



Using Avaya Experience Platform[®] Private Cloud and Avaya Aura[®] Private Cloud

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.

"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](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 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.

Third Party Components

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](http://www.mpegla.com).

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](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>).

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 LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <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.

Contents

Chapter 1: About this document	6
Overview	6
Target audience	6
Change history	6
Chapter 2: Devices	8
Avaya 9600 Series IP Deskphones	8
Avaya B100 Series Conference and SIP Phones	9
Avaya J100 Series IP Phones	9
Avaya Edge friendly Gateway	10
Local survivability with Avaya Solutions Platform S8300	12
Configuration needed for local survivability of SIP trunks in System Manager	34
Avaya Vantage™	40
Device bundles	41
Chapter 3: Applications	42
Avaya Admin Portal	42
Avaya Aura® Call Center Elite	43
Avaya Aura® X for Zoom Workplace	43
Avaya Aura® X for Zoom Workplace features	44
Avaya Callback Assist	45
Avaya Call Management System	46
Automatic Call Distribution	46
CMS Connectors and ODBC	47
Avaya Experience Portal	49
Avaya Messaging	49
Avaya Workplace Attendant	49
Avaya Workplace Client	50
Avaya Workspaces	50
CRM integration with Salesforce, Microsoft Dynamics® 365, and ServiceNow	51
Call Detail Recording	51
Call Detail Recording details	51
Components of Call Detail Recording	52
SFTP server	57
Device Enrollment Services	58
Registering a device into AXP Private Cloud and Avaya Aura® Private Cloud	58
Digital channels	59
E-Bond	60
Instant Messaging and Presence	60
Mobile Push Notifications	60
Push Notification provider	61

STIR/SHAKEN.....	61
Verint Workforce Engagement Cloud.....	62
911inform Location Discovery Solution.....	62
Chapter 4: AXP Private Cloud and Avaya Aura® Private Cloud documentation.....	64
AXP Private Cloud and Avaya Aura® Private Cloud documents.....	64
Chapter 5: Resources.....	66
Support.....	66
Opening a technical support ticket using Avaya OneCare Portal.....	66
Opening an MACD support ticket using Avaya OneCare Portal.....	67
Finding documents on the Avaya Support website.....	68
Avaya Documentation Center navigation.....	69

Chapter 1: About this document

Overview

Avaya Experience Platform® (AXP) Private Cloud with Avaya Aura® Private Cloud is an enterprise-level communication and collaboration dedicated cloud solution with a standard reference architecture, full-featured personalization, and self-administration capabilities. This solution enables geographically distributed personnel to meet, message, and collaborate.

This document provides an overview of devices, soft clients, and applications that the AXP Private Cloud with Avaya Aura® Private Cloud solution supports.

Target audience

This document is intended for the system administrator and end user of AXP Private Cloud and Avaya Aura® Private Cloud.

Change history

Date	Summary of changes
June 2025	Added the following topics, which further include sub-topics: • Local survivability with Avaya Solutions Platform S8300 on page 12 • Configuration needed for local survivability of SIP trunks in System Manager on page 34
February 2025	Updated the release month.

Table continues...

Date	Summary of changes
December 2024	- Updated the following topics as per the rebranded Avaya OneCare Portal: Opening a technical support ticket using Avaya OneCare Portal on page 66 Opening an MACD support ticket using Avaya OneCare Portal on page 67 - Deleted Avaya Spaces entitlement from the AXP Private Cloud with Avaya Aura® Private Cloud solution.
November 2024	Added the following topics: Avaya Aura X for Zoom Workplace on page 43 Call Detail Recording on page 51 Mobile Push Notifications on page 60
September 2024	- Rebranded Avaya Enterprise Cloud™ unified communication capabilities to Avaya Aura® Private Cloud. - Added the following topics: CMS Connectors and ODBC on page 47 STIR/SHAKEN on page 61 - Updated the topic Avaya Call Management System on page 46.
August 2024	- Rebranded the guide with the following changes: - Avaya Enterprise Cloud™ contact center capabilities renamed to AXP Private Cloud. - Avaya Enterprise Cloud™ represents unified communication capabilities. - Added the topic CRM integration with Salesforce, Microsoft Dynamics 365, and ServiceNow on page 51.
June 2024	Added the topic Avaya Callback Assist on page 45.
May 2024	Added the following topics: Avaya Workspaces on page 50 Digital channels on page 59
April 2024	Added the topic Verint Workforce Engagement Cloud on page 62.
January 2024	- Added the following topics: 911inform Location Discovery Solution on page 62 Instant Messaging and Presence on page 60 Finding documents on the Avaya Support website on page 68 - Updated the following topics: Avaya Workplace Attendant on page 49 Device Enrollment Services on page 58

Chapter 2: Devices

This chapter outlines the devices that the AXP Private Cloud with Avaya Aura® Private Cloud solution supports.

*** Note:**

Any Avaya phone or Avaya terminal must support SIP and TLS 1.2. to be connected to AXP Private Cloud and Avaya Aura® Private Cloud. For the US market, phones must also support MAC address details to identify the caller's location.

DECT wireless phones do not provide MAC address details and are not supported for AXP Private Cloud and Avaya Aura® Private Cloud.

Avaya 9600 Series IP Deskphones

Avaya 9600 Series IP Deskphones are a series of desk handset devices that leverage the enterprise IP network, thus eliminating the need for a separate voice network.

Avaya 9600 Series IP Deskphones offer high-quality audio with low power requirements. A context-sensitive graphical interface and a large colored touchscreen deliver increased call control. These phones also work with the Avaya Aura® environment and the IP Office platform.

*** Note:**

Avaya Aura® Private Cloud supports legacy 96x1 series phones with firmware version 7.1.3 or later. The 96x1 device family is at End of Manufacturing Support (EoMS). Any issues will be treated according to the supported policies.

For more information about Avaya 9600 Series IP Deskphones, see the following documentation:

Document Title	Description
9600 Series IP Deskphones Overview and Specifications	High-level understanding of the product features, functions, capacities, and limitations of Avaya 9600 Series IP Deskphones.
Using Avaya 9608/9608G/9611G IP Deskphones SIP	Features of 9608, 9608G, and 9611G IP Deskphones SIP.
Using Avaya 9621G/9641G/9641GS IP Deskphones SIP	Features of 9621G, 9641G, and 9641GS IP Deskphones SIP.

Avaya B100 Series Conference and SIP Phones

The Avaya B100 Series Conference Phone provides a powerful, hands-free conference phone. These phones suit the midsize and large conference rooms with SIP and Analog connections.

Avaya Aura® Private Cloud supports the following B series USB audio or speaker phones:

- Avaya B109 conference phone
- Avaya B129 Conference Phone

Avaya Aura® Private Cloud supports the following B series SIP phones:

- Avaya B169 SIP phone (End of Sale)
- Avaya B179 SIP phone (End of Sale)
- Avaya B199 SIP phone

For more information about the Avaya B100 Series conference phone, see the following documentation:

Document Title	Description
Avaya B109 Conference Phone User Guide	How to use the Avaya B109 Conference Phone with a computer, pairing and using with a Bluetooth device, settings, and descriptions of the LED display.
Using Avaya Conference Phone B199 Avaya B199 Conference Phone Quick Guide	How to use the features available on the Avaya B199 Conference Phone and end user procedures to set up various functionalities.

Avaya J100 Series IP Phones

Avaya J100 Series IP Phones provide a range of applications and features such as presence for Avaya Aura® Private Cloud, leveraging the enterprise IP network. You do not need a separate voice network. The Avaya J100 Series IP Phones offer superior audio quality with amplified handsets and low power requirements in a Session Initiation Protocol (SIP) environment.

Avaya Aura® Private Cloud supports the following J series phones:

- Avaya J129 IP Phone
- Avaya J139 IP Phone
- Avaya J159 IP Phone
- Avaya J169 IP Phone (End of Sale)
- Avaya J179 IP Phone
- Avaya J189 IP Phone

For more information about Avaya J100 Series IP Phones or a specific model, see the following documentation at https://documentation.avaya.com/bundle?labelkey=J100_Series_Phones:

Document Title	Description
<i>Using Avaya J129 SIP IP Phone in Avaya Aura® Quick Reference for Avaya J129 SIP IP Phone in Avaya Aura®</i>	How to use the features available on the Avaya J129 IP Phone and end user procedures to set up various functionalities.
<i>Using Avaya J139 SIP IP Phone in Avaya Aura® Quick Reference for Avaya J139 SIP IP Phone in Avaya Aura®</i>	How to use the features available on the Avaya J139 IP Phone and end user procedures to set up various functionalities.
<i>Using Avaya J159 SIP IP Phone in Avaya Aura® Quick Reference for Avaya J159 SIP IP Phone in Avaya Aura®</i>	How to use the features available on the Avaya J159 IP Phone and end user procedures to set up various functionalities.
<i>Using Avaya J169 and J179 SIP IP Phones in Avaya Aura®</i>	How to use the features available on the Avaya J169/J179 IP Phone and end user procedures to set up various functionalities.
<i>Using Avaya J189 SIP IP Phones in Avaya Aura®</i>	How to use the features available on the Avaya J189 IP Phone and end user procedures to set up various functionalities.

Avaya Edge friendly Gateway

Avaya Edge friendly Gateway is an optional add-on if available for your AXP Private Cloud with Avaya Aura® Private Cloud solution.

Avaya Gateways G430 or G450 (H.248) support Time Division Multiplexing (TDM), extension connectivity (Analog, Fax, and Digital), and TDM local trunking (ISDN and Analog) securely without VPN. The audio path between connected devices remains local to the gateway location.

The Edge friendly Gateway uses duplication of the WAN link as a cost-effective backup to connect the location of the gateway to the Avaya Aura® Private Cloud Core. Local survivability ensures uninterrupted connectivity using limited resources during a WAN failure.

The Edge friendly Gateway solution supports BSM and LSP based survivability. All G430 and G450 chassis – Vintage 1, 2, and 3 are compatible with the Edge friendly Gateway solution.

Note:

Avaya Aura® Private Cloud does not support any H.323 Gateways or endpoints. Supported Avaya H.248-based Gateways must be installed by Avaya or authorized partners at remote non-Data Center customer premise (not hosted in Avaya Aura® Private Cloud) locations, with an on-site support agreement.

All the standard G4xx media gateway modules are compatible with the Avaya Edge friendly Gateway, including:

- Station support
- Analog voice
- Trunk interfaces
- Integrated Services Digital Network Primary Rate Interface (ISDN PRI - T1 and E1 interface)
- Analog

All the standard port features operate the same in the Edge and Enterprise modes.

*** Note:**

For re-purposed endpoints, you bear the costs of any required fees for the firmware updates, vintage upgrades, or application of SIP and TLS 1.2, based on the requirements of Avaya Aura® Private Cloud.

The standard G4xx media gateway modules support the following devices:

- Avaya B100 Series Conference Phones
- Avaya 9600 Series IP Deskphones. Any legacy Avaya 96x1 phone with firmware version 7.1.9 or later
- Avaya J100 Series IP Phones
- Avaya Vantage™

*** Note:**

Hard endpoints such as Gateways and SIP phones are not included with the AXP Private Cloud with Avaya Aura® Private Cloud solution. All on-premises elements must be procured separately, including any required fees for installation, firmware updates, and vintage upgrades.

Avaya supports a phased migration to AXP Private Cloud and Avaya Aura® Private Cloud with a hybrid solution. The hybrid model consists of standard mode gateways pointing to the on-premises system and an Edge friendly mode gateway pointing to the Avaya Aura® Private Cloud Core.

You must upgrade your existing gateway firmware to 8.1.12 or later.

For more information about the Avaya Gateways, see the following articles:

Article	Description
Avaya G450 Branch Gateway Overview and Specification	Overview of the G450 Branch Gateway, a multifunctional gateway deployed in medium to large-sized branch locations, and information about the functionality of this gateway.

Table continues...

Article	Description
Avaya G430 Branch Gateway Overview and Specification	Overview of the G430 Branch Gateway, a multipurpose gateway targeting small and medium branches of 1 to 150 users, and information about the functionality of this gateway.

Local survivability with Avaya Solutions Platform S8300

Survivability is a key requirement for many customers, particularly medical customers. With Avaya Aura® 10.2 or later, edge-friendly branch survivability provides local survivability to the branch components at the customer premise. The branch components include one or more Branch Session Manager (BSM), Survivable Remote Server (SRS) or Local Survivable Processor (LSP), and Branch Gateway (BGW) that provide local service if core components in AXP Private Cloud are unreachable.

To support survivability, AXP Private Cloud core components remain unchanged but include the following additional components at the branch:

- G430 or G450 edge-friendly gateway
- BSM
- LSP

The local survivability feature is available to all customers of AXP Private Cloud. With the local survivability feature, customers can connect their G430s and G450s to AXP Private Cloud with S8300 on board. The edge-friendly gateway solution enables a secure connection to the current gateways, G430 and G450, through the Avaya SBC.

The edge-friendly gateway solution provides support for the following:

- Time Division Multiplexing (TDM) extension connectivity, that is, analog or fax + digital

 Note:

Fax is dependent on the service provider. For example, fax to a gateway is optimal over ISDN or POTS lines but is subject to carriers capabilities over SIP trunking.

- TDM local trunking, that is, ISDN and analog
- BSM and LSP based survivability

In the survivable mode, the following continue to be operational:

- Analog and Digital Communication Platform (DCP) stations on the branch gateways
- Local SIP phones in the branch
- Local SIP trunks
- Remote SIP users that connect or associate to that branch through VPN or other means
- Local PRI analog and BRI trunks on the branch gateways

In the survivable mode, the following are non-operational:

- Admin Portal and ability to do MACDs to the system
- Voicemail
- Core or Cloud centralized SIP trunks
- Recording

Customer prerequisites for local survivability

Task	Additional information
Complete software and firmware requirements	Ensure that the current software and firmware versions for all the components in your environment meet the Avaya requirements for the local survivability feature.  Note: Use S8300E to implement the local survivability feature. For more information on supported versions, see the Customer Readiness or Release Notes document.
Complete certificate requirements	Ensure that you create certificates for all the components by following the required rules: • Provide FQDN in the SAN field as DNS Name. • Provide IP address in the SAN field as IP Address. • Include Enhanced Key Usage. • Include Key Usage. • Provide RootCA in the .pem format. • Ensure that the RSA private keys are equal to or greater than 2048-bit. • Avaya SBC supports certificates with 2048-bit or 4096-bit keys. • Avoid using Certificate Key lengths greater than 2048 for heavy traffic contact centers due to increased processing time.

Table continues...

Task	Additional information
Complete network requirements	Ensure that you provide information related to the credentials to access the various components, hostname, DNS, domain name, IP addresses, and other details, as required by the Avaya technician or business partner. Customer must provide the IP addresses for the survivable BSM, LSP, edge-friendly gateway, SAL, and other components. All IP addresses must be forward and reverse resolvable through DNS.
Complete firewall requirements	Ensure that you meet the firewall requirements related to the source, destination, destination port, and protocol for the different connections. For more information on customer firewall and inbound firewall requirements, see the Service Description or Port Matrix document.

Upload announcement and music on hold files to Avaya media gateway

The customer needs to create a support or service team ticket to enable file transfer to the Avaya G450 or G430 media gateway. The service team enables file transfer. The customer can then use an FTP application to connect to the IP address of the gateway and load the announcement files onto the gateway.

Number	Task	Additional information
1	The customer creates an announcement.	The customer creates an announcement in a format compatible with the Avaya G450 or G430 media gateway. The G450 or G430 media gateway supports specific .wav file encodings for integrated announcements. The required criteria for these .wav files include the following: • Format: Pulse Code Modulation • Sample Rate: 8 kHz • Resolution: 16-bit • Channels: Mono • Both A-Law and Mu-Law, depending on the selected dial plan. NAR loc-param 1 dial-plans only support MU-Law, while EMEA loc-param 2, APAC loc-param 5, and CALA loc-param 7 use A-Law.

Table continues...

Number	Task	Additional information
2	Administration requirements for the announcement.	- Any Music on Hold (MOH) and integrated announcement sources must be in an audio group. Also, share the MOH and integrated announcement sources across all Avaya Media Servers (AMS) and edge-friendly gateways. - For multinational deployments, it is possible that Core or Cloud, and Survivable use different coding methods, A law and Mu Law. In such scenarios, the customer must provide announcement files in both encoding formats.
3	The customer creates an Avaya support or service team ticket to enable file transfer for the media gateway from the designated Communication Manager.	Avaya support or services team enables file transfer from the designated Communication Manager.
4	The customer uploads announcements and MOH wave files to the Avaya G450 or G430 media gateway.	Use an FTP application to connect to the IP address of the gateway and upload the announcement files to the gateway. - File protocol: FTP - Encryption: No encryption - Hostname: <media gateway IP address> - Port number: 21 - Username: <set by the Avaya support or services team in the previous step> - Password: <set by the Avaya support or services team in the previous step>
5	The customer informs the support or services team that the announcement upload process is complete. The Avaya support or services team disables file transfer for the media gateway from the designated Communication Manager and closes the ticket.	Avaya support or services team disables file transfer from the designated Communication Manager.

Configuration needed for local survivability of the on-premise branch components

Avaya edge-friendly gateway configuration

The G4xx gateway has the following certificate directories that you can use to support AXP Private Cloud:

- H248Reg: Supports TLS exchange with the Avaya SBC for H.248 control link over TCP port 2944 and MGSBC management link over TCP port 2946.

- Syslog: Supports secure Syslog transfer to the log server.
- Web: A customer managing the branch office can use HTTPS services to access log files and support file downloads, such as announcements.

The gateway requires client certificates or gw-identity in CLI commands, which the gateway uses for mutual authentication. In the AXP Private Cloud setup, enable mutual authentication for the H.248 and MGSBC TLS links.

Gateways running on release 10.2.x include a list of public root certificates from https://wiki.mozilla.org/CA/Included_Certificates in the web certificate repository. Hence, most web servers for CA root certificate download can be authenticated without requiring to download a root certificate. If you use Zscaler, download the Zscaler root certificate. Most web servers do not require mutual authentication. Hence, you need to add only the CA root certificate if you need to download files.

Configuration task	Related links	Additional information
Configure CA and identity certificates on the edge-friendly gateway: 1. Gather the required certificates. 2. Upload Customer Root CA Certificate, Customer Identity Certificate, and Cloud Root CA Certificate for the Media Gateways. 3. Load the AXP Private Cloud Entrust Root CA certificates into the H248Reg store. 4. Generate an identity certificate for each media gateway. 5. Load the gateway identity certificate into the H248Reg store.	• copy https root-ca • copy scp root-ca • copy usb root-ca • show root-ca • erase gw-identity-cert • copy https gw-identity-cert • copy scp gw-identity-cert • copy usb gw-identity-cert • show gw-identity-cert	• The certificates that you require are the following: - Root certificate from Entrust - Root certificate from Avaya - Customer root certificate - Customer identity certificate • Upload all certificates to a HTTPS server, SCP server, or a USB drive. • You need the AXP Private Cloud Entrust Root CA certificate for the Avaya SBC connection, as the gateway performs a TLS authentication. - Log in to the gateway CLI using a configured administrator account or using EASG. Log in using SSH to any gateway IP address, Services Interface, or local console. - Download the root certificates to the gateway using HTTPS, SCP, or a USB drive using the gateway CLI interface. • If you use third-party certificate services such as Entrust, where the certificate authority charges for each certificate, you can generate a single identity certificate that includes the SAN of all or each media gateway instance. Avaya SBC does not verify the client hostname. Hence, there is no requirement for CN or SAN uniqueness. You can install a single identity certificate on multiple media gateways for cost efficiency. The certificate and private key are stored in a PKCS#12 file protected by a passphrase. The passphrase is entered when the certificate is downloaded to the gateway. • Download the identity certificates to the gateway using HTTPS, SCP, or a USB drive attached to the gateway. • The gateway identity certificate is a third-party certificate stored in the pkcs12 format and protected by a passphrase. The gateway does not support CSR. - Log in to the gateway CLI using a configured administrator account or using EASG. Log

Table continues...

Configuration task	Related links	Additional information
		in using SSH to any gateway IP address, Services Interface, or local console. - If an identity certificate is already present, remove it before downloading a new one. - Download the identity certificates to the gateway using HTTPS, SCP, or a USB drive using the gateway CLI interface.

Table continues...

Configuration task	Related links	Additional information
Configure the gateway for edge mode operations: 1. Perform the initial configuration of a new gateway unboxed from the factory. 2. Configure the DNS resolver. 3. Configure the Avaya SBC address for a gateway already in use. 4. Set up a syslog receiver. 5. Check or configure password complexity.	• Configuring basic Branch Gateway connectivity • Configuring DNS resolver • Summary of MGC list configuration commands • User accounts CLI commands	• Initial configuration of a new gateway: - IP address: 10.133.100.249. - Login credentials: root/Avaya_123. - In the MGC controllers field, enter the primary and secondary Avaya SBC IP addresses or FQDN. Use the sbc@ prefix or label to indicate that the gateway connects to an Avaya SBC and not to a Communication Manager. • If a gateway is already in use, run the following CLI commands to configure it for the edge mode: - <code>clear mgc list</code>: To remove the existing Communication Manager IP addresses. - <code>set mgc list</code>: To configure the new Avaya SBC addresses, use the sbc@ prefix to indicate to the gateway that this is an Avaya SBC and not a Communication Manager address. For example, to configure an Avaya SBC with FQDN=sbc1.example.com, enter <code>sbc@sbc1.example.com</code>. To configure a primary and a secondary Avaya SBC address in the MGC list, separate the addresses with a comma. - <code>show mgc list</code> • Configure a maximum of three syslog receivers with UDP, TCP, or TLS transport. You can configure the ports.  Note: If a DNS server is configured, you can use an FQDN. However, the DNS server is only queried at the time the command is first run. The resolved IP address is stored in the gateway configuration and used subsequently. The CLI commands are the following: - <code>set logging server <IP/FQDN> [protocol] [port]</code>: Default protocol is UDP. Default ports are UDP:514, TCP:514, and TLS:6514. - <code>set logging server enable <IP/FQDN></code>

Table continues...

Configuration task	Related links	Additional information
		- show logging server condition: To verify the configuration. - copy scp/https root-ca syslog: To download the TLS certificates. - If you configure the Avaya SBC application relay for syslog, you can use the configured B interface address on the Avaya SBC as the server address. You can use the following commands to use the same certificates for H248 and syslog: copy certificate root-ca h248reg syslog and copy certificate gw-identity h248reg syslog - For logging-related commands, see Avaya G430 Branch Gateway CLI Reference. • To check or configure the password complexity for local users: - show login authentication - login authentication help - no login authentication help • To set up the AXP Private Cloud default password policy: - login authentication min-password-length 15 - login authentication password-expire 90 - login authentication passwords-dont-reuse 10

Avaya Solutions Platform S8300 R6.0.x for Kernel-based Virtual Machine

Configuration task	Related links	Additional information
Install Avaya Solutions Platform (ASP) S8300 R6.0.x: 1. Download the latest Rufus. 2. Download ASP S8300 customized Kernel-based Virtual Machine (KVM). 3. Create USB flash media drives for ASP R6.0.x software installation image. 4. Install the ASP R6.0.x KVM on S8300.	• Creating USB Flash Media Drives for an ASP R6.0.x Software Installation image • Application Note for Deployment of Avaya Solutions Platform (ASP) S8300 Release 6.0.x (KVM on RHEL 8.10)	Download ASP S8300 R6.0.x customized KVM from https://support.avaya.com/support/en/downloads .
Configure ASP S8300 R6.0.x for KVM: 1. Configure ASP S8300. 2. Option 1: Configure Server Network for Non Out of Band Management (OOBM) network. 3. Option 2: Configure Server Network for Out of Band Management (OOBM) network.	• Configuring KVM on Red Hat Enterprise Linux 8.10 Network Settings • Securing Network Configuration on ASP 130 (OoBM) • ICC configuration	• Ensure that the VLAN matches the gateway configuration by running <code>show icc-vlan</code> on the G430 or <code>show server-blade-vlan</code> on the G450. • Ensure that the OOB VLAN matches the gateway configuration by running <code>show icc-oob-vlan</code> on the G430 or <code>show server-blade-oob-vlan</code> on the G450.
Configure ASP through the Cockpit Web UI: 1. Enable administrative access. 2. Configure the time zone and NTP server.	Configuring KVM on Red Hat Enterprise Linux 8.10 Network Settings	--

Table continues...

Configuration task	Related links	Additional information
Install certificates for ASP: 1. Upload certificates and the private key file. 2. Verify that the private key file has a password. 3. Rename the files to match the KVM on the RHEL 8.10 hostname. 4. Copy the files to the cockpit directory. 5. Set certificate permissions. 6. Copy the Root CA certificate. 7. Restart the Cockpit Web UI. 8. Validate TLS connectivity. 9. Verify the certificates from the Cockpit Web UI.	• Creating the Certificate configuration file for KVM on RHEL 8.10 host • Generating the Certificate signing Request in KVM on RHEL 8.10 • Signing the Certificate Signing Request (CSR) by an Organizational CA • Replacing SSL certificates in Cockpit with a CA signed certificate	• Upload the identity certificate, root CA certificate, and private key file to the <code>/home/custadm</code> directory. • If the private key file includes a passphrase, remove the passphrase: - Run the <code>openssl rsa -noout -text -in <private_key_name>.key</code> command. - If you need to enter a passphrase after running the command, use the <code>openssl rsa -in <private_key_name>.key -out <private_key_name>-nopass.key</code> command to remove the passphrase. • Customers using an external CA or any other organizational CA, such as Microsoft CA, must have the signed certificate in the <code>cert</code> format and must rename the certificate to match the KVM on the RHEL 8.10 hostname. Preferably, the CA ROOT certificate must be in a <code>pem</code> format. However, you can convert the certificates by leveraging openssl after the certificates are transferred to the KVM on the RHEL 8.10 host. Run the following commands: 1. <code>hostname -f</code> 2. <code>mv <identity_certificate_name>.cert <identity_certificate_name>.cert</code> 3. <code>mv <private_key_name>-nopass.key <private_key_name>.key</code> • Copy the files to the cockpit directory by running the following commands: - <code>cp <identity_certificate_name>.cert /etc/cockpit/ws-certs.d/</code> - <code>cp <private_key_name>.key /etc/cockpit/ws-certs.d/</code> • Set certificate permissions by running the following commands: 1. <code>cd /etc/cockpit/ws-certs.d/</code>

Table continues...

Configuration task	Related links	Additional information
		2. <code>chmod 644</code> <code><identity_certificate_name>.cer</code> <code>t</code> 3. <code>chmod 600</code> <code><private_key_name>.key</code> 4. <code>ls -lrt</code> • Copy the Root CA certificate by running the following commands: 1. <code>cd /home/custadm/</code> 2. <code>cp</code> <code><root_certificate_name>.pem /etc/pki/ca-trust/source/anchors/</code> 3. <code>cd /etc/pki/ca-trust/source/anchors/</code> 4. <code>update-ca-trust enable</code> 5. <code>update-ca-trust extract</code> 6. <code>update-ca-trust extract</code> <code><root_certificate_name>.pem</code> 7. <code>openssl verify</code> <code><root_certificate_name>.pem</code> • Restart the Cockpit Web UI by running the following commands: 1. <code>systemctl daemon-reload</code> 2. <code>systemctl restart cockpit</code> 3. <code>systemctl status cockpit</code> • Validate TLS connectivity by running the <code>openssl s_client -connect localhost:9090 -tls1_3</code> command. • Log in to <code>https://<KVM host IP Address>:9090</code>, and verify Certificate Viewer.

Communication Manager - Local Survivable Processor or Survivable Remote Server

Configuration task	Related links	Additional information
Deploy Local Survivable Processor (LSP) VM on Kernel-based Virtual Machine (KVM): 1. Verify permissions and verify there is sufficient space. 2. Copy the Communication Manager KVM image to the Avaya Solutions Platform (ASP) R6.0.x host. 3. Convert files to a thick provisioned format. 4. Verify that the conversion is successful. 5. Copy CM10.2-system.qcow2 and CM10.2-Var_Disk.qcow2 to the /var/lib/libvirt/images directory. 6. Verify that the images are present in the /var/lib/libvirt/images directory. 7. Remove all extracted and converted images from the /var/lib/libvirt/staging directory. 8. Enable administrative access. 9. Import the virtual machine. 10. Add the CM10.2-Var_Disk.qcow2 disk image. 11. Select details for firmware, vCPU, and sockets. 12. Add the network bridge. 13. Add the network interface and bridge to LAN. 14. Start the Communication Manager virtual machine. 15. Initiate first boot of the virtual machine.	Deploying Communication Manager LSP on ASP R6.0.x (S8300 only) using KVM Cockpit	--

Table continues...

Configuration task	Related links	Additional information
Enable autostart for LSP.	Enabling Autostart on Virtual Machines using the Cockpit UI	--
Install Communication Manager - LSP or Survivable Remote Server (SRS).	Administering network parameters	Use the LSP VM.

Table continues...

Configuration task	Related links	Additional information
Configure Communication Manager - LSP or SRS: 1. Configure LSP or SRS. 2. Install the Communication Manager patch. 3. Configure cluster enablement. 4. Upload trusted certificate and server or application certificate. 5. Install trusted certificates. 6. Install server or application certificates.	• Communication Manager virtual machine configuration - Configuring Server Role - Configuring the Communication Manager network • Applying the Communication Manager patch using CLI OR Applying the Communication Manager patch using SMI • Enabling clustering • Adding a third party CA to Communication Manager • Adding TLS Trusted Certificates • Adding Server or Application Certificates	• Configure server role: - Select an LSP of the Communication Manager cluster. - For LSP Topology, click Edge. - Type a registration URL. - For Main Server's Memory Setting, click X-Large/Cluster. - For BSM SIP Entity IP Address (IPv4), type the SIP entity IP address, not the management IP address. • Install the Communication Manager patch using CLI or SMI. • Configure cluster management: - For Main Server Deployment Mode, click Cloud. - For Do you wish to have CM metrics on Prometheus (TCP Port 9000)?, click No. • Upload trusted, and server or application certificates: - Browse and choose the following files from your computer: • Azure Windows Domain Controller Root Authority Certificate • Entrust Public G2 Root Authority Certificate • Customer Root Authority Certificate • Customer Communication LSP/SRS Identity Certificate - Install trusted certificates: • Add each of the three root certificates. • Select all the check boxes in the Add to these trusted repositories area. - Install server or application certificates: • Add Customer Communication LSP/SRS Identity Certificate. • Select all the check boxes in the Add to these trusted repositories area.

Table continues...

Configuration task	Related links	Additional information
Verify LSP or SRS connectivity.		
Verify Communication Manager and SRS connectivity. 1. Save translation. 2. Verify whether survivable processors are registered. 3. Verify the Avaya WebSocket Tunnel (AWTUN) configuration. 4. Verify the AWTUN port redirection on Communication Manager. 5. Verify the AWTUN configuration files on Communication Manager. 6. Check logs for connectivity errors.	• Translations • Verifying the survivable virtual machine registration • Troubleshooting Edge LSP WebSocket tunnel	• AWTUN runs on the main Communication Manager (server side) and on the edge LSP (client side). - Run the awtun_config reload command to reload the AWTUN WebSocket tunnel. - Run the awtun_config restart command to restart the AWTUN WebSocket tunnel. • To view the port redirection rules, run the nft list chain inet nat awtun_redirect command. • AWTUN configuration files are automatically generated by the awtun-manager service and are stored in the /etc/opt/ecs/ directory: - LSPs.json: This file contains a list of LSPs in edge mode along with their serial numbers and local IP addresses. - firewall.json: This file defines which incoming (R=reversed) or outgoing connections are permitted for all the LSPs. • The awtun service creates the /var/log/awtun.log file, containing information on new connections, connection errors, and channels created from the clients that are not enabled on the main Communication Manager. • The awtun-manager service creates the /var/log/awtun_m.log file, which displays tunnel restart and reconfigurations.
Verify SSH and HTTPS connections through AWTUN on the LSP or SRS.	Configuring LSP Survivable Processor on main Communication Manager	Verify whether SSH and HTTPS connections are enabled using the awtun_config Linux shell command.

Branch Session Manager

Configuration task	Related links	Additional information
Deploy Branch Session Manager (BSM) VM on Kernel-based Virtual Machine (KVM): 1. Download the BSM KVM image. 2. Copy the BSM KVM image to the ASP R6.0.x host. 3. Extract the ova from the <code>/var/lib/libvirt/staging</code> directory. 4. Convert the <code>BSM10.2-system.qcow2</code> file to a thick provisioned format. 5. Verify that the conversion is successful. 6. Copy the <code>BSM10.2.qcow2</code> file to the <code>/var/lib/libvirt/images</code> directory. 7. Verify that the images are present in the <code>/var/lib/libvirt/images</code> directory. 8. Change files owner and permissions. 9. Remove all extracted and converted images from the <code>/var/lib/libvirt/staging</code> directory. 10. Import a virtual machine. 11. Select details for firmware, vCPU, and sockets. 12. Add network interfaces. 13. Add bridge to LAN. 14. Start the Session Manager virtual machine.	Deploying Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) using KVM Cockpit	--
Enable autostart for BSM.	Enabling Autostart on Virtual Machines using the Cockpit UI	--

Table continues...

Configuration task	Related links	Additional information
Install BSM - Session Manager.	• Configuring Session Manager • Customer configuration data for Session Manager	Use the following values: • Require Encryption Passphrase at Boot-Time (y/n): n. • Set BSM topology as edge (y/n): y. • Do you want to assign an IPv6 address?: no. • Enter network domain or 'none': Enter the customer domain. • Enter Primary DNS Server IP address or 'none': Enter the primary DNS server IP address. • Enter Secondary DNS Server IP address or 'none': none. • Enter domain search list: Enter the customer domain. • NTP is currently enabled. Would you like to disable NTP?: no. • Enter IP/FQDN of Primary NTP Server: Enter the NTP IP address. • Would you like to configure or change NTP Authentication?: no. • Enter IP/FQDN of Secondary NTP Server or 'none': none. • Do you want to enable EASG (Recommended) (yes/no)?: yes.

Table continues...

Configuration task	Related links	Additional information
Configure BSM certificates and Avaya WebSocket Tunnel (AWTUN): 1. Download and install the edge BSM certificates. 2. Install Cloud Root CA. 3. Install Customer Root CA. 4. Install identity certificates for the following BSM services: mgmt, sprit, db, syslog, and tunnel. 5. Install identity certificates for the following BSM services: WebSphere and HTTP. 6. Check the certificate status. 7. Set up AWTUN connectivity. 8. Verify whether edge topology is enabled. 9. Check the AWTUN status. 10. Verify whether AWTUN is UP. 11. Check connection to System Manager.	• certTool • Installing third-party identity certificates • edgeSetup command • Troubleshooting AWTUN on Branch Session Manager	• Download and copy the CAs required for the AWTUN tunnel in the PEM format to the BSM. You can include multiple certificates in one file. • Install Cloud Root CA for use for management DRS by running the following commands: <pre> - certTool -i <MS_root_certificate_name>.cert -t -s all -y - certTool -i <Entrust_root_certificate_name>.c rt -t -s all -y </pre> • Install Customer Root CA by running the following command: <code>certTool -i <customer_root_certificate_name>.cert -t -s all -y</code> • Install identity certificates for the following BSM services: mgmt, sprit, db, syslog, and tunnel. Run the <code>certTool --import <identity_certificate_name>.p12 --service eth0</code> command and enter the passphrase. • Install identity certificates for the following BSM services: WebSphere and HTTP. Run the <code>certTool --import <identity_certificate_name>.p12 --service eth1</code> command and enter the passphrase. • To view the tunnel trusted certificates, run the following command: <code>cert_status.sh</code>. You can view the AWTUN certificates. You cannot view all other certificates until initTM is run. The <code>edgeSetup</code> command runs initTM and initDRS. • To set up AWTUN connectivity, run the following command: <code>echo "<SMGR Enrollment Password>" edgeSetup --adc <URL of ADC> --primary_fqdn <SMGR Primary URL> --secondary_fqdn <SMGR Secondary URL> --vfqdn <SMGR Geographic Redundancy URL></code> • To view if edge topology is enabled, run the following command: <code>smconfig</code>

Table continues...

Configuration task	Related links	Additional information
		- To check the AWTUN status, run the following commands: <code>service awtun@1 status</code> <code>service awtun@2 status</code> <code>awtunstat</code> The AWTUN connection must be established before proceeding to the next step. - To view the AWTUN connection, run the following command: <code>statapp</code>. The output displays AWTUN as Tunnel. - To check the connection to System Manager, run the following command: <code>awtunstat</code>
Install the BSM patch: - Upload the BSM patch. - Install the BSM patch. - Upgrade RHEL from 8.8 to 8.10 using the following: AV-SM10.2-RHEL8.10-OSUpdate-003.tar.bz2	Installing software patches Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based virtual machines	- Install BSM patch using the following: Session_Manager_10.2.1.1.294501.bin - Upgrade RHEL to 8.10 using the following: AV-SM10.2-RHEL8.10-OSUpdate-003.tar.bz2
Check BSM connectivity.		
Check AWTUN connection between edge BSM and Core or Cloud System Manager: - Check the AWTUN status on System Manager. - Verify whether the local loopback entry exists in <code>/etc/hosts</code> on System Manager for each BSM. - Check the AWTUN status using commands on BSM. - Check the AWTUN status using commands on SRS or LSP. - Use <code>awtunstat</code> to check the current connections to AWTUN.	Troubleshooting AWTUN on System Manager Troubleshooting AWTUN on Branch Session Manager Troubleshooting Edge LSP WebSocket tunnel	--

Table continues...

Configuration task	Related links	Additional information
Check SSH and HTTPS connections through AWTUN on the BSM: 1. To enable the SSH tunnel. 2. To disable the SSH tunnel.	SSH access to Branch Session Manager	--
Check data replication (DRS) to BSM.	Verifying data replication	Verification of DRS replication is identical in AXP Private Cloud and Avaya Aura® Private Cloud. However, AXP Private Cloud with branch survivability requires that AWTUN must function correctly for DRS to succeed.
Check edge BSM connectivity: • Check the BSM service state. • Check the entity link connection status.	• Verifying the connections • Viewing the SIP Monitoring Status Summary page	• Verify that edge BSM can connect successfully to System Manager. • On the SIP Monitoring Status page, select edge BSM and check the connection status.
Check SIP communication flows between the edge core Session Managers and edge BSMs through Avaya SBC.	traceSBC	Use traceSBC on the Avaya SBC to track end-to-end message flows between the edge core Session Managers and edge BSMs. The SIP Monitoring OPTIONS traverse end-to-end.
Verify whether edge BSM can generate alarms successfully.	Generating a test alarm	Ensure that the status is active for the hostname that you select on the Serviceability Agents screen.
Verify whether the user can register from BSM.	--	To perform this test, the user must be onsite to register the phone. 1. Register the user with only the BSM IP setting in the Avaya Workplace Client configuration. 2. Open traceSM and check the <code>getHomeCapabilitiesResponse</code> PPM. 3. The PPM returns two Avaya SBC IPs, that is, for primary Session Manager and secondary Session Manager, and BSM IP.

Alarming for local survivability

Core or Cloud Edge-friendly Gateway configuration for alarming

Task	Additional content
SNMP trap reporting.	The Edge-friendly Gateway supports the generation of SNMP trap messages consistent with the gateway MIBs.
Syslog reporting.	Configure the Edge-friendly Gateway to direct the syslog traffic over TCP-TLS secure connections. Administer a maximum of three separate syslog receiver destinations.

Table continues...

Task	Additional content
Configure syslog.	Configure a maximum of three syslog receivers with UDP, TCP, or TLS transport. You can configure the ports. * Note: If a DNS server is configured, you can use an FQDN. However, the DNS server is queried after the time the command is first run. The resolved IP address is stored in the gateway configuration and used from then on. The CLI commands are the following: • <code>set logging server <IP/FQDN> [protocol] [port]:</code> Default protocol is UDP. Default ports are UDP:514, TCP:514, and TLS:6514. • <code>set logging server enable <IP/FQDN></code> • <code>show logging server condition:</code> To verify the configuration.

Core or Cloud main Communication Manager configuration for SRS or LSP alarming

Task	Related link	Additional content
Configure the SNMP FP Traps page for Edge LSP.	Configuring SNMP FP traps	--
Configure the SNMP Access page for Edge LSP.	Configuring SNMP access for the Communication Manager user	You can access the LSP agent through the tunnel if a local address is assigned to the LSP. Use the Edge field for the LSP on the SNMP Access page. * Note: • If you use a loopback address for the LSP, the main Communication Manager sends the traps. • Only SNMP v1 traps display the LSP agent IP address. You can use a different community or users to distinguish SNMPv2 and SNMPv3 traps from the LSP. • SNMP access is possible only from the main Communication Manager unless you create a UDP tunnel to the main Communication Manager.

SRS or LSP configuration for alarming

Task	Related link	Additional content
Configure syslog for Edge LSP.	Configuring Server Log Files	Select the Edge check box to indicate that it is an Edge accessible server.  Note: For security reasons, the main Communication Manager forwards the syslog messages from the LSP only if the same destination IP address or FQDN, TCP or UDP protocol, and port are configured for the main Communication Manager.

Serviceability agents configuration on System Manager for Branch Session Manager alarming

For Branch Session Managers to send traps to System Manager, perform the following serviceability agents configuration:

 Note:

You need assistance from an Avaya technician to perform tasks on System Manager.

Task	Related link	Additional content
Access the serviceability agents.	--	On the System Manager web console, click Services > Inventory > Manage Serviceability Agents > Serviceability Agents .
Configure the SNMP user profile.	Creating an SNMPv3 user profile	--
Configure the SNMP target profile.	Creating an SNMP target profile	--
Ensure that the status of the serviceability agent is active.	Verifying the Session Manager serviceability agent registration	--

Configuration needed for local survivability of SIP trunks in System Manager

 Note:

You need assistance from an Avaya technician to perform tasks on System Manager.

Local survivable SIP trunk configuration in System Manager

Configuration task	Related links	Example configuration
Log in to the System Manager web interface.	Logging on to the System Manager web console	--
Add location for the survivable SIP trunk.	Creating Locations	The network region (NR) must be the same as the Edge-friendly Gateway NR. For example, Name: NR150_NAR_SURV_TRUNK.
Add SIP entities for the local survivable SIP trunk.	Creating SIP Entities	For example: • Name: Surv-trunk. • FQDN or IP Address is the IP address of the A1 interface of the Avaya SBC. The customer must provide this information. • Type: SIP Trunk. • Network Topology: Branch. • Location: NR150_SURV_TRUNK. The location must be the same as the Edge-friendly Gateway location. • The Time Zone must be the customer time zone. • Add the following information for entity links: - Name: BSM50_Surv-trunk_5061_TLS_IPv4 - SIP Entity 1: BSM50 - Protocol: TLS - Port: 5061 - SIP Entity 2: Surv-trunk - Port: 5061 - Connection Policy: Trusted

Table continues...

Configuration task	Related links	Example configuration
Configure BSM SIP entities to the local survivable SIP trunk.	Modifying SIP Entity	Modify the BSM Edge-friendly Gateway. For example, modify BSM50 with the following values: • Location: NR150_SURV_TRUNK. • Add the following for entity links: - Name: BSM50_Surv-trunk_5061_TLS_IPv4 - SIP Entity 1: BSM50 - Protocol: TLS - Port: 5061 - SIP Entity 2: Surv-trunk - Port: 5061 - Connection Policy: Trusted

Table continues...

Configuration task	Related links	Example configuration
Configure adaptations for the local survivable SIP trunk.	Creating adaptations	- Adaptation Name: adp-SURV-TRUNK - Module Name: DigitConversionAdapter - State: enabled - Module Parameter Type: Name-Value Parameter - Name: ERHdrs - Value: P-Conference,P-Charging-Vector,P-Location,Endpoint-View,x-nt-gslid,RV-Guid,Rv-Guid-Str,Allow-Events - Name: fromto - Value: true - Name: iodstd - Value: avaya-dev10.ec.avayacloud.com - In the Digit Conversion for Incoming Calls to SM area, enter the customer-required digit conversion for incoming calls to Session Manager. - In the Digit Conversion for Outgoing Calls from SM area, enter the customer-required digit conversion for outgoing calls from Session Manager.
Configure routing policies and dial patterns for the local survivable SIP trunk.	- Configure Outbound Call Option 1: Prefer core failover local - Configure Outbound Call Option 2: Prefer local utilize core as secondary - Configure Outbound Call Option 3: Location Origination match	--

Outbound call option 1 configuration: Prefer core failover local

Configuration task	Related links	Example configuration
Create a routing policy for survivable trunk rank 100.	Creating Routing Policies	• Name: RP-SURVTRUNK-Rank-100. Other options are 1 to 9 and 100 to 999. Do not use 10 to 99. • Notes: RP to Survivable SIP Trunk. • Under the SIP Entity as Destination section, click Select to select the destination SIP entity for this routing policy. - Name: Surv-trunk - FQDN or IP Address is the IP address of the A1 interface of the Avaya SBC. The customer must provide this information. - Type: SIP Trunk • Under the Time of Day section, click Add to associate the Time of Day routing parameters with this Routing Policy. - Ranking: 100. Other options are 1 to 9 and 100 to 999. Do not use 10 to 99. - Name: 24/7
Add a dial pattern for the local survivable SIP trunk.	Creating dial patterns	Enter customer information in all the fields.

Outbound call option 2 configuration: Prefer local utilize core as secondary

Configuration task	Related links	Example configuration
Create a routing policy for survivable trunk rank 9.	Creating Routing Policies	• Name: RP-SURVTRUNK-Rank-9. Other options are 1 to 9 and 100 to 999. Do not use 10 to 99. • Notes: RP to Survivable SIP Trunk. • Under the SIP Entity as Destination section, click Select to select the destination SIP entity for this routing policy. - Name: Surv-trunk - FQDN or IP Address is the IP address of the A1 interface of the Avaya SBC. The customer must provide this information. - Type: SIP Trunk • Under the Time of Day section, click Add to associate the Time of Day routing parameters with this Routing Policy. - Ranking: 9. Other options are 1 to 9 and 100 to 999. Do not use 10 to 99. - Name: 24/7
Add a dial pattern for the local survivable SIP trunk.	Creating dial patterns	Enter customer information in all the fields.

Outbound call option 3 configuration: Local origination match

Configuration task	Related links	Example configuration
Create a routing policy for survivable trunk rank 9.	Creating Routing Policies	• Name: RP-SURVTRUNK-Rank-9. Other options are 1 to 9 and 100 to 999. Do not use 10 to 99. • Notes: RP to Survivable SIP Trunk. • Under the SIP Entity as Destination section, click Select to select the destination SIP entity for this routing policy. - Name: Surv-trunk - FQDN or IP Address is the IP address of the A1 interface of the Avaya SBC. The customer must provide this information. - Type: SIP Trunk • Under the Time of Day section, click Add to associate the Time of Day routing parameters with this Routing Policy. - Ranking: 9. Other options are 1 to 9 and 100 to 999. Do not use 10 to 99. - Name: 24/7
Add a dial pattern for the local survivable SIP trunk.	Creating dial patterns	Enter customer information in all the fields.

Avaya Vantage™

Avaya Vantage™ is a device that combines the advantages of a customizable unified communications solution and a fully functional Android device.

 Note:

Avaya Aura® Private Cloud supports Avaya Vantage™ with firmware version 3.1 or later.

For more information about Avaya Vantage™, see the following documentation:

Document Title	Description
Installing and Administering Avaya Vantage™ in an Open SIP Environment	Describes the initial setup, configuration, general administration, and troubleshooting of Avaya Vantage™ in a third-party call control environment.
Quick Reference: Using Voice Assistant for Avaya Vantage™	Describes the setup and use of Voice Assistant for Avaya Vantage™ with an Avaya Vantage™ device.
Using Avaya Vantage™	Describes the basic functions and features of Avaya Vantage™ devices.
Using Avaya Vantage™ Connect	Describes uses of the Avaya Vantage™ Connect application on an Avaya Vantage™ device.

Device bundles

The following device bundles are available for your AXP Private Cloud with Avaya Aura® Private Cloud solution:

- Avaya HC020 B109 Device Bundle
- Avaya HC020 B109OCC Device Bundle
- Avaya J179Wifi Pwr NAR Bundle
- Avaya HC010 B109 Device Bundle
- Avaya K175H DMIPwr Device Bundle
- Avaya K155H DMIPwr Device Bundle
- Avaya HC050 B199OCC NAR Device Bundle
- Avaya HC050 B199OCC EU/UK Device Bundle
- Avaya HC050 B129OCC NAR Device Bundle
- Avaya HC050 B129OCC EU/UK Device Bundle

Chapter 3: Applications

This chapter outlines the supported applications for your AXP Private Cloud with Avaya Aura® Private Cloud solution.

 Note:

This chapter has references to standard product documents. However, there are specific features of the product that AXP Private Cloud and Avaya Aura® Private Cloud support.

Avaya Admin Portal

Avaya Admin Portal is a web-based interface to manage your AXP Private Cloud deployments.

The portal supports the following browsers:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

If you cannot access Avaya Admin Portal and want to learn more about this feature, contact your Avaya Service Delivery Manager.

For more information about Avaya Admin Portal, see the following documentation:

Document Title	Description
Administering Avaya Admin Portal	General information about administering and configuring specific Avaya Admin Portal functions and features using a web-based interface.
Administering Avaya System Admin Portal	Information about advanced administration tasks for Avaya System Admin Portal.
Using Avaya Selfcare	Information for users on how to manage user-level settings and reset their password on the Selfcare end user portal.
Troubleshooting Avaya Admin Portal	Information to resolve troubleshooting errors for Avaya Admin Portal, Avaya Selfcare Portal, and Avaya System Admin Portal.
Avaya Admin Portal Web Service API	Information about user-centric and device-centric methods.

*** Note:**

- To view the support articles, go to the Avaya Admin Portal dashboard and click **Help** to redirect to documentation.avaya.com.
- For more information about new content for each release, see release notes on support.avaya.com.
- For training videos, click video tutorials at [Avaya Video Tutorials](#).

Avaya Aura® Call Center Elite

AXP Private Cloud is facilitated by Avaya Aura® Call Center Elite, a full-featured contact center solution with applications for handling inbound and outbound contacts and providing real-time and historical reporting insights.

For more information about Avaya Aura® Call Center Elite, see the following documentation:

Document Title	Description
Avaya Aura® Call Center Elite Feature Reference	High-level feature descriptions for Automatic Call Distribution and Call Vectoring and details about feature characteristics, capabilities, capacities, and interactions for Avaya Aura® Call Center Elite.
Avaya Aura® Call Center Elite Overview and Specification	Description of Avaya Aura® Call Center Elite features, functions, capacities, and limitations.

Avaya Aura® X for Zoom Workplace

Avaya Aura® Private Cloud supports integration with Zoom Workplace 6.2.0 or later. Use Avaya Aura® X for Zoom Workplace for Windows, macOS, and mobile applications on Android and iOS.

*** Note:**

Download Zoom Workplace 6.2.0 or later from the Zoom website.

Avaya Aura® X for Zoom Workplace enables integration with the Avaya Aura® elements. Zoom Workplace can register natively as a SIP client and leverage Avaya Aura® Private Cloud capabilities.

Customers can log in or register to Zoom Workplace on one mobile device and one desktop but not simultaneously on more than one of each device type.

A Zoom user has to be provisioned in Zoom account with an AADS domain. For more information about how to provision Zoom users, see [Configuring the Zoom-Avaya Aura integration](#).

To use Avaya Aura® X for Zoom Workplace, you require the following:

- A Zoom bundle.
- An Avaya UC Core or UC Power subscription.

Avaya Aura® Private Cloud manages the licenses and customized configurations of Zoom Workplace. The following are the supported capabilities:

1. Basic UC calling configuration:
 - a. Registered UC users can make and receive audio calls.
 - b. Users can elevate an active Avaya Aura® audio call to a Zoom meeting.
Users can record the meeting, and the recorded call can be stored on the local system or Zoom Cloud.
2. Avaya Aura® X for Zoom Workplace authentication for auto-configuration:
 - a. Users log in with their enterprise SSO credentials.
 - b. Zoom validates these credentials and retrieves the user extension and authentication information from Avaya Aura® Device Services (AADS).
 - c. After logging in, users can place and receive calls.

Avaya Aura® X for Zoom Workplace features

The following are the key features:

- Voicemail and Message Waiting Lamp
Avaya Aura® Private Cloud supports voicemail services and updates to the Message Waiting Lamp.
- 3-Party Avaya Aura® conferences
Zoom Workplace handles 3-party Avaya Aura® conferences locally within the client and limits conferencing to three participants.
Zoom users can migrate an Avaya Aura® call to Zoom meeting. Avaya Aura® call is placed on hold during the call migration while the meeting moves to the Zoom Cloud.
- Multiple Device Access (MDA)
Avaya endpoints or clients can bridge onto and take over an MDA call initially answered by Zoom Workplace. However, the reverse is not possible.
Zoom Workplace does not support shared control with Avaya J100 Series IP Phones.
- Handling a second call
Zoom Workplace manages the second call locally without using the standard Avaya Aura® multiple-call appearance feature. Zoom Workplace cannot manage or initiate a third call while handling two calls.
- Traditional telephony features

Use Feature Access Codes to activate call forwarding, call park, and send-all calls. You can initiate these features through Avaya J100 Series IP Phones if they are registered with Zoom Workplace as an MDA device.

- Contact Matching

During an internal call, Zoom Workplace identifies the calling or called party by their extension and displays their presence status on the phone screen and in the call log.

You can add external contacts manually or using a CSV file. You can search for or call contacts across the organization.

For more information about Avaya Aura® X for Zoom Workplace features, see Release Notes on support.avaya.com.

Avaya Callback Assist

Avaya CallBack Assist (CBA), an optional add-on to the CC Voice Agent bundles, provides callback capabilities in AXP Private Cloud.

CBA enhances customer experience during peak call times and improves agent utilization during off-peak times. It provides greater control over interactions with contact centers. You can decide whether to hold for the next available contact center agent based on your Estimated Wait Time (EWT) and queue position or to leave a message requesting a callback at a preferred time.

The handling of callback requests depends on the configured callback strategy within the Avaya Callback Assist feature. Currently, AXP Private Cloud supports the Agent-First strategy. In this strategy, CBA finds an available agent first, provides the agent with the caller information collected during the callback request, and places a call to the customer.

The following options are enabled in the customer administration web-based interface with the Avaya Callback Assist feature:

- Callback Configuration Management
- Daily Summary Report
- Pending Callbacks Report
- Pending Callbacks Summary Report
- Access Dashboards as Editor
- Call Disposition Summary Report
- Hourly Summary Report
- Pending Callbacks Cancellation
- Access Dashboard as Viewer

 Note:

The number of callback ports required depends on the customer's needs, with a maximum capacity of 38,000 Busy Hour Call Completions (BHCC).

For more information, see the following documentation:

Document Title	Description
Administering Avaya Callback Assist	How to administer and use the Avaya Callback Assist admin portal.
Avaya Callback Assist Reporting guide	How to generate various reports in the Avaya Callback Assist Reporting Dashboards application.

Avaya Call Management System

Avaya Call Management System (CMS) is a software product for businesses and organizations that receive a large volume of telephone calls processed through the Automatic Call Distribution (ACD) feature. CMS collects call-traffic data, formats management reports, and provides an administrative interface to the ACD feature on Communication Manager System.

The following features are available on AXP Private Cloud with the latest CMS release:

- CMS Web Client Report Designer
- CMS Web Client Report Scheduler
- Support for 1999 supervisors

As part of Voice Agent bundles, Avaya provides voice contact center reporting through CMS. The standard real-time and historical reports are supported. Call center supervisors can also create custom reports using the CMS Supervisor Web client. The CMS web-based reporting tool is available out-of-the-box, enabling customers to access all CMS reports directly from their web browser.

AXP Private Cloud includes the latest CMS features. For customer-specific features documentation, see the following CMS 21 documentation:

Document Title	Description
Avaya Call Management System Custom Reports	Details for system administrators about designing and creating custom reports in Avaya Call Management System.
Avaya Call Management System Call History Interface	Information for contact center administrators and support personnel about the format of the Call History data files and how to transfer these files to another computer. This document is for contact center administrators and support personnel.
Avaya CMS Supervisor Reports	Describes how to create and use CMS Supervisor reports.
Avaya CMS Supervisor Report Designer	Describes how to create new reports and edit existing reports through Report Designer and Report Wizard.

Automatic Call Distribution

CMS stores Automatic Call Distribution (ACD) data logically for processing.

CMS stores all ACD data from the communication server in real-time and historical databases.

Real-time databases

Real-time databases include tables for the current intra-hour interval data and the previous intra-hour interval data. The interval is set to 30 minutes.

Historical databases

Historical databases include tables for the intra-hour, daily, weekly, and monthly data. The intra-hour historical data is saved for 31 days.

Data Type	Default
Intra-hour historical data	31 days
Daily historical data	1 year
Weekly historical data	1 year
Monthly historical data	1 year

Note:

You can use historical data to predict future call traffic and future agent and trunk requirements.

When CMS collects data from the ACD, the real-time database stores the data for the current interval. At the end of the current interval, the following events occur:

- The data in the current interval database table is archived in the previous interval database table.
- The data in the previous interval database table is archived in the historical database as intra-hour historical data.

The data remains in the historical database as intra-hour historical data for a maximum of 370 days. At your designated data summarizing time, the intra-hour historical data is summarized into daily historical data. The daily historical data is summarized weekly and monthly. At the end of your designated week, the daily historical data is summarized into weekly historical data. On the first day of a new month, the daily historical data is summarized into monthly historical data for the previous month.

CMS Connectors and ODBC

AXP Private Cloud customers can integrate with the native CMS reporting tools system and access real-time and historical agent data.

CMS standard Connectors and ODBC are available as an optional add-on to the CC Voice Agent bundles.

The CMS Interfaces or Connectors that provide integrations are as follows:

- Historical
 - Nice IEX Historical

- External Call History (ECH) Handler
- Verint Historical
- Payroll
- Unload Interface
- Aux logging
- Real-time
 - Nice IEX Real-time
 - Generic RT Adherence
 - Verint Real-time
 - RT Socket
- ODBC

CMS Connectors

The connectivity for CMS Connectors is established through the public Internet or ExpressRoute (Microsoft peering) based on specific requirements, such as connecting to the customer's on-premises systems.

* Note:

- To ensure the security of the connection and traffic, certain connections must go through ExpressRoute (Microsoft peering).
- All CMS Connectors must use TLS or STFP for secure transport, as unencrypted connectivity is not supported.
- During deployment, by default, network connectivity for CMS Connectors is blocked. Access, as required, is provided for CMS Connectors during personalization.
- CMS Connectors failover functionality is determined during personalization.
- AXP Private Cloud Connection failover follows the standard failover functionality.

For more information about CMS Connectors, see <https://support.avaya.com/support/en/products/P1647>.

ODBC

CMS Open Database Connectivity (ODBC) connectivity in AXP Private Cloud on Microsoft Azure must be over an ExpressRoute (Microsoft peering) connection to a third-party cloud.

* Note:

- ODBC clients must use TLS for secure transport, as unencrypted ODBC connectivity is not supported.
- The single URL or FQDN concept is not followed for the ODBC client. Dedicated ports are assigned for the user to connect to the primary or the secondary CMS server Informix database. No automatic failover for an outage of the primary CMS server is supported.

All historical CMS database tables, dictionary tables, and customer-provided tables can be accessed through ODBC. For more information, see [Using ODBC and JDBC with Avaya Call Management System](#).

Avaya Experience Portal

AXP Private Cloud is facilitated by Avaya Experience Portal, which provides a single platform for automated voice, self-service, and Interactive Voice Response applications. Experience Portal supports inbound and outbound calls and HTML applications.

Avaya Experience Portal supports Session Initiation Protocol and a mixed telephony environment.

Avaya Messaging

Avaya Messaging is a feature-rich application you can customize to meet your organizational needs.

Through Avaya Messaging web access, you can access all your voice messages or voicemail. You can respond to, delete, and manage all your messages.

Avaya Workplace Attendant

Avaya Workplace Attendant is an optional add-on available with Avaya Aura® Private Cloud bundles.

Avaya Workplace Attendant is a SIP-based application designed to meet the communications requirements of front-desk personnel and call receptionists whose responsibilities include receiving calls, often in large volumes, and routinely transferring the calls to the appropriate group or individual. Avaya Workplace Attendant consists of the following modules:

- The Avaya Workplace Attendant is a Windows-based user interface. Front-desk personnel and call receptionists (called Attendants in the client) can use the integrated communications capabilities of the interface directly with a computer and headset or combine a deskphone for calls.
- The Avaya Workplace Attendant provides call queue, phone book, and presence capabilities.

For more information about Avaya Workplace Attendant, see the following documentation:

Document Title	Description
Using Avaya Workplace Attendant	How to use Avaya Workplace Attendant features.

Avaya Workplace Client

Avaya Workplace Client or User Client is a softphone application that extends communication services to Mac and Windows Desktops and Android and iOS mobile platforms. Avaya Workplace Client is included with Core, Power, and CC Voice Agent with Workplace Client bundles.

Based on your feature requirement, you can deploy Avaya Workplace Client in several ways. In the basic deployment type, you can have only voice calling. You can include additional features such as directory search, contact management, presence, instant messaging, and conferencing.

For more information about Avaya Workplace Client, see the following documentation:

Document Title	Description
Using Avaya Workplace Client for Android, iOS, Mac, and Windows	How to set up and use Avaya Workplace Client for Android, iOS, Mac, and Windows.
Avaya Workplace Client Overview and Specification for Android, iOS, Mac, and Windows	Avaya Workplace Client characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Avaya Workspaces

AXP Private Cloud is a cloud solution that delivers unified client capability through Avaya Workspaces. Avaya Workspaces is a browser-based WebRTC, a multi-experience desktop that provides a single pane of glass to empower contact center agents with contextual information across channels. The service features included in the CC Voice Agent bundle with the Workspaces client are as follows:

- Unified Agent and Supervisor Sign In
- Welcome page URL customization
- Interaction cards
- Agent and Supervisors Widget Layouts
- Disposition/Reason Codes
- Internal Calling
- Blind/Consult conference/transfer to user
- Blind/Consult conference/transfer to external number
- Screen-pop widget
- Display Routing Information with contact card
- Supervisor Observe, Coach, and Barge In

For more information about Avaya Workspaces, see [Using Avaya Workspaces for Avaya Experience Platform™ \(On-Prem + Connect\)](#).

CRM integration with Salesforce, Microsoft Dynamics® 365, and ServiceNow

As part of the CC Voice Agent bundle with the Workspaces client, Avaya supports CRM integration with Salesforce, Microsoft Dynamics® 365, and ServiceNow. Avaya Workspaces for CRM integration enables agents in your contact center to perform the following actions when using Salesforce, Microsoft Dynamics® 365, or ServiceNow functionality:

- Access the Avaya Workspaces for CRM softphone on the Salesforce, Microsoft Dynamics® 365, and ServiceNow platform.
- Handle inbound and outbound customer interactions.
- Make internal calls.

For more information, see the following documentation:

Document Title	Description
Administering Avaya Workspaces for CRM with Avaya Experience Platform™ (On-Prem + Connect) • Avaya Workspaces for CRM intergration with Salesforce • Avaya Workspaces for CRM integration with Dynamics 365 overview • Avaya Workspaces for CRM integration with ServiceNow overview	How to integrate and administer Avaya Workspaces for CRM with Salesforce, Microsoft Dynamics® 365, and ServiceNow.
Using Avaya Workspaces for CRM for Avaya Experience Platform™ Public Cloud	How agents and supervisors can use Avaya Workspaces for CRM softphone within Salesforce, Microsoft Dynamics® 365, and ServiceNow.

Call Detail Recording

The Call Detail Recording (CDR) feature is an opt-in entitlement available for AXP Private Cloud and Avaya Aura® Private Cloud. CDR enables customers to obtain detailed call data, including information about who initiated and received the call, the time of the call, and its duration. This data is primarily used for internal billing, call verification, and integration with third-party systems that require call details.

The setup for AXP Private Cloud and Avaya Aura® Private Cloud is the same and detailed within this section.

Call Detail Recording details

Two sources of CDR data will be provided: the Routing server and the Feature server elements of AXP Private Cloud. The same call may be recorded in both files. The Universal Call ID (UCID) is provided in the output of both elements so these call records can be linked if required.

The Feature server provides data that aligns with the Communication Manager CDR format, and the Routing server provides data that aligns with the Session Manager CDR file format.

In large deployments, there may be multiple call routing and feature components, each reporting CDRs for calls that pass through them. Therefore, multiple CDR files may be pushed to the SFTP server and separated by naming.

Components of Call Detail Recording

The key components of CDR are as follows:

1. File format:

Customers must confirm the default format of per-call data provided through CDR and how it is delivered.

The default CDR format settings include the following system parameters:

- CDR date format: `month/day`
- Incoming Trunk Call Splitting: `enabled`
- Outgoing Trunk Call Splitting: `enabled`

The Incoming Trunk Call Splitting and Outgoing Trunk Call Splitting parameters generate separate records when a trunk call is transferred between two users.

The default CDR output from the Feature server is listed in the following table:

Data Item	Length	Description	Example
date	6	Call started date in the mm/dd/yy format.	101824
local-time-from	5	The local starting time supported for CDR.	21:03
sec-dur	5	Call duration in seconds.	00012
ucid	20	Universal Call ID (UCID) is a unique identifier generated for every call in an Avaya network. This identifier is used to track the call as it travels across switches in the network.	00001011811729216995

Table continues...

Data Item	Length	Description	Example
cond-code	1	Call indication type such as: • 0 = intra-switch • 1 = attendant • 9 = incoming • A or 7 = outgoing • B = adjunct • C = conference	A
feat-flag	1	Feature flag indicates whether the call was answered. The following are the supported values: • 0 = not answered • 4 = reliable answer • 2 = timed answer	4 (answered)
calling-num	15	Calling number with leading blanks. This item can include a + sign if configured.	5551110103
dialed-num	23	Dialed number with leading blanks.	15559601000
vdn	16	VDN extension or blank if the call has no VDN.	5551129485
attd-console	2	If a call involves an attendant, this data item is the attendant number.	01
location-from	3	Numeric location of the calling party.	101
location-to	3	Numeric location of the called party.	201
timezone-from	6	Time zone offset of the calling party relative to UTC.	-05:00
timezone-to	6	Time zone offset of the called party relative to UTC.	-05:00
return	1	Formatting element.	-
line-feed	1	Formatting element.	-

The default CDR output from the Routing server is listed in the following table:

Data Item	Data Subitem	Description	Example
Call_time	n/a	Call started date or time.	2024-10-18T03:16:35+00:00
Duration	n/a	Call duration in seconds.	PT0.860S
Condition code	-	Call indication type such as: • 0 = intra-switch • 1 = attendant • 9 = incoming • A or 7 = outgoing • B = adjunct • C = conference	A
Parties	Dialed number	Dialed number of the party.	66880020@engageavaya.ec.avayacloud.com
	Calling number	Calling number of the party.	5551110203@engageavaya.ec.avayacloud.com
SIP Entities	terminating	The internal SIP entity for the called party.	CCCM1NAR
	originating	The internal SIP entity for the calling party.	CCCM1NAR
Feature flag	n/a	Feature flag indicates whether the call was answered. The following are the supported values: • 0 = not answered • 4 = reliable answer • 2 = timed answer	4 (answered)
BCC	n/a	Bearer Capability Class includes voice, video, or data.	M (multimedia)
Ma_uui	n/a	Message-associated user-to-user information.	0
Resource flag	n/a	Resource used by the current call.	0

Table continues...

Data Item	Data Subitem	Description	Example
Bandwidth	n/a	Bandwidth used by the current call.	1
Av_gsid	n/a	Avaya global session ID.	5e8c8030-8cff-11ef-96cd-0022482c4869
Ucid	n/a	Universal call ID #1.	0002009A6711D31B
Ucid2	n/a	Universal call ID #2.	<empty>
IP addresses	calling	IP address of the calling party.	10.16.93.9
	called	IP address of the called party.	10.16.88.5
Usage	voice	When voice data on the call is used.	Y
	video	When video data on the call is used.	n
	fax	When fax data on the call is used.	n
	text	When text data on the call is used.	n
	other	When other media data on the call is used.	n
codec	n/a	Index of codec used.	8
Tenant IDs	calling	Calling party tenant ID.	default
	called	Called party tenant ID.	default
verstat	n/a	Verification status (STIR/SHAKEN).	<empty>
Attestation_info	n/a	Attestation information (STIR/SHAKEN).	<empty>

2. File creation:

CDR data is stored in file format, and matching records from Feature and Routing servers are linkable using the UCID.

The following points detail the CDR files on:

- Feature server

CDR files transmitted to the customer's SFTP server are in the following naming format:

Sxxxxxx-www-yyymmdd-hh_mm (with no file extension)

A summary file (C-S000001-vmcmX-yyymmdd-hh_mm) aggregates all daily records with updates each time a new call record is appended.

Where:

- `s` indicates the main Feature server. For Avaya Aura® Private Cloud, LSP and ESS designations do not apply.
- `xxxxxxx` represents the last six digits of the system ID.
- `www` is part of this `vmcmX`. `vmcmX` is the Virtual Machine (VM) name of Feature server.

- Routing server

Routing server CDR files have `.xml` extension and include an additional sequence number if multiple files are generated for the same timestamp. File names also contain a hexadecimal string identifying the originating routing service.

For example, if the current date is 13 October 2024, the CDR files are organized as the following:

- CDR241013 (Today)

- One or more files for each Feature server, named `C-S000001-vmcmX-241013-hh_mm`.
- Multiple files for each Routing server, named `S00XXXX-XXXX-241013-hh_mm_n.xml`.

Where:

`XXXX-XXXX` represents any identifier for Routing server.

- CDR241012 (Yesterday)

- One or more files for each Feature server, named `C-S000001-vmcmX-241012-hh_mm`. The Feature server file does not have `C-` in the file name.
- Multiple files for each Routing server, named `S00XXXX-XXXX-241012-hh_mm_n.xml`.

- Directories for previous days (for example, CDR241011 and CDR241010)

Contains files similar to the directory of yesterday.

AXP Private Cloud will push call detail records to a customer-provided SFTP server. This can be done over the Internet or ExpressRoute, depending on what is used. The provided SFTP server that the CDR data will be pushed to must support TLS 1.2 and support secure key authentication.

Customers must provide the Fully Qualified Domain Name (FQDN) or IP address, username, and SFTP authentication through SSH keys for an existing SFTP server or a newly configured SFTP server intended for CDR reporting to Avaya for configuration. Customers must share these details securely with Avaya. If there are any changes to the SFTP server configuration, customers must notify Avaya prior to the configuration changes to avoid potential service disruptions.

AXP Private Cloud subsequently transfers CDR reports from the Feature server and Routing server to the designated SFTP server, enabling customers to retrieve and utilize these reports as needed.

*** Note:**

- If a customer requests, tracking for internal calls can also be enabled.
- Customers should indicate the use of CDR to Avaya when purchasing and provide the details of the SFTP server as the solution is being provisioned.

SFTP server

The CDR files are stored in a customer's SFTP server. The files are transmitted in encrypted form but stored on the SFTP server unencrypted. Security of these CDR files will be the customer's responsibility after they are on the SFTP server.

The customer can choose to delete the records from the SFTP server in line with their retention policy, although care must be taken. If a file is deleted by mistake, Avaya might be unable to resend the data. CDR data is not stored long-term within AXP Private Cloud.

The customer must provide the FQDN or IP address of the SFTP server to the Avaya Service Delivery Manager (SDM). Data transfer occurs on port 22, and CDR data is updated within 15 minutes after each call on the solution. CDR data is retained on Feature and Routing servers for up to 20 days.

Potential Failures and Recovery Procedures

Various elements within the AXP Private Cloud will be active at a given time; as such, the element sending the CDR may vary and is reflected in files created and updated on the customer's SFTP server. For more information, see [Components of Call Detail Recording](#) on page 52.

Customer SFTP server failure or connection to SFTP server failure

Failure: If the customer's SFTP server is down or becomes inaccessible.

Recovery:

- After the SFTP server is restored, the Feature and Routing servers send the CDR files that were not transmitted during the outage.
- If the outage lasts longer than the retention period of 20 days (default value), older records beyond the retention period are lost and cannot be recovered.
- Resolving SFTP server or connection issues quickly is crucial to prevent data loss.
- Avaya will receive an alert if the transfer fails and will contact the customer's administrator to address the issue.
- The customer's IT team is responsible for monitoring the SFTP server to promptly identify and resolve any issues.

Device Enrollment Services

Device Enrollment Services securely authenticate and redirect Avaya endpoints and devices to a file server. It simplifies and automates the discovery of the provisioning server, thus reducing the cost involved in deploying new devices.

Device Enrollment Services use an enrollment code to register the devices into AXP Private Cloud and Avaya Aura® Private Cloud. Avaya generates the enrollment code during AXP Private Cloud and Avaya Aura® Private Cloud provisioning.

 Note:

Not all devices support Device Enrollment Services.

Registering a device into AXP Private Cloud and Avaya Aura® Private Cloud

About this task

You can register devices into AXP Private Cloud and Avaya Aura® Private Cloud. You can also register devices you previously deployed using Device Enrollment Services (DES).

 Note:

You can register devices in bulk. For bulk registration, contact Avaya, as you cannot access the AXP Private Cloud and Avaya Aura® Private Cloud Device Enrollment Services account. If you have previously deployed devices and used Device Enrollment Services, you have a Device Enrollment Services account and can do bulk de-register under the account. Device Enrollment Services performs bulk claims on the devices using their serial number or MAC address. If customers prefer to continue using their DES account and managing their devices, they must contact Avaya.

Before you begin

You must release one or more devices from the Device Enrollment Services account if it was previously deployed using Device Enrollment Services.

For more information about account types and device support, see the [Using Avaya Device Enrollment Services to Manage Endpoints guide](#).

Procedure

1. Reset the device to its default settings.
 - The device restarts.
 - The device prompts to activate auto-provisioning.
2. Select **Yes**.
 - Avaya sends the enrollment code to your registered email ID.
3. Type the enrollment code.
 - The device displays the login screen.

Digital channels

Digital channels is an optional add-on bundle to the CC Voice Agent bundle with Workspaces client. Use this bundle to adopt digital channels such as chat, email, and messaging, utilizing the same WebRTC client (Avaya Workspaces). This bundle will enable agents to switch between handling digital and voice interactions using the same client.

For more information about switching between voice and digital interactions using Avaya Workspaces, see [Using Avaya Workspaces for Avaya Experience Platform™ \(On-Prem + Connect\)](#).

 Note:

Customers must perform integrations for the chat channel and messaging SDK, as required.

Avaya Workspaces supports the following digital channels:

- **Chat:**

Avaya Workspaces provides a JavaScript SDK for chat that can be embedded into a customer's website to enable chat functionality. Alternatively, customers can use provided APIs to integrate chat into their existing solutions. Customers are responsible for providing and implementing their chat solutions. They can do this independently using the developer documentation at <https://developers.avayacloud.com/onecloud-ccaas/docs/integrate-your-own-chat> or by contacting Avaya Customer Experience Services (ACES) for a custom Statement of Work (SOW) to scope implementation services.

- **Email:**

Avaya Workspaces receives the email messages as email interactions. Agents use email management capabilities to craft personalized responses to customer inquiries, empowering organizations to efficiently address bulk emails without increasing their contact center agent count. Email attribute-based routing is supported based on subject and email body content.

- **Messaging:**

Avaya Workspaces supports messaging, enabling contact center customers to engage in rich, persistent, and asynchronous conversations. This enables the exchange of rich media and ensures messaging history and shared content between users and agents remain accessible within the conversation channel. Customers can develop native Messaging applications for Android, iOS, and the Web using Client APIs. Customers can independently develop these customizations or collaborate with ACES for a custom SOW.

- **Voice:**

Voice interactions are routed to Avaya Workspaces to ensure contact center customers receive optimal service.

For more information about using these digital channels, see [Using Avaya Workspaces for Avaya Experience Platform™ \(On-Prem + Connect\)](#).

E-Bond

E-bond is an optional add-on if available for your AXP Private Cloud with Avaya Aura® Private Cloud solution.

E-bond provides an integration solution to interface with your ticketing Service management system for incident record exchange and service request exchange. For example, the incident record and service requests (MACDs) exchange with the Avaya Managed Services Platform (AMSP). The E-bond and communication exchanges are conducted securely over the public Internet.

Instant Messaging and Presence

Instant Messaging (IM) and Presence are deployed on a non-HA single server. Presence Services enables you to send and receive instant messages with individuals and groups, conduct ongoing conversations, and retain conversation history. Use Instant Messaging to create IM chat rooms for internal and external users. Use Presence to share and view the status of other users, whether working remotely or from the office.

For more information about Presence and instant messaging, see the following documentation:

Document Title	Description
Using Avaya Workplace Client for Android, iOS, Mac, and Windows	How to use the Presence and instant messaging feature in Avaya Workplace Client for Android, iOS, Mac, and Windows.
Using Avaya J189 SIP IP Phone in Avaya Aura®	How to use the Presence feature in Avaya J189 IP Phone.

Mobile Push Notifications

Mobile client is an existing entitlement for the AXP Private Cloud with Avaya Aura® Private Cloud solution. The mobile push notification mechanism enables clients to receive incoming call alerts and other notifications, such as new calls and voicemail messages from the mobile Push Notification service (APNs) through Avaya Workplace Client and Zoom Workplace. The mobile Push Notification service sends notifications automatically. Therefore, an application can receive notifications even when suspended or in Sleep mode.

The mobile Push Notification service is compatible with the Avaya Workplace Client on mobile (iOS) 3.16 or later.

The AXP Private Cloud with Avaya Aura® Private Cloud solution can send push notifications about the following telephony-related events:

- Incoming calls.
- Incoming calls on a bridged line appearance.
- Incoming calls on an enhanced pickup group.
- Incoming calls on a team button.
- Message waiting notifications.

Push Notification provider

The AXP Private Cloud with Avaya Aura® Private Cloud solution interacts with the mobile Push Notification service through a push notification provider. You must register with the push notification provider before activating push notifications. The default provider is the Avaya Push Notification provider, which must be used to support push notifications for Avaya Workplace Client. To use push notifications for third-party SDK-based applications, use a third-party push notification provider.

Note:

Azure Network Security Group (NSG) and firewall rules apply to the mobile Push Notification service.

STIR/SHAKEN

Internet Telephony Service Providers (ITSPs) implement the calling number verification using several SIP RFCs, collectively known as Secure Telephony Identity Revisited (STIR) or Signature-based Handling of Asserted Information using toKENs (SHAKEN). The STIR/SHAKEN feature is a framework of interconnected standards designed to reduce caller ID spoofing on public telephone networks, such as robocalls and phone scams.

AXP Private Cloud and Avaya Aura® Private Cloud can pass the call verification status to Avaya Workplace Client and J1XX handset endpoints when provided through the SIP trunk (Carrier or Tie trunk). This feature enables the user to view the verification status of incoming calls on the display. Currently, Avaya Workspaces and associated WFM integrations do not support this feature.

This feature can be activated during the personalization process and must be requested if required. Any changes to the STIR/SHAKEN feature configuration will be made through a MACD ticket submitted to Avaya.

This feature is compatible with the following versions:

- Avaya J100 Series IP Phones 4.1.2.0 and later.
- Avaya Workplace Client 3.35 and later.

For more information about STIR/SHAKEN call verification status icons, see [Using Avaya Workplace Client for Android, iOS, Mac, and Windows](#).

Verint Workforce Engagement Cloud

Verint Workforce Engagement Cloud for AXP Private Cloud is ideal for contact centers or enterprises who want to securely record customer interactions, increase agent productivity, and gain deeper insights into the customer experience delivered.

The Verint Workforce Engagement Cloud suite feature set is similar to the latest Avaya Workforce Engagement release. To access the Avaya Workforce Engagement documents, click the following link: <https://sales.avaya.com/en/pss/workforce-optimization>

For more information about the Verint portal, see the following webpage: <https://www.verint.com/engagement/our-offerings/solutions/workforce-engagement/>

Accessing technical documentation

To access the technical documentation of the Verint Workforce Engagement Management Cloud solution feature, do the following steps:

1. Click the following Verint Connect Portal: <https://connect.verint.com/>
2. A new user of Verint Connect must register with the following URL: <https://appext.verint.com/userregistration/>
3. After registration, the user can access the marketing content, not product-specific content.
A new user registration triggers workflow for more granular permissions and may occur a few hours after registration.
4. Access is authorized after a Verint Workforce Engagement Cloud order is placed for an Avaya customer with a valid contract.

911inform Location Discovery Solution

911inform Location Discovery Solution tracks the location of an IP device to ensure public safety. It helps you determine the exact location of IP devices that connect to its communication network.

When 911inform Location Discovery Solution detects an IP device registration, it monitors the device as follows:

- If the device registers to an IP address with a known dispatchable location, 911inform Location Discovery Solution automatically updates the associated device location record.
- If the device registers to an unknown IP address, 911inform Location Discovery Solution sends an SMS and email alert with a link to register to the user's contacts.

The key features of 911inform Location Discovery Solution are:

- Real-time location - Call records are updated in real-time when a user confirms and saves their location information.
- Efficient tracking of devices - 911inform Location Discovery Solution provides a dynamic location update architecture that tracks each device through their MAC address and not the telephone number.
- Fast and automated data collection - The location is based on the device, not the user. Updates to the real-time location are required if the device moves.
- Interactive floor plans - 911inform Location Discovery Solution digitizes and processes floor plans of each building in scope. The floor plans are interactive, enabling emergency locations to be updated in real-time, critical data such as storage of hazardous materials, and bidirectional communication. The 911inform Location Discovery Solution platform displays all this data.

911inform geofencing - mobile networking solution

911inform mobile networking solution relays 911 call locations from cellular phones through geographic location services. This solution provides the ability to identify the location of these calls quickly and accurately with the floor plans of the buildings.

The notification-based platform is accessible through a browser, and no application is required. It facilitates communication and situational awareness, enabling the management of any emergency event. For example, networked communication lines and enhanced building transparency controls are provided to predetermined organizational users by providing the following:

- Notification of emergency events through a text message and email.
- Real-time communication with all public safety officials.
- Enhanced visual cues through interactive building floor plans for quick navigation.
- Access and navigation plan to the emergency location.

Chapter 4: AXP Private Cloud and Avaya Aura® Private Cloud documentation

This chapter outlines the AXP Private Cloud and Avaya Aura® Private Cloud documentation.

AXP Private Cloud and Avaya Aura® Private Cloud documents

As part of the deployment, additional documentation is available to support the AXP Private Cloud with Avaya Aura® Private Cloud solution:

Document Title	Description
Getting Started with Avaya Experience Platform® Private Cloud and Avaya Aura® Private Cloud	Information about devices and applications supported in AXP Private Cloud and Avaya Aura® Private Cloud.
Administering Avaya Admin Portal	Information about using Avaya Admin Portal to manage the Avaya Cloud deployments, including how to activate or reconfigure new or existing services for your cloud deployment and make routine user-level changes.

Table continues...

Document Title	Description
Security for Avaya Experience Platform® Private Cloud and Avaya Aura® Private Cloud	Information about AXP Private Cloud and Avaya Aura® Private Cloud security goals, such as: • Confidentiality • Integrity • Availability Adheres to the following IT security and data privacy requirements of AXP Private Cloud and Avaya Aura® Private Cloud: • Payment Card Industry-Data Security Standards (PCI-DSS) • Health Insurance Portability and Accountability Act (HIPAA) • General Data Protection Regulation (GDPR)

Chapter 5: Resources

Use the following sections to locate resources and support for your AXP Private Cloud with Avaya Aura® Private Cloud solution.

Support

For end user support, contact your system administrator or use your local help and problem reporting procedures. For administrators, open a ticket using Avaya OneCare Portal. You can access the Avaya Support website at <http://support.avaya.com/> for up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues.

Opening a technical support ticket using Avaya OneCare Portal

About this task

Open a technical support ticket to request a service change, report an issue, or submit your query related to the Avaya applications.

Note:

When you log in to the Avaya OneCare Portal using your credentials, it automatically populates your first name, last name, and email address.

Before you begin

You must have the Avaya OneCare Portal login credentials.

Procedure

1. Go to <https://onecare.avaya.com>.
2. Click the **Avaya Cloud Solutions Support** tile.
3. Click the **Avaya Aura® Private Cloud** tile for communication and collaboration capabilities or the **Avaya Experience Platform® (AXP) Private Cloud** tile for contact center capabilities.
4. To access the personalized Services Catalog, click **Sign In**.
Avaya OneCare Portal displays the Sign On dialog box.
5. Type your email address and password.

6. Click **Sign On**.

Avaya OneCare Portal displays Multi-Factor Authenticator (MFA).

7. On the Verify your identity dialog box, select the preferred MFA method and approve the sign-in request.

8. Click the **Avaya Aura® Private Cloud and AXP Private Cloud Tech Support** tile.

Avaya OneCare Portal displays the Avaya Aura® Private Cloud and AXP Private Cloud Tech Support dialog box.

9. From the **Select your type of request** drop-down list, select **Request Technical Support (Incident)**.

10. From the **Select the option** drop-down list, select the required capability.

11. In the **AccountNo/FL/SoldTo** field, type your account number, Functional Location (FL), or sold to location.

12. In the **Subscription ID** field, type your Avaya subscription ID.

13. In the **Phone Number** field, type your contact number.

14. From the **Priority / Impact** drop-down list, select a value.

15. In the **Short Description** field, type a brief introduction of the technical issue.

16. In the **Describe your request/issue in detail** field, type the description of the technical issue.

17. **(Optional)** To attach a file, click **Upload file**.

a. Locate the file on your computer.

b. Click **Open**.

18. Click **Submit**.

Opening an MACD support ticket using Avaya OneCare Portal

About this task

Open an MACD support ticket to perform actions such as move, add, change, or delete outside the scope of the Avaya Admin Portal.

Note:

When you log in to the Avaya OneCare Portal using your credentials, it automatically populates your first name, last name, and email address.

Before you begin

You must have the Avaya login credentials.

Procedure

1. Go to <https://onecare.avaya.com>.
2. Click the **Avaya Cloud Solutions Support** tile.

3. Click the **Avaya Aura® Private Cloud** tile for communication and collaboration capabilities or the **Avaya Experience Platform® (AXP) Private Cloud** tile for contact center capabilities.
4. To access the personalized Services Catalog, click **Sign In**.
Avaya OneCare Portal displays the Sign On dialog box.
5. Type your email address and password.
6. Click **Sign On**.
Avaya OneCare Portal displays Multi-Factor Authenticator (MFA).
7. On the Verify your identity dialog box, select the preferred MFA method and approve the sign-in request.
8. Click the **Avaya Aura® Private Cloud and AXP Private Cloud Tech Support** tile.
Avaya OneCare Portal displays the Avaya Aura® Private Cloud and AXP Private Cloud Tech Support dialog box.
9. From the **Select your type of request** drop-down list, select **Request Moves Adds and Changes (MACD)**.
10. From the **Select the option** drop-down list, select a level.
11. In the **AccountNo/FL/SoldTo** field, type your account number, Functional Location (FL), or sold to location.
12. In the **Subscription ID** field, type your Avaya subscription ID.
13. In the **Phone Number** field, type your contact number.
14. In the **Short Description** field, type a brief introduction of the technical issue.
15. In the **Describe your request/issue in detail** field, type the description of the technical issue.
16. **(Optional)** To attach a file, click **Upload file**.
 - a. Locate the file on your computer.
 - b. Click **Open**.
17. Click **Submit**.

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.

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.

Index

Numerics

911inform Location Discovery Solution [62](#)

A

Admin Portal [42](#)
 alarming configuration [32](#)
 announcement [14](#)
 applications [42](#)
 Automatic Call Distribution (ACD) [46](#)
 Avaya Aura X for Zoom Workplace [43](#)
 features [44](#)
 Avaya Experience Portal [49](#)
 Avaya messaging [49](#)
 Avaya Solutions Platform
 survivability [12](#)
 Avaya support website [66](#)
 Avaya Vantage [40](#)
 Avaya Workspaces [50](#)

B

B109 [9](#)
 B129 [9](#)
 B169 [9](#)
 B179 [9](#)
 B199 [9](#)

C

Call Detail Recording [51](#)
 components [52](#)
 details [51](#)
 SFTP server [57](#)
 call management system [46](#)
 callback assist [45](#)
 change history [6](#)
 CMS Connectors [47](#)
 collection
 delete [69](#)
 edit [69](#)
 generating PDF [69](#)
 sharing content [69](#)
 configuration
 alarming [32](#)
 local survivability [15, 21, 24, 28](#)
 local survivability of SIP trunks [34](#)
 content
 publishing PDF output [69](#)
 searching [69](#)
 sharing [69](#)

content (*continued*)
 sort by last updated [69](#)
 watching for updates [69](#)
 CRM integration
 Microsoft Dynamics [51](#)
 Salesforce [51](#)
 ServiceNow [51](#)

D

device bundles [41](#)
 devices [8, 9](#)
 9600 series [8](#)
 J100 series [9](#)
 digital bundle [59](#)
 digital channels [59](#)
 document changes [6](#)
 documentation [66](#)
 documentation center [69](#)
 finding content [69](#)
 navigation [69](#)
 documentation portal [69](#)

E

e-bond [60](#)
 Edge Gateway [10](#)

F

finding content on documentation center [69](#)

I

instant messaging and presence [60](#)

K

knowledge base [66](#)

L

local survivability [12](#)
 alarming [32](#)
 ASP S8300 for KVM [21](#)
 Branch Session Manager [28](#)
 configuration of on-premise branch components
 [15, 21, 24, 28](#)
 customer prerequisites [13, 14](#)
 LSP [24](#)
 SIP trunks in System Manager [34](#)

local survivability (<i>continued</i>)	
SRS	24

M

mentor videos	66
messaging	49
mobile push notifications	60
push notification provider	61
music on hold file	14

O

ODBC	47
------------	--------------------

P

prerequisites for local survivability	13
---	--------------------

S

S8300	
survivability	12
searching for content	69
SFTP server	
potential failures and recovery procedures	57
SHAKEN	61
sharing content	69
SIP	61
soft clients	
workplace attendant	49
workplace client	50
sort documents	69
STIR	61
support	66

U

Unified client	50
----------------------	--------------------

V

Verint Workforce Engagement Cloud	62
voice interactions	
callback assist	45

W

watchlist	69
-----------------	--------------------