Deploying Avaya Session Border Controller on Google Cloud Platform

Release 10.2.1
Issue 1
December 2024

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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.

Service Provider

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 to comply 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, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (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

Contents

Chapter 1: Introduction

Purpose

This document describes the procedures to deploy Avaya SBC using the Google Cloud Platform.

This document is intended for people who install and configure Avaya SBC at a customer site.

Chapter 2: Architecture overview

Overview

Google Cloud Platform is a cloud services platform that enterprises use to run applications on the virtual cloud. Google Cloud Platform integrates the cloud services needed to develop, test, deploy, and manage applications, while taking advantage of the efficiencies of cloud computing.

Supporting Avaya applications on the Google Cloud Platform Infrastructure as a Service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure.
- Customers can move from CAPEX to an operational expense (OPEX).
- Reduces the maintenance cost of running data centers.
- Provides a common platform for deploying applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

Types of network connection

You can connect applications in a hybrid network on Virtual Private cloud (VPC) in the following ways:

Connection type	Resource
VPN Connection	For more information, go to https://cloud.google.com/network-connectivity/docs/vpn and search for *Cloud VPN overview* section.
GCN Direct	For more information, go to https://cloud.google.com/network-connectivity/docs/interconnect and search for *Dedicated Interconnect Overview* section.

Customer responsibilities

- The customer must set up, maintain, and troubleshoot:
  - The Google Cloud Platform environment
  - The network connectivity to Google Cloud Platform

  - The operating systems required for the software-only applications

- While Avaya provides recommendations for Google Cloud Platform instance use, the customer can choose the correct Google Cloud Platform instance. Google Cloud Platform instances have different levels of reliability, network performance, supported storage, and Input/output operations per second (IOPS). The customer can choose the Google Cloud Platform instances that provide the level of support deemed necessary.
- Avaya support is limited to isolated issues at the environment level. When the issue is related to the application execution environment, the customer or Avaya Business Partner must resolve the issue by raising tickets with Google Cloud Platform.
- Avaya provides information about the tasks that customers must perform on the Google Cloud Platform Management Console. Google might periodically update the information. Therefore, for the latest and most accurate information, see Google Cloud Platform documentation.

  For more information about customer responsibilities, see *Service Agreement Supplement for Avaya Support Advantage Essential and Preferred Support* on the Avaya Support website.

Chapter 3: Planning and preconfiguration

Prerequisite knowledge, skills, and tools

Before deploying the product, ensure that you have the following knowledge, skills, and tools.

Knowledge

- Google Cloud Platform setup
- Linux® Operating System
- Avaya SBC

Skills

Ability to administer the Google Cloud Platform Management console, Avaya Aura® applications, and Avaya SBC.

Tools and utilities

- A browser for accessing the Google Cloud Platform Management Console.
- PuTTY, PuTTYgen, WinSCP, and WinZip.

Supported instance types for footprints

Footprint	Instance type	vCPU	RAM (GB)	HDD (GB)	NICs
EMS	e2-medium	2	4	160	2
SBC	c2-standard-4	4	16	160	4
EMS+SBC	c2-standard-4	4	16	160	4

Network interfaces

The number of network interfaces that you set up depends the type of Avaya SBC instance that you are deploying.

The following table shows the minimum number of interfaces required for each type:

Type	Minimum number of interfaces	Maximum number of interfaces
EMS	1	2
SBC	4	6
EMS+SBC	4	4

The following table shows the relationship between the number of network interfaces and their configuration when deployed:

Number of network interfaces	Type of Avaya SBC configuration	Interface ports order
1	EMS only	M1
2	EMS only	M1, A1
4	EMS or EMS+SBC or SBC	B1, A1, M1, M2
6	EMS or EMS+SBC or SBC	M1, A1, B1, M2, A2, B2

Note:

EMS requires only M1 interface. A1 interface is ignored.

Password policies

The `root` and `ipcs` passwords are set during product installation. The EMS GUI has a separate password. The default user IDs and passwords are:

User name	Password
`root`	`@V@Y@_123`
`ipcs`	`Avaya_123`
`ucsec` (GUI only)	`ucsec`

Note:

After factory reset, the golden password for the root user is `Avaya_123`.

Security alert:

You must change the default passwords for the CLI root and ipcs login IDs after first boot during the installation procedure. You are prompted to enter and confirm the new password. Password restrictions are enforced on the root, ucsec, and ipcs accounts. The new password must meet the following criteria:

- Minimum of 8 characters.
- One uppercase letter, one lowercase letter, and one number.
- One special character from the following: hyphen (-), underscore (_), at sign (@), asterisk (*), or exclamation point (!).You must not use the number sign (#), dollar sign ($), or ampersand (&).

Related links

Console and SSH passwords complexity on page 11
EMS GUI password complexity on page 11
Grub password complexity on page 12
Password hashing mechanisms on page 12

Console and SSH passwords complexity

The Console and SSH passwords must adhere to the following requirements:

- Contain at least eight characters.
- Contain at least two uppercase characters, not including the first character of the password.
- Contain at least one lowercase character.
- Contain at least one special character.
- Contain at least two digits, not including the last character of the password.

The Console and SSH passwords do not have a limit on the maximum length and are hashed by MD5 hash algorithm.

Note:

Password Authentication Module (PAM) enforces password security, and hashes are stored in: `/etc/shadow`

Related links

Password policies on page 10

EMS GUI password complexity

The EMS GUI password must fulfill the following norms:

- Have at least eight characters.
- Contain mixed uppercase and lowercase characters.
- Contain at least one special character.
- Contain at least one number.

The EMS GUI password does not have a limit on the maximum length and is hashed by MD5 hash algorithm.

Related links

Password policies on page 10
Change Password field descriptions on page 12

Change Password field descriptions

Name	Description
Current Password	The password currently used for logging in.
New Password	The new password that replaces the old password.
Repeat password	The new password repeated for confirmation.

Related links

EMS GUI password complexity on page 11

Grub password complexity

The Grub password must adhere to the following requirements:

- Contain at least eight characters.
- Contain uppercase and lowercase characters.
- Contain at least special character except %, &, and $.
- Contain at least two digits.

You can change the Grub password with the **`sbceconfigurator.py change-grub-password`** command.

Related links

Password policies on page 10

Password hashing mechanisms

Release	GUI	API / Peon (User only)	Platform
8.x	SHA-256	PBKDF2/SHA-512	SHA-512
10.1.x	SHA-256	PBKDF2/SHA-512	SHA-512
10.2.x	Argon2	PBKDF2/SHA-512	SHA-512

Related links

Password policies on page 10

Generating SSH Keys

Procedure

1. Generate SSH keypair for use with Google Compute Engine using the following command:

   ```
   # ssh-keygen -t rsa -f ~/.ssh/google_compute_engine
   ```

2. In the Google Developers Console, click **Computer** > **Compute Engine** > **Metadata** > **SSH Keys** > **Edit**.

3. Enter the output generated from `~/.ssh/google_compute_engine.pub` file, and click **Save**.
4. To enable SSH agent to use this identity file for each new local console session, run the following command on the console:

```
# ssh-add ~/.ssh/google_compute_engine
```

5. To automate the command, add the below line to your `~/.ssh/config` file.

```
IdentityFile ~/.ssh/google_compute_engine
```

6. You can now connect via standard SSH to the new VM instances created in your Google Compute Engine project.

```
# ssh -i ~/.ssh/google_compute_engine  <username>@<instance_external_ip>
```

Chapter 4: Prerequisite procedures

Downloading software from Avaya PLDS

About this task

When you place an order for an Avaya PLDS-licensed software product, PLDS creates the license entitlements of the order and sends an email notification to you. The email includes a license activation code (LAC) and instructions for accessing and logging into PLDS. Use the LAC to locate and download the purchased license entitlements. In addition to PLDS, you can download the product software from http://support.avaya.com/ by navigating to the Support by Product menu at the top of the page.

Procedure

1. To access the Avaya PLDS website, type http://plds.avaya.com/ in your web browser.
2. Type your login ID and password.
3. On the PLDS home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon () for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. In **Download Pub ID**, type the download pub ID.
8. In the **Application** field, click the application name.
9. In the **Download type** field, click one of the following:
   - **Software Downloads**
   - **Firmware Downloads**
   - **Language Packs**
   - **Miscellaneous**
10. In the **Version** field, click the version number.
11. Click **Search Downloads**.

12. Scroll down to the entry for the download file, and click the **Download** link.
13. Select a location where you want to save the file, and click **Save**.
14. **(Optional)** On Internet Explorer, if you receive an error message, click the install ActiveX message at the top of the page to start the download.

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSN), and Product Correction Notices (PCN) for the product or solution on the Avaya Support Web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

Converting a QCOW2 image to a raw file format

Before you begin

1. Download the `sbce-10.2.1.0-101-24795.qcow2` image file from PLDS. For more information, see Downloading software from Avaya PLDS on page 14.
2. Ensure that you have access to Linux QEMU tools. For more information, see https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_virtualization/managing-storage-for-virtual-machines_configuring-and-managing-virtualization#managing-virtual-disk-images-by-using-the-cli_managing-storage-for-virtual-machines.

Procedure

1. Log on to the Linux server using root credentials.
2. Copy the QCOW2 image file to a temporary directory.
3. Run the following command to convert the QCOW2 image to a raw file format:

   ```
   qemu-img convert image_name disk.raw
   ```

4. Run the following command to reduce the image size:

   ```
   tar -czSf disk.raw.tar.gz disk.raw
   ```

Importing an image to Cloud Compute Engine

Procedure

1. Run the following command to upload the image to Google Cloud Storage:

   ```
   gsutil cp disk.raw.tar.gz gs://asbce-images/
   ```

2. Run the following command to import the image to Google Compute Engine:

   ```
   gcloud compute images create asbce-813ga --source-
   uri gs://asbce-images/disk.raw.tar.gz --guest-os-features
   MULTI_IP_SUBNET,UEFI_COMPATIBLE
   ```

Chapter 5: Deploying and configuring Avaya SBC

Signing in to Google Cloud Platform

Before you begin

Create a Google Cloud Platform account.

Procedure

1. In your web browser, type https://cloud.google.com/
2. Click **Sign In** and select the Google Cloud Platform account.
3. On the Google Cloud Platform dashboard, go to **Compute Engine**.

Creating a virtual machine

Procedure

1. In Google Developers Console, click **Compute** > **Compute Engine** > **VM instances**.
2. Select your project and click **Continue**.
3. Click **Create instance**.
4. Enter the following details in the Create a new instance window:
   a. **Name**: Assign a name to the VM.
   b. **Zone**: Select a zone for the VM.
   c. **Machine type**: Select a machine configuration for the VM.
5. Click **Create**.
6. In the **Boot disk** section, click **Change**, and do the following:
   a. Select the **Custom Images** tab.
   b. Click **Select a project**, select the project that contains the image, and click **Open**.
   c. In the **Image** list, click the image to import.
   d. Select the type and size of your boot disk.

e. To confirm the boot disk options, click **Select**.

7. In the **Firewall** section, select one of the following:
   - **Allow HTTP traffic**: To enable HTTP traffic to the VM.
   - **Allow HTTPS traffic**: To enable HTTPS traffic to the VM.
8. In the Identity and API access section, select the **Allow full access to all Cloud APIs** field.

Configuring the network interfaces

Procedure

1. On the Networking tab, click **Add network interface.**
2. Choose a network.
3. If there are multiple subnets in the VPC network, choose a subnet.
4. To assign a custom internal IP address to the interface, on the **Internal IP** drop-down menu, choose **Custom** and then type the IP address.
5. To indicate that you do not want an external IP address, on the **External IP** drop-down menu, choose **None**.
6. To assign a static external IP address, on the **External IP** drop-down menu, choose **New static IP**, type **Name** and **Description**, and click **Reserve**.
7. To add more network interfaces, click **Add network interface** and follow steps 2-6 above.

   Note:

   Add four network interfaces in the following order: SBC_B1, SBC_A1, SBC_M1, and SBC_M2.
8. On the Management page, in the **Metadata** section, configure the following fields:
   - Set the **Key 1** field to `nic0` and **Value 1** field to `B1`.
   - Set the **Key 2** field to `nic1` and **Value 2** field to `A1`.
   - Set the **Key 3** field to `nic2` and **Value 3** field to `M1`.
   - Set the **Key 4** field to `nic3` and **Value 4** field to `M2`.

Running the first boot configuration

Before you begin

In the Google Cloud Portal, verify that the Overview window for the VM you created earlier is open. You can find the VM under All Resources if you need to open it. The Overview window

allows you to see whether the VM is running, stop or restart the VM, get the public IP address of the VM, and see the activity of the CPU, disk, and network components.

Be prepared to change the password during the first boot configuration. You cannot keep the default password.

Note:

Prior to running cloud configurator, you must ensure that the following resources are configured correctly:

- CPU
- Disk
- Network interfaces

Procedure

1. Log in to the console using SSH to the Avaya SBC virtual machine from the subnet that is enabled for your system. Use the password `@V@Y@_123`.

   `ssh root@<`*`SBC_VM_IP_ADDRESS`*`> -p 22`

   If there is a problem using SSH, you can use the Serial Console.

2. Run the following command twice:

   `/usr/local/ipcs/icu/scripts/CloudConfigurator.py -s`

   The system displays a prompt to accept the EULA agreement and then displays a configuration screen similar to configuration on VMware and hardware. For more information on deploying Avaya SBC using CLI methods, see *Deploying Avaya SBC in Virtualized Environment* document.

3. After the system reboots, wait for several minutes for the system processes to stabilize and you receive the “Boot process complete” message.

4. Power off and power on the VM from the Google Cloud Portal page.

Chapter 6: Deploying High Availability on Google Cloud Platform

About deploying High Availability on Google Cloud Platform

You can deploy Avaya SBC in a High Availability (HA) configuration on the Google Cloud Platform.

Avaya SBC supports HA functionality using the Google Load Balancers. For more information, refer https://cloud.google.com/load-balancing/docs/network.

Google Cloud Network load balancer is a pass-through load balancer.

Checklist for deploying Avaya SBC in High Availability on Google Cloud Platform

No.	Task	Reference	✔
1	Create an instance group.	Creating an instance group on Google Cloud Platform on page 21	
2	Create a health check.	Creating a health check on Google Cloud Platform on page 22	
3	Create an external load balancer.	Creating an external load balancer on Google Cloud Platform on page 22	
4	Configure frontend configuration for external load balancer.	Configuring frontend configuration on page 23	
5	Configure backend configuration for external load balancer.	Configuring backend configuration on page 23	
6	Configure network for external load balancer.	Configuring network on page 24	
7	Configure signaling interface for external load balancer.	Configuring signaling interface on page 24	

Table continues…

No.	Task	Reference	✔
8	Create an internal load balancer.	Creating an internal load balancer on Google Cloud Platform on page 26	
9	Configure frontend configuration for internal load balancer.	Configuring frontend configuration on page 26	
10	Configure backend configuration for internal load balancer.	Configuring backend configuration on page 23	
11	Configure network for internal load balancer.	Configuring network on page 27	
12	Configure signaling interface for internal load balancer.	Configuring signaling interface on page 24	

Creating an instance group on Google Cloud Platform

About this task

An instance group is a group of virtual machine instances managed as a single entity.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Compute Engine** > **Instance Groups**.
3. Click **Create instance group** > **New unmanaged instance group**.
4. On the Create instance group page, provide the following information:

- **Name**: Name of the instance group.
- **Zone**: Select the zone for the primary Avaya SBC.
- **Region**: Select the region of your servers.
- **Network**: Select the network for your virtual machine.
- **Subnetwork**: Select the subnetwork for your virtual machine.
- **Select VMs**: Select the primary Avaya SBC virtual machine from the list.

5. Click **Create**.
6. Repeat steps 1 to 5 to create another instance group. For **Zone** and **Select VMs** fields, select secondary Avaya SBC.

Creating a health check on Google Cloud Platform

About this task

Google Cloud Platform enables you to create or select a health check when you complete the backend configuration of the load balancer in the console. The overall health state of each backend determines eligibility to receive new requests or connections.

You can use the same health check to configure the TCP and UDP load balancers.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Compute Engine** > **Health checks**.
3. Click **Create a health check**.
4. On the Create a health check page, provide the following information:

- **Name**: Name for the health check.
- **Description**: Description of the health check.
- **Scope**: Choose `Regional` and select **Region**.
- **Protocol**: Select `TCP`.
- **Port**: Enter `5060`.
- **Check interval**: Define the duration from the start of one probe to the start of the next one as `1 second`.
- **Timeout**: Define the duration for which Google Cloud waits for a response to a probe as `1 second`.
- **Healthy threshold**: Define the duration that Google Cloud waits for a response to a probe as `2`.
- **Unhealthy threshold**: Define the number of sequential probes that must fail for the VM instance to be considered unhealthy as `2`.

5. Click **Create**.

Configuring an external load balancer on Google Cloud Platform

Creating an external load balancer on Google Cloud Platform

Before you begin

- Create an instance group if it is not already created.

- Create a health check,if it is not already created.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Network services** > **Load balancing** and click **Create a load balancer**.
3. For **TCP Load Balancing**, click **Start configuration**.
   a. For **Internet facing or internal only**, select **From Internet to my VMs**.
   b. For **Multiple regions or single region**, select **Single region only**.
   c. For **Backend type**, select **Backend Service**
4. For **Backend Services**, enter **Name** and **Region**.
5. Click **Continue**.

Configuring frontend configuration

Procedure

1. On the **New TCP load balancer** screen, click **Frontend configuration**.
2. In the **Name** field, type the name.
3. On the Frontend configuration screen, perform the following:
   a. For **IP version**, select **IPv4**.
   b. From **Network Service Tier**, select **Premium**.
   c. From **IP Address**, select the IP address.
   d. For **Ports**, select **All**.
4. Click **Done**.

Note:

This IP address gathered from these configuration steps is added to the network interface.

Configuring backend configuration

Procedure

1. On the **New TCP load balancer** screen, enter a **Name**.
2. From the **Region** field, select **Region**.
3. On the Backend configuration screen, perform the following:
   a. For new back-ends, choose the instance group that you added and click **Done**.
   b. Click **Add backend**.
   c. Choose another instance group you added and select **Use this instance group as a failover group for backup**.

d. Click **Done**.

e. Select **Health check**.

f. For **Drop traffic**, toggle on the **Enable (Drop new connections if no healthy VMs)** option.

4. Click **Save**.

Configuring network

About this task

To pass the traffic between the external load balancer and Avaya SBC, it is necessary to enable the Pass through flag when configuring Avaya SBC behind the load balancer.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBC**.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   The EMS server displays the Network Management screen.
4. In the content pane, click **Add**.

   The EMS server displays the Add Network pop-up window.
5. In the **Name** field, type the network name.
6. In the **Default Gateway** field, type the default gateway of the network.
7. In the **Network Prefix or Subnet Mask** field, type the subnet mask of the network.
8. From the **Interface** list, select interface.
9. Add the IP address for B1 network interface.
10. Click **Add**.
11. Add the IP address gathered from the frontend configuration and enable the **Passthrough** check box.

    Note:

    Passthrough option enables configuring different network IP addresses for same network interface. Passthrough network IP addresses must be routable on the same subnet that is configured on Avaya SBC.
12. Click **Finish**.

Configuring signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The EMS Server displays the Signaling Interface page.
4. In the content pane, click **Add**.
5. Administer the appropriate options.

   Signaling interface must use the IP address gathered from the load balancer front end.
6. Click **Finish**.

Signaling interface field descriptions

Name	Description
Name	The name of the signaling interface.
IP Address	The network name, identified by the interface name and VLAN tag, and IP address of the Avaya SBC used by SIP signaling messages traversing the network. Signaling interface must use the IP address gathered from the load balancer front end.
TCP Port	The port that the Avaya SBC security device processes for TCP packets.
UDP Port	The port that the Avaya SBC security device processes for UDP packets.
TLS Port	The port that the Avaya SBC security device processes for TLS packets.
TLS Profile	The TLS profile for the **TLS Port** specified above.
Enable Shared Control	OneX Client Shared control support on the Avaya SBC security device. This check box must be enabled only on the Internal Side Interface of Avaya SBC, that is, towards call server. You must enable the Avaya SBC TLS port before enabling this check box.
Shared Control Port	The port that the Avaya SBC security device processes for OneX shared control packets.

Note:

Port configuration is the choice of the user. However, if the user has a data firewall then the user must synchronize the ports configured in the Avaya SBC with the ports in the data firewall. If the user has no data firewall, no action is required.

Configuring an internal load balancer on Google Cloud Platform

Creating an internal load balancer on Google Cloud Platform

Before you begin

- Create an instance group if it is not already created.
- Create a health check,if it is not already created.

Procedure

1. Log on to the Google Cloud Platform.
2. Navigate to **Network services** > **Load balancing** and click **Create a load balancer**.
3. For **TCP Load Balancing**, click **Start configuration**.
   a. For **Internet facing or internal only**, select **Only between my VMs**.
   b. For **Multiple regions or single region**, select **Single region only**.
   c. For **Load Balancer type**, select **Pass-through**
4. For **Backend Services**, enter **Name** and **Region**.
5. Click **Continue**.

Configuring frontend configuration

Procedure

1. On the **New TCP load balancer** screen, click **Frontend configuration**.
2. In the **Name** field, type the name.
3. On the Frontend configuration screen, perform the following:
   a. For **IP version**, select **IPv4**.
   b. From **Network Service Tier**, select **Premium**.
   c. In **IP Address**, enter the IP address gathered from the front end configuration.

      Note:

      Do not enable the Passthrough flag.
   d. For **Ports**, select **All**.
4. Click **Done**.

Configuring backend configuration

Procedure

1. On the **New TCP load balancer** screen, enter a **Name**.
2. From the **Region** field, select **Region**.
3. On the Backend configuration screen, perform the following:
    a. For new back-ends, choose the instance group that you added and click **Done**.
    b. Click **Add backend**.
    c. Choose another instance group you added and select **Use this instance group as a failover group for backup**.
    d. Click **Done**.
    e. Select **Health check**.
    f. For **Drop traffic**, toggle on the **Enable (Drop new connections if no healthy VMs)** option.
4. Click **Save**.

Configuring network

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **SBC**.
3. In the navigation pane, click **Network & Flows** > **Network Management**.

   The EMS server displays the Network Management screen.
4. In the content pane, click **Add**.

   The EMS server displays the Add Network pop-up window.
5. In the **Name** field, type the network name.
6. In the **Default Gateway** field, type the default gateway of the network.
7. In the **Network Prefix or Subnet Mask** field, type the subnet mask of the network.
8. From the **Interface** list, select interface.
9. Add the IP address for A1 network interface.
10. Click **Add**.
11. Add the IP address gathered from the frontend configuration.
12. Click **Finish**.

Configuring signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. From the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.

   The EMS Server displays the Signaling Interface page.
4. In the content pane, click **Add**.
5. Administer the appropriate options.

   Signaling interface must use the IP address gathered from the load balancer front end.
6. Click **Finish**.

Signaling interface field descriptions

Name	Description
Name	The name of the signaling interface.
IP Address	The network name, identified by the interface name and VLAN tag, and IP address of the Avaya SBC used by SIP signaling messages traversing the network. Signaling interface must use the IP address gathered from the load balancer front end.
TCP Port	The port that the Avaya SBC security device processes for TCP packets.
UDP Port	The port that the Avaya SBC security device processes for UDP packets.
TLS Port	The port that the Avaya SBC security device processes for TLS packets.
TLS Profile	The TLS profile for the **TLS Port** specified above.
Enable Shared Control	OneX Client Shared control support on the Avaya SBC security device. This check box must be enabled only on the Internal Side Interface of Avaya SBC, that is, towards call server. You must enable the Avaya SBC TLS port before enabling this check box.
Shared Control Port	The port that the Avaya SBC security device processes for OneX shared control packets.

Note:

Port configuration is the choice of the user. However, if the user has a data firewall then the user must synchronize the ports configured in the Avaya SBC with the ports in the data firewall. If the user has no data firewall, no action is required.

Chapter 7: Licensing requirements

About licensing requirements

Avaya SBC uses the Avaya Product Licensing and Delivery System (PLDS) to create licenses and download Avaya SBC software. PLDS is not integrated with WebLM. Use PLDS to perform operations such as license activations, license upgrades, license moves and software downloads.

There are two licensed versions of Avaya SBC:

- Standard Services delivers non-encrypted SIP trunking.
- Advanced Services adds Mobile Workspace User, Media Replication, and other features to the Standard Services offer.

Avaya Aura® Mobility Suite and Collaboration Suite licenses include Avaya SBC.

Avaya SBC uses WebLM version 8.0 or later for licensing requirements. You can install the Avaya SBC license file on a primary Element Management System (EMS) using the Device Management page.

Important:

You must not enable the local WebLM option and install an Avaya SBC license file on the secondary EMS if used in an active-active deployment. If you install a license file on a secondary EMS in an active-active deployment, the licensing system will always show that the secondary EMS is in **OK** state.

Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. You have a 30-day grace period from the day of installation or upgrade to install the license. Avaya SBC works normally during the grace period.

Important:

Licenses and a WebLM server are required for new installations or upgrades.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

The primary host ID of WebLM is used for creating the license file.

- Licensed features
- Licensed capacity

All hardware Avaya SBC devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBC on hardware, use a WebLM server installed on VMware or System Manager WebLM.

Avaya SBC supports pooled licensing. As opposed to static license allocation, Avaya SBC dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBC devices can use a pool of licenses dynamically across the devices as required.

For integration with Microsoft® Teams, Avaya SBC requires the Premium license and Premium HA license permissions in addition to the Standard Services and Advanced Services licenses.

For the use of AMR-WB codec, Avaya SBC requires counting license for AMR-WB codec license and AMR-WB codec HA tracking license. This is applicable to both static and dynamic licenses.

Initial Grace Period: Initial Grace Period is when Avaya SBC is newly installed and has no connection established to licensing server. When in initial grace period Avaya SBC only allows 100 licenses per feature.

Grace Period: Grace Period is when Avaya SBC loses its connection to licensing server after serving. In Dynamic Licensing Mode, when in Grace Period, State licensing statistics would show 0 and will be updated when connections with the licensing server are restored.

On upgrading to 10.2.1, EMS might display following warnings:

- *This system has one or more SBC(s) that does not have a valid AMR license configuration.*

  This may cause calls to fail or may cause other problems with the attached SBC(s). Check the device settings and license settings to ensure that calls will be processed properly.
- *This system has one or more SBC(s) that appear to have no licensing configuration.*

  This may cause calls to fail or may cause other problems with the attached SBC(s). Check the device settings and license settings to ensure that calls will be processed properly.

These warnings can be corrected by properly configuring licenses for all required features.

Avaya SBC licensed features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_PREM_SESSION	Specifies the number of premium session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_PREM_HA_SESSION	Specifies the number of premium service HA session licenses. Premium licenses are required when using Microsoft Teams.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Meetings Server video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBC elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that the download of virtual system installation files for VMware, KVM, Amazon Web Services, and Microsoft® Azure is permitted.
VALUE_SBCE_ENCRYPTION_1	Specifies that both media and signaling can be encrypted for Avaya SBC. This license is required when using any advanced licenses.

Table continues…

License feature	Description
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBC. The quantity of this license must match the quantity of standard licensing in the system being managed.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies Avaya SBC encryption only for signaling.
VALUE_SBCE_NG911	Specifies the number of AMR-WB codec licenses.
VALUE_SBCE_NG911_HA	Specifies the number of AMR-WB codec HA licenses.

License installation

You can install Avaya SBC license on either of the following servers:

- The WebLM server on System Manager
- The local WebLM server

Installing a license on WebLM server on System Manager

Before you begin

Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com/.

About this task

If you experience problems while installing the license file, see the License file installation errors section in *Administering standalone Avaya WebLM*.

Procedure

1. Log in to the System Manager web interface.
2. On the home page, in the **Services** section, click **Licenses**.
3. In the left navigation pane, click **Install license**.
4. Browse to the location where you saved the license file, and select the file to upload.
5. Click **Install**.
6. Verify that the license is installed. If the installation is successful, a new menu item named ASBC appears in the left navigation pane. Click **ASBC** to view the licensed features.

Installing a license file on the local WebLM server

Procedure

1. Log in to the WebLM application. If you are logging in for the first time, the system prompts you to change the default password.
2. In the left navigation pane, click **Install License**.

   The system displays the Install License page.
3. In the **Enter license path** field, select the downloaded license from your computer and click **Install**.

   After the license is successfully installed, the system displays a new menu **ASBC**.
4. Click **ASBC** to view the license information.

Configuring the WebLM server IP address using the EMS web interface

Before you begin

Install the Avaya SBC license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Navigate to **Device Management** > **Licensing**.
3. Do one of the following tasks:
   - For a WebLM server or standalone server installed on System Manager , in the **WebLM Server URL** field, type the URL of the WebLM server and click **Save**.

     The URL format of the WebLM server installed on System Manager is:

     `https://<SMGR_server_IP>:52233/WebLM/LicenseServer`

     The URL format of the standalone WebLM server is:

     `https://<WEBLM_server_IP>:52233/WebLM/LicenseServer.`
   - For an external WebLM server, type the link for the external WebLM server in **External WebLM Server URL** and click **Save**.
4. Click **Refresh Existing License** to refresh the existing licenses.
5. Click **Verify Existing License** to verify the existing WebLM license to confirm it is trusted.

If the WebLM license is trusted, a pop window will display the certificate details. Otherwise, you can select the option to trust the WebLM certificate manually.

6. On the Dashboard screen, check the **License State** field.

   If the configuration is successful, the **License State** field shows `OK`.

7. Click the **Devices** tab.
8. Locate the Avaya SBC device you configured, and click **Edit**.

   The EMS server displays the Edit Device dialog box.

9. In the **Standard Sessions**, **Advanced Sessions**, **Scopia Video Sessions**, and **CES Sessions** fields, type the number of licensed sessions depending on the license you purchased.
10. Click **Finish**.

Configuring the WebLM server IP address using CLI

Before you begin

Install the Avaya SBC license file on a WebLM Release 8.0 or later server installed on System Manager, a local WebLM, or a standalone WebLM server. For more information about installing license files and WebLM, see *Administering standalone Avaya WebLM*.

Get the URL for the WebLM server.

Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command to configure an external WebLM server URL:

   `sbceconfigurator.py config-weblm-url <WebLM URL>`

3. Reboot Avaya SBC.

About centralized licensing

Using Centralized Licensing feature, the WebLM server can directly distribute the licenses to Avaya SBC connected to different Element Management System (EMS) in different networks.

The Centralized Licensing feature provides the following advantages:

- Eliminates the need to install and configure multiple WebLM servers, one for each Avaya SBC setup.
- Eliminates the need to log in to each WebLM server to manage licenses for each Avaya SBC setup.

- Reduces the VMware licensing cost for installing and configuring multiple WebLM OVAs on VMware.
- Provides a centralized view of license usage for Avaya SBC.

Note:

- The setup does not support the Centralized Licensing feature.
- The Centralized Licensing feature is optional. Use the Centralized Licensing feature when you have more than one Avaya SBC setup.

Chapter 8: Verifying a successful deployment

You can verify the successful deployment of EMS using one of the following methods:

- Access the EMS server using the web interface.
- Access the EMS server through console.
- Establish a CLI session through a secure shell session (SSH).

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.

Installing and verifying successful installation of EMS and SBC

Procedure

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

   Note:

   The following step is not applicable for the single server deployment of Avaya SBC.
3. On the Device Management page, do the following:
   a. In the **Devices** tab, click **Add**.
   b. In the Add Devices window, enter the Avaya SBC details, such as the host name and the management IP address.
   c. Click **Finish**.

   On the Device Management page, the **Status** column of the Avaya SBC device displays Registered.
4. Click **Install**.
5. In the Install Wizard, enter the configuration. For more information, see *Administering Avaya Session Border Controller*.
6. Click **Finish**.

   In the **Devices** tab, the **Status** column of the device displays **Commissioned** indicating that the device is successfully deployed and configured.

Logging in to the EMS using SSH

Procedure

1. Log in to SSH client using PuTTy.
2. Type the IP address for Avaya SBC.
3. Specify the port as **22** or **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 SBC.

Chapter 9: Resources

Documentation

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

Title	Description	Audience
Design		
Avaya Session Border Controller Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBC.	Sales engineers, solution architects, and implementation engineers
Avaya Session Border Controller Release Notes	Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions.	Sales and deployment engineers, solution architects, and support personnel
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform servers.	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation		
Deploying Avaya Session Border Controller on a Hardware Platform	Describes how to plan and deploy an Avaya SBC system on the supported set of hardware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Virtualized Environment Platform	Describes how to plan and deploy an Avaya SBC system on customer-provided VMware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Google Cloud Platform	Describes how to plan and deploy an Avaya SBC system on a Google Cloud Platform.	Sales and deployment engineers, solution architects, and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Session Border Controller on an Amazon Web Services Platform	Describes how to plan and deploy an Avaya SBC system on Amazon Web Services.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Microsoft® Azure Platform	Describes how to plan and deploy an Avaya SBC system on a Microsoft® Azure platform.	Sales and deployment engineers, solution architects, and support personnel
Avaya Session Border Controller Port Matrix	Describes the incoming and outgoing port usage required by the product.	Sales and deployment engineers, solution architects, and support personnel
Upgrading Avaya Session Border Controller	Describes how to upgrade to the latest release of Avaya SBC.	Sales and deployment engineers, solution architects, and support personnel
Installing the Avaya Solutions Platform 110 Appliance	Describes how to install Avaya Solutions Platform 110 Appliance servers.	Sales and deployment engineers, solution architects, and support personnel
Administration		
Administering Avaya Session Border Controller	Describes configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Session Border Controller	Describes troubleshooting and maintenance procedures for Avaya SBC.	Implementation engineers
Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers.	Implementation engineers
Using		
Working with Avaya Session Border Controller and Microsoft® Teams	Describes how to set up, maintain, and use Avaya SBC with Microsoft Teams.	Implementation engineers and administrators
Working with Avaya Session Border Controller Multi-Tenancy	Describes how to set up, maintain, and use the Avaya SBC Multi-tenancy feature.	Implementation engineers and administrators
Working with Avaya Session Border Controller Geographic-Redundant Deployments	Describes how to set up, maintain, and use the Avaya SBC Geographic-redundant deployment feature.	Implementation engineers and administrators

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.

  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. 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
20600W	Avaya Session Border Controller 8.1 Technical Delta
21098W	Session Border Controller 8.0 Technical Delta
20660W	Administering the Avaya Session Border Controller for Enterprise - SIP Trunk
60660W	Administering Avaya SBC Release 8 for Remote Worker
20660T	Administering Avaya SBC Release 8 Test
20800C	Implementing and Supporting Avaya SBC — Platform Independent
20800T	Avaya SBC Platform Independent and Support Test
20800V	Implementing and Supporting Avaya SBC — Platform Independent
26160W	Avaya SBC Fundamentals
7008T	Avaya SBC for Midmarket Solutions Implementation and Support Test
7008W	Avaya SBC for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions

Table continues…

Course code	Course title
71300	Integrating Avaya Communication Applications
72300	Supporting Avaya Communication Applications

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.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select 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 www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords 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 example, Contact Centers.

Note:

Videos are not available for all products.

Support

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

Index

P

R

S

T

V

W