining whether Avaya SBCE is running on a TILEncore Gx–36 Intelligent Application	
	adapter	90
	Listing static and dynamic flows through the Tilera Application Shell	91
	Checking counters for the Tilera Gx card	
	Checking network synchronization between the host and the TILEncore Gx Intelligent	
	adapter	93
	Determining whether Avaya SBCE is installed on VMware or KVM	
	Determining whether Avaya SBCE is installed on KVM	
	Determining whether Avaya SBCE is installed on VMware	
	Resetting the root or ipcs password	
Ch	apter 5: Resources	96
	Documentation	
	Finding documents on the Avaya Support website	97
	Accessing the port matrix document	
	Avaya Documentation Portal navigation	
	Training	
	Viewing Avaya Mentor videos	
	Support	100

# **Chapter 1: Introduction**

# **Purpose**

This document describes how to use troubleshooting tools and utilities.

This document is intended for people who perform troubleshooting tasks.

# **Change history**

Issue	Date	Summary of changes
1	February 2019	Release 8.0 document.
2	March 2019	Added the "Resetting the root or ipcs password" section.
		Updated the "Swapping Avaya SBCE devices in HA pair deployment" section.
3	August 2019	Updated the document with following Release 8.0.1 changes:
		Updated "Ethernet Port Labels" section with the information of Portwell CAF-0251 server.
		Updated the instances of 8.0 to 8.0.1

# **Chapter 2: Troubleshooting fundamentals**

# **Network configuration**

# **Network configuration checklist**

Use this checklist while troubleshooting network configurations.

No.	Task	Description	~
1	Create a site network map.	Identifies where each device is physically located on your site. Use the map to systematically search each part of your network for problems.	
2	Identify logical connections.		
3	Document device configurations.	Maintain online and paper copies of device configuration information.	
4	Store passwords in a safe place.	Keep records of your previous passwords if you must restore a device to a previous software version and need to use the old password that was valid for that version.	
5	Create a device inventory checklist.	List all devices and relevant information for the network including device type, MAC addresses, ports, and attached devices.	
6	Create an IP address and port number list.	List the IP addresses and port numbers of all devices.	
7	Maintain a change control system.		
8	Create a support contact list.	Store details for support contracts, support numbers, engineering details, telephone and fax numbers.	

# Verifying integration configuration

You can verify the operational status of the EMS by either attempting to access the EMS server using the web interface or by establishing a CLI session via a secure shell session (SSH) and manually checking the status of various internal processes.

# Logging on to the EMS web interface

#### **Procedure**

- 1. Open a new browser tab or window.
- 2. Type the following URL:

```
https://<Avaya EMS IP address>
```

3. Press Enter.

The system displays a message indicating that the security certificate is not trusted.

4. Accept the system message and continue to the next screen.

If the Welcome screen is displayed, the EMS is operating normally and available for use. You can log in to EMS and perform normal administrative and operational tasks. See *Administering Avaya Session Border Controller for Enterprise*.

5. Type the username and password as ucsec.

On first login, system prompts you to change the password.

6. Enter a new password and login with the new password.

# Logging in to EMS through console

To log in to EMS through a console, use the same connection that was used during installation that is serial connection for Portwell servers and VGA connection for non-Portwell servers.

# Logging in to Avaya SBCE server through a serial console for Portwell servers

#### Before you begin

Change the BIOS settings and enable serial redirection.

#### About this task

Connect the laptop to the serial port on the Avaya SBCE server by using the cable that Avaya provided or a DB9 null modem cable.

#### **Procedure**

1. Configure the serial connection parameters of the 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
	Note:
	Because the com port number is not fixed, use Device Manager to find out the correct port number.

2. Press Enter to establish a serial connection.

The system displays a prompt asking for the User Name and Password.

3. Provide the required information and press **Enter**.

# Logging in to EMS through VGA connection for non-Portwell servers

## Before you begin

Connect the monitor to EMS through a VGA cable. Connect a keyboard to EMS.

#### **Procedure**

1. Press Enter to establish a communications connection.

The system prompts you to enter the username and password.

2. Enter your username and password, and press Enter.

# Logging in to the EMS using SSH

#### **Procedure**

- 1. Log in to SSH client using PuTTy.
- 2. Type the IP address for Avaya SBCE.
- 3. Specify the port as 222.
- 4. Select the connection type as SSH and press Enter.
- 5. Enter the user name and password to log in.

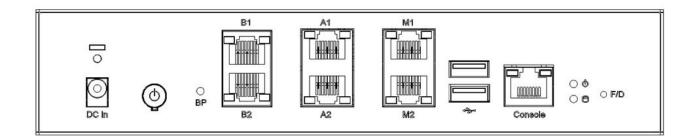
# Note:

You cannot gain access to shell with user account ucsec.

User account ipcs or user accounts that have shell access can be used for logging in to Avaya SBCE.

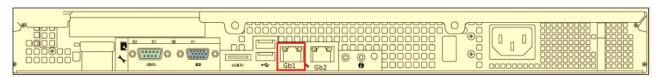
# **Ethernet port labels**

# Portwell CAD 0230



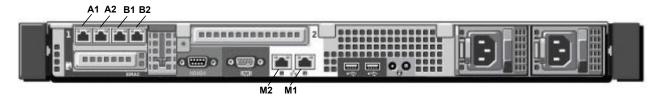
Ethernet port labels	Number of ports
M1, M2, A1, A2, B1, B2	6

# **Dell EMS**



Ethernet port labels	Number of ports
Gb1	2 (1 unused - the right port is unused)

# **Dell R320**



Ethernet port labels	Number of ports
M2, M1, A1, A2, B1, and B2	6

# **Dell R330**

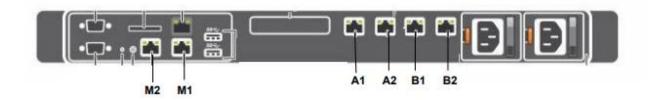


Table 1: Type -1

Ethernet port labels	Number of ports
M2, M1, A1, A2, B1, B2	6

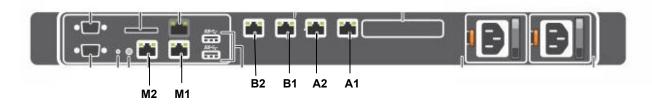
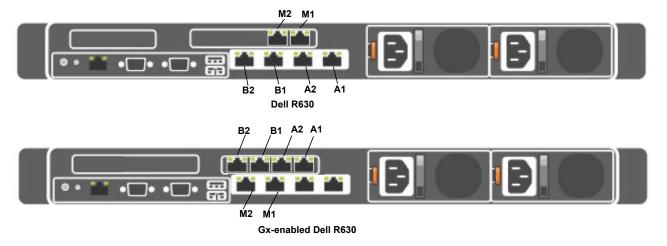


Table 2: Type -2

Ethernet port labels	Number of ports
M2, M1, B2, B1, A2, A1	6

# **Dell R630**



Ethernet port labels	Number of ports
M2, M1, B2, B1, A2, and A1	6

# **HP DL360 G8**

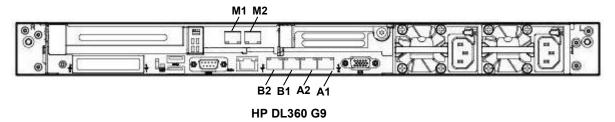


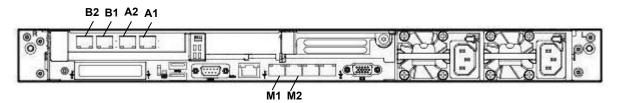
Ethernet port labels	Number of ports
M1, M2, B2, B1, A2, and A1	6



When you configure the server as EMS, A1, A2, B1, B2, and M2 are not used.

# **HP DL360 G9**

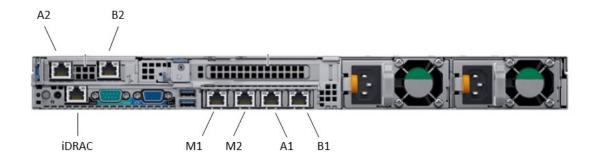




Gx-enabled HP DL360 G9

Ethernet port labels	Number of ports
M1, M2, B2, B1, A2, and A1	6

# Dell<sup>™</sup> PowerEdge<sup>™</sup> R640 Server or Avaya Converged Platform 100 series server

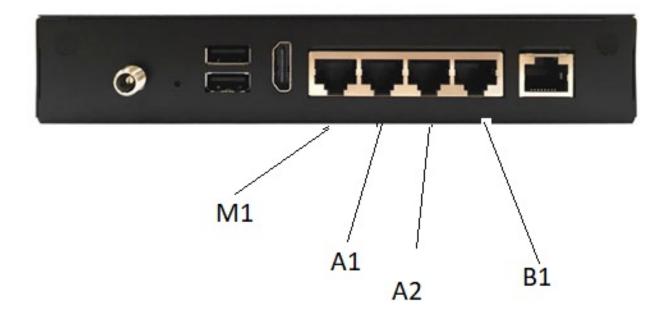


The port usage for Avaya Converged Platform 100 series profile 3 and profile 5 is same:

• The interface A2 or B2 can be of RJ45 type for profile 3 or optical type for profile 5.

Ethernet port labels	Number of ports
M1, M2, A1, A2, B1, B2	6

# Portwell CAF-0251



Ethernet port labels	Number of ports
M1, A1, A2, B1	4

# Loss of audio and active call drops during HA failover

During high availability failover, you might notice loss of audio or active call drops. This issue can occur if the internal IP of Avaya SBCE and the internal Avaya Aura® core are on the same subnet. To resolve this issue, move the internal IP of Avaya SBCE to a different subnet. For more information, see the Configuring High Availability section in *Administering Avaya Session Border Controller for Enterprise*.

# **System Monitoring**

# **Dashboard**

The Dashboard screen displays system information, installed devices, alarms, and incidents. The screen displays additional separate summary windows, such as Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The summary windows contain active, up-to-the-minute alarms, incident, statistical, log, diagnostic, and user information, and review and exchange textual messages with other administrative user accounts.

The Content area of the Dashboard screen contains various summary areas that display top-level, systemwide information, such as:

- Which alarms and incidents are currently active.
- · Links to available Quick Links.
- List of installed Avaya SBCE security devices.
- Avaya SBCE deployment information.
- Area for viewing and exchanging text messages with other administrators.

# **Dashboard content descriptions**

Name	Description
System Time	The current system time.
Version	The system software version.
Build Date	The system software build date.
License State	The license state.
Aggregate Licensing Overages	The aggregate license information.
Peak Licensing Overage Count	The peak licensing count.

Table continues...

Name	Description
Last Logged in at	The date and time when the user last logged in.
Failed Login Attempts	The number of failed login attempts.
Installed Devices	A list of all Avaya SBCE security devices currently deployed throughout the network.
Incidents (past 24 hours)	A list of current incidents reported by Avaya SBCE security devices to the EMS web interface.
Active Alarms (past 24 hours)	A list of current alarms reported by Avaya SBCE security devices to the EMS web interface.
Add	A user-editable text message exchange area.
Notes	The text message created by using the <b>Add</b> function.

# Manage system alarms

Current system alarms are reported to the EMS web interface. The alarms are displayed as a red indicator on the Alarm viewer page and on the dashboard for the respective device.

The notifications provide the information necessary to clear the condition causing the alarm notification.

# Viewing current system alarms

#### About this task

The Alarms screen displays a summary of all currently active system alarms. If no alarms are active, the system displays a blank screen. The Alarms screen is accessed only if the **Alarm Status Indicator** on the toolbar indicates an alarm status, flashed red. Use the following procedure to view current system alarms.

## **Procedure**

- 1. Log in to the EMS web interface web interface with administrator credentials.
- 2. In the navigation pane, click EMS Dashboard.
- 3. On the toolbar, click **Active Alarms** or click on the specific alarm you want to view from the **Alarms (past 24 hours)** section of the Dashboard screen.

The EMS server displays the Alarms Viewer screen.

4. Select the Avaya SBCE device for which you want to view the alarms.

The Alarms section displays all the currently active alarms for the selected Avaya SBCE security device.

For the field description of each security reporting component of the Alarms screen, see Alarm Viewer field descriptions.

## **Alarm Viewer field descriptions**

Name	Description
ID	Sequential, numerical identifier of the alarm being reported.
Details	The specific or descriptive name of the active alarm.
State	Current state of the alarm: ON
	The <b>State</b> field for any displayed alarm is always: ON
Time	Date and time when the alarm was generated.
Device	The Avaya SBCE device that generated the alarm.

# Clearing system alarms

#### About this task

You can either delete a selected alarm or all alarms. Most of the alarms are cleared automatically when the condition to create these alarms no longer exist. However, there are some alarms that need to be cleared manually.

#### **Procedure**

- 1. Log in to the EMS web interface web interface with administrator credentials.
- 2. In the navigation pane, click EMS Dashboard.
- 3. To clear the selected alarm or all alarms, on the Alarms screen, click Clear Selected or Clear All.

The EMS server displays a confirmation pop-up window.

4. Click OK.

# Viewing system incidents

#### About this task

You can view a complete descriptive list of all system incidents that have occurred since the last viewing period by using the Incident screen. The screen displays the last five incidents at any point of time. With this feature, you can view system-wide incidents according to category, such as DoS, Policy, and Scrubbing. When the Incident screen is open, the latest incident information is available, and the operator can scroll through the incidents list. The screen can display up to 15 incidents at one time. Use the following procedure to view current system incidents.



You can only view the incidents. They cannot be edited or deleted.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS Dashboard**.

3. On the toolbar, click **Incidents**.

The EMS server displays the Incidents Viewer page.

You can view the incidents by clicking the specific incident on the Incidents (past 24 hours) section of the Dashboard screen.

4. Using the **Device** and **Category** fields, choose a search filter to find and display the particular incidents that you want to view.

The Incident screen display changes to reflect the search criteria when a selection is made.

- 5. To ensure that the EMS server displays all required incidents, periodically click **Refresh** to refresh the display.
- 6. Click Clear Filters.

The EMS server clears the filtering criteria of the **Device** and **Category** fields and sets the value of the fields to All.

7. Click **Generate Report** and select the start and end date to generate the report.

# Viewing system SIP statistics

#### About this task

The Statistics screen provides a snapshot display of certain cumulative, system-wide generic and SIP-specific operational information.



You can only view the statistics information. You cannot edit or delete the statistics information. However, you can reset the counters for the SIP statistics.

### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. On the **Status** toolbar, click **SIP Statistics**.



## Warning:

Do not click SIP Statistics repeatedly. If you repeatedly click and trigger frequent loading of the Statistics page, the Statistics Viewer page shows a communication error.

The EMS server displays the Statistics Viewer screen.

- 3. To view the statistics, click one of the following tabs:
  - SIP Summary
  - CES Summary
  - Subscriber Flow
  - Server Flow

- Policy
- From URI
- To URI
- Transcoding Summary
- Dynamic License Summary

#### **Related links**

Statistics Viewer field descriptions on page 21

# **Statistics Viewer field descriptions**

# **SIP Summary tab**

Name	Description
Active TCP Registrations	The number of active SIP registrations with TCP transport.
Active UDP Registrations	The number of active SIP registrations with UDP transport.
Active TLS Registrations	The number of active SIP registrations with TLS transport.
Active Calls	The number of active SIP calls.
Active SRTP Calls	The number of active calls using media as SRTP.
Active Subscriptions	The number of active subscriptions.
Active Video calls	The number of active video calls.
Active Transfer sessions	The number of active transfer sessions.
Active Shared Control sessions	The number of shared control sessions.

# **CES Summary tab**

Name	Description
1XM User Logins Failed	The number of failed Avaya one-X® Mobile user logins.
1XM User Logins Succeeded	The number of successful Avaya one-X <sup>®</sup> Mobile user logins.

## **Subscriber Flow tab**

Name	Description
Streaming	Specifies whether live statistics are displayed.
Subscriber Flow	Selects the subscriber flow for which statistics are displayed.
Name	Specifies the name of the statistic.
	This column lists the same statistics that the system displays in the <b>SIP Summary</b> tab.
Value	Specifies the value of the statistic.

# **Server Flow tab**

Name	Description
Streaming	Specifies whether live statistics are displayed.
Server Flow	Selects the server flow for which statistics are displayed.
Name	Specifies the name of the statistic.
	This column lists the same statistics that the system displays in the SIP Summary tab.
Value	Specifies the value of the statistic.

# Policy tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Policy Group	Selects the policy group for which statistics are displayed.
Name	Specifies the name of the statistic.
	This column lists the same statistics that the system displays in the SIP Summary tab.
Value	Specifies the value of the statistic.

# From URI tab

Name	Description		
Streaming	Specifies whether live statistics are displayed.		
URI Group	Selects the source URI group for which statistics are displayed.		
Name	Specifies the name of the statistic.		
	This column lists the same statistics that the system displays in the SIP Summary tab.		
Value	Specifies the value of the statistic.		

# To URI tab

Name	Description		
Streaming	Specifies whether live statistics are displayed.		
Policy Group	Selects the destination URI group for which statistics are displayed.		
Name	Specifies the name of the statistic.  This column lists the same statistics that the system displays in the SIP Summary tab.		
Value	Specifies the value of the statistic.		

# **Transcoding Summary**

Name	Description		
Streaming	Specifies whether live statistics are displayed.		
Total Active Transcoding Sessions	The number of active transcoding sessions.		
<b>Total Transcoding Sessions</b>	The number of transcoding sessions.		
Total Transcoding Sessions Failed	The number of failed transcoding sessions.		
Total Transcoding Sessions Modifications	The number of transcoding sessions that resulted in a change in codec		
Total Transcoding Sessions Modifications Failed	The number of transcoding sessions that resulted in a failure while changing codecs.		

# **License Summary**

Name	Description		
Streaming	Specifies whether live statistics are displayed.		
Standard Sessions Reserved	The number of standard session licenses that are reserved.		
Standard Sessions In-Use	The number of standard session licenses that are currently in use.		
Advanced Sessions Reserved	The number of advanced session licenses that are reserved.		
Advanced Sessions In-Use	The number of advanced session licenses that are currently in use.		
Scopia Video Sessions Reserved	The number of Avaya Scopia® video session licenses that are reserved.		
Scopia Video Sessions In- Use	The number of Avaya Scopia® video session licenses that are currently in use.		
CES Sessions Reserved	The number of CES session licenses that are reserved.		
CES Sessions In-Use	The number of CES session licenses that are currently in use.		
Transcoding Sessions Reserved	The number of transcoding session licenses that are reserved.		
Transcoding Sessions In- Use	The number of transcoding session licenses that are currently in use.		

## Related links

Viewing system SIP statistics on page 20

# Viewing periodic statistics

# Before you begin

Enable periodic statistics in **Network & Flows > Advanced Options**, and specify a collection interval.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials
- 2. On the Status toolbar, click Periodic Statistics.
- 3. To view the statistics, click one of the following tabs:
  - Summary
  - Subscriber Flow
  - Server Flow
  - Policy Group
  - To URI
  - From URI

#### Related links

Periodic statistics field descriptions on page 24

# Periodic statistics field descriptions

Name	Description		
Total Registrations	The number of active SIP registration requests received.		
Total Subscriptions	The number of active subscription requests received.		
Registrations Rejected	The number of rejected registrations.		
Subscriptions Rejected	The number of rejected subscriptions.		
Deregistrations	The number of de-registered requests.		
Unsubscriptions	The number of unsubscribed requests.		
Total Calls	The number of SIP calls received.		
Calls Terminated	The number of terminated SIP calls.		
Calls Rejected	The number of SIP calls rejected by Avaya SBCE because of policy violation.		
Calls Rejected by SBC	The number of SIP calls rejected by Avaya SBCE.		
Total Transferred Calls	The number of transferred SIP calls.		
Calls Failed in Transfer	The number of SIP calls failed in transfer.		
Total Redirected Calls	The number of redirected call.		

Table continues...

Name	Description			
Calls Failed in Redirection	The number calls failed in redirection.			
Total SRTP Calls	The number of SRTP calls.			
SRTP Calls Terminated	The number of terminated SRTP calls.			
SRTP Calls Rejected	The number of rejected SRTP calls.			
SRTP Calls Rejected by SBC	The number of SRTP calls rejected by Avaya SBCE.			
Total Video Calls	The number of video calls.			
Video Calls Terminated	The number of terminated video calls.			
Total Video Calls Rejected	The number of rejected video calls.			
Video Calls Rejected by SBC	The number of video calls rejected by Avaya SBCE.			
Transcoded Sessions	The number of transcoded sessions.			
Transcoded Sessions Terminated	The number of terminated transcoded sessions.			
Failed Transcoded Session	The number of failed transcoded sessions.			
Early Media Calls	The number of early media calls.			
Audit/Media Inactivity Detected	The number of calls in which Avaya SBCE detected any inactivity.			
Media Relinquished Calls	The number of media relinquished calls.			
Shared Control Calls	The number of shared control calls.			
Shared Control Calls Terminated	The number of terminated shared control calls.			
Info Sessions	The number of info sessions.			
Info Sessions Rejected	The number of rejected info sessions.			

#### Related links

Viewing periodic statistics on page 24

# **Real Time SIP Server Status**

Avaya SBCE Release 6.3 onwards, you can view the current status of the configured SIP servers. The EMS server displays the connectivity status for trunk servers and enterprise call servers. You can use the **Server Status** option of the **Status** toolbar to view the status of the connection. The Server Status screen displays the list of servers based on the settings on the Server Configuration screen.

For the servers to show up in the Status window, you must configure server heartbeat in Server Configuration.

# Viewing the status of the SIP servers

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. On the **Status** toolbar, click **Server Status**.

The EMS server displays the Status screen.

The EMS server displays server information, such as Server Profile, FQDN, IP address, Transport, Port, Heartbeat Status (UP/DOWN/UNKNOWN), Registration Status (REGISTERED/NOT REGISTERED/UNKNOWN) and Time when the status field was last updated.

# Viewing system logs

## About this task

SysLog Viewer displays the syslog file according to certain user-definable filtering criteria, such as log type, time period, and severity. Use the following procedure to define and view syslog reports.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. Select the **Logs** option from the toolbar, and click the **System Logs** menu.

The EMS server displays the Syslog Viewer screen. On this screen, you can specify criteria in the **Query Options** section to filter the results displayed.

3. In the Start Date and End Date fields, filter the results displayed in a search report to fall within starting and ending dates and times. In previous Avaya SBCE Syslog Viewer windows, there were four separate fields: Start Date, Start Time, End Date, and End Time.



#### Note:

The date and time entries are combined in a single field, mm/dd/yyyy [hh:mm], with the time entry, [hh:mm], being optional. An End Date or End Time entry is not required when you enter a Start Date or Start Time.

You can also select additional search criteria in the **Query Options** section.

4. In the **Keyword** field, type one or more words to define the limits of the log report, and click Search.

The system runs the report and displays the output.



#### Note:

Keyword searches are case-insensitive and tokenized. Each keyword term entered in the **Keyword** field is searched. However, for a log line to be included in a report, all keyword terms that are entered in the **Keyword** field must be found in that log line.

# **Syslog Viewer field descriptions**

# **Query Options section**

The Query Options section on the Syslog Viewer screen contains options for filtering the Syslog logs.

Name	Description		
Keyword	Search keywords for viewing logs.		
Start Date	Date and time from which you want to view logs.		
	You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.		
End Date	Date and time up to which you want to view logs		
	You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.		
Show	Number of entries to be displayed on a page.		
Class	Class of the logs to be displayed.		
	The options are:		
	• All		
	• Platform		
	• Trace		
	Security		
	• Protocol		
	• Incidents		
	Registration		
	• Audit		
	• GUI		
	• Unknown		
Severity	Severity of the logs to be displayed.		
	The options are :		
	• Unknown		
	• Info		
	• Notice		
	• Warning		
	• Error		
	• Critical		
	• Alert		
	• Emergency		

#### Results section

Name	Description		
Timestamp	Timestamp of the log message.		
Host	Device for which the log is generated.		
Severity	Severity of the message.		
Class	Class of the message.		
Summary	Summary of the message.		

# Viewing audit logs

#### About this task

Audit Log Viewer displays the contents of the audit log. The audit log contains a record of security related events, such as logins, session starts, session ends, new user additions, and password attempts/retries/changes. Use the following procedure to view the Audit Log Viewer information.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. On the toolbar, click Logs > Audit Logs.

The EMS server displays the Audit Log Viewer page.

- 3. In the **Start Date** and **End Date** fields, you can filter the results that are displayed in a search report to fall within starting and ending dates and times.
- 4. In the **Keyword** field, type one or more words to define the limits of the log report, and click **Search**.

In the Results section, the EMS server displays the report output.

- 5. To see additional details about a particular log line in a report, select the log line.
  - The EMS server displays the Audit Log Details page.
- 6. On the **Monitoring & Logging > Syslog Management** page, you can set the log level rules for the Audit Log and other logs.

Audit Logging is enabled in the Log Level row for the Audit class and Audit Facility as LOG\_LOCAL6.

The Log Level Facility name, LOG\_LOCAL6, is reserved for Audit Logging and cannot be changed. The LOG\_LOCAL6 file path destination cannot be changed either. The file path is /archive/syslog/ipcs/audit.log.

# Viewing diagnostics results

#### About this task

The Diagnostics screen provides a variety of tools to aid in troubleshooting Avaya SBCE operation. Available tools include a full diagnostic test suite, and individual tabs to monitor certain functional aspects of Avaya SBCE, such as TCP and TLS activity.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. On the toolbar, click **Diagnostics**.

The EMS server displays the Diagnostics page.

- 3. Click Full Diagnostics.
- 4. Click Start Diagnostic.

The tests listed in the **Task Description** column of the display are sequentially run, with the results of the test displayed in the **Status** column. If an error is encountered while running a test, the test continues until all tests are run. The EMS server displays the reason for the error in the **Status** column.

5. Click Ping Test.

The ping test can be used to verify basic IP connectivity to elements beyond the gateways. For example, ASM or the trunk server.

# Viewing administrative users

#### About this task

The Active Users page provides a summary of all active system administrative accounts currently logged on to the EMS web interface.



You can only view the users account information. You cannot modify the information.

Use the following procedure to view the system administrative accounts that are currently logged on to the interface.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. On the toolbar, click **Users**.

The EMS server displays the Active Users page.

# Managing Avaya SBCE logging level

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click Monitoring & Logging > Debugging.
- 3. On the Debugging page, click **Subsystem Logs** tab.
- 4. Select or clear the check boxes corresponding to the type of execution log that you want to enable or disable.
- Click Save.

#### Result

The EMS server displays a message at the top of the screen: Configuration update successful.

# Roll back to an earlier release

For information about upgrading to Avaya SBCE Release 8.0.x and rolling back to an earlier release, see *Upgrading Avaya Session Border Controller for Enterprise*.

# **Enhanced Access Security Gateway**

The Enhanced Access Security Gateway (EASG) system is a key element in protecting passwords and preventing unauthorized use of maintenance and administration login. EASG provides a secure method for Avaya support personnel to access Avaya SBCE remotely. Access is under the control of the customer. EASG is a 128–bit AES encrypted challenge-response mechanism for authentication. With this mechanism, Avaya SBCE can maintain secure access for services, administration, and maintenance. On Avaya Enterprise Communications System (ECS) products, Avaya services personnel use the EASG challenge and corresponding response for a single access attempt only. After each login, EASG uses a new challenge and response.

# Checking EASG status

## Before you begin

Log in to the application with the customer account.

#### **Procedure**

- 1. On the command line interface, type EASGStatus.
- 2. Press Enter.

The system displays one of the following:

- EASG is enabled if EASG is enabled.
- EASG is disabled if EASG is disabled.

# Enabling and disabling EASG using web interface

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS**.
- 3. In the navigation pane, click **System Administration > AAA**.
- 4. Click the **EASG** tab.
- 5. In the EASG Authentication Status section, do one of the following:
  - To enable EASG, click Enable.
  - To disable EASG, click Disable.

# **Enabling and disabling EASG using CLI**

#### About this task

Avaya recommends enabling EASG. By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements and allowing Avaya to resolve product issues in a timely manner. See the Avaya support site for additional information for registering products and establishing remote access and alarming.

By disablingAvaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

# Before you begin

Log in to the application with the customer account.

#### **Procedure**

- 1. On the command line interface, do one of the following:
  - To enable EASG, type EASGManage --enableEASG.

• To disable EASG, type EASGManage --disable EASG.

The system displays the message Do you want to continue [yes/no] ?

- 2. Type yes or no.
- 3. Press Enter.

# **EASGManage**

Use **EASGManage** to enable or disable the EASG authentication, check the status of EASG feature for the specified users, and display information about the available EASG users.

# **Syntax**

EASGManage [--enableEASG] [--disableEASG] [--enable user] [--disable user] [--userStatus user] [--listUsers] [--printDisableWarning] [--printEnableWarning]

**--enableEASG** Enables Enhanced Access Security Gateway (EASG) authentication.

**--disableEASG** Disables EASG authentication.

**--enable** Enables EASG authentication only for the Avaya Services logins

specified in the *user* variable. If the main EASG enable/disable switch is disabled, no Avaya Services logins will have access, no matter what this setting reflects for an individual Avaya Services Login. EASG supports only Avaya services logins, such as init, inads, and craft.

**--disable** Disables EASG authentication only for the Avaya Services logins

specified in the *user* variable.

**--userStatus** Displays the EASG status of the user specified in the *user* variable.

**--listUsers** Lists the available EASG users.

**--f** Forces the enable or disable action to run without prompts.

**--printDisableWarning** Displays the warning message for disabling EASG on the system.

**--printEnableWarning** Displays the warning message for enabling EASG on the system.

# Loading and managing site certificate

#### About this task

A customer can load a site certificate using EASGSiteCertManage --add <pkcs7\_file\_path> and will need to specify a Site Authentication Factor (SAF). The SAF will need to be provided to the technician and is also used by EASG Site Manager to generate a response to the EASG challenge.

# Before you begin Procedure

1. Log in to a Linux<sup>®</sup> shell by using the customer account.

The customer account is created during the deployment procedure.

2. At the command line type:

```
[cust@host ~]$ EASGSiteCertManage --add johndoe.p7b
You are about to install this site certificate into your trusted repository:
Technician Name: johndoe
Expiration Date: Nov 10 17:02:15 2016 GMT
Do you want to continue [yes/no]? yes
Please enter a site authentication factor (SAF) for the technician to use when
getting access to your machine. The SAF is alphanumeric with at least 10
characters and no more than 20 characters.
   Please enter your SAF: Site Authentication Factor
   Please confirm your SAF: Site Authentication Factor
Site Certificate installed successfully.
[cust@host ~]$
```

Save the Site Authentication Factor to share with the technician once on site.

3. You can view information about a particular certificate by using EASGSiteCertManage --show <pkcs7\_file\_path> and the certificate name is obtained from certificate list output.

**4.** The customer can delete the site certificate using EASGSiteCertManage --delete <pkcs7\_file\_path> and the certificate name is obtained from the certificate list output.

```
[cust@host ~]$ EASGSiteCertManage --delete johndoe.p7b
Successfully removed Site Cert: johndoe.p7b
[cust@host ~]$
```

# Support contact checklist

Use this checklist to collect the critical information that you must gather before you contact Avaya Technical Support.

Try to resolve the issue by using this document before you contact Avaya. Contacting Avaya is the final step only after you are unable to resolve the issue.

Gather the following information before you contact Avaya Technical Support:

No.	Task	Description	Notes	~
1	Your full name, organization, and telephone number where an Avaya representative can contact you about the problem.			
2	The Sold To number.	Also known as the Functional Location (FL) number.		
3	Detailed description of the problem.			
4	The type of service contract your organization has with Avaya.			
5	Your product release information.	Include the software versions, hardware deployment type, operating system, third-party software and database versions.		
6	Description of any Avaya Professional Services contracts.			
7	Description of remote access availability.			
8	Date and time when the problem started.	Refer to log files if applicable.	If the problem is intermittent, determine when the problem started and stopped.	
9	Frequency of the problem.			
10	What InSite Knowledge Base solutions have you tried?	Use the Advanced Search option to narrow your search to specific categories and document types.		
11	Detailed information about recent system upgrades, network changes, or custom applications.	Include the date and the time when the changes were made. Also include information about who made the changes.		
12	Appropriate logs and packet captures of the issue.	Take packet captures when the issue occurs and save appropriate logs to facilitate investigation.		

# **Chapter 3: Monitoring and analysis**

# Tools and utilities

# traceSBC tool

The tcpdump tool is the main troubleshooting tool of Avaya SBCE, which can capture network traffic. Using tcpdump is a reliable way to analyze the information arriving to and sent from Avaya SBCE. However, tcpdump has its own limitations, which can make troubleshooting difficult and time consuming. This traditional tool is not useful in handling encrypted traffic and real-time troubleshooting.

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the unencrypted private key of the Avaya SBCE is needed to decrypt the TLS and HTTPS traffic.

The traceSBC tool offers solutions for both issues. traceSBC is a perl script that parses Avaya SBCE log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, you can use the tool easily even in case of TLS and HTTPS. traceSBC can parse the log files downloaded from Avaya SBCE. traceSBC can also process log files real time on Avaya SBCE, so that you can check SIP and PPM traffic during live calls. The tool can also work in the noninteractive mode, which is useful for automation.

# Log files

Avaya SBCE can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files real-time by opening the latest log files in the given directories. traceSBC also checks regularly if a new file is generated, in which case the old one is closed and processing continues with the new one. A new log file is generated every time the relevant processes restart, or when the size reaches the limit of ~10 M.

## Log locations:

SIP messages are found at /archive/log/tracesbc/tracesbc\_sip/ and PPM messages can be found at /archive/log/tracesbc/tracesbc ppm/.

Active files are of the following format:

-rw-rw---- 1 root root 112445 Aug 21 10:12 tracesbc\_sip\_1408631651

Inactive or closed files are of the following format:

```
-rw-rw---- 1 root root 175236 Aug 21 06:33
tracesbc_sip_1408617250_1408620820_1 or
-rw-rw---- 1 root root 31706 Jul 10 13:34
tracesbc sip 1436549674 1436553270 1.gz
```

# SIP and PPM logging administration

SIP logging is always enabled by default. You can enable PPM, STUN, TLS, and AMS logging, if required.

# **Advantages**

## Memory

After 10000 captured messages, traceSBC stops processing the log files to prevent exhausting the memory. This check is done during the capture when the tool is parsing the log files. The tool counts the number of SIP and PPM messages in the logs. This number is not the number of messages sent or received on the interfaces. This counter is a summary of messages from all logs, not for each log. Note that this safeguard is present only for real-time mode. When the tool is used in nonreal-time mode, this counter does not stop processing the logs specified in the command line. The counter continues processing the logs specified in the command line to be able to process more files or messages in off-line mode.

#### **Processor**

A built-in mechanism is available to prevent high CPU usage. Throttling is not tied to CPU level. In the current implementation, throttling is done by releasing the CPU for a short period after each line of the file is processed. The result is that CPU occupancy is low on an idle system when the tool actively processes large log files. You can disable throttling by the –dt command line parameter which can be useful when processing large log files offline. However, in this case CPU occupancy might go up to 100%, and so you must not use this option on a live system.

# **Operation modes**

#### Non real-time mode

The tool starts with at least one file in the command line parameters. The tool automatically detects the type of files, processes the files, and finally displays messages from the different files in one diagram ordered by the timestamp. If filters are set, only the messages that match the filters are displayed in the diagram. In this mode, enabling live capture is not an option.

#### **Examples:**

```
# traceSBC tracesbc_sip_1408635251
# traceSBC /archive/log/tracesbc/tracesbc_sip/tracesbc_sip_1408635251 archive/log/
tracesbc/tracesbc_ppm/tracesbc_ppm_1408633429
```

#### Real-time mode

In this mode, traceSBC must be on active Avaya SBCE. traceSBC is started without specifying a file in the command line parameters. The tool automatically starts processing the log files. The live capture can be started and stopped anytime without affecting service.

#### Example:

```
# traceSBC
```

#### **Automatic mode**

In this mode, traceSBC must be on the Avaya SBCE and the command is called with -a and -w parameters at a minimum.

### Example:

```
# traceSBC -a "sip|ppm" -w /tmp/trace.log
```

Use this mode for test automation. You can also use this mode to stop capture when a certain condition is met, and then save filtered messages automatically. Multiple stop triggers are present. such as number of packets, time, regular expression, and a combination of these. When a stop trigger fires, or when you press CTRL+C, the tool automatically saves the filtered messages and stops the captures.

### User interface

#### Window header

The window header shows the hostname, the name of the script, the number of captured messages, and the number of displayed messages that matched the filters. The header also displays warning messages such as MAX NUM PACKETS 10000 EXCEEDED.

### Ladder diagram

The ladder diagram displays the filtered messages. The arrow shows the direction of the message between the SBC and the host from where the message arrived or was sent to. The IP of the host is at the top of the column. If the host is an Avaya phone, traceSBC attempts to extract the user information from the message, and replaces the IP with the user handle. To navigate between the messages, use the UP/DOWN arrow keys. The message is highlighted. To see the details of the message, press Enter. The header of the message detail form shows the source and destination IP or port and the transport protocol.

### Status bar

The bottom line has two areas, and its content depends on which mode the tool is in. The left side of the status bar shows the filename in nonreal-time mode, or shows Multiple files when the tool was called with more than one file. In real-time mode, this area shows which trace is active. Red means disabled, and green means enabled.

The rest of the status bar lists the available commands:

s=Start / s=Stop: Starts or stops live capture, which means the tool enables or disables the appropriate logging. Capture can be enabled for SIP and PPM individually. Stop disables all logging at the same time and stops processing the log files. This command shows only if the tool was started in real-time mode.

#### Note:

Depending on the traffic and the capture modes at the time of stopping the trace, the log files might contain more messages than the messages already captured by the tool.

q=Quit: Quit from the tool. If capture is running, the tool shows a pop-up to confirm the exit without stopping the logging.

f=Filters: Set new filter options. The filter options set in the dialog window override the command line filter settings. If no New Filter is entered, the Current Filter will remain active. To clear all filters, type e or erase in the New Filter field.

w=Write: Export filtered messages to a file. The dialog prompts you for a filename. The system saves SIP messages in the specified file to the current directory. The system saves PPM messages in a separate file with .ppm extension. The system also exports SIP messages in pcapng format to a file with .pcapng extension. SIP messages can be exported if text2pcap and tshark utilities are available on the machine where traceSBC is run.

i=IP / i=Name: Toggle between IP and user name presentation of the hosts in the header of the ladder diagram.

**T=RTP**: Turn RTP simulation on or off. When a session is established early or confirmed, the tool inserts a line in the diagram. This line represents the RTP stream between the two hosts described by the SDP. The diagram also shows the negotiated codec type.

### Note:

The RTP stream is created based on the negotiated information in SDP. However, there is no guarantee that these RTP streams come to the system.

u=Full Screen: Use the full screen for the message detail box without having the left and right side of the frame. This option is useful not only to see more about the message, but to easily copy or paste the content.

d=Calls: Shows the summary of all calls.

### **Trace**

With the Trace function, you can trace an individual packet or group of packets comprising a call through Avaya SBCE. The information shows how the call traversed the Avaya SBCE-secured network.

## **Configuring Packet Capture**

### About this task

Use the following procedure to set the filtering options and to capture packets or message flow.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **SBCE**.
- 3. In the navigation pane, click **Monitoring & Logging > Trace**.
- 4. Click **Packet Capture** or the **Captures** tab for the required information.
- 5. Navigate to a directory for saving the Packet Capture (pcap) file and click **Save** to save the file to the new directory.
- 6. Use Wireshark or a similar application to open up the Packet Capture (pcap) file. If Wireshark is already installed, you can double-click the file to open it with Wireshark. Otherwise, start Wireshark first and then either open the file from within the Wireshark application or double-click the Packet Capture file.

### Note:

You can view the file using Wireshark (originally named Ethereal), a free and opensource packet analyzer application used for network troubleshooting, analysis, and software protocol development. You can download and install Wireshark, or a similar network analyzer program, to view the Packet Capture (pcap) file.

## tcpdump

You can use topdump to capture packets from the CLI if you need to capture more than 10000 packets. After the captures are taken, ensure you stop the command.

For packet capture started through GUI, the output files are stored in /archive/pcapfiles/IPCS2.

### Running tcpdump in CLI

#### **Procedure**

- 1. Log on to the EMS server through SSH with ipcs user credentials.
- 2. At the command prompt, type cd /archive/pcapfiles/IPCS2.
- 3. Type tcpdump -ni any -s 0 -w 'filename.pcap', where filename is the name of the packet capture file.
- 4. To run packet captures on a specific interface, type tcpdump -i any -s 0 -w 'filename.pcap'

To run packet captures on a specific interface, use tcpdump -I data\_interface. For Tilera Gx card, you cannot use the *any* interface option. Packet capturing on Avaya SBCE negatively impacts packet latency.

- 5. Wait for the capture to end, and press Ctrl+C.
- 6. Type chown ipcs:ipcs filename.pcap.

The system displays the packet capture file in the **Captures** tab in the EMS web interface.

## showflow

A flow is a connection between an endpoint and Avaya SBCE. Types of flows are:

- Static: A static flow is configured on the Avaya SBCE only one time. Static flows do not change until the administrator changes the flows. Static flows are used, for example, for connections between endpoints and an Avaya SBCE signaling address.
- Dynamic: A dynamic flow is a transient connection between an endpoint and Avaya SBCE.
   Software creates, modifies, and deletes dynamic flows to support the transfer of media packets through Avaya SBCE.

Many flows can exist on Avaya SBCE simultaneously. To troubleshoot issues with Avaya SBCE, you can use the **showflow** command to display flows with varying levels of detail.

### **Syntax**

showflow 310 flow-type detail-levelfilter-ip

### flowtype

The flow type can be:

- · static: Shows all static flows.
- · dynamic: Shows all dynamic flows.
- turn client side: Shows all TURN flows on the listen interface of Avaya SBCE.
- turn far side: Shows all TURN flows on the relay interface of Avaya SBCE.
- blacklist: Shows all IP addresses that are currently blacklisted. Packets from blacklisted addresses do not match any flows.
- whitelist: Shows only those static flows that require whitelisting of the endpoint IP address.

#### detaillevel

You can specify the detail level for dynamic flows. The detail level for all other flows is fixed. When levels exceed the default detail level 0, you can see the default flow information and also additional information for the flow. The detail levels for dynamic flows can be:

- 0: Shows the default level of information. If a detail level is not specified in the command, the system uses 0 detail level.
- 1: Adds more decrypt information to every flow.
- 2: Adds more encrypt information to every flow.
- 3: Adds the physical port number for the output of the flow. Packets matching this flow are sent out of this physical port.
- 4: Adds relay information. Packets matching this flow are changed according to this relay before they are forwarded.
- 5: Adds VLAN identifiers and flow statistics.
- 6: Adds SIPREC information. This option does not change non-SIPREC flows.
- 7: Adds encrypt information for a SIPREC flow. This option does not change non-SIPREC flows.
- 8: Adds decrypt information for a SIPREC flow. This option does not change non-SIPREC flows.

#### filter-ip

If you specify a filter IP address, the **showflow** command displays dynamic flows that use the IP address that you specified as:

- An input or a packet source
- An output or a packet destination

When you specify a filter IP address, the showflow command displays dynamic flows pertaining to an endpoint with that IP address. If you do not provide a filter IP address, the system displays all dynamic flows.

### **Description**

**Showflow** is a root-level console command to display the flows that are currently active on Avaya SBCE.

### Example

The following example displays full details of all dynamic flows with 10.20.30.40 as a source or destination:

**showflow** 310 dynamic 8 10.20.30.40

The following example displays all static flows:

showflow 310 static

## **Debugging logs**

## **Enabling application debug logs**

### About this task

The debugging logs are located at /archive/log/ipcs/ss/logfiles/elog/. You can collect the logs from the console.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **Monitoring & Logging > Debugging**.
- Click the Subsystem Logs tab.
- 4. Select the device on which you want to toggle the log settings.
- 5. Do one of the following:
  - To turn on all debug information on the device, select the **Debug**, **Info**, and **Warning** log level check boxes at the top of the table.
  - To select a specific log level for all subsystems, select the **Debug**, **Info**, or **Warning** log level check box at the top of the table.
  - To select log levels for a specific subsystem, select the **Debug**, **Info**, or **Warning** log level check box next to the subsystem.
- 6. Click Save.

## **Debugging field descriptions**

## **Subsystem Logs**

Name	Description		
Process	Specifies the process for which you want to enable logs.		
	This field displays processes such as:		
	• LogServer		
	• OAMPSERVER		
	• SYSMON		
	• SSYNDI		
	TURNCONTROLLER		
Subsystem	Specifies the subsystem for which you want to enable logs.		
Debug	Specifies that debug logs are enabled for a subsystem.		
	If you select the <b>Debug</b> check box in the table header, the system selects debug logs for all processes.		
Info	Specifies that informational logs are enabled for a subsystem.		
	If you select the <b>Info</b> check box in the table header, the system selects informational logs for all processes.		
Warning	Specifies that warning logs are enabled for a subsystem.		
	If you select the <b>Warning</b> check box in the table header, the system selects warning logs for all processes.		

## **GUI logs**

Name	Description	
GUI	Controls master log levels for all GUI logs.	
	The options are:	
	• Info	
	• Warn	
	• Error	
IH	Creates detailed logs generated by a GUI IH client. IH handles statistics retrieval from the application.	
SOAP	Creates detailed logs generated by a GUI SOAP client. SOAP handles communication with EMS and Avaya SBCE Communication Manager servers, for example, restart application, reboot device, and uninstall device.	

Name	Description		
EMS-CM Relay	Creates detailed logs generated by SOAP relay module. This module handles communication relay between EMS Communication Manager and Avaya SBCE Communication Manager. For example, for device registration and configuration retrieval.		
Shell Commands	Creates detailed logs when you start any external process.		
File Uploads	Creates detailed logs for user file uploads, for example, upgrade packages, scrubber packages, and certificates.		
Licensing	Creates detailed logs generated by a GUI WebLM client.		
Third Party Components	Controls a master log level for third-party logs. This log level covers any logs from third-party libraries that the GUI uses.		
	The options are:		
	• Debug		
	• Info		
	• Warn		
	• Error		
SSH	Controls log levels for a third-party SSH library used for backup or restore and remote actions. The options are:		
	Inherit		
	• Debug		
	• Info		
	• Warn		
	• Error		

## **Third-Party Logs**

Name	Description
Nginx	Controls log levels for nginx.
	The options are:
	• Info
	• Notice
	• Warn
	• Error
	• Crit
	• Alert
	• Emerg

Name	Description	
Transcoding	Controls log levels for transcoding.	
	The options are:	
	• None	
	• All	

## Disabling application debug logs

### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **Monitoring & Logging > Debugging**.
- 3. Click the **Subsystem Logs** tab.
- 4. Deselect all the **Debug/Info/Warning** log level check boxes. If you want to deselect a specific log level check box for all devices, click the check box on the top of the table.
- 5. Click Save.

## **Enabling GUI debug logs**

### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS**.
- 3. In the navigation pane, click **Monitoring & Logging > Debugging**.
- 4. In the content area, click **GUI Logs** tab.
- Select the required log levels.
- 6. Click Save.

## **Disabling GUI Logs**

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS**.
- 3. In the navigation pane, click **Monitoring & Logging > Debugging**.
- 4. In the content area, click **GUI Logs**.
- 5. Clear the required log levels.

### 6. Click Save.

## **Debug logs location**

The debug logs can be collected from the console.

The elog files for processes running on Avaya SBCE are available at /archive/log/ipcs/ss/logfiles/elog/. The elog files for processes running on EMS are available at /archive/log/ipcs/sems/logfiles/elog/.

PCF logs for the Tilera Gx adapter are available in the host kernel log file at /archive/syslog/ipcs/kern.log.

Table 3: Elog locations for processes

Process	elog Path	Purpose		
EMS				
SYSMON	/archive/log/ipcs/sems/ logfiles/elog/SYSMON	To debug connectivity issues between Avaya SBCE and EMS, process restart due to ping failure, and HA issues		
OAMPSERVER	/archive/log/ipcs/sems/ logfiles/elog/OAMPSERVER	To manage SNMP configuration of EMS		
LOGSERVER	/archive/log/ipcs/sems/ logfiles/elog/LogServer	To debug issues related to logging for other processes		
Avaya SBCE	Avaya SBCE			
SBC SYSMON	/archive/log/ipcs/ss/ logfiles/elog/SYSMON	To debug connectivity issues between Avaya SBCE and EMS, process restart due to ping failure, and HA issues		
SSYNDI	/archive/log/ipcs/ss/ logfiles/elog/SSYNDI	To debug SIP application and media issues		
OAMPSERVER	/archive/log/ipcs/ss/ logfiles/elog/OAMPSERVER	To debug SNMP and statistics		
TURNCONTROLLER	/archive/log/ipcs/ss/ logfiles/elog/ TURNCONTROLLER	To debug issues with TURN/ STUN		

TraceSBC logs for SIP are available at /archive/log/tracesbc/tracesbc\_sip. TraceSBC logs for PPM are available at /archive/log/tracesbc/tracesbc ppm

Core dumps are generated at /archive/crash. Smdumps for each process is available at /usr/local/ipcs/smdump/.

## **Traps**

To see Avaya SBCE alarms on System Manager, you must upload the Avaya SBCE common alarms definition file (cadf) to System Manager. For more information, see *Administering Avaya Session Border Controller for Enterprise*.

Trap	Component of Avaya SBCE from which the Trap is generating	Cause
ipcsCPUUsageNotification	EMS	CPU utilisation exceeds a set
	SBCE	threshold
ipcsMemoryUsageNotification	EMS	Memory utilisation exceeds a set
	SBCE	threshold
ipcsDiskUsageNotification	EMS	Disk space utilization exceeds a
	SBCE	set threshold
ipcsDiskFailureNotification	EMS	Hard Disk fails
	SBCE	
ipcsNetworkFailureNotification	EMS	Network fails
	SBCE	
ipcsHAFailureNotification	SBCE: For HA deployment mode	HA failure
		When Avaya SBCE generates this trap, the primary SBCE goes down and secondary SBCE switches to primary state.
ipcsHAHeartBeatFailureNotificati on	SBCE: For HA deployment mode	Connection between SM and Avaya SBCE breaks OR
		SM stops sending responses
ipcsScpFailureNotification	EMS	SCP of Log Archive fails
	SBCE	
ipcsCopyFailureNotification	EMS	Copy of Log Archive fails
	SBCE	
ipcsProcessFailNotification	EMS	A process starts after the process
	SBCE	fails
ipcsDatabaseFailNotification	EMS	Either the database is down or
	SBCE	connectivity to the database has been lost

## **Incidents**

The following sections describe the incidents that can occur in Avaya SBCE.

## Denial of Service (DoS) incidents

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsSingleSourceDoS	SBCE	Avaya SBCE detects a single source DoS
ipcsSingleSourceCallWalk DoS	SBCE	Avaya SBCE detects a call walk DoS
ipcsPhoneDoS	SBCE	Avaya SBCE detects a phone DoS
ipcsPhoneStealthDoS	SBCE	Avaya SBCE detects a phone stealth DoS
ipcsServerDoS	SBCE	Avaya SBCE detects a server DoS or blocks a server DoS
		The incident occurs due to any of the following reasons:
		Initiated Threshold Crossed - Action Whitelist
		Pending Threshold Crossed- Action Whitelist
		Failed Threshold Crossed- Action Whitelist
		attack from Server side - Initiated Threshold Crossed- Action SIV
		attack from Server side - Pending Threshold Crossed- Action SIV
		attack from Server side - Failed Threshold Crossed- Action SIV
		Initiated Threshold Crossed- Action Limit
		Pending Threshold Crossed- Action Limit
		Failed Threshold Crossed- Action Limit
ipcsPhoneStealthDDoS	SBCE	Avaya SBCE detects a phone stealth DDoS
ipcsDomainDoS	SBCE	Avaya SBCE detects a domain DoS

### **Blacklist/Whitelist incidents**

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsBlackipcsListCallBloc ked	SBCE	Avaya SBCE comes across a blacklisted caller

## Scrubbing related incidents

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsDroppedScrubMsg	SBCE	Avaya SBCE comes across a SDP parser error or scrubber anomaly
ipcsRejectedScrubMsg	SBCE	Avaya SBCE comes across a scrubber anomaly
ipcsDetectedScrubMsg	SBCE	Avaya SBCE comes across a scrubber anomaly

## **Protocol discrepancy incidents**

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsACKMsgOutofDialogu e	SBCE	Avaya SBCE gets an out of dialogue ACK message
ipcsBYEMsgOutofDialogu e	SBCE	Avaya SBCE gets an out of dialogue BYE message
ipcsCANCELMsgOutofDia logue	SBCE	Avaya SBCE gets an out of dialogue CANCEL message
ipcsNOTIFYMsgOutofDial ogue	SBCE	Avaya SBCE gets an out of dialogue NOTIFY message
ipcsPRACKMsgOutofDial ogue	SBCE	Avaya SBCE gets an out of dialogue PRACK message
ipcsREINVITEMsgOutofDi alogue	SBCE	Avaya SBCE gets an out of dialogue REINVITE message
ipcsREFERMsgOutofDial ogue	SBCE	Avaya SBCE gets an out of dialogue REFER message
ipcs1XXMsgOutofTransac tion	SBCE	Avaya SBCE gets an out of dialogue 1xx class response
ipcs2XXMsgOutofTransac tion	SBCE	Avaya SBCE gets an out of dialogue 2xx class response
ipcs3XXMsgOutofTransac tion	SBCE	Avaya SBCE gets an out of dialogue 3xx class response
ipcs4XXMsgOutofTransac tion	SBCE	Avaya SBCE gets an out of dialogue 4xx class response
ipcs5XXMsgOutofTransac tion	SBCE	Avaya SBCE gets an out of dialogue 5xx class response
ipcs6XXMsgOutofTransac tion	SBCE	Avaya SBCE gets an out of dialogue 6xx class response
ipcsAuthRealmMismatch	SBCE	Avaya SBCE comes across a realm mismatch

## **Policy related incidents**

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsCallDenied	SBCE	Calls to the Avaya SBCE are denied due to any of the following reasons:
		Video is disabled or disallowed
		Audio is disabled or disallowed
		Maximum number of video sessions is exceeded
		Maximum number of audio sessions is exceeded
		Maximum number of audio sessions per endpoint is exceeded
		Maximum number of video sessions per endpoint is exceeded
		No Server Flow is matched for incoming message
		No Server Flow is matched for outgoing message
		No Subscriber Flow is matched
		Prop method disallowed out of dialog message
		Standard method disallowed out of dialog message
		No Routing Rule is matched
		Codec is disallowed
		Method is disallowed

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsRegistrationDenied	SBCE	Avaya SBCE denies registration because of any of the following reasons:
		No Server Flow is matched for incoming message
		No Server Flow is matched for outgoing message
		No Subscriber Flow is matched
		Prop method disallowed out of dialog message
		Standard method disallowed out of dialog message
		No Routing Rule is matched
		Method is disallowed
ipcsSubscriptionDenied	SBCE	Avaya SBCE denies subscription because of any of the following reasons:
		No Server Flow is matched for incoming message
		No Server Flow is matched for outgoing message
		No Subscriber Flow is matched
		Prop method disallowed in dialog message
		Standard method disallowed in out of dialog message
		No Routing Rule is matched
		Method is disallowed

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsRedirectionDenied	SBCE	Avaya SBCE denies redirection because of any of the following reasons:
		No Server Flow is matched for incoming message
		No Server Flow is matched for outgoing message
		No Subscriber Flow is matched
		Prop method disallowed in dialog message
		Standard method disallowed in dialog message
		Prop method disallowed in out of dialog message
		Standard method disallowed in out of dialog message
		No Routing Rule is matched
		Method is disallowed

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsMessageDropped	SBCE	Avaya SBCE drops a message because of any of the following reasons:
		No Server Flow is matched for incoming message
		No Server Flow is matched for outgoing message
		No Subscriber Flow is matched
		Response prop header is disallowed
		Response standard header is disallowed
		Response prop header is mandatory
		Response standard header is mandatory
		Response prop header is disallowed
		Response standard header is disallowed
		Request prop header is mandatory
		Request standard header is mandatory
		Prop method disallowed in dialog message
		Standard method disallowed in dialog message
		Method is disallowed
		Prop method disallowed in out of dialog message
		Standard method disallowed in out of dialog message

### **Route incidents**

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsPrimaryRadiusServer Unreachable	EMS	Primary Radius server is unreachable
ipcsSecondaryRadiusSer verUnreachable	EMS	Secondary Radius server is unreachable

### TLS certificate failure incidents

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsTlsCertificate	SBCE	Avaya SBCE comes across a TLS certificate error because of any of the following causes:
		Could not create TLS context - for default client mode
		No cipher list is provided
		Could not create TLS context for either server or client mode
		Could not read Certificate
		Could not read private key
		Private key does not correspond to the loaded certificate
		Unable to load Root Certificate or CA list
		Unable to load CRL list
		Unable to cipher list provided
		No cipher list provided

## Media anomaly detection incidents

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsPacketSizeViolation	SBCE	Avaya SBCE comes across a packet size violation
ipcsSSRCViolation	SBCE	Avaya SBCE comes across a synchronization source
ipcsSeqNoViolation	SBCE	Avaya SBCE comes across a sequence number violation
ipcsTimestampViolation	SBCE	Avaya SBCE comes across a timestamp violation
ipcsMediaInActivityFromB othSides	SBCE	Avaya SBCE comes across a media inactivity from both sides of the call
ipcsUnsupportedMedia	SBCE	Avaya SBCE comes across unsupported media
ipcsRTPDoSAttack	SBCE	Avaya SBCE comes across an RTP denial of service attack
ipcsMediaPortUnavailable	SBCE	No free media ports are available
ipcsRTPInjectionAttack	SBCE	Avaya SBCE comes across an RTP injection attack

### **HA** link failover incident

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
ipcsHAGracefulFailover	SBCE	The primary server has gone down voluntarily
ipcsHAKaFail	SBCE	High Availability keep alive messages fail
ipcsHATakeoverDone	SBCE	HA takeover is completed
ipcsHASecondaryDown	SBCE	HA secondary server is down and HA will not be available until the secondary server is up

### License incidents

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
sbcLicenseExceeded	SBCE	Avaya SBCE gets requests after the maximum number of licensed sessions is exceeded

### **TURN/STUN** incidents

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
sbcTurnStunMediaRelayC reationFailed	SBCE	Media relay flow creation failed
sbcTurnStunMediaRelayD eletionFailed	SBCE	Media relay flow deletion failed
sbcTurnStunServerError	SBCE	Avaya SBCE detects a TURN/STUN error because of any of the following reasons:
		Invalid User Name is configured
		Invalid Realm is configured
		Invalid Password is configured
		Invalid Realm is configured
		Relay Port is unavailable
		TCP/TLS Listener has failed
		Invalid User Account is configured
		Invalid User Name is configured

### **CES Proxy incidents**

Incident Name	Component of Avaya SBCE from which the incident is generating	Cause
sbcCesProxy1xMUserLog inFailed	SBCE	Login attempts from an Avaya one-X <sup>®</sup> Mobile user to the CES proxy fails because of any of the following reasons:
		Protocol Type validation failed
		CesProxy data is not present
		Avaya SBCE received an invalid response other than login response
		Object Type validation failed
		Login request data type validation failed
		Login request key id validation failed
		API object type validation failed
		API data type and key Id validation failed
		API data type validation failed
		API key id validation failed
		Object type validation failed
		Avaya one-X <sup>®</sup> Mobile user login failed

## Logs collection

Using log collection feature you can:

- Collect and download logs from a web interface for investigating and troubleshooting an issue.
- Sort the collected logs by File Name, File Size, and Last Modified.
- Sort the collected logs in ascending and descending order.
- Delete the logs that you do not require.

## Collecting and downloading logs

### About this task

Use this procedure to collect and download logs from a web interface for investigating and troubleshooting an issue.

### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click SBCE.
- 3. In the navigation pane, click **Monitoring & Logging > Logs Collection**.
- 4. In the application pane, click the type of device for which you want to collect logs.
- 5. In the content area, click the **Collect Logs** tab and do the following:
  - a. Select the type of logs that you want to collect.
  - b. Click Collect Logs to collect the selected logs.

The EMS server saves the collected logs in **Log Archive**.

- 6. In the content area, do the following:
  - a. Click **Log Archive**.
  - b. Select the log file that you want to download.

The EMS server saves the log file on your computer.

## **Collect logs field descriptions**

Name	Description
All Logs	Specifies database and application logs that show the status of the system and configuration information. Crash dumps logs are not included in the <b>All logs</b> option because of the large size. Crash dumps logs can be collected separately.
	Note:
	The remaining options are clear when you select the <b>All Logs</b> check box .
Database logs	Specifies the database dump logs.
Application logs	Specifies SSYNDI logs.
GUI logs	Specifies the web interface and jsp logs.
	Note:
	The <b>GUI logs</b> option is available for EMS only.
Upgrade Logs	Specifies upgrade related logs.
Crash Dumps	Specifies heap dumps.
From Date & Time	Specifies the <b>From Date &amp; Time</b> after which any log file modified or generated will be collected.

Name	Description
To Date & Time	Specifies the <b>To Date &amp; Time</b> before which any log file modified or generated will be collected.
	Note:
	Logs generated and modified between From Date & Time and To Date & Time time range will be collected.

## **Collect Archive field descriptions**

Name	Description
File Name	The file name of the collected logs.
File Size	The size of the collected logs in bytes.
Last Modified	The date and time when the collected logs were last modified.

Button	Description
Delete	Deletes the selected log.

## **SNMP MIB**

Management Information Base (MIB) are defined in RFC-1213. Avaya SBCE supports rfc1213.mib.

## **MIB-II** support

Avaya SBCEsupports MIB-II (RFC1213) for Avaya SBCE data interfaces.

## **SBCE OID Descriptions**

This section describes the key Object Identifiers (OIDs).

## **Private Enterprise OIDs support**

Avaya SBCE supports the following private enterprise OIDs.

ipcs stats sip calls: . 1.3.6.1.4.1.6889.2.77.1.3.1	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstat ssip.ipcsstatssipcalls
ipcs stats sip protocol: . 1.3.6.1.4.1.6889.2.77.1.3.3	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstat ssip.ipcsstatssipprotocol
Ipcsincidencesinfo: . 1.3.6.1.4.1.6889.2.77.4	.iso.org.dod.internet.private.enterprises.Avaya.ipcsincidencesinfo
Ipcsalarmsinfo: . 1.3.6.1.4.1.6889.2.77.2	.iso.org.dod.internet.private.enterprises.Avaya.ipcsalarmsinfo

## **Key OIDs**

## **Ipcsstatssipcalls**

ipcssipcTotalRegistrationRequests	Number of Registration Requests received at node. This number does not include the registration triggered by node for keeping the pinhole open.
ipcssipcTotalRegistrationsChallenged	Number of Registrations Challenged by node and also includes the number of challenges from the Call Server. The number of registrations challenged by IPCS node includes the SIP 401/407 based Radius Authentication Responses (AAA feature) and SIP 407 based SIV Authentication Responses (DOS feature).
ipcssipcTotalRegistrationsRejected	Number of Registrations Rejected by the node and also includes the failed registration responses observed from the call server at the node. Failed registration responses include the SIP 4xx-6xx class responses excluding SIP 400, SIP 401/407 Responses. The registrations are rejected by the node due to failed registration challenges, failed registration processing, and registrations blocked due to security features.
ipcssipcTotalCallsReceived	Total Number of SIP Calls received at the node. This number equals Calls Blocked + Calls Allowed.
ipcssipcTotalCallsBlocked	Number of SIP calls Blocked by the node due to SIP Parse errors, failed AAA challenges, and calls blocked due to security features.
ipcssipcTotalCallsAllowed	Number of SIP calls classified by the node as Legitimate.

# Classification of Requests/Responses matching a particular Domain Policy Group at the node

ipcsTotalINVITES	Number of SIP INVITE messages
ipcsTotalINVITERetransmits	Number of SIP INVITE Retransmits
ipcsTotalINVITE100Responses	Number of SIP INVITE 100 Responses

Number of SIP INVITE 1XX class Responses
excluding SIP 100 Response.
Number of SIP INVITE 200 Responses
Number of SIP INVITE 200 Response Retransmits
Number of SIP INVITE 4XX 6XX Responses
Number of SIP INVITE 4XX 6XX Response Retransmits
Number of SIP BYE requests
Number of SIP BYE Retransmits
Number of SIP BYE 200 Responses
Number of SIP CANCEL requests
Number of SIP CANCEL 200 Responses
Number of SIP ACK requests for INVITE 200 OK Response
Number of SIP ACK requests for INVITE 4xx-6xx class Responses
Number of SIP ACK timeouts ie. Number of ACK requests missing for the INVITE 200 OK/4xx-6xx class responses
Number of NonInvite Requests
Number of NonInvite 1xx Responses
Number of NonInvite 2xx Responses. Also includes the 200 OK responses for BYE and CANCEL requests

## **Out of Dialog Requests dropped**

ipcsTotalOutOfDialogReferMesFromNW	Number of Out of Dialog REFER requests dropped at the node
IpcsTotalAckMessageOutOfDialogue	Number of Out of Dialog ACK requests dropped at the node
IpcsTotalByeMessageOutOfDialogue	Number of Out of Dialog BYE requests dropped at the node
IpcsTotalCancelMessageOutOfDialogue	Number of Out of Dialog CANCEL requests dropped at the node
IpcsTotalNotifyMessageOutOfDialogue	Number of Out of Dialog NOTIFY requests dropped at the node
ipcsTotalReinviteMessageOutOfDialogue	Number of Out of Dialog RE-INVITE requests dropped at the node

## **Out of Dialog Responses dropped**

ipcsTotal1XXMessageOutOfDialogue	Number of Out of Dialog 1XX class responses dropped by the node
ipcsTotal2XXMessageOutOfDialogue	Number of Out of Dialog 2XX class responses dropped by the node
ipcsTotal3XXMessageOutOfDialogue	Number of Out of Dialog 3XX class responses dropped by the node
ipcsTotal4XXMessageOutOfDialogue	Number of Out of Dialog 4XX class responses dropped by the node
ipcsTotal5XXMessageOutOfDialogue	Number of Out of Dialog 5XX class responses dropped by the node
ipcsTotal6XXMessageOutOfDialogue	Number of Out of Dialog 6XX class responses dropped by the node

## **Out of Transaction Responses dropped**

ipcsTotal1XXMessageOutOfTransaction	Number of 1XX Messages received out of transaction dropped by the node
ipcsTotal2XXMessageOutOfTransaction	Number of 2XX Messages received out of transaction dropped by the node
ipcsTotal3XXMessageOutOfTransaction	Number of 3XX Messages received out of transaction dropped by the node
ipcsTotal4XXMessageOutOfTransaction	Number of 4XX Messages received out of transaction dropped by the node
ipcsTotal5XXMessageOutOfTransaction	Number of 5XX Messages received out of transaction dropped by the node
ipcsTotal6XXMessageOutOfTransaction	Number of 6XX Messages received out of transaction dropped by the node
ipcsTotalCancelMessageOutOfTransaction	Number of CANCEL requests received out of transaction dropped by the node

### **WebRTC statistics**

OID	Description
ipcswebrtcStunBindingSuccess	Number of successful STUN bindings
ipcswebrtcStunBindingFailure	Number of failed STUN bindings
ipcswebrtcAllocateSuccess	Number of successful TURN allocations
ipcswebrtcAllocateFailure	Number of failed TURN allocations
ipcswebrtcRefreshSuccess	Number of successful TURN allocation refreshes
ipcswebrtcRefreshFailure	Number of failed TURN allocation refreshes
ipcswebrtcChannelBindSuccess	Number of successful channel bindings
ipcswebrtcChannelBindFailure	Number of failed channel bindings

## **Other OIDs**

OID	Description
ipcssipcTotalActiveRegistrations	The number of active SIP registrations.
ipcssipcTotalActiveCalls	The number of active SIP calls.
ipcssipcTotalActiveTCPRegistrations	The number of active SIP registrations with TCP transport.
ipcssipcTotalActiveUDPRegistrations	The number of active SIP registrations with UDP transport.
ipcssipcTotalActiveTLSRegistrations	The number of active SIP registrations with TLS transport.
ipcssipcTotalActiveSRTPCalls	The number of active calls using media as SRTP.
ipcssipcTotalRegistrations	The number of active SIP registration requests received.
ipcssipcTotalTCPRegistrations	The number of SIP registrations received with TCP transport.
ipcssipcTotalUDPRegistrations	The number of SIP registrations received with UDP transport.
ipcssipcTotalTLSRegistrations	The number of SIP registrations received with TLS transport.
ipcssipcTotalCalls	The number of SIP calls received.
ipcssipcTotalCallsFailed	The number of failed SIP calls.
ipcssipTtlCallsDeniedDueToPolicy	The number of SIP calls rejected by Avaya SBCE because of policy violation.
ipcssipcTotalRegistrationsDroppedByMissingP olicy	The number of SIP registrations dropped by Avaya SBCE because of missing policy.
ipcssipcTotalInvitesDroppedByMissingPolicy	The number of SIP invites dropped because of missing policy.
ipcssipTtlSessDroppedDueToMaxNumofConc SessExc	The number of SIP sessions dropped by Avaya SBCE because the maximum number of concurrent sessions was exceeded.
ipcsTotalCANCELSent	The number of SIP CANCEL requests.
ipcsTotalCANCEL200Responses	The number of SIP CANCEL 200 responses.
ipcsTotalCANCELRetransmits	The number of SIP CANCEL retransmits.
ipcsTotalFromAndToHeaderMatchFailure	The number of From and To header match failures.
ipcsTotalRegMesWithMoreContacts	The number of registration messages with more contacts.
ipcsTotalMesWithAddrIncomplete	The number of messages with incomplete addresses.
ipcsTotalAuthHeaderMatchFailure	The number of Auth header match failures.
ipcsTotalContactSrcAddrMatchFailure	The number of Contact Source Address match failures.
ipcsTotalViaMatchFailure	The number of Via match failures.
ipcsTotal3XXMesFromNW	The number of 3XX messages from network.

OID	Description
ipcsTotalRegistrationMatchFailure	The number of Registration Match failures.
ipcsTotalContactSDPConnMatchFailure	The number of Contact SDP Match failures.
ipcsTotalSpoofedSipBye	The number of spoofed SIP Bye requests.
ipcsTotalSpoofedReinvite	The number of spoofed Reinvite requests.
ipcsTotalSpoofedCancel	The number of spoofed Cancel requests.
ipcsTotalSpoofedCancelToRemote	The number of spoofed Cancel To Remote requests.
ipcsTotalSpoofed200	The number of spoofed 200 responses.
ipcsTotalSpoofedErrorResp	The number of spoofed error responses.
ipcsTotalRegistrationFailed	The number of failed registrations.
sbcTotal1xMCesUserLoginFailed	The number of failed Avaya one-X® Mobile user logins.
sbcTotal1xMCesUserLoginSucceeded	The number of successful Avaya one-X® Mobile user logins.
ipcsTestAlarmNotification	The test alarm notification.
ipcsCPUUsageNotification	The notification sent when CPU usage exceeds 80%.
ipcsMemoryUsageNotification	The notification sent when memory usage exceeds 80%.
ipcsDiskUsageNotification	The notification for disk usage exceeding a set threshold.
ipcsDiskFailureNotification	The notification for disk failure.
ipcsNetworkFailureNotification	The notification for network failure.
ipcsHAFailureNotification	The notification for HA failure.
ipcsHAHeartBeatFailureNotification	The notification for failure to receive heartbeat from both HA servers.
ipcsScpFailureNotification	The notification for SCP failure.
ipcsCopyFailureNotification	The notification for copy failure.
ipcsProcessFailNotification	The notification for process failure.
ipcsDatabaseFailNotification	The notification for database failure.
ipcsRSAFailureNotification	The notification for RSA failure.
ipcsIncidenceNotification	The notification about incidents.
ipcsStdSessionLicenseUsageExceed	The notification sent when Session License usage threshold is exceeded.
ipcsAdvSessionLicenseUsageExceed	The notification sent when advanced Session License usage threshold is exceeded.
ipcsCesProxySessionLicenseUsageExceed	The notification sent when CES proxy Session License usage threshold is exceeded.
ipcsTranscodeSessionLicenseUsageExceed	The notification sent when transcoding Session License usage threshold is exceeded.
ipcsVideoSessionLicenseUsageExceed	The notification sent when video Session License usage threshold is exceeded.

OID	Description
ipcsMaxStdConcurrentSessionLimitExceed	The notification sent when the maximum standard concurrent Session License limit is exceeded.
ipcsMaxAdvConcurrentSessionLimitExceed	The notification sent when the maximum advanced concurrent Session License limit is exceeded.
ipcsMaxCESProxyConcurrentSessionLimitExc eed	The notification sent when the maximum CES proxy concurrent Session License limit is exceeded.
ipcsMaxTransConcurrentSessionLimitExceed	The notification sent when the maximum transcoding concurrent Session License limit is exceeded.
ipcsMaxVIDConcurrentSessionLimitExceed	The notification sent when the maximum video concurrent Session License limit is exceeded.

### Statistics details with examples

### Call between two remote workers through Avaya SBCE

In the following scenario, a call is made from A to B.

- Number of Registrations in Statistics: Counter increases by 2
  - One registration per phone, so in total 2 registrations from both A and B
  - In a multi-Session Manager deployment, if the phone is configured with the IPs for two different Session Managers as external IP1 and external IP2, the registration counter increases by 2 for one phone. Therefore, if both phones A and B are configured for multi-Session Manager deployment, the counter increases by 4.
- Number of Invites in Statistics: Counter increases by 2
  - The counter increases whenever Avaya SBCE receives an INVITE First INVITE from phone A towards Avaya SBCE, which is sent to the call server Second INVITE from Call Server towards Avaya SBCE, which is sent to phone B
- Number of Invites 200 Responses in Statistics: Counter increases by 2
  - The counter increases whenever Avaya SBCE receives a 200 OK for INVITE sent First 200 ok response from phone B towards Avaya SBCE which is sent to the call server Second 200 ok response from Call Server towards Avaya SBCE which is sent to phone A
- Number of Bye in Statistics: Counter increases by 2
  - The counter increases whenever Avaya SBCE receives a Bye First Bye from phone A towards Avaya SBCE which is sent to the call server Second Bye from Call Server towards Avaya SBCE which is sent to phone B

### Call between a remote worker and an internal phone through Avaya SBCE

In the following scenario, a call is made from A to C and the call is disconnected at A.

- Number of Registrations in Statistics: Counter increases by 1
  - One registration per phone, so in total 1 registration
  - Phone C registration will not be seen by Avaya SBCE as this phone is an internal phone

In a multi-Session Manager deployment, if the phone is configured with the IPs for two different Session Managers as external IP1 and external IP2, the registration counter increases by 2 for one phone. Therefore, if phone A is configured for multi-Session Manager deployment, the counter increases by 2.

Number of Invites in Statistics: Counter increases by 1

The counter increases whenever Avaya SBCE receives an INVITE INVITE from phone A towards Avaya SBCE, which is sent to the call server

Number of Invites 200 Responses in Statistics: Counter increases by 1

The counter increases whenever Avaya SBCE receives a 200 Ok for INVITE sent 200 ok response from phone C towards Avaya SBCE, which is sent to phone A

Number of Bye in Statistics: Counter increases by 1

The counter increases whenever Avaya SBCE receives a Bye Bye from phone A towards Avaya SBCE, which is sent to the call server

## **Avaya SBCE MIB**

The latest Avaya SBCE MIB file is available in the downloads section on the support website at <a href="http://support.avaya.com/downloads/">http://support.avaya.com/downloads/</a>.

## System alarms

## System alarms list

This section covers the description of the following alarms.

- CPU alarms on page 65
- Memory alarms on page 65
- <u>Disk Partition Space Alarms</u> on page 66
- Disk Failure alarms on page 67
- Link Failure Alarms on page 67
- Process Failure Alarms on page 68
- <u>Database Failure Alarms</u> on page 68
- Component Failure Alarms on page 69

Some system alarms require manual intervention, while some get cleared automatically. For information about clearing these alarms, see the Clearing event and Manual intervention columns.

## **CPU** alarms

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
CPU	CPU utilization is over 80%	CPU utilization is between 80%-89%	No	Alarm	Minor	CPU utilization is between 80%-89%	CPU utilization goes below 80% or above 89%.	No
CPU	CPU utilization is over 90%	CPU utilization is between 90%-99%	No	Alarm	Major	CPU utilization is between 90%-99%	CPU utilization goes below 90% or becomes 100%.	No
CPU	CPU utilization is 100%	CPU utilization is 100%.	Yes	Alarm	Critical	CPU utilization is 100%.	CPU utilization becomes 100%.	No

## Memory alarms (including Swap Space)

Alarm	Message	Condition	Service affectin g	Туре	Severity	Descriptio n	Clearing event	Manual intervent ion
Memory	Memory utilization is over 80%	Memory utilization is between 80%-89%.	No	Alarm	Minor	Memory utilization is between 80%-89%.	Memory utilization goes below 80% or above 89%.	No
Memory	Memory utilization is over 90%	Memory utilization is between 90%-99%.	Yes	Alarm	Major	Memory utilization is between 90%-99%.	Memory utilization goes below 90% or becomes 100%.	No
Memory	Memory utilization is 100%	Memory utilization is 100%.	Yes	Alarm	Critical	Memory utilization is 100%.	Memory utilization becomes 100%.	No

## Disk partition space alarms

Alarm	Message	Condition	Service affectin g	Туре	Severity	Descriptio n	Clearing event	Manual intervent ion
Disk partition space	Disk partition <partition _name=""> utilization is over 80%</partition>	Disk partition utilization is between 80%-89%.	No	Alarm	Minor	Disk partition utilization is between 80%-89%.	Disk partition utilization goes below 80% or above 89%.	No
Disk partition space	Disk partition <partition _name=""> utilization is over 90%</partition>	Disk partition utilization is between 90%-99%.	Yes	Alarm	Major	Disk partition utilization is between 90%-99%.	Disk partition utilization goes below 90% or becomes 100%.	No
Disk partition space	Disk partition <pre><pre><pre><pre></pre></pre></pre></pre>	Disk partition utilization is 100%.	Yes	Alarm	Critical	Disk partition utilization is 100%.	Disk partition utilization becomes 100%.	No

## Hard disk failure alarm

Alarm	Message	Condition	Service affectin g	Туре	Severity	Description	Clearing event	Manual interventi on
Hard disk failure	Hard disk <disk_id> failure</disk_id>	Hard disk failure	Yes	Alarm	Critical	The hard disk drive has failed and cannot be used.	The alarm is cleared only when the kernel detects no failures when testing the hard disk drive. This will only happen when the hard disk drive is replaced.	Yes. Hard disk drive must be replaced.

## Link failure alarm

Alarm	Message	Condition	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
Link failure	Network link failure <interface &gt;</interface 	Network link goes down on the given interface.	Yes. No traffic can be sent or received on the failed link.	Alarm	Critical	A link on a particular interface in down and cannot be used.	Network connectio n is restored and alarm manually cleared by user.	Yes. User needs to manually restore the link.

## **Process failure alarm**

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
Process failure	Applicatio n failure	One or more system processe s failed to send a heartbeat ping.	Yes. Port By-pass is automatic ally enabled.	Alarm	Critical	One or more system processe s is malfuncti oning	Malfuncti oning process is restarted either automatic ally by the system or manually by the Security Administr ator and the alarm cleared.	Yes. Required if automatic self-start is not successfu I.

## **Database failure alarm**

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
Database failure	Database failure	Connectivity to the database has been lost.	Yes. Port By-pass is automatic ally enabled after multiple failed restarts.	Alarm	Critical	Either the database is down or connectivi ty to the database has been lost.	The database failure being cleared either automatic ally by the system or manually by the Security Administrator.	Yes. Required if automatic self-start is not successfu I.

## Component failure alarm

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
Compone nt failure	Compone nt failure	One or more elements (signaling , media, intelligenc e, or EMS) in a multicompone nt configurat ion has failed to send a heartbeat ping.	Yes	Alarm	Critical	One or more SBCE server elements (signaling , media, intelligenc e, or EMS) is malfuncti oning.	The malfuncti oning elements could be restarted manually and the alarm cleared manually.	Required if self restart in not successfu I.

## **GUI** and console alarm list

- New User Added Alarms on page 69
- New Administrator Added Alarms on page 70
- <u>User Privilege Change Alarms</u> on page 70
- <u>User Deleted Alarms</u> on page 70
- Login Failure Alarms on page 71

### New user-added alarm

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
New User Added	New User Added: <userna me&gt;</userna 	A new GUI/ System user was added.	No	Alarm	Informatio nal	A new user was added to the system.	Alarm either cleared by the administr ator or it times-out.	No

## **New Administrator-added alarm**

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
New Admin- added	Admin User Added: <userna me&gt;</userna 	A new GUI/ System admin user was added.	No	Alarm	Informatio nal	A new admin user was added to the system.	Alarm either cleared by the administr ator or it times-out.	No

## User privilege change alarm

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
User Privilege Change	User Privilege Changed: <userna me&gt;</userna 	A user's access privilege was changed (either from admin to normal or from normal to admin).	No	Alarm	Informatio nal	A user's access privilege was changed (either from admin to normal or from normal to admin).	Alarm either cleared by the administr ator or it times-out.	No

## User deleted alarms

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
User Deleted	User deleted: <userna me&gt;</userna 	A new GUI/ System admin user was deleted.	No	Alarm	Informatio nal	A user was deleted from the system.	Alarm either cleared by the administr ator or it times-out.	No

## Login failure alarm

Alarm	Message	Conditio n	Service affecting	Туре	Severity	Descripti on	Clearing event	Manual intervent ion
Login failure	User login failure: <userna me&gt;</userna 	A user had multiple consecuti ve login failures.	No	Alarm	Warning	A user had more than a certain number of consecuti ve login failures.	Alarm either cleared by the administr ator or it times-out.	No

## **Chapter 4: Maintenance procedures**

## **Backup and restore**

The Backup and restore feature provides ability to create and restore snapshots of EMS and configured SBCEs.

The backup information is stored to a user-defined location either on the local EMS server or on a configured remote server. The location should be secure and physically separate from the Avaya SBCE equipment chassis for later retrieval or restoration.

### Note:

- For EMS, you can take a configuration backup manually and restore as needed, or you can configure snapshots automatically.
- For SBCE, you can only take backup manually.
- You can backup and restore only the functional SBCE devices.
- You can download the snapshot by using the download link provided in the Snapshot tab.

## **Designating a Snapshot Server**

### **About this task**

Configuration data snapshots contain information such as (identity?) certificates and (security?) keys, which can be misused to gain unauthorized access to Avaya SBCE.

You can only restore a snapshot to the same Avaya SBCE product version on an EMS of the same hardware group. When restoring the snapshot, it is recommended that the EMS server is configured with the same management IP used when the snapshot was created. If the EMS server hardware group or the Avaya SBCE product version does not match, the restore operation will fail and the system settings will revert to the earlier state.

### Before you begin

#### Ensure that:

- The selected storage directory on the designated remote server is accessible only to authorized users.
- The storage directory does not have read, write, or execute permissions for unauthorized users.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS**.
- 3. In the navigation pane, click **Backup/Restore**.

The EMS server displays the Backup/Restore page.

4. Click the **Snapshot Servers** tab.

The EMS server displays the snapshot server profiles in the content area.

5. On the Snapshot Servers page, click Add.

The EMS server displays the Add Snapshot Servers page.

6. Add the requested information in the fields, and click **Finish**.

#### Next steps

Creating system snapshots on page 74

### **Add Snapshot Server field descriptions**

Name	Description
Profile Name	A descriptive name for the designated snapshot server.
Server Address (ip:port)	The IP address and port number of the snapshot server to transfer the configuration data or snapshots using secure FTP.
User Name	The user name of the administrative account that is authorized to back up the Avaya SBCE configuration data.
Authentication Type	The option to enable the SSH authentication. The options are:
	• Password
	Use ipcs SSH key
	If you select <b>Use ipcs SSH key</b> , the <b>Password</b> and <b>Confirm Password</b> fields are unavailable.
Password	The password to authenticate the administrative account.
Confirm Password	The field to enter the password again for confirmation.
Repository Location	The path of the directory on the snapshot server where the configuration backup snapshots are stored.
Host Key	The key that is used to authenticate the login of the host.

## **Creating system snapshots**

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS** for creating snapshot for the EMS server or **SBCE** for device specific snapshot configuration.
- 3. In the navigation pane, click **Backup/Restore**.
- 4. On the Backup/Restore page, click the **Snapshots** tab.
- 5. Select the designated snapshot server.
- 6. Click Create Snapshot.

The EMS server displays the Create Snapshot window.

7. Enter a name for the snapshot, and click **Create**.

#### Result

The server creates a snapshot of the EMS security configuration and sends it to all the configured snapshot servers. A banner on the Create Snapshot pop-up window informs you that the snapshot has been successfully created. When the process is complete, the snapshots screen displays the newly created snapshot.

#### Related links

Designating a Snapshot Server on page 72

## Configuring automatic snapshots

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS**.
- 3. In the navigation pane, click **Backup/Restore**.
- 4. On the Backup/Restore page, click the **Automatic Snapshot Configuration** tab.

The EMS server displays the Automatic Snapshot Configuration page. The **Summary** section displays the configuration of a previously saved backup. Otherwise, the default setting of **Never** is displayed.

- 5. In the **Configuration** section, select one of the following:
  - Never
  - Daily
  - **Weekly**: The EMS server displays a group of check boxes to choose the day. For example, Su, Mo, Tu, We, Th, Fr, and Sa.
  - **Monthly**: The EMS server displays a group of check boxes to choose the day. For example, Su, Mo, Tu, We, Th, Fr, and Sa. It also displays another row of check boxes for occurrence. For example, 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, and Last.

6. In the **Time** field, select the time.

The EMS server displays a Select Time window.

7. Click Save.

## Restoration of a system snapshot

You can restore Avaya SBCE configuration data snapshot on EMS manually or configure automatic restoration of the snapshots...

#### Manual

The manual method of restoring configuration snapshots is a two-step process. The snapshot is first retrieved from the snapshot server and then uploaded to the EMS for restoration. To restore EMS to a previous snapshot configuration, you must:

- Retrieve a snapshot. See Retrieving a snapshot file on page 76
- Restore a snapshot. See Restoring a snapshot file using Restore by File option on page 76

#### **Automatic**

The automatic method is a process that restores EMS to the previous configuration without further intervention. See "Restoring a snapshot file".



#### Caution:

During both methods, EMS goes into the offline mode when the files are being transferred and the device is being reconfigured.

Avaya SBCE detection or mitigation features are unavailable for the entire duration of the restore procedure, making the EMS and Avaya SBCE single server deployment vulnerable to intrusions and attacks.

Restoration procedures must be completed only during times of relative EMS server inactivity or during scheduled periods of maintenance.

You can restore snapshots to an EMS system of the same hardware category, manufacturer, and model of EMS. The following table lists the hardware categories and virtualized environment:

Server	NICs	Hardware category
CAD 0230	6	110
Dell R320	6	310
Dell R630	6	310
HP DL360 G8	6	311
HP DL360 G9	6	311
VMWare SBCE	6	110
Nutanix	6	110

Table continues...

Server	NICs	Hardware category
Avaya Converged Platform 100 series server with profile 3	6	310
Avaya Converged Platform 100 series server with profile 5	6	310
Portwell CAF-0251	4	110

### Retrieving a snapshot file

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS** for retrieving snapshot for the EMS server or **SBCE** for the device specific retrieval of the snapshot.
- 3. In the navigation pane, click **Backup/Restore**.
- 4. On the Backup/Restore page, click **Snapshots** tab.
- 5. In the drop-down box, select snapshot server.
- 6. Select the check box next to the snapshot to retrieve, and click **Download**.

#### Result

The EMS server saves the snapshot file in the default download directory.

#### **Next steps**

Restore the downloaded configuration data snapshot.

## Restoring a snapshot file using Restore by File option

#### About this task

After you retrieve the snapshot file from the snapshot server, save the file on the local workstation. You can upload the file to the EMS server where the file is decompressed and used to reconfigure the EMS to a previous state.

Use the following procedure to upload the snapshot from your local workstation to the EMS server and reconfigure the EMS.

#### Before you begin

Retrieve a snapshot file.

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click **EMS** for restoring a snapshot for the EMS server or **SBCE** for device specific snapshot restoration.
- 3. In the navigation pane, click **Backup/Restore**.
- 4. On the Backup/Restore page, click the **Snapshots** tab.
- 5. Click Restore by File.

- 6. In the Restore by File window, click Chose File.
- 7. In the pop-up window, select a snapshot file, and click **Open**.

The EMS server enters the selected snapshot file in the **Restore Point File** field of the Restore by File window.

#### 8. Click **Upload**.

The EMS server displays a warning window for confirmation to proceed with the restoration procedure.

#### 9. Click OK.

The EMS server goes offline and transfers the snapshot file to the EMS server. The file is then decompressed and used to reconfigure the EMS software to a previous configuration.

After the EMS server successfully restores a snapshot, in an HA configuration, both Avaya SBCE devices reboot. In a standalone configuration, the EMS+SBCE single box reboots. The EMS server takes several minutes to reboot after backup configuration.

#### Related links

Retrieving a snapshot file on page 76

#### Restoring a snapshot file

#### Before you begin

Create a system snapshot.

#### Procedure

- 1. Log in to the EMS web interface with administrator credentials.
- In the navigation pane, click EMS for restoring a snapshot for the complete EMS server or SBCE for device specific snapshot restoration.
- 3. In the navigation pane, click **Backup/Restore**.
- 4. Using the drop-down menu in the content area, select the snapshot server that contains the snapshot file that you want to retrieve.

The EMS server displays all snapshot files on the selected snapshot server in the content area.

5. Select the snapshot file that you want to restore to the EMS or SBCE by clicking the corresponding **Restore** option.

The EMS server displays a warning pop-up window, asking for confirmation to proceed with the automatic restoration procedure.

#### 6. Click OK.

The EMS or SBCE goes offline and reconfigures the snapshot file.



#### Note:

After the system successfully restores a snapshot, in an HA configuration both Avaya SBCE devices reboot. In a standalone configuration, the EMS+SBCE single box reboots. The system takes several minutes to reboot after backup configuration.

## Deleting a system snapshot

#### **Procedure**

- 1. Log in to the EMS web interface with administrator credentials.
- 2. In the navigation pane, click EMS for deleting the snapshot for the complete EMS server or **SBCE** for device-specific snapshot deletion.
- 3. In the navigation pane, click Backup/Restore.
- 4. Select the local server or the designated snapshot server from where you want to delete the file.
- 5. Select the file and click the corresponding **Delete** option.
  - The EMS server displays a warning message asking for confirmation to delete.
- 6. Click OK.

#### Result

The EMS server deletes the snapshot file.

## Handling duplicate hostnames in a multiserver deployment

#### About this task

The host name of Avaya SBCE servers in multi-server deployments must be unique. If the Avaya SBCE servers have identical host names, you cannot change the state of the servers to the Commissioned state.



#### Note:

This procedure is service affecting. If the current version is Release 6.2.x, then update the hostnames before upgrading to Release 7.0.

#### Before you begin

- 1. Log in to each Avaya SBCE server, and run the hostname command to determine if the hostnames are duplicated.
- Note down the management IP address of the Avaya SBCE servers.
- 3. Ensure that all Avaya SBCE servers are in the Commissioned mode.

#### **Procedure**

- 1. Take a snapshot of the system and save the snapshot offline. For information about creating snapshots, see *Making a system snapshot*.
- 2. Determine the server for which the hostname needs to be changed.
  - a. Using PuTTY, establish an SSH session with the EMS server with ipcs user credentials.
  - b. Using PuTTY, establish an SSH session with Avaya SBCE server with ipcs user credentials by using the following command: ssh -p 222 a.b.c.d.
  - c. Note the server for which a password is required. If you have two Avaya SBCE servers with the same hostname, then establishing SSH connection to one of them requires a password.
- 3. Change the hostname and Avaya SBCE properties.
  - a. Using PuTTY, establish an SSH session with Avaya SBCE server for which the password was required
  - b. Type sudo su.
  - c. To back up /etc/hostname use the following command: cp /etc/hostname /etc/hostname.bak.
  - d. Edit /etc/hostname by using vi, and change the hostname to a unique hostname.
  - e. Take a backup of /usr/local/ipcs/etc/sysinfo by typing cp /usr/local/ipcs/etc/sysinfo /usr/local/ipcs/etc/sysinfo.bak.
  - f. Using vi, edit the sysinfo file.
    - Change the **ApplianceName** property to the new hostname.
    - Change the STATE property to INSTALLED.
- 4. Verify whether the EMS server can connect to the Avaya SBCE server.
- 5. Restart the Avaya SBCE server.
- 6. Using PuTTY, establish an SSH session and ensure that the session from the EMS server to all Avaya SBCE servers does not require password.
- 7. Check the EMS web interface and confirm that the Avaya SBCE servers are in the Commissioned mode.

## Acquiring WebLM license on Avaya SBCE

#### About this task

If Avaya SBCE fails to acquire licenses from System Manager, you must enable license acquisition for Avaya SBCE from WebLM on System Manager.

#### Before you begin

Download the System Manager pem file from the System Manager security page.

#### **Procedure**

- 1. Copy the System Manager pem file to /home/ipcs on EMS.
- 3. Type the keystore password.
- 4. Type "/etc/init.d/ipcs-ems stop".
- 5. Type "/etc/init.d/ipcs-ems start".
- Refresh the license.

## Connecting Avaya SBCE with an external WebLM server

#### About this task

Use the following procedure to connect Avaya SBCE with an external WebLM server when external WebLM server's Root CA certificate is not included in the Avaya SBCE trusted WebLM certs.jks keystore.

#### **Procedure**

- 1. Export the external WebLM server Root CA certificate.
- 2. Import the external WebLM server Root CA certificate into the Avaya SBCE trusted\_WebLM\_certs.jks keystore.

# Swapping a Avaya SBCE device in single server deployment

#### About this task

Use this procedure to swap an Avaya SBCE device in single server deployment.

#### Before you begin

Ensure that you have created and saved the backup file of a functional Avaya SBCE device.

#### **Procedure**

- 1. Log in to the EMS web interface with the administrator credentials.
- 2. In the navigation pane, click **Device Management**.

The EMS server displays the Device Management screen in the content area.

- 3. On the Device Management page, click **Devices** tab.
- 4. Install a new Avaya SBCE with a different IP address. For more information, see *Deploying Avaya Session Border Controller for Enterprise*.
- 5. In the **Devices** section, do the following:
  - a. Click Add.
  - b. In the **Hostname** and **Management IP** fields, provide the relevant information.
  - c. Clear the HA check box.
- 6. When the state of the newly added Avaya SBCE device becomes Registered, click **Swap Device**.
- 7. Select the backup file of the new device added in the **Device to Replace** field.
  - **Important:**

The backup file is a master .tar file. Avaya recommends not to unzip the .tar file.

8. Click Finish.

The EMS server does not display the old Avaya SBCE device in the **Devices** tab.

## Swapping Avaya SBCE devices in HA pair deployment

#### About this task

Use this procedure to swap an Avaya SBCE device in an HA pair deployment.

#### Before you begin

Ensure that one of the Avaya SBCE devices in the HA pair is non-functional.

#### **Procedure**

- 1. Log in to the EMS web interface with the administrator credentials.
- 2. In the navigation pane, click **Device Management**.

The EMS server displays the Device Management screen in the content area.

- 3. On the Device Management page, click **Devices** tab.
- 4. Install a new Avaya SBCE with different IP address.

For more information, see Deploying Avaya Session Border Controller for Enterprise.

- 5. In the **Devices** section, do the following:
  - a. Click Add.
  - b. In the **Hostname** and **Management IP** fields, provide the relevant information.

- c. Clear the HA check box.
- 6. When the state of the newly added Avaya SBCE device becomes Registered, click **Swap Device**.
- 7. Select the IP address of the new device added in the **Device to Replace** field.
- 8. Click Finish.

The EMS server does not display the old Avaya SBCE device in the **Devices** tab.

## Swapping an EMS server in single server deployment

#### About this task

Use this procedure to swap an EMS server in single server deployment

#### Before you begin

Ensure that you have created and saved the backup file of a functional EMS server.

#### **Procedure**

- 1. Log in to the EMS web interface with the administrator credentials.
- 2. In the navigation pane, click **Device Management**.

The EMS server displays the Device Management screen in the content area.

- 3. On the Device Management page, click **Devices** tab.
- 4. When the state of the EMS becomes Commissioned, click **Swap Device**.
  - Note:

The EMS server displays the **Swap Device** option only when there is no SBCE device installed on the system.

5. Select the backup file of the new device.

## Important:

The backup file is a master .tar file. Avaya recommends not to unzip the .tar file.

6. Run the following command to change the EMS IP address on the installed Avaya SBCEs:

```
sbceconfigurator.py change-ems-ip <old ems ip> <new ems ip>
```

Note:

The IP addresses of the old and the new EMS must be different.

7. Reboot all the connected EMS servers.

## Swapping a primary EMS server in HA pair deployment

#### **About this task**

Use this procedure to swap the primary EMS server in HA pair deployment.

#### Before you begin

Ensure that the primary EMS server is non functional.

#### **Procedure**

- 1. Log in to the EMS web interface with the administrator credentials.
- 2. In the navigation pane, click **Device Management**.

The EMS server displays the Device Management screen in the content area.

- 3. On the Device Management page, click **Devices** tab.
- 4. When the state of the EMS becomes Commissioned, click **Swap Device**.
  - Note:

The EMS server displays the **Swap Device** option only when there is no SBCE device installed on the system.

- 5. Provide the IP address for the secondary EMS server.
- 6. Run the following command to change the EMS IP address on the installed Avaya SBCEs:

```
sbceconfigurator.py change-ems-ip <old_ems_ip> <new_ems_ip>
```



The IP addresses of the old and the new EMS must be different.

7. Reboot all the connected EMS servers.

## Swapping a secondary EMS server in HA pair deployment

#### About this task

Use this procedure to swap the secondary EMS server in HA pair deployment.

#### **Procedure**

- 1. Log in to the EMS web interface with the administrator credentials.
- 2. In the navigation pane, click **EMS**.
- In the navigation pane, click **Device Management**.
   The EMS server displays the Device Management screen in the content area.
- 4. On the Device Management page, click **Devices** tab.

- 5. Click **Uninstall** corresponding to the secondary EMS from the primary EMS web interface. The EMS server displays a confirmation pop-up to confirm your selection.
- 6. Click OK.
- 7. Deploy and configure a new EMS as secondary EMS. For more information, see *Deploying Avaya Session Border Controller for Enterprise*.
- 8. On the Device Management page, click **Devices** tab.
- 9. Click **Restart Application** corresponding to all the EMS connected servers. The EMS server displays a confirmation pop-up.
- 10. Click **OK** to confirm.

#### Result

Secondary EMS will be added in the Devices section.

## Avaya SBCE reconfiguration script options

Table 4: sbceconfigurator.py command options

#	Command	Description	Usage
1	change-ip- gw-mask	Changes the management IP address, gateway, and subnet mask.	sbceconfigurator.py change-ip-gw-mask <mgmt_ip> <gw_ip> <nw_mask></nw_mask></gw_ip></mgmt_ip>
2	change-ems- ip	Changes the primary or active EMS IP address on the secondary or standby EMS.	sbceconfigurator.py change-ems-ip old EMS IP address new EMS IP address
		Changes the secondary or standby     EMS IP address on the primary or     active EMS and all the Avaya SBCE     servers connected to EMS.	
		<ol> <li>Changes the primary or active EMS IP address on the connected Avaya SBCE servers, which were not reachable while changing the primary or active EMS IP address.</li> </ol>	
3	change- hostname	Changes host name.	sbceconfigurator.py change-hostname HOSTNAME
4	change-ntp- ip	Changes NTP IP address.	sbceconfigurator.py change-ntp-ip NTP IP

Table continues...

#	Command	Description	Usage
5	change-dns- ip-fqdn	Changes DNS IP address.	sbceconfigurator.py change-dns-ip-fqdn DNS IP
6	change-nw- passphrase	Changes network passphrase.	sbceconfigurator.py change-nw-passphrase passphrase
7	change-ssl- certs	Generates self-signed certificate for EMS and single servers.	sbceconfigurator.py change-ssl-certs first, last name Org.unit Org.Name City State 2-digit-country_code
8	change- sbce-ip	Changes the Avaya SBCE IP address on the EMS database.	sbceconfigurator.py change-sbce-ip sbce-old-ip
		Sequence to execute this command:	sbce-new-ip
		Change Management IP address, gateway, mask on theAvaya SBCE server by using the command change- ip-gw-mask	
		Run the change-sbce-ip command on EMS CLI to notify the EMS about the Avaya SBCE IP change.	
9	factory- reset	Use the following procedure to reset Avaya SBCE to the factory default state:	sbceconfigurator.py factory-reset
	(For SBC only)	<ol> <li>To uninstall the Avaya SBCE device in a multiple server deployment from GUI, click Device management &gt; Devices and click Uninstall.</li> </ol>	
		This operation clears the device- specific configuration and is not required on EMS and a single server deployment.	
		<ol><li>Run sbceconfigurator.py factory-reset.</li></ol>	
		This operation clears the device- specific configuration on EMS or a single server deployment.	
		Run this command from either a serial console or VGA session. Do not run this command from an SSH putty session since network connectivity will be lost during this operation.	

# Changing management IP, gateway and network mask details for a single server deployment

#### **Procedure**

- 1. Log in to the server as a super user.
- 2. Type sbceconfigurator.py change-ip-gw-mask < Management IP> < Gateway IP> < Network Mask > .

The server restarts indicating that the management IP has been changed successfully.

## Changing management IP for an HA deployment

## Changing management IP, gateway IP, and network mask details on primary EMS

Use the following command to change management IP, gateway, and network mask details on the primary EMS server.

sbceconfigurator.py change-ip-gw-mask <MGMT IP> <GW IP> <NW MASK>

The script does the following:

- 1. Checks if the database is functional.
- 2. If the database is functional, proceeds with stopping application processes.
- 3. Checks if all the Avaya SBCE servers connected to EMS are reachable. If any Avaya SBCE server is unreachable, exits or proceeds with changing the EMS IP address on the reachable Avaya SBCE servers. Later, when the devices are reachable from EMS, users can regenerate or change the EMS IP addresses on the devices.
- 4. Prints out the log messages, which shows the current status on screen.
- 5. The EMS server then reboots. The user needs to ssh using the new EMS IP address.
- 6. EMS generates certificates automatically and sends it to all Avaya SBCEs.

Change in management IP requires a change in the NTP address configuration on all Avaya SBCE servers connected to EMS.

## Note:

All Avaya SBCE servers must have the changed EMS IP address.

#### Changing primary EMS IP on unreachable Avaya SBCE

#### **About this task**

Use this procedure only when Avaya SBCE is unreachable while changing the primary EMS IP address.

#### **Procedure**

- 1. Log in the EMS web interface as a super user.
- 2. Type sbceconfigurator.py change-ems-ip < EMS\_OLD\_IP > < EMS\_NEW\_IP > and press Enter.

#### Changing NTP address on Avaya SBCE devices

#### About this task

Changing management IP of EMS requires a change in the NTP address configuration on all the Avaya SBCE servers connected to EMS. For the proper functionality of OpenVPN, ensure that the date and time on the Avaya SBCE servers match the date and time on the EMS server. The recommended procedure is to configure the EMS IP as the NTP IP address of the Avaya SBCE devices.

#### **Procedure**

- 1. Log on to the Avaya SBCE device as a super user.
- 2. Type sbceconfigurator.py change-ntp-ip NTP-IP, where NTP-IP is the new NTP IP address.

## Changing IP address of the primary EMS server on the secondary EMS server Procedure

- 1. Log on to the EMS device as a super user.
- 2. Type sbceconfigurator.py change-ems-ip *EMS\_old\_IP EMS\_new\_IP* and press Enter.

# Changing management IP, gateway IP, and network mask details on secondary EMS

#### **Procedure**

- 1. Log on to the Avaya SBCE server as a super user.

The Avaya SBCE restarts indicating a successful completion of the management IP change. After changing the management IP, the primary EMS and Avaya SBCE devices must be notified about the new Avaya SBCE IP address of the secondary EMS.

- 3. Log on to the primary EMS and Avaya SBCE devices as a super user.
- 4. Type sbceconfigurator.py change-ems-ip Old\_EMS\_IP New\_EMS\_IP.

The system changes the IP address of the secondary EMS.

## Note:

Ensure that you change the IP address of the secondary EMS in the primary EMS and each Avaya SBCE device.

## Changing management IP, gateway IP, and network mask details on Avaya SBCE

#### **Procedure**

- 1. Log on to the Avaya SBCE server as a super user.
- 2. Type sbceconfigurator.py change-ip-gw-mask < Management IP> < Gateway IP> < Network Mask >.

The Avaya SBCE restarts indicating successful completion of the management IP change. After changing the management IP, the EMS must be notified about the new Avaya SBCE IP address.

- 3. Log on to the EMS server as a super user.
- 4. Type sbceconfigurator.py change-sbce-ip Old\_SBCE\_IP New\_SBCE\_IP.

The system changes the IP address of the Avaya SBCE in the EMS database.

## **Changing hostname**

#### **Procedure**

- 1. Log in to the Avaya SBCE CLI using administrative privileges.
- 2. Type sbceconfigurator.py change-hostname Hostname.
- 3. Restart the system.

For the hostname change to take effect, you must perform a soft reboot of the Avaya SBCE.

## Changing network passphrase

#### About this task

Network passphrase is important for EMS-Avaya SBCE authentication. If you change the network password for an Avaya SBCE, ensure that you change the passphrase on all systems connected to the Avaya SBCE.

#### **Procedure**

- 1. Log in to the Avaya SBCE CLI using administrative privileges.
- 2. Type sbceconfigurator.py change-nw-passphrase New Passphrase.

The server restarts for enabling the new passphrase. The server is either the EMS or its connected SBCE's where the command is executed.

## Regenerating self-signed certificates

#### **Procedure**

- 1. Log in to the EMS CLI using administrative privileges.
- 2. Run the following command: sbceconfigurator.py change-ssl-certs.

## Changing DNS IP and FQDN

#### **Procedure**

- 1. Log in to the Avaya SBCE CLI using administrative privileges.
- Type sbceconfigurator.py change-dns-ip-fqdn DNS IP FQDN.
   The EMS server changes the DNS IP and FQDN.

## Enabling or disabling network interfaces using CLI

#### **Procedure**

- 1. Log in to the Avaya SBCE CLI using administrative privileges.
- 2. Run the following command to enable or disable the network interfaces:

sbceconfigurator.py data-interface-enable <interface name>
sbceconfigurator.py data-interface-disbale <interface name>

## ipcs-options commands

Option Name	EMS only	EMS and SBC(Singlebox)	SBC Only
Custom routes	~	~	~
Configure TimeZone	~	•	~
View TimeZone	~	•	V
Secondary EMS IP	~	_	~

Table continues...

Option Name	EMS only	EMS and SBC(Singlebox)	SBC Only
Self-signed Certificate	~	~	
Regenerate SSH Keys	_	•	<b>&gt;</b>
Enable RSS	_	~	~
Disable RSS	_	~	~

- Custom Routes: Deprecated. This option is no longer supported.
- Configure TimeZone: Used to select a new time zone.
- **View Timezone**: Used to view the currently selected time zone.
- Secondary EMS IP: Used to set the IP address of the secondary EMS.
- Self-Signed Certificate: Used to create a new self-signed certificate to be used for the EMS web administration.
- Regenerate SSH Keys: This option regenerates the SSH keys and reboots the server.
- **Enable RSS**: This option enables Receive Side Scaling (RSS) to tune network performance.
- Disable RSS: This option disables Receive Side Scaling (RSS) to tune network performance.



Receive-Side Scaling (RSS) option allows inbound network traffic to be processed by multiple CPUs. Use RSS to clear interruption during inbound traffic processing caused by overloading a single CPU and to reduce network latency. By default, this option is enabled. Do not use this option unless advised by the Avaya Support team.

# Determining whether Avaya SBCE is running on a TILEncore Gx-36 Intelligent Application adapter

#### About this task

Avaya SBCE supports the TILEncore Gx36 Intelligent Application adapter in HP DL360 G9 and Dell R630 servers.

Use this procedure to know whether Avaya SBCE is running on the TILEncore-Gx36 card.

#### Before you begin

Determine whether the server is Gx-enabled by running the lspci -v | grep -i tilera command. If the system displays anything after running the command, the server is Gx-enabled.

#### **Procedure**

- 1. Log in to the host with root credentials.
- 2. Run grep TILERA EQUIPPED /usr/local/ipcs/etc/sysinfo command to check the status of the Gx-enabled card.
  - If TILERA EQUIPPED STATUS is set to Yes. The system can be configured with a Gxenabled card.
- 3. If the Gx-enabled card does not boot successfully, type ip link ls command to check the interfaces on the host server.

The system displays the A1, A2, B1, B2 data interfaces of Avaya SBCE, which shows that the software on the Gx-enabled card is running.



The system takes several minutes for booting the system, establishing communication with the host and showing up the interfaces. Therefore, you must wait for five minutes before checking the interfaces and logging in to the TILEncore-Gx36 card.

4. Type exit to logoff from the Tilera console.

If you logged in through the tile-console command, type ctrl-\, then press q to exit.

#### Related links

Listing static and dynamic flows through the Tilera Application Shell on page 91

Checking counters for the Tilera Gx card on page 92

Checking network synchronization between the host and the TILEncore Gx Intelligent adapter on page 93

## Listing static and dynamic flows through the Tilera Application Shell

#### About this task

The Tilera Application Shell provides an interface for applications running on the Tilera Gx adapter.

#### Before you begin

Log in to the host as root.

#### **Procedure**

- 1. Run grep TILERA EQUIPPED /usr/local/ipcs/etc/sysinfo command to check the status of the Gx-enabled card.
  - If TILERA EQUIPPED STATUS is set to Yes. The system can be configured with a Gxenabled card.
- 2. Type /build/bin/tash.

The system displays the pcf prompt.

- 3. To view static flows, do the following:
  - a. At the pcf prompt, type static-flows.
  - b. Type show.

The system lists all static flows

- 4. To view dynamic flows, do the following:
  - a. At the pcf prompt, type dynamic-flows.
  - b. Type show info\_level, where info\_level is a number from 1 to 10 that specifies varying amount of information about each flow.

Do not use this command when a lot of calls are in progress. During high traffic conditions, this command takes time to complete and impacts calls in progress.

#### Related links

<u>Determining whether Avaya SBCE is running on a TILEncore Gx–36 Intelligent Application adapter</u> on page 90

## Checking counters for the Tilera Gx card

#### Before you begin

Log in to the host as root.

#### **Procedure**

1. Run grep TILERA\_EQUIPPED /usr/local/ipcs/etc/sysinfo command to check the status of the Gx-enabled card.

If TILERA\_EQUIPPED\_STATUS is set to Yes. The system can be configured with a Gx-enabled card.

2. Type /build/bin/tash.

The system displays the pcf prompt.

- 3. At the pcf prompt, type counters.
- 4. Type the name of the counter category to see values for all counters of a type.

Type status to see the current values for all PCF status counters.

#### **Related links**

<u>Determining whether Avaya SBCE is running on a TILEncore Gx–36 Intelligent Application adapter</u> on page 90

# Checking network synchronization between the host and the TILEncore Gx Intelligent adapter

#### Before you begin

Log in to the host as root.

#### **Procedure**

1. Run grep TILERA\_EQUIPPED /usr/local/ipcs/etc/sysinfo command to check the status of the Gx-enabled card.

If TILERA\_EQUIPPED\_STATUS is set to Yes. The system can be configured with a Gx-enabled card.

2. Type /build/bin/tash.

The system displays the pcf prompt.

3. Type netsync.

This command is used to send the neighbour entries and routing tables to the Tilera Gx card from the host.

4. Type neigh.

The system displays neighbour entries for network synchronization.

#### Related links

<u>Determining whether Avaya SBCE is running on a TILEncore Gx–36 Intelligent Application adapter</u> on page 90

# Determining whether Avaya SBCE is installed on VMware or KVM

## Determining whether Avaya SBCE is installed on KVM

#### **Procedure**

- 1. Log in to the KVM host with root permissions.
- 2. At the console, type virt-manager.

The system displays the Virtual Machine Manager GUI.

- 3. Type 2 for CLI mode.
- 4. Shutdown the VM by using the virsh shutdown KVM-SBCE-8.0 command.

The system shuts down the KVM-SBCE-8.0 instance.

5. To view all the KVM guests installed on the KVM host server use the virsh list- - all command.

This command displays the Id, Name and State of all the KVM guests running on the KVM server

## Determining whether Avaya SBCE is installed on VMware

#### **Procedure**

- 1. Log in as a root user to get root privileges.
- 2. Type dmidecode | grep 'VMware'.

If Avaya SBCE is installed on VMware, the system displays Product Name: VMware.

If Avaya SBCE is installed on any other server, the system does not display any data.

## Resetting the root or ipcs password

#### **Procedure**

- 1. At the boot menu, press e to edit the first boot entry.
- 2. If server prompts to enter the user name and password for grub menu, enter the user name as root and password as @v@y@ 123.
- 3. From the grub options, navigate to the end of the line that starts with **linux16** and enter:
- 4. Press Ctrl+x.

This option will boot to the initramfs prompt with a root shell.

The root file system is mounted in read-only mode to /sysroot and must be remounted with read/write permissions to make changes.

- 5. To remount the root file system with read/write permissions, run the following command: mount -o remount, rw /sysroot
- 6. Once the file system has been remounted, run the command: chroot /sysroot
- 7. To reset the password, do one of the following:
  - To reset the root password, run the following command: echo "root:SIPera\_123" | chpasswd
  - To reset the root password, run the following command: echo "ipcs:SIPera\_123" | chpasswd

You can enter any password in place of SIPera 123.

8. Enter the exit command twice.

Once the reboot has completed, you can use the root or ipcs account with the newly set password.

## **Chapter 5: Resources**

## **Documentation**

The following table lists the documents related to this product. Download the documents from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>

Title	Description	Audience			
Design	Design				
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			
Avaya Converged Platform Overview and Specification	Describes the key features of Avaya Converged Platform	IT Management, sales and deployment engineers, solution architects, and support personnel			
Implementation and administration					
Installing the Dell PowerEdge R630 Server	Hardware installation and preliminary configuration.	Implementation engineers			
Installing the HP ProLiant DL360 G9 Server	Hardware installation and preliminary configuration.	Implementation engineers			
Upgrading Avaya Session Border Controller for Enterprise	Procedures for upgrading to Avaya SBCE 8.0.x.	Implementation engineers			
Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment	Procedure to deploy Avaya SBCE on VMware.	Implementation engineers			
Installing the Avaya Converged Platform 110 Series	Describes how to install Avaya Converged Platform 110 Series.	Sales and deployment engineers, solution architects, and support personnel			
Administering Avaya Session Border Controller for Enterprise	Configuration and administration procedures.	Implementation engineers and administrators			
Maintenance and Troubleshooting					

Table continues...

Title	Description	Audience
Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Troubleshooting and maintenance procedures for Avaya SBCE.	Implementation engineers and Sales engineers
Maintaining and Troubleshooting the Dell PowerEdge R630 Server	Troubleshooting and maintenance procedures for the Dell PowerEdge R630 Server.	Implementation engineers and Sales engineers
Maintaining and Troubleshooting the HP ProLiant DL360 G9 Server	Troubleshooting and maintenance procedures for the HP ProLiant DL360 G9 Server.	Implementation engineers and Sales engineers

## Finding documents on the Avaya Support website

#### **Procedure**

- 1. Go to <a href="https://support.avaya.com">https://support.avaya.com</a>.
- 2. At the top of the screen, type your username and password and click **Login**.
- 3. Click Support by Product > Documents.
- 4. In **Enter your Product Here**, type the product name and then select the product from the list.
- 5. In **Choose Release**, select an appropriate release number.
- 6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
  - For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
- 7. Click Enter.

## Accessing the port matrix document

#### **Procedure**

- 1. Go to https://support.avaya.com.
- 2. Log on to the Avaya website with a valid Avaya user ID and password.
- 3. On the Avaya Support page, click **Support By Product > Documents**.
- 4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
- 5. In **Choose Release**, select the required release number.
- 6. In the **Content Type** filter, select one or more of the following categories:
  - Application & Technical Notes

#### Design, Development & System Mgt

The list displays the product-specific Port Matrix document.

7. Click Enter.

## **Avaya Documentation Portal navigation**

Customer documentation for some programs is now available on the Avaya Documentation Portal at <a href="https://documentation.avaya.com">https://documentation.avaya.com</a>.

## Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open <a href="https://support.avaya.com">https://support.avaya.com</a>.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using My Docs (☆).

Navigate to the **My Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add content from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (<a>)</a>.

Navigate to the My Content > Watch list menu, and do the following:

- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google
   +.
- Send feedback on a section and rate the content.

#### Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

## **Training**

The following courses are available on the Avaya Learning website at <a href="www.avaya-learning.com">www.avaya-learning.com</a>. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

### 🐯 Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
2060W	What is new for Avaya Session Border Controller for Enterprise
2066W	Administering the Avaya Session Border Controller for Enterprise
2080C	Implementing and Supporting Avaya Session Border Controller — Platform Independent
2080T	Avaya Session Border Controller for Enterprise Platform Independent and Support Test
2080V	Implementing and Supporting Avaya Session Border Controller — Platform Independent
26160W	Avaya Session Border Controller for Enterprise Fundamentals
7008T	Avaya Session Border Controller for Midmarket Solutions Implementation and Support Test
7008W	Avaya Session Border Controller for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions

## **Viewing Avaya Mentor videos**

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

#### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

#### **Procedure**

- To find videos on the Avaya Support website, go to <a href="https://support.avaya.com/">https://support.avaya.com/</a> and do one of the following:
  - In Search, type Avaya Mentor Videos, click Clear All and select Video in the Content Type.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to <a href="www.youtube.com/AvayaMentor">www.youtube.com/AvayaMentor</a> and do one of the following:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

### Note:

Videos are not available for all products.

## **Support**

Go to the Avaya Support website at <a href="https://support.avaya.com">https://support.avaya.com</a> 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.

## Index

A		clearing	
		alarms	<u>19</u>
accessing port matrix	<u>97</u>	CLI	
acquiring		accessing	<u>10</u>
WebLM license		CLIPCS	
administrative users	<u>29</u>	accessing	
alarms		collect archive field descriptions	<u>57</u>
field descriptions		collecting	
managing	<u>18</u>	logs	<u>55</u>
audit logs		collection	
viewing	<u>28</u>	delete	<u>98</u>
Avaya SBCE		edit name	
traps		generating PDF	
Avaya support website	<u>100</u>	sharing content	
		collect logs field descriptions	
В		component failure alarm	<u>69</u>
<b>5</b>		configuring	
back panel		automatic snapshots	
ACP 100 series server	15	packet capture	<u>38</u>
backup		connecting	
	··· <u>·-</u>	SBCE with an external WebLM server	<u>80</u>
_		content	
C		publishing PDF output	98
		searching	
call		sharing	98
trace		watching for updates	
call between a remote worker and an internal phone throu	•	CPU alarms	
Avaya SBCE			
call between two remote workers through SBCE	<u>63</u>	<b>-</b>	
changing		D	
DNS IP		de alaba a and	
FQDN		dashboard	4=
gateway IP on a single server	<u>86</u>	component descriptions	
gateway IP on Avaya SBCE	<u>88</u>	dashboard	
gateway IP on secondary EMS		screen	
hostname	<u>88</u>	database failure alarm	<u>68</u>
management IP on a single server	<u>86</u>	debugging	
management IP on Avaya SBCE	<u>88</u>	field descriptions	<u>42</u>
management IP on secondary EMS	<u>87</u>	debug logs	
network mask	<u>86</u>	location	<u>45</u>
network mask details on Avaya SBCE	<u>88</u>	deleting	
network mask details on secondary EMS		system snapshot	<u>78</u>
network passphrase		Dell R320	
changing hostname of Avaya SBCE servers		ethernet port labels	<u>12</u>
Changing IP address of the primary EMS server on the		Dell R330	
secondary EMS server	87	port labels	<u>13</u>
changing NTP address on Avaya SBCE devices		Dell R630	
changing primary EMS IP on unreachable SBCE		ethernet port labels	
checking		designating a snapshot server	<u>72</u>
counters	92	determining	
network synchronization		installation on KVM	<u>93</u>
Checking EASG status		installation on VMware	94
classification of requests/responses matching a particular		diagnostics results	
domain policy group at the node		disabling	
Tours point, group at the node		The state of the s	

disabling (continued)		ipcs password	
network interfaces using CLI	<u>89</u>	reset	<u>94</u>
disabling application debug logs	<u>44</u>	lpcsstatssipcalls	<u>58</u>
disabling EASG			
disabling GUI debug logs		1	
disk partition space alarms		L	
documentation portal		link failure alarm	67
finding content			
navigation		listing static and dynamic flows through the tilera shell	
document changes			
accurrent orlangee	······	Loading and managing site certificate	
_		logging	
E		logging in EMS	
FACC	20	logging in to EMS	
EASG		logging in to EMS through console	
disabling		login failure alarm	
enabling		logs	
EASGManage	<u>32</u>	collection	<u>55</u>
EMS,			
GUI	<u>10</u>	M	
enabling		•••	
EASG from EMS		making a system snapshot	<mark>7</mark> 4
EASG from GUI		managing	
network interfaces using CLI	<u>89</u>	SBCE logging level	30
enabling debug logs	<u>41</u>	memory alarms	
enabling EASG	<u>31</u>	MIB	
enabling GUI debug logs	<u>44</u>	OIDs	
		webRTC statistics	
_		MIB support	
F		My Docs	
field descriptions		Wy Docs	<u>90</u>
add snapshot server	73		
alarms		N	
debugging		netsync	<u>93</u>
periodic statistics		network configuration	
syslog viewer		checklist	
system viewer		new administrator-added alarm	<u>70</u>
finding content on documentation portal		new user-added alarm	<u>69</u>
finding port matrix	<u>97</u>		
		0	
G			
		out of dialog requests dropped	59
GUI and console alarm list	<u>69</u>	out of dialog responses dropped	
		out of transaction responses dropped	
Н		out or trained strong transport and production in the strong training train	<u> </u>
П			
HA failover issues		P	
troubleshoot	17		
hard disk failure alarm		packet capture	
HP DL360 G9	<u>07</u>	configuration	<u>38</u>
ethernet port labels	14	periodic statistics	
ethernet port labels	<u>14</u>	field descriptions	
		viewing	<u>24</u>
I		port labels	
		Dell EMS	
incidents		Dell R330	
IP, gateway, and network mask change	<u>86</u>	HP DL360 G8	<u>14</u>
ipcs options commands		Portwell CAD 0230	<u>12</u>

port matrix	. <u>97</u>	system logs	<u>26</u>
Portwell CAD 0230		system statistics	<u>20</u>
port labels	.12	system viewer	
Portwell CAF 0251		field descriptions	<mark>2</mark> 1
port labels	.16		
private enterprise OIDs		<b>T</b>	
support	.57	Т	
process failure alarm		ton dunon	20
purpose		tcpdump	
purpose	<u>∪</u>	running in CLI	<u>36</u>
		Telnet	
R		establishing session	<u>10</u>
		TILEncore Gx36 intelligent adapter	
real time		Avaya SBCE	<u>90</u>
SIP Server Status	_	trace	
regenerating self-signed certificates	. <u>89</u>	call	<u>38</u>
related documentation	<u>96</u>	traceSBC	
restoration of a system snapshot	<u>75</u>	log files	<u>35</u>
restoration of configuration data	<u>75</u>	overview	<u>35</u>
restore		traceSBC advantages	<mark>36</mark>
restoring a snapshot file	.77	traceSBC operation modes	
restoring a snapshot file manually		traceSBC user interface	
retrieving		training	
a snapshot file	76		
roll backon			
root password	<u> </u>	U	
reset	04		
16361	. <u>54</u>	user deleted alarms	
		user privilege change alarm	<u>70</u>
S		using	
		showflow	<u>39</u>
SBCE OID descriptions			
SBCE reconfiguration command options	. <u>84</u>	V	
screen		<b>Y</b>	
dashboard		verifying integration connection	10
searching for content	<u>98</u>	VGA connection	
sharing content		videos	
showflow		viewing	<u>oc</u>
examples	<u>39</u>	administrative users	20
syntax	39	alarms	
using	.39	audit logs	
SNMP MÏB	_	diagnostics results	
SSH		incidents	
establishing session	10		
statistics		logs	
support1		periodic statistics	
support contact	100	statistics	
checklist	33	status of the SIP servers	
swapping	. 00	system alarms	
Avaya SBCE devices in single server deployment	80	system incidents	
· · · · · · · · · · · · · · · · · · ·		system logs	
swapping Avaya SBCE devices		system statistics	
swapping EMS server in HA pair deployment		viewing	<u>19</u> , <u>20</u> , <u>29</u>
swapping EMS server in single server deployment	. <u>02</u>		
syslog viewer	07	W	
field descriptions		**	
system alarm list		watch list	Q.
system alarms <u>18</u> ,			<u>oc</u>
managing			
system incidents	<u>19</u>		